SECURITY AND PRIVACY IN 6G COMMUNICATION TECHNOLOGY

Edited By
Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh, and Amit Singhal

Scrivener Publishing

WILEY

Security and Privacy in 6G Communication Technology

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Security and Privacy in 6G Communication Technology

Edited by

Parita Jain

Puneet Kumar Aggarwal

Mandeep Singh

Sushil Kumar Singh

and

Amit Singhal

WILEY

This edition first published 2026 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA
© 2026 Scrivener Publishing LLC
For more information about Scrivener publications please visit www.scrivenerpublishing.com.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at http://www.wiley.com/go/permissions.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Limit of Liability/Disclaimer of Warranty
While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials, or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Library of Congress Cataloging-in-Publication Data

ISBN 9781394311002

Cover image: Generated with AI using Adobe Firefly
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The development of sixth-generation (6G) communication technology marks a transformative shift in wireless networks, promising ultra-high speeds, low latency, and seamless connectivity for a wide range of applications, including the Internet of Things (IoT), smart cities, artificial intelligence (AI), and blockchain-based architectures. While these advancements unlock unparalleled opportunities, they also introduce new security threats and privacy challenges that must be addressed to ensure safe, reliable, and resilient communication infrastructure. This book, *Security and Privacy in 6G Communication Technology*, brings together contributions from leading researchers and industry experts, providing a comprehensive overview of security challenges, privacy risks, and innovative solutions in 6G networks. Through 14 chapters, this book presents in-depth discussions on key security frameworks, advanced cryptographic techniques, privacy-preserving architectures, and future research directions to establish secure and privacy-compliant 6G ecosystems.

Chapter 1: A Comprehensive Study of Security and Privacy Issues of 6G Wireless Communications Networks
This chapter lays the groundwork by exploring the fundamental security and privacy challenges in 6G networks. With massive IoT integration, AI-driven automation, and ultra-low latency services, new vulnerabilities emerge in data transmission, identity authentication, and network integrity. The chapter highlights cryptographic solutions, identity management protocols, and AI-powered security strategies to address these risks.

Chapter 2: Key Security Issues and Solutions in 6G Communications
Chapter 2 provides a detailed examination of cyber threats, unauthorized access, and data breaches in 6G networks. It discusses quantum-resistant encryption, blockchain-based authentication, and AI-driven intrusion detection as effective countermeasures. The chapter also evaluates how these solutions can ensure the performance, scalability, and reliability of 6G networks.

Chapter 3: Strategies for Ensuring Security and Privacy in 6G Networks
This chapter presents advanced privacy-preserving strategies for 6G, including zero-trust security models, decentralized identity management, and AI-enhanced cybersecurity measures. It emphasizes federated learning as a key technique to balance data privacy and network efficiency, ensuring that user data remains protected

Chapter 4: Enhancing Security and Privacy Frameworks in 6G Networks
Focusing on existing security frameworks, this chapter analyzes their applicability in 6G networks. It introduces post-quantum cryptographic techniques and distributed ledger technology (DLT) as solutions to overcome the limitations of traditional security models. Additionally, the chapter explores next-generation encryption to protect sensitive communications.

Chapter 5: Adaptive Security Protocols for Dynamic 6G Environments
This chapter presents adaptive security protocols designed to dynamically respond to evolving cyber threats in 6G networks. AI-driven threat detection, real-time authentication mechanisms, and automated anomaly detection are discussed as methods to build a self-healing and resilient security infrastructure.

Chapter 6: BFL-IoV: Blockchain and Federated Learning for Secure 6G IoV Networks
Blockchain and federated learning (FL) play a crucial role in securing the Internet of Vehicles (IoV) in 6G networks. This chapter discusses how decentralized consensus mechanisms enhance security, whereas FL allows privacy-preserving AI models for secure, real-time decision-making in smart transportation and critical infrastructures.

Chapter 7: Leveraging Machine Learning for Enhanced 6G Security
Machine learning (ML) is an essential tool for automated cybersecurity in 6G networks. This chapter explores how ML can be used to identify network anomalies, predict cyber threats, and enhance encryption techniques. It also discusses AI-powered fraud detection and intelligent access control mechanisms.

Chapter 8: Applications of Machine Learning in Strengthening 6G Security
Building on the previous discussion, this chapter investigates how AI is applied in real-time threat analysis, autonomous security monitoring, and predictive cybersecurity. AI-driven encryption methods and intelligent security automation ensure that 6G networks remain protected against rapidly evolving cyberattacks.

Chapter 9: Edge Computing and Privacy Challenges in 6G Networks
Edge computing facilitates low-latency applications in 6G, but it introduces new security concerns. This chapter examines decentralized data processing vulnerabilities, including unauthorized access, AI-based cyberattacks, and data breaches. It proposes privacy-preserving techniques such as secure multi-party computation and homomorphic encryption.

Chapter 10: Resilient Security Architectures for 6G-Enabled Smart Cities
Smart cities rely on 6G to enable real-time automation, AI-driven governance, and IoT integration, but cybersecurity remains a major concern. This chapter explores four key security architectures—AI-powered security, quantum-resistant security, blockchain-based security, and adaptive security—to protect smart urban environments from cyber threats.

Chapter 11: Innovative Solutions for User Privacy in 6G Networks
User privacy is a critical concern in hyper-connected 6G environments. This chapter presents decentralized identity management, differential privacy techniques, and regulatory frameworks for enhancing user data protection. It highlights how privacy laws must evolve to support next-generation wireless communication.

Chapter 12: Analytic Study on Existing Communication Technologies for Smart Grid: Beyond the 5G and Extension Toward 6G
Chapter 12 focuses on 6G-enabled smart grids, discussing how ultra-fast and intelligent communication can optimize energy management, real-time automation, and distributed power systems. It highlights security challenges in smart grids and proposes AI-driven security mechanisms to safeguard critical infrastructure.

Chapter 13: Power-Efficient Techniques for Sustainable 6G Networks
This chapter evaluates the integration of AI-driven security frameworks in 6G networks. It discusses intelligent threat detection models, self-adaptive security mechanisms, and AI-powered encryption protocols to create autonomous cybersecurity solutions that protect 6G communications from advanced persistent threats.

Chapter 14: Cybersecurity in 6G: Challenges and Future Directions
The final chapter provides an overview of cybersecurity challenges in 6G, including AI-driven cyber threats, quantum-based attacks, and IoT security vulnerabilities. It introduces zero-trust architectures, secure

multi-party computation, and blockchain-based authentication as key approaches to strengthening 6G network resilience. The chapter concludes with future research directions, outlining the need for next-generation security paradigms.

By presenting cutting-edge discussions on security and privacy challenges in 6G networks, this book serves as an essential resource for researchers, industry professionals, and policymakers. The contributions from esteemed authors provide practical insights and solutions to establish a secure, resilient, and privacy-compliant 6G ecosystem. As 6G networks continue to evolve, security research must advance proactively to anticipate and mitigate cyber threats. It is our hope that this book inspires further innovations in 6G security, ensuring that future wireless technologies remain trustworthy, efficient, and secure.

Mandeep Singh
Editor
Security and Privacy in 6G Communication Technology

1

A Comprehensive Study of Security and Privacy Issues of 6G Wireless Communications Networks

Pawan Kumar[1]*, Mandeep Singh[2], JaiShree Jain[1], Anu Chaudhary[1] and Shashank Sahu[1]

[1]Department of CSE, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India
[2]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India

Abstract

Due to the rapid growth of smart Internet-of-Things devices or internet-based applications and high-speed networks, the fifth-generation (5G) communications network will roll out from twhe market in future, and the sixth-generation (6G) communications network will completely replace the 5G networks with their advanced features. The 6G network is faster and more reliable than 5G networks in terms of their advanced features like high data speed (1 terabit per second), low latency time, capability to handle large networks, advanced security features for data transmission, and minimized energy consumption. Security and privacy of networks is the primary concern of any communication network. The book chapter aims to present a comprehensive study of the future evolution of 6G network with their key features, applications, challenges, security issues, and requirements to establish 6G wireless communications. Research more focuses on the study of the security and critical privacy issues associated with 6G technologies. Overall, this paper provides useful information for industries and academic researchers and discusses the potential for opening up new research directions related to the security of 6G networks.

***Keywords*:** 6G security, privacy, communication, security threats, physical layer security, AI/ML security

**Corresponding author*: drpawancse@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (1–28) © 2026 Scrivener Publishing LLC

1.1 Introduction

The growth rate of mobile volume data has increased rapidly in the last recent years due to increasing large number of mobile users, internet subscribers, connective devices, M2M (machine-to-machine) connections, etc. It is also expected that the volume of data will increase with a high growth rate in the coming years. According to a statistics report of the International Telecommunication Union, it is expected that mobile traffic data will reach up to 607 and 5,016 exabytes per month at the end of the year 2025 and 2030, respectively. Furthermore, it is also expected that 70% of the world population access mobile internet services by 2025, and, if we are talking about the Asia Pacific Region, then it will reach up to 13.5 billion devices. Nowadays, wireless broadband has become a very emerging and demanded technology in the field of communication, and its applications are used in various areas such as transportation, healthcare systems, infrastructure development, home internet, and military applications, performing better results. Although presently most industries and academics are using 5G wireless technology for commercial purposes for data transmission, 5G technology has several drawbacks. A very big challenge for telecommunication industries with 5G communication is the handling of massive internet traffic data in terms of reliability of data and latency time, providing better efficient energy and intelligence, and managing the security and privacy aspect of data. Managing of increasing data growth rate with low latency time is a big challenge for the existing 5G data communication systems. For example, the delay of air interface in haptic internet-based telemedicine is 1 ms in 5G networks, but it requires a delay of less than 0.1 milliseconds (ms). For better management of all the above issues, there is a need for a new advanced communication technology that overcomes the all these issues [1, 2]. A new advanced 6G communication technology was introduced that not only overcomes the problems of 5G but also provides a high-speed wireless communications network along with ultra-high reliability and low latency time. The 6G network was introduced by China Global and Huawei Technologies in November 2021 and launched a satellite for 6G communications, but it is estimated to be used publicly worldwide by the end of the year 2030. This chapter is divided into five subsections. The first section contains a detailed description of the introduction part. The second section explains the historic evolution of all communication generations starting from 1G networks to present 5G networks along with their key features. The third section focuses on the complete study of 6G communication networks with their applications, benefits, and drawbacks and about the challenges in establishing 6G networks.

The fourth section of the book chapter consists of the information about the all security metrics or measures that are in all communication generations, and it also focuses on four important key security features that need to be focused on for tomorrow's 6G networks. The last section of the book chapter concludes with the conclusion of the chapter.

1.1.1 History of Wireless Communication

In the last few years, remarkable advancements have been made in the field of mobile communication in term of communication and information transfer. In the early days, mobile phones were limited in size, and their data speed was very less as compared to today's high-speed smartphones. Mobile networks are processing huge improvementswith time in the field of telecommunication through different journeys starting from 1G (first-generation wireless network) to 6G (sixth-generation wireless network). The capability areas of wireless communication systems are also expanding with time. Each generation of mobile networks performed a significant milestone in the development of mobile communications [3]. The outline of all five generations of mobile networks along with their features is given in Figure 1.1, and the complete description is discussed below.

1G (First-Generation Mobile Networks): 1G network was based on an analog technology system and was initially introduced by Japan in 1979 and, later on, in 1980, used by other countries of the world. The 1G mobile networks used the frequency-division duplexing (FDD) method for radio-frequency transfer between transmitter and receiver. In 1G mobile communication, users can communicate with each other through phone

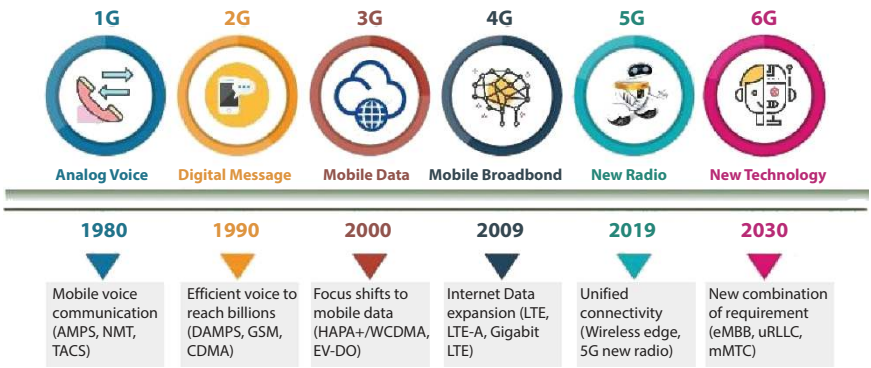

Figure 1.1 Generation evolution of communication networks from 1G to 6G.

calls only, but the drawback of this approach is that it is not applicable to receiving or sending text messages to other users. The distance coverage area of 1G technology was also very small, even though a large numbers of cell towers were required for signal transfer, and that was the reason why a large number of signal tower were installed around the country for signal transfer. 1G mobile network communication has no facility for roaming support among different operators, users can only transfer signals within a specified range of tower. The quality of sound was also not good, it provides less security and privacy, and information was easily hacked due to low encryption techniques. Data transfer speed of 6G communication was very less and varies in range of up to 2.4 kbps only [4, 5].

2G (Second-Generation Mobile Networks): 2G mobile communication networks was used digital cellular networks for data transfer among mobile users and were launched in the year 1991 in Finland. It was operated on GSM (Global System for Mobile Communication) methodology and operates on frequency bands of ranges varying from 900 MHz to1800 MHz. A 2G generation network provides a high data rate speed and large coverage area as compared to a 1G network. It also supported both voice and SMS communication for data transfer and transfer data with a data speed of 64 kbps.

3G (Third-Generation Mobile Networks): 3G communication networks provided high data transfer speed as compared to 1G and 2G communication networks with data speed of 144 Kbps to 2Mbps. 3G communication networks were well suitable for audio, video, and web-based applications. Three types of mobile access techniques (code division, wide band division, and wide band code division multiple access) were used for communication in 3G technology.

4G (Fourth-Generation Networks): 4G network was launched in 2009, and it provided large bandwidth, high security, and fast internet access service as compared to 3G technology and other previous generation technology. 4G is 10 times faster than in speed as compared to 3G technology with consist of 100 Mbps data transfer speed. 4G technology, based on Long-Term Evolution (LTE) technique, that enables voice calls, mobile data, and text messages on a 4G mobile phone.

5G (Fifth-Generation Network): 5G is the latest iteration of cellular technology and the successor of 4G. It providesfaster downloading and uploading data speed as compared to 4G and 3G. It establishes the more reliable and efficient connection among mobile users. 4G network is also capable to connect a number of devices at the sametime with the network.

Downloading speed of 4G lies in between range of 10 and 20 Gbps, and it is 100 times faster in speed as compared to 4G network [6, 7].

1.1.2 Overview of 6G Networks

Even though 5G technology has not been implemented fully throughout the world, limitations of 5G networks motivate researchers, to begin new advanced research in the field of communication-related to 6G networks. In this regard, the first 6G world's summit was organized in Finland in March 2019, and top communication expertsof the world drafted together a first 6G network white paper. From this summit, the 6G network was unofficially born, and several countries of the world have announced to build their research projects in the field of the 6G network. For example, China started their research of 6G in the year 2018 and launched a satellite along with Huawei to test terahertz (THz) signal transmission in the year 2020, and they are expected or planned to use 6G technology commercially in their country up to 2030.

1.1.2.1 Advancement in 6G Technology

Now, 5G network is widely used in most countries of the world, and it creates a road map for designing future generations of a new advanced 6G mobile communication network. After comparing and analyzing previous generations, it has been clear that, with the introduction of the new technology, the network speed and coverage area also increased gradually. The main target of the 6G network is to cover a large global area and provide fast network services to users with the inclusion of artificial intelligence (AI) applications. Although it is in its initial stages and may be use commercially in 2030 worldwide, it is estimated by researchers that 6G technology will become the backbone of communication technology. As compared to existing 5G technology, 6G provides large capacity, high data rates, high security, and privacy, and, probably, the quality of network will increase with decrease latency time. 6G will be operated with a transmission range of speed between 1 and 10 terabit per second (Tbps). The frequency of the proposed technology will behigher from all existing communication generations, and the latency range lies from 10 to 100 ms. The connectivity density and traffic capacity range from 10 devices/km^2 to Gb/s/m^2, respectively. The energy efficiency of the spectrum will also increase exponentially in comparison to the 5G network, and, on the other hand, 6G holds unlimited capacity of wireless connection [13, 14].

1.1.2.2 Importance of Developing 6G Technology

As discussed above, the density of traffic data of mobile users is increasing rapidly due to the increasing size of mobile users. The importance of 6G technology also increases due to its high bandwidth speed. Due to the increasing of large number of devices, more numbers of sensors, wearable devices, and integrated headsets are required to manage the communication system and existing generations suffer problems of high mobility.

The USA also started their 6G research in the year 2018 with the Federal Communications Commission and established a Next G Alliance with top brand companies including Apple, Google, and AT&T in the year 2020 to open up a higher frequency spectrum for experimental use. South Korea has signed an Memorandum of Understanding (MOU) with LG, Samsung, and SK Telecom companies and plans to invest $11.7 billion to build 6G technology [8, 9]. They are planning to use the 6G network commercially in their country up to 2026 three years before China. Japan also started their research in 6G technology in the year 2020 and is planning to launch next-generation 6G mobile data technology by 2030. Finland's Nokia leading its research into Hexa-X 6G in 2020 and the University of Oulu devoting $300 million to Finland for the 6G program. Germany also launched a 6G research project for the Next Generation Mobile Networks in 2020. University of Surrey of UK established a 6G Innovation Centre in collaboration with Russia's Skolkovo Institute of Science and Technology in the year 2020 and has announced to creation of a device that helps to develop 6G system components. The 6G mobile network is currently being developed for wireless communications based on cellular technology, and it is the successor to 5G technology. Most people think that 6G networks should only the faster version or update version of a 5G network at a higher speed only, but it also improves and extends the 5G technology in all aspects such as unlimited coverage area, high data transfer speed (1,000 times faster than 5G), and lower latency time. In recent years, 6G technology has become the new revolutionary generation in the area of mobile communication due to its prominent features like providing higher bandwidth and reliability, better QoS and coverage, low latency and power consumption, and better privacy and security. 6G technology has several key features over currently used 5G technology. 6G focuses on transmitting data at ultra-high frequencies ranging from hundreds of gigahertz (GHz) or THz, and it is very high in speed as compared to 5G technology that supports frequencies ranging up to 100 GHz theoretically but practically utilized frequencies ranging up to 39 GHz. Another important feature of 6G technology is improving the efficiency of the free spectrum.

In 5G technology, transmission or reception of data transfer permits at the same time on a specific frequency and uses two-way communication for data transfer and divides their frequency streams with the help of the FDD technique. 6G advanced approach uses sophisticated mathematics to transmit and receive data on the same frequency simultaneously and also helps for boosting the efficiency of the current spectrum. 5G networks are based on a hub-and-spoke architecture, and end-user (phones) devices connect to anchor nodes (cell towers) that are connected to a backbone. 6G might use every machine as an amplifier for one another's data and allow each device to expand coverage in addition to using it. It also added new dimensions to AI and brought new strength and vitality into the next-generation communication. The use of AI with 5G features transforms the paradigm shift into an intelligent network. 6G communication is also expanded by applying artificial intelligence to various other new technologies and helps to enhance spectral efficiency like visible light communication (VLC), index modulation, intelligent reflecting surface, and sub-THz and THz with a frequency range of 100 GHz to 3 THz [10–12]. A futuristic vision of the 6G network is specified in Table 1.1. The management of large infrastructure is also becoming very difficult for existing communication technology. The 6G technology has the capability to manage a large volume of data provides seamless and high-quality communication and will solve all these issues with a global coverage area as compared to existing generations. The existing communication generations are also insufficient for indoor communication, and reachability to rural and undeveloped regions is very low in the existing generation; on the other hand, the reachability of 6G network can be more effective in rural and undeveloped areas. Now, every sector is using the smart technology for developing for example smart building construction, automation of smart factories, and production, making smart healthcare and transport system, for smart surveillance, agriculture, etc. The 6G technology can play a vital role for development of all above abovementioned fields with its advanced features of high data speed bandwidth, high reliability, low latency time, etc. With the introduction 6G technology in the communication field, it is expected that many Internet of Things (IoT)–based devices use internet facilities and that helps to make human daily life more comfortable and easy. 6G technology will provide more substantial support to IoT devices by providing IoT-based houses, vehicles, and industries. 6G also plays a very effective part in improving the healthcare sector and facilitate the smart healthcare services [15–17]. The defense sector can also take advantage from new-generation technology to fulfill the UAVs requirement of high data speed.

1.1.3 Features of 6G Networks

- Use of new broad-spectrum bands that range up to THz.
- Very high or maximum data transfer rate of 1 Tbps. Speed and data rate experienced by a single user to speed of 1 Gbps, but, in the case of 5G technology, single user can achieved 100-Mbps data speed and maximum data transfer rate of 20 Gbps. 6G provides more than double the spectral efficiency of 5G networks. It is expected that the reliability of 6G networks is up to 99.99999%.
- 6G wireless networks provide ultra-low latency of less than 0.1 ms for real-time applications and improve the efficiency and performance of communication networks. The current 5G technology also lowers the latency time but just equal to 0.1 ms. The decreased latency time helps in providing better emergency responses, in remote surgical procedures and also in automation of industry.
- 6G will more focuses on M2M connections. In the existing technology, 4G and 5G networks are capable of supporting or handling 100,000 and one million devices per square kilometer, respectively, and perform efficiently, and, on the other hand, advanced 6G technology will manage or support 10 million linked devices per square kilometer [18].
- 6G networks require an extensive radio-frequency range, and to manage it need a very energy-efficient chip to meet the requirement for high bandwidth. A very big challenge for researchers is to optimize power consumption on that foundational chip so that it can perform better energy-efficiently in these frequency ranges [19].
- 6G technology provides high privacy and security as compared to previous-generation networks.
- 6G networks provide better network reliability than 5G networks, and the reliability of networks might be enhanced by simultaneous transmission and device-to-device connectivity. A 6G network will be better in network penetration and stability than a 5G network. As we discussed above, 6G networks use M2M connections that help in increasing network dependability and also decreasing error rates [20].
- The 6G networks will be available to cloud and can be access privately and publicly on cloud.

- 6G technology uses more features of AI and machine learning (ML) for optimal connectivity and allows AI/ML to determine the optimal method of communication between two endpoints.
- 6G technology jitter time is very less and equal to 1 ms. The advanced feature of high bandwidth speed and low latency time of 6G network reduces the jitter time of real-time videos.
- The processing delay in 6G network is less than or equal to 10 ns.

A tabular representation of the features of the 6G network is described in Table 1.1.

Table 1.1 Key features of 6G networks.

Requirements	**6G services**
Service Types	MBRLLC/mURLLC/HCS/MPS
Devices Types	Smart implants/Sensors/XR and BCI devices/DLT devices
Jitter	1 micro second
Individual data rate	100 Gbps
Latency	0.1 ms
Mobility	Up to 1000 Km/h
Reliability	Up to 99.99999%
Frequency	Sub-THz band, non-RF, Optical, VLC etc.
Multiplexing	Smart OFDM plus IM
Power consumption	Ultra Low
Processing delay	<= 10 ns
Security and Privacy	Very high
Wireless power transfer/ wireless charging	Support (BS to devices power transfer)
Autonomous V2X	Fully

1.1.4 Applications of 6G Networks

6G technology holds a large number of innovative applications due to its advanced features in various areas of communication. All advanced features of 6G technology will make it next future-generation technology in thefield of mobile communication [21, 22]. Some important futuristic and specific industrial applications of 6G technologyare discussed below:

- Immersive Extended Reality: 6G network provides high-quality bandwidth and ultra-low latency time for augmented, virtual, and mixed reality. These advanced features of 6G technology help in the uprising of the gaming industry, education sector, training, entertainment, and healthcare industry and provide a seamless experience with high data bandwidth to virtual reality/augmented reality.
- Holographic Communication: New technology provides advanced holographic communication and facilitates the 3D realistic representation of individual objects. This technology helps to make teleconferencing and telepresence more easy and interactive.
- Autonomous Self-Driving Vehicles: 6G can also play a very vital role in enhancing working structure of autonomous vehicles and help to make transport and communication management system more efficient and safer. It can manage the real-time exchange of data and vehicle-to-vehicle communication and also identify the real-time position of vehicles efficiently. 6G can also help in enhancing the required infrastructure connectivity of autonomous vehicles for communication. The advanced feature of high bandwidth speed and low latency speed helps to establish real-time communication between other vehicles and self-driving cars.
- Smart Cities: 6G applications play a very crucial role in efficient and sustainable smart development of city, including intelligent traffic management, smart water management, smart shopping, smart infrastructure development, environmental monitoring, smart energy optimization, and public safety. It collects and analysis real-time data and make appropriate decision with time for betterment result. Some advanced applications of smart cities help in the improvement of other services also [23, 24].

- Remote Healthcare: Due to the high-reliability and ultra-low latency features of 6G networks, a new revolution has arisen in the healthcare industry due to remote healthcare services. Now, many healthcare services are taking the advantages of the existing remote healthcare communication technologies like in remote surgeries, remote monitoring of patients, real-time telemedicine, and wearable of health monitoring devices. 6G enables doctors to perform better result as compared to 5G technology for real-time remote surgery with high-definition video. The high bandwidth speed features of 6G technology also play very crucial and helpful role for doctors to operate patient remotely. Sometimes, in rural areas, due to large distances, it is very difficult to provide good facilities to patients on time and in this situation remote healthcare plays a very vital role [25].
- Industrial Automation: 6G will enable or fulfill the communication needs of next-generation Industry 4.0. With the help of 6G applications, machine and devices can communicate to each other at real time. It can be very helpful for managing and keeping watch on real-time processes like in manufacturing control, robotics, supply chain management system, marketing, sales, and also in predictive maintenance. This smart control can help in increasing the production and efficiency of products.
- Internet of Things: Efficiency of IoT-based devices highly depends upon their connectivity. Nowadays, most electronic devices are designed on IoT-based technology, and 6G can provide high support for the connectivity of these devices; it can enable or handle seamless integration of the billions of IoT devices, smart agriculture, enabling smart homes, smart energy grids, and efficient asset tracking and management [26].
- High-Definition Multimedia: Advanced feature of ultra-high data rates of 6G can help in streaming of high-definition and 3D multimedia. It can enable streaming of high-quality videos, ultra-high-definition television, exciting gaming experiences, and high-fidelity audio streaming.
- Environmental Monitoring: 6G can also be useful for monitoring advanced environmental systems by addressing the

climate change and sustainability challenges. It can be helpful in air quality monitoring, improving water quality, identifying weather patterns, management of natural resources, informed decision-making, etc.

- Emergency and Disaster Management: 6G can also enhance the emergency and disaster management capabilities by providing real-time communication, real-time situation awareness, and their coordination. It can also support making more efficient disaster response and early warning systems. It can also be helpful during emergencies to manage the monitoring of remote critical infrastructure.
- Remote Monitoring and Sensing: New-generation technology provides features of remote monitoring and sensing of various specified fields such as agriculture precision, monitor of infrastructure, remote healthcare monitoring, environmental monitoring, weather forecasting, disaster management, and smart traffic management systems. This can be achieved by deployment of various sensors, intelligent drones, and deployment of efficient satellites for collection of real-time data. Through which we can make timely and accurate decisions based on sensor data of a specific field and take appropriate action [27].
- Education: 6G can be used for a new revolution in the education sector. Students and teacher can connect to each other virtually without need of any physical media and can share the useful resource to each other also. As we all seen in during COVID-19, online classes help students to interact with their teachers, 6G high bandwidth speed can also be very fruitful for students.
- High-Fidelity Mobile Entertainment: 6G technology also provides high-fidelity of streaming and creates a new entertainment experience. This also helps in the seamless streaming of large-size interactive videos (size up to 8K), advanced mobile real-time gaming, and virtual concerts and making multimedia applications more interactive [28, 29].

A pictorial representation of futuristic and specific industrial applications of 6G technology is given in Figure 1.2.

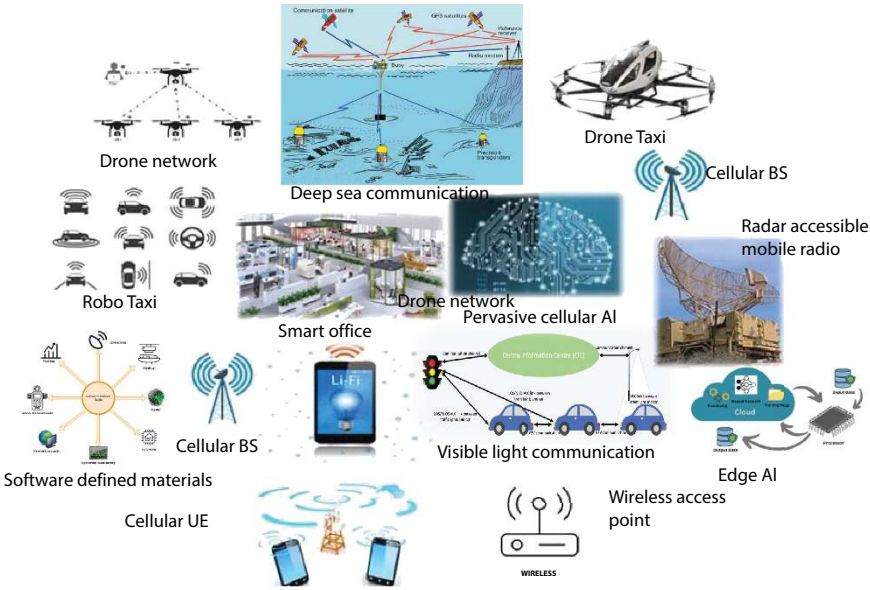

Figure 1.2 The futuristic and specific industrial applications of 6G technology.

1.1.5 Disadvantages of 6G Networks

Every technology has its advantages and disadvantages. Although the new era of mobile communication technology is the 6G networks, as mentioned above, 6G technology has advance key features as compared to other previous generation technology in term of high data rate speed and low latency time, but it requires more energy that increases energy cost for the user. The establishing, managing, maintaining, and building costs of 6G network are very high, and its cost is also varying from country and region-wise [30, 31]. Some disadvantages of 6G technology are discussed below:

- High Establishment Cost: The establishment of 6G network nationwide will require significantly more development and infrastructure cost that includes cost of deployment of new towers and antennas, andcaballing of fiber optic. This higher price cost may directly or indirectly be collected from consumers for accessing services of 6G network and devices.
- High Energy Consumption: The higher bandwidth speed of 6G requires more energy consumption for translation of data.

This impacts on our environment and needs for a sustainable solution to reduce power of network.

- Health Concerns: While, after implementation, we can reach on final conclusion, some concerns are arising, due to use of higher radio frequencies in 6G networks that are associated directly with human health, and probability of health risks may be increased. Further research and transparent results will address these concerns deeply.
- Ethical Considerations: It is necessary to carefully consider the all ethical implications of 6G technology before it is applicable to worldwide. Privacy, security, and misuse of data must be the primary concern of any communication technology, and all three issues must be addressed before the deployment of 6G technology. The new advanced 6G advanced technology has to ensure to provide an efficient and safer environment to customers.
- Uncertainties and Delays: 6G technology is not fully implemented yet and it is still there under the development phase as subject to change, and its final phase is completed after implementations. There might be several unforeseen challenges and delays have to manage before 6G reaches to its final phase.

1.1.6 Challenges of 6G Networks

Due to the advanced features of high-speed data of 6G networks, all telecom industrial partners are planning to establish new future-generation networks (6G networks). The 6G will be the new era of future communication networks. Even though there are a large number of features of 6G technology, there are some challenges to establishing 6G networks, and some are discussed below:

- Remote Areas Accessibility of Network: According to the survey, three billion people in the world still do not have access to internet services, especially in remote areas. This failure is due to the high deployment cost of base stations and caballing of fiber optics, and, sometimes, geographical conditions also affect the failure of services. To achieve 100% coverage worldwide, it needs to deploy a space network, which is a necessary requirement of 6G technology. This fully developed space network covers and spreads the network signals to all corners and can be easily accessed by

remote areas. One hundred percent reachability and coverage of the network to all is a big challenge for 6G networks.

- THz Communication: The 6G network provides high bandwidth frequency speed in THz frequency that varies in between the frequency range of 100 GHz to 10 THz. Such types of high bandwidth have not been used before in any communication networks, and it is estimated that high THz frequency has to face some problems like higher network deployment cost and challenges of covering large areas.
- Perception and Location: Presently, mobile users used radio spectrum for telecommunication. But in new advanced 6G era, the radio spectrum is not used in telecommunication for mobile operators. The 6G technology sensors are deployed to sense location of the mobile user. These sensors help to customers to access the communication services. It is tough for companies to cover a large area by deploying several sensors [32].
- Best use of Spectrum: The big drawback of current existing communication technology is the unused of radio spectrum. Even though countries manage their radio spectrum by properly distributing and authorizing spectrum, still, there is a lot of waste of spectrum. The new 6G technology used the dynamic spectrum approach for sharing the technology. Advancements in AI, IoT devices, blockchain, and some other relevant technologies such as mobile wireless technology are helping in controlling, distributing, and managing spectrum more effectively and intelligently with high flexibility. The full use of spectrum is also a big challenge for 6G technology.
- AI Network: Now, AI-based applications are used in various fields like identification of AI images, voice recognition, education, the healthcare industry, and wireless communication. Low network latency and high reliability are highly required components of wireless communication for better development of network services. A significant challenge in managing the network key performance indicators (KPI) process is from existing operations that help in assessing the health and performance of the network. These issues are resolved by induction of AI into given network and help in facilitating intelligent automation of network and transformation. This will require a massive amount of data and need for a computing resources that exert demand at maximum for AI. Therefore, new 6G era needs more interaction between networks and AI.

- Network Security: Network security plays a very crucial role in the era of any communication technology. The 5G technology consist of various key features like low latency time, high reliability, large bandwidth speed, and high network security. Introducing new 6G era technology, advanced post-quantum cryptography, and quantum key distribution technologies will be applied to the network to ensure absolute network security. Network security is also a very big challenge for 6G technology.
- Flexibility, Redundancy, and Self-Healing Capability: Nowadays, all industries are using the diverse applications of 5G for the smooth running of their day-to-day working. The industry is using 5G/6G technology for their digital operation and manufacturing. It also helps in handling of administration work also that requires a high level of network reliability and stability. The main role of the telecom industry is to develop a redundant, flexible, and self-healing network that helps in providing stable and efficient network services during network breakdown.
- Low-Carbon Transformation: Low-carbon emission is the main objective and essential trend for ICT industry. Due to increases in network bandwidth, it requires more energy and resource consumption. A big challenge for network operators is to deploy a low-carbon and energy-saving network that is highly responsible for performing social duties. In the future, a big challenge to develop an intelligent network enabled with AI that is capable or helping network operators with energy saving.

1.2 Security Evolution of Communication Networks

This is the main section of a book chapter, which focuses on security threats and privacy concerns of different cellular network generations. The existing mobile generation techniques have encountered with many challenging security concerns such as involvements of eavesdropping and physical attackers, some encryption issues, and many authentication problems. The threat of landscape increased along with more complex and competent attackers. 1G (first-generation) network used analog modulation techniques for data transfer and delivery of voice communications services. 1G generation has also several security problems such as problems of handover and

guarantee of no security. In addition to this, 1G network do not ensure any assurance of secure or private transmission of data. Unauthorized user can easily attack on network and access the data easily. 2G (second-generation) mobile generation uses digital modulation techniques for data transfer. Time division multiple access (TDMA) technique is used for transferring both voice as well as short message, and the GSM technique is used to provide authentication, personal security protection, privacy to data, and also transmission protection services. 2G is used for authentication of authorized users. The advanced encryption algorithm is used for the protection signaling, and user data and SIM function are used to create encryption keys. Unfortunately, although several security advancements are applied to the existing generation, still, there are a number of vulnerabilities available in the security of 2G networks. The authentication of one-way security is a big issue in 2G, and users will be easily authenticated by the network but cannot authenticate against of network [19]. An unauthorized station can easily steal a user's personal information. As we know, the 3G network came into the existence year 2000 and is generally used for increasing data speed of transmission up to a range of 2 Mbps and used to provide internet facility to user. The real-time streaming of datain (TV streaming, video streaming, and internet browsing) is easily accessible in the 3G network as compared to theprevious generation of mobile communication. As compared to 2G technology, 3G technology uses the two-way technique of authentication for data transfer and provides a more secure network than 2G networks. The 3D generation system controlled the complete security system of both the air interface and user authentication system. Air interface security systems provide users a reliable and secure communications over wireless links with the help of a two-way technique to authenticate both users and receiving and sending networks on both sides. The main security issues with 3G technology are internet protocol threats and, sometimes, communication channel attacks between the home networks and end devices also affect 3G technology. Some common wireless communication threats are integrity threats, unauthorized access of data, Denial-of-Service (DoS) attacks, and access to unauthorized service. The introduction of 4G networks offered a new revolution in the field of communication with a high download transmission speed of up to 1 Gbit per second and an upload communication speed of 500 Mbit per second. 4G networks as compared to the previous generation provided high spectrum efficiency and low latency, capable of handling complex problems easily such as HD TV and DVB. 4G technology contains IP core secure networks, backbone and access networks, and strong diversity of intelligent mobile users. 4G communication network has several security threats related to wireless

radio communication, tampering problems, eavesdropping, viruses, operating system attacks, threats of data alteration, and issues with network authentication. Users have the freedom to directly interact with mobile terminals and, because of that, create more security problems than previous existing radio station.

The 4G network also faces MAC layer weaknesses like reply and eavesdropping attacks. 4G systems have common security issues with data integrity, problems with access of unauthorized users, and tracking of location. 5G network approaches is more commercialize than other mobile network due to growing capacity of handling large size of devices and providing high quality of services to all devices of network. To understand security or privacy issues of mobile networks, there is a need to first understand the network architecture of 5G network. The network architecture of 5G network consists of three component networks access, backhaul, and core networks. In first component, network access has security issue with the handover between different devices and technologies and that increases the more probability of threats. The second component, backhaul networks, lies between core and networks access components and connected with the help of microwave connections, satellite links, wireless channels, and traditional lines. This network has minimum device connection, and, because of that, there are privacy and security problems than other components. The main security issues with the core network are conveyed due to the moving of the backhaul network. High data transfer rates create security problems for traffic probability attacks of Denial-of-Service (DoS), and two approaches are generally developed to manage those issues. The first approach permits communication among many devices with the help of lightweight and management of key authentication. The second approach focuses on device grouping through grouping-based methods, and privacy and security issues in 5G will create undoubtedly problems in field of mobile in coming years and that must be addressed and resolved timely. 5G network becomes more dynamic due to the cloud, SDN (Software-define-networking), and NFV (Network Functions Virtualization) technologies and, as a result, causes many threats and weaknesses in the network. Managing signal load by increasing more new devices and services is challenging job for new 6G applications. The 6G network capacity area is larger than 5G network handling more number of devices and requirement of high security network to handle the high data transfer network. The latency effect caused by security processes also needs to be addressed, and effective security approaches require high services to ensure good services and for continuity and availability of resources [33, 34]. Figure 1.3 summarizes the complete evolution and security related issues from 1G to upcoming new 6G generation.

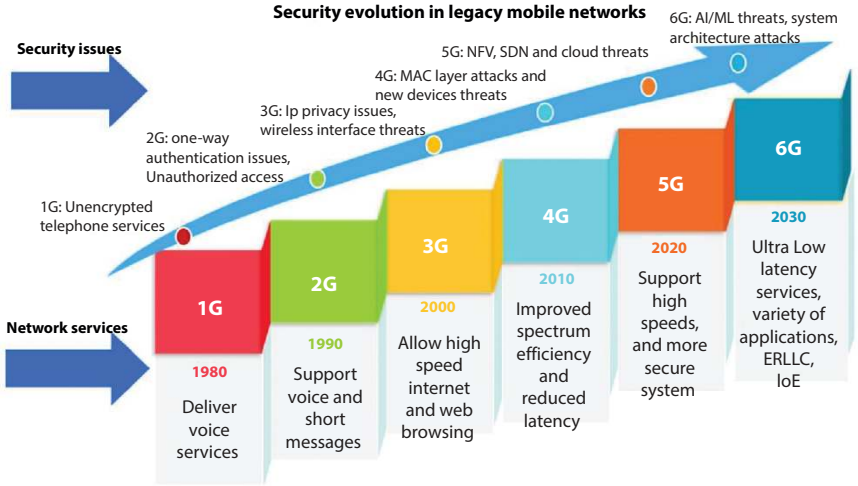

Figure 1.3 The security evolution of mobile communications from 1G to the predicted future 6G.

1.3 Privacy and Security Issues with 6G Networks

As we all know, the new era of mobile communication is the 6G network, and it transforms our daily digital life by adding with high unprecedented data speed and fast connectivity. 6G network provides a more open network to users as compared to the previous generation network. As we know, size of data is also increasing rapidly and very difficult to manage or handle such a large volume size of data. Surveillance of networks and unauthorized access of data from outsiders is also a major concern for researchers. Security and privacy of data is a very big challenge for researchers. The existing security methods like firewalls and IPsec are not good tool for protecting such large network from outsider in 6G network. The advanced 6G security protocols must be strongly encryption method that consistently monitors of network to handle user privacy by cyber threats. The 6G security protocol works on concept of zero-trust architecture (ZTA) for security of their network. The zero-trust (ZT) security level emphasizes on the protection of the network system from everything, uses the concept of ZT, and enables the relationships among entities of the network, rules of access, and all protocol processes. Therefore, ZTA is the best tool for security architecture of 6G, and, up to certain extent, security requirements are easily managed by using the ZT concept. Privacy is also a major concern for 6G security [35]. Privacy protection is a basic key feature for evaluating the performance requirements of any wireless communication networks.

1.3.1 Privacy Challenges in 6G Networks

The three main key challenges associated with privacy of the 6G network are discussed below:

a) A large number of data exchanges of small chunks in the 6G network may impose a high impact on the privacy of people, and, sometimes, it attracts the more extensive attention of governmental and other good business entities. If the accessibility and collectability of data in the 6G era become easy, then it will have a significant impact on protecting user privacy information.
b) When intelligence is forwarding toward the new edge of smart networks, more demanded or sophisticated applications will be run on our mobile handset that is causing a high probability of threat attacks. However, the privacy protection incorporating approaches in resource-constrained devices are highly challenging job.
c) Maintaining a high balance between user privacy and performance services is highly notable. Identification and finding the information of the location of mobile users need more careful consideration for accessing the right accurate data from the owner, and this also helps in the supervision and regulations of data and privacy protection.

1.3.2 Security Challenges in 6G Networks

Some common security challenges that have to be faced with 6G networks in our digital daily lives are discussed below:

AI and ML (AIML): AIML is the backbone of 6G network, and, due to increasing network complexity aggressively, the advancement in AI and big data related to 6G networks permits a new future generation of smart wireless applications and services. These services are furnishing the diverse communication requirements and structure of networks. The complexity helps to make the systems more fruitful and susceptible toward cyber-attacks. Sometimes, internal errors in AI algorithms also create a very critical issue that causes system failure and disrupts network operations. The concern is not limited to just external attacks but, sometimes, internal errors present in AI algorithms that can cause of system failures and disrupt working of network operations.

Data Privacy and Security: Increasing the volume size of data in the 6G network helps to facilitate faster communications among mobile users but also maximizes or increases the risk of managing large-volume data. Security and privacy of given data become a major concern for researchers of large-size data and the need for a strong or more powerful security protocol for advanced encryption. These advance and powerful encryption techniques and security protocol protect the network by the attack of unauthorized user and save the access or leakage of data from unauthorized users.

6G technology has the ability for analyzing and process data with high speed, but surveillance of unauthorized access of data is also a major concern for 6G technology. In 6G technology, doors are opened for all, and a more sophisticated surveillance is required. These advanced techniques can lead to unauthorized accessing or monitoring of data and also raise all serious concern about privacy of data. Safeguarding against unauthorized intrusions can be helpful to protect right of individual and help in maintaining trust and belief in 6G networks.

Autonomous Technology: 6G technology strengthens capacity of the autonomous systems and in drone systems, and self-driven vehicles predict their decisions that are based on previous dataset or autonomous system. The security of all these autonomous systems is also a very serious concern for 6G technology. Hacking or malfunctioning risk also increases and needs to take serious safety measures that are necessary requirement for managing these autonomous systems.

IoT Security Challenges: Nowadays, mostly electronic devices are smart devices that are based on IoT technology. These all devices are connected with each other through internet and the growth rate or expansion of IoT-based connected devices increases the vulnerability toward cyber threats. Every individual connected device that behaves as an entry level for entry of cyber-attacks and for managing of large devices requires a comprehensive security strategy. This advanced security approach helps to manage IoT-based ecosystem to prevent from unauthorized access of data and also secure our network.

Spectrum Expansion: 6G network spectrum includes a wide range of spectrum with a range of millimeter-wave with THz and optical fiber communications. Even though the wide range of 6G network spectrum has several benefits, still, it has also opened up new routes for misuse of

spectrum and interference by unauthorized access. Needs to require robust security protocols and also strong regulatory measures have to be taken for managing that help to avoid the exploitation of spectrum resources and networks.

ERLLC Service Challenges: Achieving or enhancing a ultra-low latency time requires a high-security protocol for Enhanced Ultra-Reliable and Low Latency Communication (ERLLC) services for the safeguarding service and also resource availability over the generation of interconnected devices in era of Internet-of-Everything (IoE) era. Without appropriate security measures, the mobility and nature of the interconnection of IoE devices could be easily exploited from attackers and compromise the network integrity and also disrupt all critical services.

1.4 Proposed Security Solution for 6G Networks

1.4.1 Distributed and Scalable AI/ML Security

As we know, the 6G network is an autonomous network that will perform its all network operations by itself without involvement of human interaction such as configuration, monitoring, healing, and optimization of networks. The induction of AI/ML techniques plays very crucial role part in field of wireless communication especially in security and privacy of 6G networks. AI/ML techniques can be very fruitful for controlling, managing, analyzing, and accessing large-scale distributed and generated data in 6G networks. The distributed AI/ML applied indifferent phases for providing advantages to cybersecurity protection in 6G in terms of high accuracy, network autonomy, and predictive security analytics. Still, several difficult challenges in using AIML for cybersecurity aspect are as follows:

Trustworthiness: The relevancy of AI/ML in future-generation networks depends upon the trustworthiness of AI/ML components. It is one of the most important issues for the existence of AI/ML in 6G Technology. To achieve this purpose, some trusted tools are applied to check the trustworthiness such as formal verification techniques and computing enablers.

Visibility: Monitoring and visibility is very crucial for controlling and accountability of a network. AI/ML tools need to keep more visibility on distributed and scaled distributed data.

AI Ethics and Liability: The integration of AI/ML applications in 6G security provides fairness and ethical security protection solutions to all users at the same time. If functioning of security systems is failed due to any reasons, then AI/ML applications provided liability to system.

Scalability and Feasibility: In a distributed scaled network, transmission of data should be more secure and also preserve privacy. Scalability and feasibility are the big challenges for AI/ML security functions for the communication, computation, and storage of resources.

Privacy in AI/ML: The different ML techniques are used for the privacy of data in AI/ML like deep learning,neural networks, and various supervised learning classification algorithms. These all are used to provide the privacy protection for data protection, image, location identification, and also communication of devices.

1.4.2 Distributed Ledger Technology (DLT)

From last few years, blockchain approaches have achieved highest attention in field of mobile telecommunication sector. DLT technology has several advantages in field of 6G networks, and it is applied in various services of 6G networks. Some of them are nonrepudiation, immutability, disintermediation, provenance proof, integrity of network, and pseudonymity. DLT has features for protection of the integrity of data of AI-based system through immutable records. It also builds a trust among different distributed stakeholders, by establishing a confidence in AI-driven systems or in multi-domain-based environments. This trust also helps to users to adopt autonomy with confidence. The drawback of 6G and AI networks is the security management of systems, and it is very difficult toprevent the method of failure of AI-dependable systems. Therefore, for prevention of failure of 6G networks, more needed focus on the liability and responsibility of the network and trust with liability are ensured delivery of E2E services in 6G networks. DLT technology can also be used for securing VNF management and slice brokering forautomatic SLA security solutions, for scalable the IoT management PKI, secure roaming services, and offloading handling. Blockchain technology also plays a very key role in the privacy preservation of 6G systems, and commoncommunication channels permit network users to identify pseudo names in place of their direct individual identification or about location information.

1.4.3 Quantum Security

Quantum computing aims to apply 6G communication technology for the prevention, security vulnerabilities mitigation, and detection. In future, this new computing communication network can be a novel research approach that tries to find the possibilities for replacing these quantum channels along with a noiseless classical channel, and these communication channels can achieve very high-reliability features in 6G. Along with very high advancements in the area of quantum computing, it is observed that quantum-based safe cryptography may be inculcated in the world of post-quantum-based technology. The second approach is applied for solving discrete logarithmic problems that can be capable of solving the current asymmetric cryptography in a given polynomial time with the help of induction of high quantum algorithms. Quantum computing may intrinsically provide information about the nature of a quantum, about its absolute randomness and all complete security concerns that all are required to improve the quality of transmission. The post-quantum integration cryptography approach uses security at the physical layer that ensures complete link security of 6G networks. A new novel approach of the research era may be open new ideas for researchers from the induction of ML-based techniques for cyber-security and along with encryption methods of quantum for establishing communication links or connections in 6G networks. Quantum ML methods may help in increasing the security level and privacy in the field of communication technology along with quantum techniques improvement in both solving supervised problems of classification and unsupervised learning tasks of clustering. We have several 6G areas or applications, where a very high probability of applying quantum security approaches or methods. For example, several application areas such as ocean and satellite communication, terrestrial networks, and THz network communications systems are some common potentials areas where we can apply quantum communication methods in wireless communication. Quantum key distribution is an example where quantum mechanics is successfully applied to establish secrecy between legitimate parties.

1.4.4 Physical Layer Security (PLS)

PLS is the primary security concern for each layer of a network. It is jointly used with all layers and implements redundant protection. PLS methods will provide a new adaptive layer additionally to 6G communication for protection and enables new technologies for example THz technology communication.

THz communication is a key feature of its range in between 1 GHz and 10 THz for 6G networks. At such frequency level, the probability of signal transmission will increases that permits to allow unauthorized users access to be entered into same legitimate user narrow path for intercepting signals and this process offers strong security level at the physical layer. Sometimes, it has been also observed that an eavesdropper also can intercept the signals, in the transmissions line-of-sight by putting an object at desired path of data transmission and scattering radiation frequency toward him. The countermeasure of the above eavesdropping method, a backscatter characterizing channel, was introduced to detect some parts of eavesdroppers. In THz communications, intruders can easily access and understand the malicious behavior of data transmission exposure, but the new PLS provides secure solutions for THz transmissions, for example, material electromagnetic signatures can be used for authentication of THz frequencies at the physical layer. Another example is the VLC technology that attracts high interest such as large data rates, available big spectrum, and inherent security against robustness interference, etc., as compared with high radio-frequency communications. VLC also offers high-security protection as a comparison to RF systems with their advanced communication features. Light wave cannot pass or penetrate through the walls. They are very vulnerable also for eavesdropping on the unauthorized access of nodes that are located in area of transmitter coverage. Confidentiality of VLC systems is a very crucial issue for the practical designing of VLC methods, where PLS methods can be very helpful in providing an interesting solution for concerned problems and for this instance. Joint VLC and ML capabilities of accurate localization can be used for detection of anomaly.

1.5 Conclusion

With almost in coming years, the network research phase of the 5G network is coming to an end and probablysoon be deployed from the market. Now, 6G network research has become the main agenda of research for many researchers. Undoubtedly, 6G network advanced services will bring communication networks to a very higherlevel as compared to the existing previous generations. In this chapter, we conducted the detailed description of all features, applications, benefits, and drawbacks of 6G networks. The book chapter also concludes the all security andprivacy issues that are related to 6G networks. First, we discussed an overview of the evolution of communication networks from 1G to 5G networks and also explain the importance of 6G networks in field of mobile communication

transmission. We also examined the four important key areas that are uncovered during security issues and these all are needs to focus on tomorrow's related 6G network technologies. We hope that this detailed discussion will help in people's interest toward security of 6G networks and help in further research.

References

1. Saad, W., Bennis, M., Chen, M., A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.*, 34, 3, 134–142, 2019.
2. de Alwis, C., Kalla, A., Pham, Q.V., Kumar, P., Dev, K., Hwang, W.J., Liyanage, M., Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. *IEEE Open J. Commun. Soc.*, 1–1, 2021.
3. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., Zorzi, M., Toward 6G Networks: Use Cases and Technologies. *IEEE Commun. Mag.*, 58, 3, 55–61, 2020.
4. Ziegler, H., Viswanathan, Flinck, H., Hoffmann, M., Räisänen, V., Hätönen, K., 6G Architecture to Connect the Worlds. *IEEE Access*, 8, 173508–173520, 2020.
5. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., HewaM. Liyanage, T., *et al.*, 6G White Paper: Research Challenges for Trust, Security and Privacy. *arXiv preprint arXiv:2004.11665*, 2020.
6. Singh, M., Sukhija, N., Sharma, A., Gupta, M., Aggarwal, P. K. Security and Privacy Requirements for IoMT-Based Smart Healthcare System: Challenges, Solutions, and Future Scope, in: *Big Data Analysis for Green Computing: Concepts and Applications*, 2021, https://doi.org/10.1201/9781003032328-2.
7. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A., Overview of 5G Security Challenges and Solutions. *IEEE Commun. Stand. Mag.*, 2, 1, 36–43, 2018.
8. Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M., A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surv. Tutor.*, 22, 1, 196–248, 2019.
9. Ranaweera, P., Jurcut, A.D., Liyanage, M., Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Commun. Surv. Tutor.*, 1–1, 2021.
10. Wijethilaka, S. and Liyanage, M., Survey on network slicing for internet of things realization in 5g networks. *IEEE Commun. Surv. Tutor.*, 2021.
11. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., Zeng, K., Physical Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet Things J.*, 6, 5, 8169– 8181, 2019.

12. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H., A Survey on Security and Privacy Issues in Internet- of-Things. *IEEE Internet Things J.*, 4, 5, 1250–1258, 2017.
13. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in Computer and Information Science*, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
14. Benzaid, C. and Taleb, T., AI for Beyond 5G Networks: A CyberSecurity Defense or Offense Enabler? *IEEE Netw.*, 34, 6, 140–147, 2020.
15. Hewa, T., Gür, G., Kalla, A., Ylianttila, M., Bracken, A., Liyanage, M., The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions, in: *2020 2nd 6G Wireless Summit (6G SUMMIT)*, IEEE, pp. 1–5, 2020.
16. Dogra, A., Jha, R.K., Jain, S., A Survey on beyond 5G Network with the Advent of 6G: Architecture and Emerging Technologies. *IEEE Access*, 2020.
17. Blinowski, G., Security of Visible Light Communication Systems—A Survey. *Phys. Commun.*, 34, 246–260, 2019.
18. Singh, M., and Malik, A., Multi-Hop Routing Protocol in SDN-Based Wireless Sensor Network: A Comprehensive Survey, in: *Software-Defined Network Frameworks: Security Issues and Use Cases,* pp. 121–141, CRC Press, 2024, https://doi.org/10.1201/9781040018323-8.
19. Singh, M., Gupta, M., Sharma, A., Jain, P., Aggarwal, P. K., Role of Deep Learning in Healthcare Industry: Limitations, Challenges and Future Scope, in: *Deep Learning for Healthcare Services,* pp. 1–22, 2023, https://doi.org/10.2174/9789815080230123020003.
20. Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M., Jain, R., Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet Things J.*, 6, 4, 6822–6834, 2019.
21. Fang, H., Qi, A., Wang, X., Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement. *IEEE Netw.*, 34, 3, 24–29, 2020.
22. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P. K., IoT and blockchain technology in 5G smart healthcare, in: *Blockchain Applications for Healthcare Informatics: beyond 5G*, pp. 137–161, Elsevier, 2022, https://doi.org/10.1016/B978-0-323-90615-9.00004-9.
23. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in renewable energy harvesting for EV charging infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 75–90, IGI Global, USA, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.
24. Ma, C., Li, J., Ding, M., Yang, H.H., Shu, F., Quek, T.Q.S., Poor, H.V., On Safeguarding Privacy and Security in the Framework of Federated Learning. *IEEE Netw.*, 34, 4, 242–248, 2020.
25. Chkirbene, Z., Erbad, A., Hamila, R., Gouissem, A., Mohamed, A., Guizani, M., Hamdi, M., Weighted Trustworthiness for ML based Attacks Classification, in: *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, pp. 1–7, 2020.

26. Benzaid, C. and Taleb, T., ZSM Security: Threat Surface and Best Practices. *IEEE Netw.*, 34, 3, 124–133, 2020.
27. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S., Quantum Machine Learning. *Nature*, 549, 7671, 195–202, 2017.
28. L. Xiao., Sheng, G., Liu, S., Dai, H., Peng, M., Song, J., Deep Reinforcement Learning-enabled Secure Visible Light communication against Eavesdropping. *IEEE Trans. Commun.*, 67, 10, 6994–7005, 2019.
29. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P. K., Singh, M., Edge computing-based design for IoT security, in: *Network Optimization in Intelligent Internet of Things Applications: Principles and Challenges,* pp. 298–309, CRC Press, 2024, https://doi.org/10.1201/9781003405535-22.
30. Saxena, P., Jain, P., Aggarwal, P., Singh, M., Goel, S., Batra, M., Communication requirements and performance metrics for electric vehicle charging: A comprehensive review, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 15–30, IGI Global, USA, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch002.
31. Li, J., Kuang, X., Lin, S., Ma, X., Tang, Y., Privacy Preservation for Machine Learning Training and Classification based on Homomorphic Encryption Schemes. *Inf. Sci.*, 526, 166–179, 2020.
32. Mishra, S., Shukla, A., Arora, S., Kathuria, H., Singh, M., Controlling Weather Dependent Tasks Using Random Forest Algorithm. *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bengaluru, India, pp. 1–8, 2020, doi: 10.1109/ICAECC50550.2020.9339508.
33. d'Aquin, M., Troullinou, P., O'Connor, N.E., Cullen, A., Faller, G., Holden, L., Towards an 'Ethics by Design' Methodology for AI Research Projects, in: *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 54–59, 2018.
34. Cho, J.-H., Sharma, D.P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T.J., Kim, D.S., Lim, H., Nelson, F.F., Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. *IEEE Commun. Surv. Tutor.*, 22, 1.
35. Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E., Winfield, A., *The Ethics of Artificial Intelligence: Issues and Initiatives*, European Parliamentary Research Service, March 2020, [Online].Available:https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452.

2

Key Security Issues and Solutions in 6G Communications

Abhishek Pandit and Krupali Gosai*

Marwadi University, Rajkot, Gujarat, India

Abstract

The transition to 6G networks promises an unexpected growth in terms of speed, connectivity, and support for real-time, data-intensive applications across sectors. These advancements bring a new set of security concerns that go beyond those of previous generations. In this review work, we include the evolving landscape of 6G communication systems, focusing on both traditional security issues and advanced challenges introduced by emerging technologies such as artificial intelligence, federated learning, and quantum computing. To address these complexities, we propose a threat model taxonomy and categorize mitigation strategies into three primary areas: cryptographic techniques, entity-based security, and intrusion detection systems. Within this framework, we also classify various authentication methods essential for securing 6G networks including handover verification, shared and physical layer authentication, and token-based and multi-factor verification. It concluded with potential research directions to meet the dynamic security requirements of 6G networks, aiming to support a secure, resilient, and scalable communication environment for future applications.

***Keywords*:** 6G technology, security measures, threat models, artificial intelligence, federated learning

2.1 Introduction

The Sixth Era (6G) adaptable organization correspondence is ready to change universal availability inside the following couple of many years or potentially even sooner. In contrast to the Fifth Generation (5G), 6G aims

**Corresponding author:* krupaligosai17@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (29–56) © 2026 Scrivener Publishing LLC

to achieve gigabit-per-second bit rates, provide extended bandwidth, and significantly reduce latency. This development is necessary for the Web of Things (WoT) to indulge what is in store landscape of billions of consistent devices. 6G innovation will utilize both "balance" and "imbalance" to drive efficiency and viability in savvy Internet-of-Things (IoT) frameworks. By integrating evenness into remote advancements, network clients will actually want to normally switch between different specialist organizations and advancements, bringing about predictable nature of administration [quality of service (QoS)], quick 3D handovers, and backing for mental systems administration and summed up transparency. Future applications like completely immersive virtual reality, real-time analytics powered by AI, and vast IoT ecosystems in smart cities, healthcare, transportation, and other fields will be made possible by this evolution. To protect the integrity, safety, and privacy of this hyperconnected society, a complex array of security issues must be resolved in addition to the revolutionary potential of 6G. Because 6G networks depend on cutting-edge technology like artificial intelligence (AI), edge computing, and quantum communication, they present new security challenges as they develop. 6G network increased attack surface creates new opportunities for cyberthreats, such as quantum decryption, Distributed Denial of Service (DDoS), and eavesdropping. This risk comprises user information, interfere with essential services, and erode confidence in 6G.

As shown in Figure 2.1, in generation of networks, it possible to commercialization of 6G that is projected to begin around 2032, and this

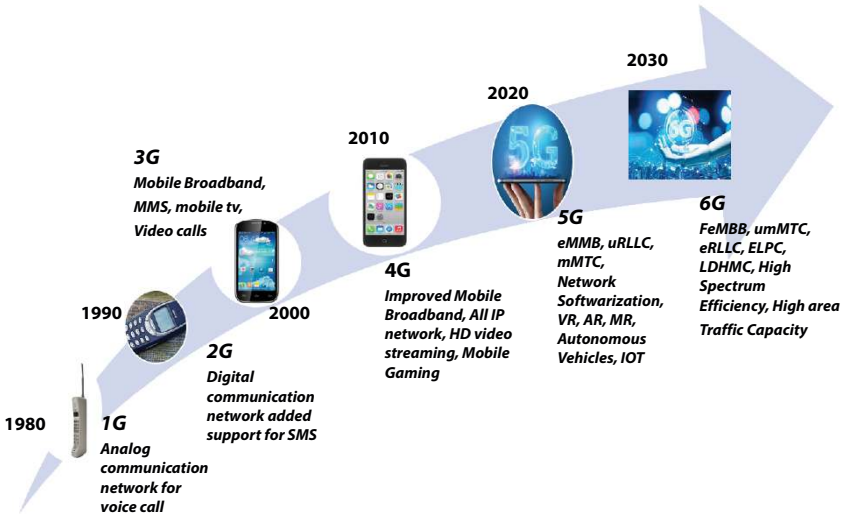

Figure 2.1 Generation of networks.

multi-dimensional expansion will introduce serious cybersecurity intimidations linked to secrecy, respectability, and accessibility [Confidentiality, integrity, and availability (CIA)], known as the CIA ternion. Furthermore, the IP-based network development of 6G will include customary susceptibilities that need the progression of cutting-edge safety models [1]. The possibility of 3D handover will empower gadgets to keep with associated across different groups, which will be defenseless against issues like pantomime, snooping, Circulated Refusal of Administration (DDoS) assaults, Man-in-the-Center (MitM) assaults, disavowal, and replay assaults. Ensuring minimal latency and seamless bandwidth will be challenging when integrating protected and privacy-preserving architectures. Thus, creating a robust, universal level well-being planning for QoS in 6G networks will be critical for the systematic emergence of this new communication era.

2.1.1 Security Considerations for 6G Communication

6G, the next generation mobile network, is anticipated to offer amenities with high data rates, increased capacity, and low latency, as well as handle a substantially higher number of coupled devices. The fast progression of 6G communication systems presents a number of security issues that need to be resolved to guarantee their dependability, security, and confidentiality [2].

Important security factors consist of the following:

- **Increased Attack Surface:** The number of devices that are linked has reached billions, which means that there are exponentially more opportunities for hostile actors to get in. Numerous device kinds, each with unique vulnerabilities, are included in this expanded attack surface, including smartphones, IoT devices, sensors, and autonomous systems.
- **Data Privacy:** In order to preserve user privacy and adhere to data protection laws, enhanced capabilities for data collecting and processing need for strict controls.
- **Advanced Attacks:** As a result of technological breakthroughs like AI and quantum computing, cyber-attacks are becoming more sophisticated.
- **Protection of Vital Infrastructure:** Because 6G networks will support vital infrastructure, ensuring their security

is essential to averting interruptions that might have far-reaching effects.
- **Authentication and Access Control:** To prevent unwanted usage and security breaches, it is essential to provide safe network access using strong authentication techniques and access control systems.

2.1.2 Survey Objectives

The primary objectives of this survey are as follows:

- To give a wide-ranging outline of the arising 6G correspondence worldview, focusing on its advantages over 5G.
- To inspect both conventional and creative security ideas pertinent to 6G.
- To establish a taxonomy of 6G-specific threat models with a focus on essential security standards: privacy, integrity, accessibility, validation, and access control (CIA3).
- To analyze and classify a variety of methods for dealing with threats, plus cryptographic Intrusion Detection Systems (IDSs), entity attributes, and methods.
- To investigate a wide variety of authentication methods that are suitable for 6G environments.
- To propose future examination headings to address developing security challenges in 6G communication.

2.1.3 Overview of 6G Communication Paradigm

2.1.3.1 Evolution from 5G to 6G

The evolution from 5G to 6G represents a substantial leap in mobile network technology, categorized by the following:

- Higher Data Rates: 6G aims to attain data rates in the range of several gigabits per second, far surpassing the capabilities of 5G.
- Ultra-Low Latency: The reduction in latency will support real-time applications and services, enhancing user experience and enabling new use cases.

- Enhanced Connectivity: 6G will support a larger number of connected devices, driving the development of the IoT ecosystem.
- Advanced Applications: The progress will facilitate the development of advanced applications such as holographic communication, tactile internet, and immersive virtual reality experiences [3].

2.1.3.2 Key Features of 6G Networks

- High Capacity and Speed: Increased bandwidth and data rates to support high-demand bids and facilities.
- Super Dependable Low-Inactivity Correspondence: Basic for applications requiring quick criticism and high unwavering quality, like independent vehicles and distant medical procedure.
- Huge Machine-Type Communication: Enabling the linking of a vast amount of IoT devices, supporting smart cities, industrial automation, and more.
- AI-Driven Network Management: Leveraging AI for efficient network management, optimization, and security threat detection.
- Energy Efficiency: Emphasis on reducing the energy consumption of network infrastructure to support sustainable development goals.

2.1.4 Emerging Technologies in 6G

The 6G will be heavily inclined by a number of emerging technologies. Mode of communication:

- Artificial Intelligence (AI): AI resolves production an energetic role in the operation of networks, advancement execution, and improving security through cutting edge danger location and mitigation methods.
- Quantum Registering: Quantum processing offers the possibility to reform information handling capacities and acquaint quantum-safe cryptographic techniques with improve safety.
- Federated Learning (FL): This innovation empowers decentralized AI, training models across multiple devices without sharing raw data, preserving data privacy data, which is necessary for 6G networks that are private and secure [4].

2.2 Security Challenges for 6G Communications

2.2.1 Security Implications

Immense Connectivity and Increased Data Rates: It is anticipated that 6G networks will support a huge number of connected devices and provide extremely high data speeds of up to several gigabits per second. Networks are now more exposed to cyberattacks because of the larger attack surface created by this notable increase in connectivity. Solid safety efforts are fundamental to shielding the huge capacities of information being sent and forestalling unlawful admittance to private information.

2.2.2 AI and Machine Learning Integration: Security Concerns

The aptitude and improvement of 6G organizations rely strongly upon man-made intelligence (computer-based intelligence) and AI (ML), which upgrade execution and open up new help open doors. In any case, their management makes extra security weaknesses. Cyberattacks like malware distribution, phishing, and network intrusion could be automated and made more effective with AI-powered attacks. Choices that are made erroneously can result from adversarial attacks that use false information to influence AI models. Using robust training datasets, ongoing monitoring, and techniques for anomaly detection, it is essential to secure AI algorithms in order to combat these risks and maintain network integrity. AI's remarkable elements and great capacities have prompted its far and wide use in remote and versatile systems administration. The vast amounts of information produced by numerous WoT devices can be harnessed by AI techniques to citation valuable insights, thereby enhancing network operations and presentation. As of late, combined learning (CL) or FL has arisen as another computer-based intelligence worldview that powers on-gadget treatment power and improves client data protection. The basic idea is to train a common model together with other devices. The gadgets train nearby models, but they only portion informs with a federal server rather than the raw data [5].

There are three forms of FL: horizontal, vertical, and federated transfer learning. Throughout the current years, different man-made intelligence procedures have been utilized to address various complications in remote organizations. The significance of AI and FL increases as 6G is anticipated to be based on AI/ML. To defeat the restrictions of concentrated AI, for example, security fears and significant correspondence above, FL is getting momentum as a feasible dispersed AI arrangement, empowering the vision of "universal AI" in 6G interchanges. FL offers various advantages for 6G,

including correspondence effective circulated AI, supporting for heterogeneous information from different gadgets and administrations coming about in non-indistinguishably distributed (non-IID) datasets and security assurance by keeping information neighborhood and empowering enormous scope organization.

2.2.3 Network Slicing: Isolation and Security Issues

One of the foremost elements of 6G is network cutting, which allows you to make various virtual organizations on a private actual foundation that are custom fitted to explicit use cases and needs. Because of this ability, service providers can dynamically allocate resources and optimize performance for a wide range of applications, significantly increasing the network's adaptability and efficiency. In any case, it, moreover, presents huge security moves that ought to be addressed to ensure the protected and strong action of these virtual associations. One of the most important security concerns with network slicing is maintaining proper isolation between slices. An assailant who accesses one cut might move straight and compromise different cuts, bringing about broad security breaks without sufficient detachment. Strenuous access control measures are necessary to ensure that each cut functions independently. These demands enforce stringent regulations regarding who has access to each slice and what they can do with it. Continuous monitoring mechanisms are also required to quickly identify and respond to security threats. By planning the diverse security capabilities across different cuts, computerized security organization can aid danger the board and alleviation. This includes incorporating advanced security actions and protocols that are able to adapt to the potent concept of organization cutting. With esteems to controlling the security of each cut, devices like virtual organization capabilities (VNFs) are totally essential. These conventions work with secure correspondence between different organization parts, guaranteeing that information stays safeguarded as it travels through the organization [6].

2.2.4 Security Implications with Ultra-Low Latency

A sign of 6G is extremely low levels of inactivity, permitting continuous applications like autonomous vehicles, distant medical procedures, and expanded reality. Executing specific safety efforts, which ordinarily bring about delays, is troublesome in light of the fact that this requires exceptionally elevated directing and fundamentally decreased handling times. To protect these time-sensitive applications from likely threats, it is essential to modify the requirement for trifling inactivity and implement stringent security protocols. Fast and

successful validation components like lightweight cryptographic conventions and pre-shared keys are fundamental to accomplishing speedy confirmation without compromising security. Furthermore, security examination driven by AI and constant checking can recognize and answer dangers progressively, guaranteeing that security is maintained without influencing execution. To promptly answer dangers and recognize peculiarities, these frameworks should have the option to handle a lot of data at a rapid [7].

2.2.5 Terahertz Communications

The Terahertz (THz) recurrence range, crossing from 0.1 to 10 THz, blends the properties of optical and microwave groups to help super high broadcast rates, powerful enemy of obstruction abilities, and consistent reconciliation of detecting and correspondence capabilities.

Initially, THz communications aim to meet system demands for broadcast speeds in the direction of terabits per second, representing a significant advancement over existing methods. This technology promises numerous applications, including minor communications, latent holographic communications, high-speed and high-capacity data transfers, and short-range broadcasts. Additionally, THz communications can facilitate high-precision positioning and high-resolution sensing applications. THz communications, for instance, are susceptible to narrow beam eavesdropping, necessitating novel defenses against such threats. In the context of 6G, ensuring that THz communications are secure and efficient remains an important area of ongoing research and development.

2.2.6 Unique Security Concerns

The interesting highlights of 6G, like 3D network, incorporated detecting, and high-level UIs, present explicit security concerns. New difficulties arise when trying to ensure safe communication in three-dimensional space, including aerial and submerged environments. Militainment needs secure handover systems and hearty 3D encryption measures. Security as gadgets cross different organization zones and circumstances becoming more intricate, necessitating real-time threat detection, dynamic encryption techniques, andadaptive authentication to guarantee safe and smooth communication across diverse 6G environments. The coordination of recognizing capacities with correspondence abilities can make new vectors for snooping and data catch endeavor, lacking broad security frameworks to address likely shortcomings. The development of detailed security protocols to protect these unique elements necessitates a thorough understanding of the interaction between correspondence and detecting advancements.

2.2.7 Integration of Internet of Things and Edge Devices

With 6G, it will be much modest to participate edge devices and the IoT, making it possible to process data dispersed and make decisions in real time. In any case, the trouble of preservation that these frameworks produce is because of their dispersed nature. Executing vigorous safety efforts is difficult because of the way that edge gadgets much of the time have limited assets. Lightweight cryptography provides effective security solutions that are essential for protecting resource-constrained devices without overburdening their limited capabilities. Ensuring secure correspondence, data uprightness, and contraption approval in a decentralized IoT environment is essential to hinder unapproved access and data breaks. The variety and dynamic nature of IoT deployments necessitate that these security measures be scalable and adaptable for their effectiveness.

In 6G networks, the extensive network of IoT and edge devices has increased privacy issues over user data. From location monitoring in smart city apps to health data on wearables, these gadgets gather and send huge amount of sensitive and personal data. The following are some of the main privacy issues with user data in relation to IoT and edge devices in 6G networks:

- Massive data collection
- Unauthorized access and data security
- Data ownership and user control
- Data processing at the edge

These are the main issues in a fully connected 6G era, anticipating these privacy concerns will be crucial to building confidence and guaranteeing user security [8].

2.2.8 Expanded Attack Surface and Privacy Concerns

Due to the wide-ranging connectivity and advanced capabilities of 6G, there are more opportunities for malicious actors to exploit vulnerabilities, which results in an expanded attack surface. This improved connectivity raises significant secrecy concerns as an increasing amount of personal information is collected and processed. In 6G networks, user privacy must be protected by management through strict security actions like information anonymization, secure information stockpiling, and client consent. Differential protection and secure multi-party calculation are two strategies that can assist with defending client information while likewise working

with valuable information investigation. These measures must be planned to handle the continued evolution of connectivity in order to guarantee privacy protection in 6G networks despite the increasing volumes of data and difficulty of the systems.

2.2.9 User Data and Anonymity

Protection of client information and keeping up with privacy develop in significance with 6G's superior information assortment abilities. Security risks can be reduced by limiting the storage of sensitive data and collecting only the necessary information to provide specific types of assistance. Gap protection strategies license helpful information examination while saving the security of individual client information. Ensuring that clients are clearly informed about data collection practices and obtaining their explicit consent is essential for maintaining trust and transparency. Secure information sharing and information minimization, for example, can help uphold client confidentiality and protect complex data from unauthorized access. These measures must be robust and transparent in order to adhere to shifting privacy regulations and maintain user confidence [9].

2.2.10 Quantum Computing Threats

The roles that quantum systems play in networking and communication can be broken down into two broad categories: quantum computing and quantum communication. Quantum correspondence, as made sense of by Gisin *et al.*, [21] includes moving a quantum state from a shipper to a beneficiary, authorizing errands that are either unimaginable or wasteful utilizing traditional methods. Quantum key conveyance (QKC), quantum-safe straight correspondence, quantum secret distribution, quantum instant transportation, and the production of a quantum system by quantum channels, memory, and servers are among the many interesting utilization of quantum correspondence. One of the most encouraging utilizations of quantum correspondence is quantum key dissemination (QKD), where cryptographic keys are safely circulated. Procedures involving quantum entrapment for QKD are known as snare-based QKD. Because any disturbance to the quantum state can be recognized by looking at the relationships between the imparting substances, these methods can easily identify any man-in-the-middle attacks. Quantum correspondence is expected to assume a serious part in getting 6G correspondences. The non-cloning theorem, quantum entanglement, superposition, and non-locality foundational principles provide strong security measures. Quantum correspondence is

expected to help cutting edge administrations, for example, holographic telepresence, material web, cerebrum PC interfaces, and incredibly gigantic and insightful interchanges. Among these, QKD conventions have shown the most progression, with various common-sense implementations exhibiting their possible appropriateness in 6G organizations. Extra animating procedure of quantum correspondence is secure significant distance correspondence, which lines up with the imagined focal point of 6G on significant distance and high-versatility interchanges (HVIs). Because dealing with extremely long-distance communications requires this focus on HVI, the secure distribution of information over vast distances is especially important for 6G networks [10, 11].

2.3 Legacy Security Concepts in 6G

2.3.1 Confidentiality, Integrity, and Availability

Confidentiality, integrity, and availability (CIA) are foundational values in network security, often referred to as the CIA triad. These principles remain crucial in the context of 6G communications.

Confidentiality: It is ensuring that only approved parties have access to complex information in 6G networks. Advanced encryption techniques will be required to safeguard data both at rest and in transit in light of the anticipated proliferation of devices and data. As quantum computing capabilities advance, the need for encryption algorithms that are resistant to quantum fluctuations will grow.
Integrity: Shielding information from unapproved alteration or obliteration is one method for guaranteeing information trustworthiness. In 6G associations, the test will be to stay aware of data trustworthiness across an astoundingly extraordinary and scattered environment. Blockchain and hash-based message confirmation codes (HMACs) are two techniques that can be utilized to ensure that information does not change during transmission or capacity.
Availability: Availability guarantees that approved gatherings can get to and use network administrations upon demand. To forestall and relieve disavowal of-administration assaults, the super dependable low-dormancy correspondence in 6G will require hearty safety efforts. In 6G conditions, network overt repetitiveness, adaptation to non-critical failure, and modern danger identification frameworks will be fundamental for keeping up with high accessibility [12].

2.3.2 Authentication

Authentication is the method involved with collateral the character of a client or gadget prior to giving access to network assets. In 6G, confirmation components should advance to deal with the expanded number and diversity of connected devices' difficulty.

- **Multi-Factor Authentication (MFA):** To improve security, 6G networks will implement MFA, which combines different types of validation, for example, something you know (secret key), something you take (security token), and something you are (biometric check).
- **Physical Layer Authentication:** This method influences unique characteristics of the physical communication channel to authenticate devices. Techniques such as channel state information (CSI) and radio-frequency fingerprinting can provide an additional layer of security at the physical layer.
- **Quantum Authentication:** Quantum-based authentication methods will provide vigorous protection against eavesdropping and replay attacks as quantum technologies advance. QKD and quantum advanced marks are cases of innovations that can be utilized to upgrade verification security in 6G organizations.

2.3.3 Access Control

Access control mechanisms ensure that only authorized users and devices can access specific network resources. In 6G networks, these mechanisms need to be more dynamic and context-aware to handle the diverse and highly mobile environment.

- **Portion-Based Contact Control:** It allocates access approvals built on the parts of users inside an organization. This method simplifies management and safeguards that user have the appropriate level of access based on their responsibilities.
- **Attribute-Based Access Control:** It reflects various potentials (e.g., user characteristics, supply type, and environmental conditions) to make access decisions. This tactic provides greater flexibility and fine-grained control, which is essential in the active and heterogeneous 6G ecosystem.

- **Context-Aware Access Control:** In 6G, context-aware access control systems will operate real-time context info (such as location, time, and user conduct) to make more informed and adaptive access control decisions. This ensures that access plans can dynamically adjust to varying circumstances and potential threats [13].

2.4 6G Security Innovations

2.4.1 AI Integration

Computerized reasoning (man-made intelligence) will undertake a fundamental part in refining the security of 6G organizations. With the immoral flood of information and the intricacy of organization traffic, customary security instruments might miss the mark. AI can assistance *via* robotizing danger recognition and reaction, decreasing an opportunity to recognize and relieve security breaks. The vast amounts of network data that machine learning algorithms can analyze can be used to find anomalies, such as unusual behavior patterns that could indicate a cyberattack. Moreover, simulated intelligence can be utilized to anticipate potential security dangers in view of verifiable information, empowering proactive safety efforts. For example, simulated intelligence-driven security frameworks can naturally regulate to new dangers by uplifting their calculations, making 6G organizations stronger against advancing digital dangers [14].

Let us take one real-time scenario where AI-driven threat detection and mitigation in a 6G smart city have been deployed which handles massive IoT connections while ensuring data security and privacy. That is implemented using AI-powered anomaly detection and threat prediction using advanced machine learning algorithms for behavioral analysis and real-time detection. Also, edge AI provides distributed security which localized response mechanisms and privacy preservation. Moreover, intelligent access control and authentication for continuous biometric authentication using AI play crucial role to deal with this type of sensitive data. Most interesting AI integration in quantum-resistant cryptography to enhance encryption and prediction of quantum attacks.

2.4.2 Quantum Computing Impact

Quantum computation [7] presents the two open doors and complications for 6G security. On one hand, quantum PCs have the conceivable to pause customary encryption calculations, posing a serious danger to information classification. This requires the improvement of quantum-safe cryptographic techniques to safeguard 6G interchanges. To defend against quantum attacks, research is existence done on post-quantum cryptography, which includes algorithms like lattice-based, hash-based, and code-based cryptography. Then again, quantum advances, moreover, offer new security arrangements. QKC can give practically strong encryption by utilizing the morals of quantum mechanics to safely share encoding keys. The non-cloning hypothesis of quantum mechanics guarantees that any endeavor to catch the keys will be perceptible, consequently giving a remarkable degree of care.

2.4.3 Federated Learning Role

FL is arising as a vital part of 6G security, especially with esteems to information protection and decentralized network conditions. FL improves secrecy by allowing multiple devices to train machine learning models together without sharing their raw data. This decentralized methodology is especially useful for IoT gadgets and edge calculation circumstances in 6G organizations, where info is numerous times touchy and conveyed across various gadgets. Keeping the information nearby and just sharing model updates cut the gamble of information breaks and defend consistence with information assurance guidelines. Additionally, FL can use a variety of datasets from a variety of sources to improve the robustness of AI models, resulting in security mechanisms that are more universally valid and resilient. By aggregating real-time insights from multiple devices, FL in 6G can also aid in the speedy detection of security threats, allowing for quicker and more coordinated responses to cyberattacks [15].

Case Study: Enhancing Security in a 6G Smart Healthcare Network With Federated Learning

Millions of linked devices, including wearable health monitors, hospital equipment, and patient smartphones, create and exchange sensitive data in real time inside a 6G-enabled smart healthcare network. However, the tremendous amount of sensitivity health data introduces unique security challenges that include data privacy risks, potential unauthorized access, and the threat of cyber-attacks. By using a decentralized approach to machine learning, FL enables edge devices to train models locally and share only encrypted model updates with a central server, reducing the

need for raw data to leave devices. By facilitating real-time, decentralized threat detection, the use of FL with a 6G network enhances security and data privacy and also improves patient data confidentiality while ensuring dependable, low-latency connectivity by significantly reducing the danger of data disclosure and centralized vulnerabilities. Furthermore, the network's capacity to recognize unexpected type of cyberthreats was enhanced by the collaborative intelligence from several devices [16].

2.5 Threat Models in 6G Communication

The record wide-ranging threat model for 6G communication is provided in this section. As we can see in Figure 2.2, a 6G threat model where we find more than 32 attacks on 6G mobile network communication security was inspected in relation to authentication and privacy-preserving strategies. Numerous separate standards still exist in the literature to produce a classification of the threat model due to the symmetrical conduct of remote organization dangers. Threats to 6G mobile networks [9] were broken down into five categories by our survey.

The danger model is a lengthy CIA group of three that incorporates dangers connected with secrecy, respectability, accessibility, validation, and access control (CIA3). Understanding and solving 6G's security issues are essential as the technology develops to accommodate high-speed data, massive IoT networks, and advanced real-time applications.

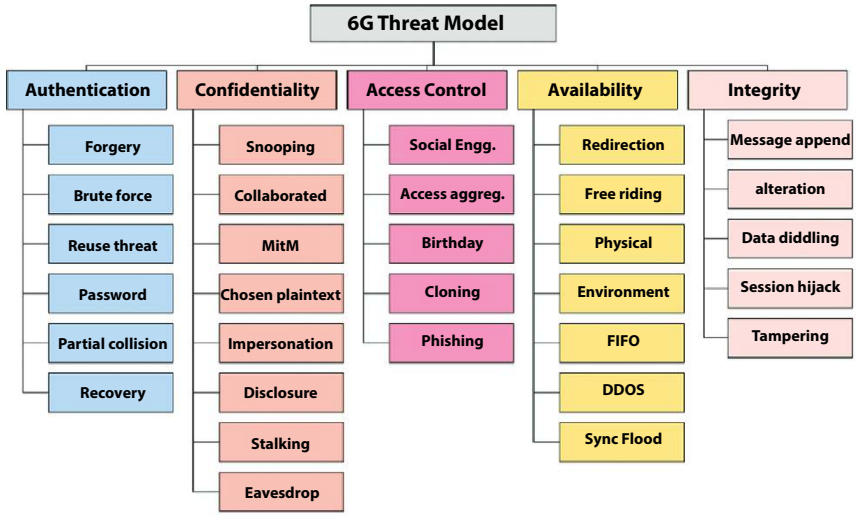

Figure 2.2 6G threat model [10].

In 6G networks, threat modeling assists identifying, presenting and mitigating security threats before they have an influence on the network's availability, confidentiality, and integrity. In Figure 2.3, real-time scenario of 6G threat model plays very crucial role to breach security of networks, and most frequent threats are as follows:

- **Eavesdropping:** Unauthorized user acquiring data communications is known as eavesdropping. It is a significant danger of interception due to the massive growth in data traffic and linked devices. Attackers may get confidential user or device data by intercepting conversations across the 6G networks mostly for mitigating this type of attacks by using end-to-end encryption with quantum-resistant protocols, frequency-hopping techniques, and deploying secure device authentication.
- **DDoS Attacks:** This attack causes excessive traffic levels to overwhelm network infrastructure, making it unavailable to authorized users. It can affect both the infrastructure and endpoints of a 6G network with billions of linked devices, impacting with crucial services. Some of the mitigation techniques like network segmentation, AI-based anomaly detection and traffic load balancing can help to secure network from DDoS attacks.

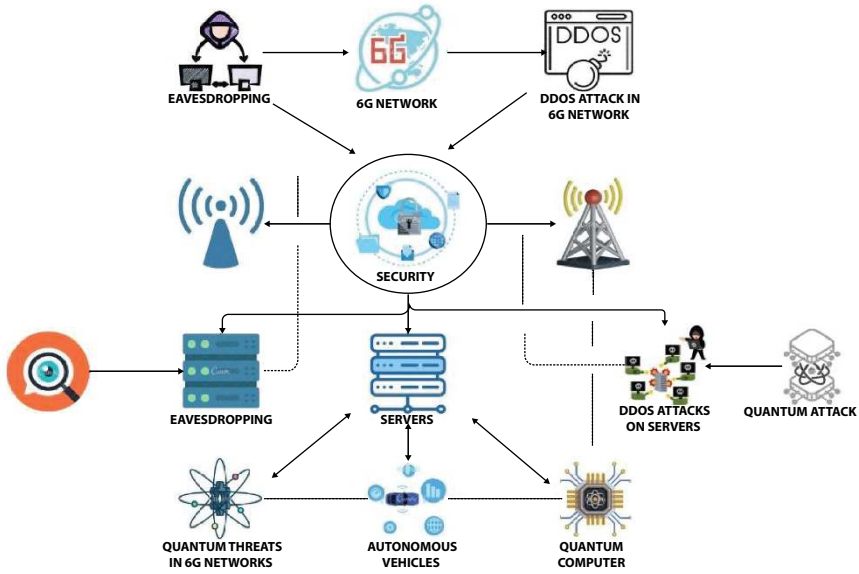

Figure 2.3 Scenario of 6G threat model.

- **Quantum Threats:** Sensitive information might be exposed if hackers used quantum attacks to decode data sent *via* 6G networks. Using quantum-resistant cryptography, regularly updating encryption protocols, and making quantum-safe standards will help to mitigate such attacks.
- **Man-in-the-Middle (MitM) Attacks:** An attacker can intercept, change, or inject data undetected by placing themselves between two communicating devices in a MitM attack. This kind of attack could comprise real-time applications in 6G, such as telemedicine or autonomous driving [17].

2.5.1 Threat-Countering Techniques in 6G Communication

The procedures for countering pressures to validation moreover and protection saving frameworks for 6G versatile organizations are the main topic of this section. Three categories exist for these countermeasures: intrusion detection, entity attributes, and cryptography. Additionally, our classification offers a comparative summary of the current defenses.

2.5.1.1 Cryptographic Methods

Both traditional and non-conventional methods of safeguarding new mobile communication scenarios require the use of cryptographic algorithms. Cryptography uses both symmetric and asymmetric principles. In 6G networks, base stations and access points are identified using a variety of techniques based on public key infrastructure. Such method is the Paillier cryptosystem, which combines key generation, encryption, and decryption; however, more research works are necessary to identify any flaws related to quantum computing. For 6G IoT networks, group signature schemes—in particular, short group Rivest-Shamir-Adleman (RSA)-based signatures—are being studied. However, quantum computing attacks pose a threat to the implementation of RSA in low-processing sensor communication. With Cybertwin architecture developing as a significant 6G feature, combining network assistance, behavior recording, caching, and security, symmetric key-based techniques are also essential [18].

2.5.1.2 Quantum-Resistant Cryptography

Traditional cryptography techniques might become outdated as quantum computing develops. Quantum-resistant or the creation of the objective of post-quantum cryptography is to create algorithms that are hardy to attacks from quantum computers. Quantum computers, as opposed to conventional

computers, employ quantum bits, or qubits, to do complicated computations at previously unheard-of rates, perhaps cracking popular encryption systems like RSA and ECC (Elliptic Curve Cryptography). To guarantee the security of next communication systems, researchers are currently investigating a number of quantum-resistant cryptographic techniques. Some of the likely approaches incorporate multivariate polynomial cryptography, hash-based cryptography, code-based cryptography, and web-based cryptography. This technique relies on precise puzzles that quantum computers remain believed to have difficulty solving. Lattice-based cryptography is the construction of cryptographic primitives depending on the hardness of lattice problems, including the knowledge with errors issue and the direct vector issue. Strong security guarantees efficient key-generating and encryption/decryption techniques abound in lattice-based systems. Digital signatures are produced in hash-based cryptographic systems *via* hash functions. Using cryptographic hash systems are collision-resistant, and they are regarded as safe against quantum assaults. So, it becomes more crucial for 6G networks because the use of quantum computers in the future may make traditional cryptography techniques obsolete, which would present serious security threats. Let us investigate its significance for 6G, weigh its benefits and drawbacks, and contrast it with more conventional cryptographic techniques. As you can see in Table 2.1, we identify how quantum-resistant cryptography differs from traditional cryptography.

Importance of Quantum-Resistant Cryptography for 6G
Critical infrastructure, autonomous systems, and extremely sensitive user data are among the immense amounts of connection and data that 6G networks are expected to manage. It is crucial because of the following reasons:

- **Protection Against Quantum Attacks:** 6G networks will carry sensitive and crucial information that must be protected against the risk posed by quantum computing.
- **Protection of Critical Infrastructure:** Smart energy grids, autonomous vehicles, and smart cities will depend on 6G network.
- **Long-Term Data Security:** It ensures that data remains secure even as quantum computing becomes more accessible.

2.5.1.3 Homomorphic Encryption

Preserving data privacy and security, homomorphic encryption lets calculations on encrypted data happen without decryption needed. In cloud

Table 2.1 Quantum-resistant cryptography vs. traditional cryptography.

Key aspects	Traditional cryptography	Quantum-resistant cryptography
Security basis	It is based on factoring and discrete algorithms.	It is based on lattice problems and hash functions.
Size	Moderate key size	Mostly larger key size
Quantum vulnerability	Vulnerable to quantum algorithms	Designed to be resistant to quantum attacks
Requirements of computation	Efficient on classical devices	Complex structure and higher computations
Advantages	• Security against classical attacks • Standardization • Interoperability • Scalable key sizes	• Resilience against quantum algorithms • Versatility • Longevity • Compatibility
Limitations	• Increasing key size reduces efficiency • Performance limitations with asymmetric encryption • Potentially vulnerable to advances in attack techniques	• Increased key size and processing requirements • Lack of standardization • Performance trade-offs • Implementation complexity

computing and data analytics, where private data has to stay under protection throughout processing, this is very helpful. The primary advantage of homomorphic encryption is that it can operate on ciphertexts, ensuring data secrecy even in situations of compromise. Integration of homomorphic encryption into 6G has the potential to improve security, foster user confidence, and assurance privacy, despite the fact that further research is mandatory to address its current computational issues.

2.5.1.4 Entity Attributes

In 6G communication, entity attribute-based countermeasures encompass together standard and non-conventional methods. Although context-aware security systems are the best for handling networks, they have issues with

interference and regressive compatibility. Although it has scalability issues, SDN technology delivers intelligent interference mitigation and DDoS detection. Also helpful for QR-based authentication techniques is the susceptibility to certain assaults such as QR phishing. Still, in its early stages, quantum communication, specifically, quantum key distribution, needs further study beyond simulations. While GPS spoofing and regulatory concerns exist, three-dimensional location-based resource management for unmanned aerial vehicle (UAV) networks and privacy in vehicular networks are crucial.

2.5.1.5 Biometric Authentication

Using special biological features such fingerprints, face recognition, iris scans, and speech patterns, biometric authentication checks identities. By utilizing difficult to copy or stealable elements, this approach improves security. Biometric authentication can assist applications including mobile payments, access control, and personalized services by offering flawless and safe access to services and devices in the framework of 6G networks.

2.5.1.6 Device Fingerprinting

Device fingerprinting uses hardware configurations, software versions, and network behaviors—unique traits to identify machines. This is a passive continuous kind of authentication as it is not depended on user involvement. Device fingerprinting in 6G networks guarantees that only identified devices access important resources and services, hence improving security. For security access control, anomaly detection, and fraud prevention, device fingerprinting is invaluable. Still, it also begs privacy issues and may be avoided by advanced attackers. Development of more robust fingerprinting methods and resolving privacy concerns by anonymizing and safe data management methods drives most of the research.

2.5.1.7 Intrusion Detection Systems (IDSs)

For 6G networks, researchers have proposed several threat detection strategies. Simplified threat matrices facilitate effective detection, but they need maintenance agreements to prevent incompatibilities. The Non-Orthogonal Multiple Access (NOMA) sparse signature matrix serves as a detection system, although it is only compatible with wireless networks and might not work with non-NOMA IoT devices. Although a better Low-Energy Adaptive Clustering Hierarchy (LEACH) technique improves flooding attack detection, it still requires more attack coverage. While authentication based on CSI

can help identify intrusions, it has compatibility and performance problems. Secure intrusion detection and mitigations are using AI and ML methods more, and deep learning is showing promise for intelligent threat detection. 6G networks with cognitive radio support provide automatic security measures, although evaluating secrecy performance presents difficulties. In 6G, safe ecosystems and dependable service delegation are made possible by SDN-enabled blockchain resource allocation and secure data aggregation. IDS implementation is optimized by virtual representations, such as digital twins. To guarantee efficacy and compatibility in a variety of network contexts, more investigation is needed.

2.6 Authentication Techniques in 6G Communication

2.6.1 Handover Authentication

As shown in Figure 2.4, cellular data traffic has increased due to the proliferation of mobile devices and network innovations, underscoring the importance of safe and smooth mobility during handovers. Handover authentication protocols are difficult to design because of their low computing power and open wireless networks. In next-generation networks, such as terrestrial satellites, handover authentication is essential for security and mobility. Multi-domain scenarios provide issues for handover authentication in 6G networks. While a suggested architecture lowers overheads and delays, it ignores inter-layer management and higher-layer constellations. For safe delivery, blockchain and lightweight cryptography are taken into consideration, with mobile edge computing cutting latency. The diverse environment of 6G, including cars,

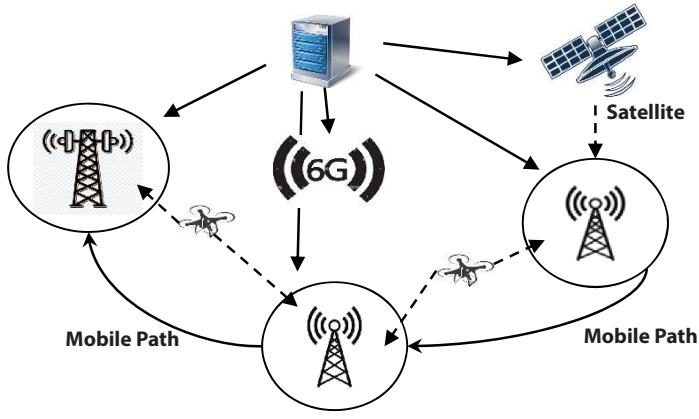

Figure 2.4 Handover authentication.

drones, and UAVs, makes handover management more difficult. Poor propagation, fading, and shadowing are difficulties, particularly when using millimetre waves. It is suggested to use a multi-connectivity architecture to increase coverage and changeover efficiency [19].

2.6.2 Mutual Authentication

In resource-constrained IoT devices, mutual authentication and key agreement depend heavily on lightweight cryptographic methods. It was suggested to use an arbitrary HMAC and ECC-based Device-to-Device (D2D) mutual authentication technique, which offers far less complexity and latency while thwarting many assaults. Similarly, a reciprocal authentication approach based on MAC addresses and fingerprints was suggested, demonstrating enhanced validation of trust. Mutual authentication is also used by Maritime Transport Systems to safeguard vessel location data. Although Secure Hash Algorithm 1(SHA-1) offers a multi-server design that lowers latency, it still leaves open the possibility of dictionary and brute force assaults. Batch authentication meets the demands of mutual authentication and anonymity in 6G-enabled vehicle networks. Bilinear pairing was proposed as a safe and anonymous mutual authentication technique, although it poses data privacy problems owing to possible trust authority breaches.

2.6.3 Physical Layer

The physical communication layer is usually not the first layer at which authentication measures are applied. On the other hand, it has become more popular because of its low bandwidth dependence and resistance to interference. Waveforms are subjected to a covert modulation using this technique. Improved authentication and interference resistance in time-varying circumstances have been suggested *via* spread spectrum-based secret modulation and adaptive machine learning algorithms. By taking use of channel features and randomization in wireless connection parameters, physical layer security techniques—like Multiple Input Multiple Output (MIMO) technology—offer lower complexity and lower latency.

2.6.4 Deniable Authentication

Particularly in wireless networks, pre-sharing system limitations prior to security verification in communication exposes susceptible device features and may result in security issues. By skipping the "Encryption-then-MAC" paradigm, deniable authentication (DA) protocols enable the sender to

refuse the validation procedure to any third party. Entities are prohibited from beginning MAC-based authentication *via* these protocols. For Wi-Fi authentication, a source-hiding system with hash functions that project has been proposed that rejects third-party links and therefore ensures security. MANETs, or mobile *ad hoc* networks, are fundamental to contemporary communication. Network heterogeneity is addressed using an identity-based DA protocol for MANETs, validated using a random oracle model. There is not much research that specifically covers DA deployment, problems, and solutions in 6G networks.

2.6.5 Token-Based Authentication

With token-based authentication over 6G network, each user or device receives a digital "token" from a reliable source after establishing its identity. This token provides safe access to additional network resources by functioning as a temporary pass. The primary advantage is that devices save time and improve security by not having to transmit usernames and passwords repeatedly. For example, smart factory using a 6G network for token-based authentication where each robot and machinery has a unique function led to secure and smooth every work that benefit to speedup manufacturing process along with safety and scalability.

2.6.6 Authentication Using Certificates

Authentication using certificate systems, which are widespread in contemporary applications and smart infrastructures, combine a number of cryptographic algorithms and handshaking protocols. A suggested certificate authentication technique based on lightweight cryptography provides untraced ability and anonymity while fending against assaults like replay, DoS, MitM, and impersonation. Certificate-based authentication has been deemed unsuitable for next-generation networks, but, with enhancements like as handshake delegation, pre-validation, and session resumption, it is now more feasible for IoTs with limited resources. Certificate-based authentication, in contrast to attribute-based methods like biometrics or OTPs, concentrates on MitM attacks in wireless network communication. It offers solutions with distinct credentials based on public keys.

2.6.7 Key Agreement–Based Validation

The foundation of most authentication techniques is key agreement, which is necessary for privacy-protected authentication between users, sensors,

and gateways. It boosts several security mechanisms that rely on cryptographic algorithms. Key agreement procedures, on the other hand, could be squeezed by vulnerabilities like procedure signature, replay, key reuse, and deniability moderating, important conciliation, server belief concerns, and identity handling. A significant trial exists in establishing a secret key contract across unauthenticated public channels where outbreaks can rapidly multiply. For instance, misusing biometric credentials might result in serious privacy abuse, and the healthcare system finds it difficult to safeguard session keys between medical servers and patients.

2.6.8 Multi-Factor Authentication

It ensures that only authorized users or devices can access specific network resources. Strong security is essential for 6G networks because they are faster, link more devices, and handle large amounts of sensitive data. It makes security better by widening the range of keys and protecting them from brute force attacks and occupied third-party parameters. Extra components utilized by MFA incorporate programming tokens, shrewd adaptable applications, outsider declarations, SMS- and email-based one-time passwords, USB-based tokens, brilliant cards, PINs, RFID, actual keys, and area-based methods. In particular, technological advancements have enabled the expansion of biometric credentials for MFA to include DNA specifications, iris or retinal scans, voice validation, hand math, face acknowledgment, and ear cartilage calculation. Cross-confirmation selections for MFA can be followed down in various organizations. The absolute most common assaults against MFA incorporate opposite animal power, phishing, stick phishing, certification stuffing, MitM, and key lumberjacks. MFA is turning out to be progressively suggested for circumstances including tremendous, dissimilar, and 6G-empowered correspondence. Blockchain-based verification for heterogeneous gadgets gives joint confirmation and access control, in spite of issues with versatility, key administration, and agreement above. Structured security rules that adhere to the CIA trinity are provided by next-generation cloud computing architectures through the use of MFA. AI approaches are increasingly being used for event-based authentication in MFA across dispersed edge and cloud nodes with less reliance on humans. MFA in 6G will make our connected world more secure, helping to protect everything from personal devices to smart systems [20].

2.7 Future Directions

Following a thorough review of the existing state of research in the field of protected 6G networks, we judgmentally identified prospective directions for the upcoming 6G communication examination that will demand attention from both academia and industry.

2.7.1 Improving AI Security in 6G and Developing Quantum-Safe Protocols

In 6G networks, AI is progressively vital for activities like security monitoring and network optimization. Subsidiary calculations against ill-disposed assaults and guaranteeing safe model training are fundamental parts of the further development of man-made intelligence security. Strategies like unified learning can be explored to safeguard security. Also, homomorphic encryption can be used to manipulate encoded data without revealing crucial information. Focusing on quantum-safe cryptographic protocols as quantum computing continues to evolve, which implement post-quantum cryptography algorithms like lattice-based and hash-based encryption methods, these are considered resilient against quantum decryption capabilities.

2.7.2 Advancing Federated Learning for Privacy-Preserving Security

FL is vital for cooperative model training in decentralized settings while preservation data privacy. Upgrading protection techniques, for example, differential security and safe total ought to be the focal point of future examination. In 6G networks, FL must be altered to accommodate various devices and dynamic learning environments to develop adaptive FL frameworks. Incorporating secure aggregation protocols to further reinforce privacy by applying model updates are aggregated in a way that prevents the disclosure of personal device information. AI governance framework that monitors and controls model behavior across the network can help maintain compliance.

2.8 Conclusion

The significant developments and difficulties in the field of 6G network security have been brought to light by this review. We examined many authentication methods, highlighting their advantages and disadvantages for next-generation networks, such as token-based, certificate-based, and physical layer security. It has been determined that DA protocols, mutual authentication systems, and lightweight cryptographic solutions are necessary for safe communication in IoT devices with limited resources. Additionally, integrating blockchain technology with AI has the potential to improve security, but it also brings new difficulties that must be resolved. Compact security systems will be predictable for the execution of 6G organizations to oblige its extremely exclusive and different climate. Future quantum threats should be addressed by creating quantum-safe protocols. While federated learning advances are crucial for maintaining security in decentralized networks. To deal with the huge number of connected gadgets, new verification strategies should be made, and interruption discovery frameworks should be enhanced to deal with the developing intricacy of cyberattacks. Through these drives, 6G organizations will actually need to offer quick, trustworthy, and secure network for different purposes, including driverless vehicles and shrewd urban communities.

References

1. Kulkarni, A., Goudar, R. H., Rathod, V., G. M, D., & Hukkeri, G. S., New directions for adapting intelligent communication and standardization towards 6G. *EAI Endorsed Trans. Scalable Inf. Syst.,* 12, 1, 2024, https://doi.org/10.4108/eetsis.5126.
2. Abdel Hakeem, S.A., Hussein, H.H., Kim, H., Security requirements and challenges of 6G technologies and applications. *Sensors*, 22, 5, 1969, 2022.
3. Sun, Y., Liu, J., Wang, J., Cao, Y., Kato, N., When Machine Learning Meets Privacy in 6G: A Survey. *IEEE Commun. Surv. Tutor.*, 22, 4, 2694–2724, 2020, Article 9146540. https://doi.org/10.1109/COMST.2020.3011561.
4. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P. K., Singh, M. Edge Computing-Based Design for IoT Security, in: *Network Optimization in Intelligent Internet of Things Application,* pp. 298–309, Chapman and Hall/CRC, 2024.
5. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., IoT and blockchain technology in 5G smart healthcare, pp. 137–161, Elsevier eBooks, 2022a, https://doi.org/10.1016/b978-0-323-90615-9.00004-9.

6. Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., *AI and 6G Security: Opportunities and Challenges*, pp. 616–621, 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.
7. Shafie, A., Yang, N., Han, C., Jornet, J. M., Juntti, M., Kürner, T., Terahertz communications for 6G and beyond wireless networks: Challenges, key advancements, and opportunities. *IEEE Netw.*, 37, 3, 162–169, 2022.
8. Han, C., Wu, Y., Member, S., Chen, Z., Terahertz Communications (TeraCom): Challenges and Impact on 6G Wireless Systems, *arXiv preprint arXiv:1912.06040*, pp. 1–8, 2020.
9. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P. K., Advancements in Renewable Energy Harvesting for EV Charging Infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles,* pp. 119–152, IGI Global Scientific Publishing, 2025.
10. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in Computer and Information Science*, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
11. Zohaib, M., *Integrating antum Computing and Blockchain: Building the Foundations of Secure, Efficient 6G Technology*, pp. 27–34, doi: 10.1145/3663531.3664755.
12. Liu, Y., Yuan, X., Xiong, Z., Kang, J., Wang, X., Niyato, D., Federated Learning for 6G Communications: Challenges, Methods, and Future Directions. 105–118, 2020, doi: 10.23919/JCC.2020.09.009.
13. Singh, M., Sukhija, N., Sharma, A., Gupta, M., Aggarwal, P., Security and privacy requirements for IOMT-Based Smart Healthcare System, pp. 17–37, CRC Press eBooks, 2021, https://doi.org/10.1201/9781003032328-2.
14. Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., Ylianttila, M., The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.*, 2, 1094–1122, 2021.
15. Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., Ibrahim, A. A. A., Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. *Symmetry*, 15, 6, 1147, 2023.
16. Saxena, P., Jain, P., Aggarwal, P., Singh, M., Goel, S., Batra, M., Communication requirements and performance metrics for electric vehicle charging: A comprehensive review, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 15–30, IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch002.
17. Mishra, S., Shukla, A., Arora, S., Kathuria, H., Singh, M., Controlling Weather Dependent Tasks Using Random Forest Algorithm. *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bengaluru, India, pp. 1–8, 2020, doi: 10.1109/ICAECC50550.2020.9339508.

18. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-Based wireless sensor network, pp. 121–141, CRC Press eBooks, 2024, https://doi.org/10.1201/9781003432869-8.
19. Saad, W., Bennis, M., Chen, M., A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.*, 34, 3, 134–142, 2019.
20. De Alwis, C., Kalla, A., Pham, Q. V., Kumar, P., Dev, K., Hwang, W. J., Liyanage, M., Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. *IEEE Open J. Commun. Soc.*, 2, 836–886, 2021.
21. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., Quantum Cryptography. *Rev. Mod. Phys.*, 74, 1, 145–195, 2002. https://doi.org/10.1103/RevModPhys.74.145.

3

Strategies for Ensuring Security and Privacy in 6G Networks

Azamat Ali[1]* and Mikhai Tyurkin[2]

[1]School of Liberal and Creative Arts (Journalism and Mass Communication), Lovely Professional University, Punjab, India
[2]School of Arts and Humanities, Department of Media, HSE University, St. Petersburg, Russia

Abstract

The emergence of 6G communication technology brings revolutionary improvements in connectivity and data exchange. However, it introduces significant security and privacy challenges. This chapter explores critical issues related to preserving security and privacy in 6G networks and discusses potential solutions to address these challenges. As 6G networks support an unprecedented number of connected devices and applications, robust protection against threats becomes essential. Additionally, safeguarding user data is paramount. The chapter highlights key challenges, including securing massive volumes of data, protecting against sophisticated cyber threats, and managing privacy in an increasingly interconnected environment. It reviews newer technologies and approaches for enhancing security, such as innovative encryption techniques, novel trust models, and privacy-enhancing technologies. The chapter also examines how regulatory and standards frameworks influence the design and operation of secure and privacy-resilient 6G systems. Through case studies and analysis of current research, it provides practical insights into effective strategies for mitigating risks and ensuring compliance. By addressing these critical issues, the chapter offers actionable recommendations for stakeholders, including network operators, policymakers, and technology developers. Its ultimate goal is to enable the development of secure and privacy-preserving 6G networks that meet the evolving demands of future communication landscapes.

**Corresponding author*: azamatcug@gmail.com; ORCID: https://orcid.org/0000-0003-2931-2166
Mikhai Tyurkin: ORCID: https://orcid.org/0009-0006-3926-0581

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (57–80) © 2026 Scrivener Publishing LLC

***Keywords*:** 6G networks, security challenges, privacy preservation, encryption techniques, regulatory frameworks

3.1 Introduction

The sixth generation of the communication technology, referred to as 6G, is going to revolutionise how humans interact with digital and physical environments. So, 61G takes the benefits of what 5G has offered. As of now, still in its early days of development 6G will surely provide much greater data rates than 5G. It would also ensure ultra-low latency and will connect hundreds or thousands of devices such as [1]. The pundits foresee the 6G to work within the terahertz spectrum. This implies that the speed at which data would be transferred is several times greater than in 5G. The peak may go as high as 1 terabit per second. Besides the remarkable improvement in speed, 6G will also enable a range of support for increasingly complex and dynamic applications compared to its predecessors. For instance, this could include completely autonomous systems, holographic communications, and immersive virtual reality [2].

If anything, the difference in scope and capability is perhaps one of the greatest distinctions between 5G and 6G. While 5G essentially upgraded mobile broadband, 6G will take connectivity to the extreme by integrating artificial intelligence (AI) and machine learning (ML) into its core [3]. This will allow for more intelligent and adaptive network management. Systems would, therefore, predict and react to new conditions in real time. Also, 6G will be energy efficient. It will allow for the friendly green communications system to emerge. This will be through the harvesting of energy and IoT zero-energy devices [4]. The applications of 6G are revolutionary. New improvements in the sectors of health, transportation, and entertainment will benefit industries. In healthcare, 6G would facilitate remote surgeries with ultra-low latency and high precision. In transport, autonomous vehicles would rely on real-time, high-speed data exchange between vehicles and infrastructures [5]. Beyond this, the 6G is most likely to fuel the evolution of smart cities. In such cities, the interrelated devices and sensors would immediately communicate each other, optimizing energy consumption, strengthening public safety, and streamlining urban mobility. Taken as a whole, the move from 5G to 6G is completely one gigantic leap in communication technology. A huge deal of promise bears out to reshape industries and daily life.

With the emergence of 6G networks, security and privacy are more required. Sufficient secure data management is also needed for huge amounts of data generated from 6G networks to prevent cyber threats.

The enhanced data traffic, along with the hyper-connectivity nature of 6G, leaves an expansive attack surface that can expose networks to a high cyberattacks risk level [6]. Moreover, integrating AI and ML into network management will introduce new vulnerabilities. The attackers will use the weaknesses of AI algorithms to break network integrity [7]. Thus, there is a need to strengthen security frameworks to prevent data breaches and other malicious activities in 6G. This is also one of the significant issues of 6G: huge volumes of data to be transmitted and stored are challenging in terms of security management. Data breaches, unauthorized accesses, as well as corruption of data are on the risk with devices as well as sensors collecting as well as transmitting real-time data. Furthermore, the high velocity of data transmissions and a large number of devices connected, much more so with Internet of Things (IoT), make it challenging to monitor and ensure the security of these data flows [8]. Advanced encryption and security mechanisms will also be required with the application of 6G edge computing. This is because, in edge computing, data processing is decentralized and done closer to the source. In this scenario, sensitive information needs to be shielded from possible threats. For instance, privacy will be a major challenge in the 6G network [3].

Privacy in such a network as 6G will be difficult to protect because, with this technology, comprehensive monitoring and tracking of user activities will be possible. Some of the primary technologies of 6G applications include AI, augmented reality (AR), and virtual reality (VR). These technologies would work correctly by accessing enormous volumes of personal data. Related data collection, storage, and usage risks will be higher [9]. Protecting user privacy is necessary for the trust of users in 6G technologies. Users should feel that data is treated appropriately so that it reflects the privacy of its owners as well as follows the laws regarding it. Issues of security and privacy related to 6G will have an incredibly strong-reaching effect on every user, business entity, and government in the world. The factors above are likely to affect individual users, businesses, and governments according to how strong the security and privacy will be. Individual users will experience personal data theft, financial loss, or identity fraud resulting from a breach of security or privacy. Compromised security may also result in the loss of sensitive information and intangible theft of intellectual property that would hurt business reputations. In regard to national security, governments may experience threats in the sensitive sectors like energy, healthcare, or defense. Most importantly, considering the advancement in 6G, there is a need for collaboration among the stakeholders involved with each other. They must engage in developing and implementing integrated security and privacy measures to effectively deal with these challenges.

3.2 Security Challenges in 6G Networks

3.2.1 The Expanding Threat Landscape

As 6G networks evolve, they expand the threat landscape from the proliferation of connected devices. IoT, autonomous systems, and other smart devices are likely to mushroom exponentially with 6G deployments. This will exponentially increase the possible means through which hackers could get into the system [2]. This massive connectivity will involve billions of devices-from personal gadgets to smart infrastructure and industrial systems. It will be impossible to protect all endpoints. The difficulty in security management over this broad range of devices will pose its biggest challenge. Many of these devices will have limited computing powers and storage [6]. Due to this, the adversaries will even exploit vulnerabilities in less secure devices to launch attacks on the broader network.

AI-powered cyberattacks shall, in all likelihood, be one of the most evolved threats in the era of 6G. Because AI forms the core in 6G, both in its management of networks as well as in its cyber defense, the attacker too is likely to utilize AI. It will enable them to automate and perfect their attacks. For instance, AI-based malware shall be able to learn its environment and adapt behaviour in such a manner that avoids detection systems [7]. In this regard, quantum computing is a huge threat to any sort of traditional cryptographic methods. Quantum algorithms will break encrypted schemes that are in use at present to secure the networked communication. This means that important information may become susceptible to intercepts [9]. Therefore, the 6G technology will require new methods of encryption that are not susceptible to attacks from a quantum-powered computer.

3.2.2 Securing Massive Data Volumes

The capability of the 6G network to transfer massive amounts of data at unprecedented speed raises crucial issues related to the security of the data. Increasingly, with lots of devices generating numerous data in real time, it makes things tougher for integrity, confidentiality, and availability. Data integrity is ascertained such that it ensures no alteration and corruption have been carried out on the information. Data confidentiality ensures that sensitive information has not leaked to unauthorized parties. Availability ensures that data becomes accessible at the time of need [10]. However, these goals are hard to be achieved without new solutions in security, especially due to an immense volume of data to be managed by 6G networks. The nature that 6G communication environments will entail also worsens data security due to high speed involved

in transmission. A more limited time frame exists for being able to detect and mitigate attacks when data is transmitted at faster speed. This increases the possibility of data breaches and loss [8]. The attackers can avail themselves of this environment by intercepting data in transit for unauthorized access to sensitive information. Moreover, there are more exposed areas in applying edge computing. In the case of edge computing, computation is not concentrated on one site but rather distributed to a place significantly closer to the sources of the data. Because edge devices are not as strong as central data centers, it has been an entry point wherein attackers may compromise the data being processed [3].

3.2.3 Challenges in Network Infrastructure

Networks in 6G are expected to rely hugely on very advanced network infrastructure technologies such as virtualization and software-defined networking. The technologies are very effective, very flexible, and scalable but introduce new security challenges: virtualization means multiple virtual networks could run on the same piece of physical infrastructure. It seems to raise concerns that may make isolation between networks an issue. Vulnerability exists in one virtual network to potentially breach others using the same physical infrastructure [7]. The software defined networking (SDN) splits the control plane from the data plane, and the main attacks target the centralized controllers. In case the attacker gains control over the SDN controller, they will find it possible to manipulate the network traffic. There is a possible disruption of services in the entire network as a result of the breaches [6]. Among many important features of 6G, network slicing builds multiple virtual networks over the same physical infrastructure. Different slices are custom-created with regard to some specific use cases [5].

Network slicing can provide efficient resource allocation and performance enhancement but introduces new attack vectors. Malicious actors can leverage the weaknesses in the architecture of network slicing. This can facilitate unauthorized access to pieces that might compromise sensitive data and critical services. Another basic element of the 6G infrastructure is edge computing, which is equally exposed. Although the edge computing approach minimizes latency and increases performance by processing data nearer to the user, it extends the attack surface as data is diffused across many edge devices [8].

3.2.4 Securing AI-Driven Systems

AI in 6G networks will provide a better management of the networks relative to automation, efficiency, and adaptability. However, it increases critical security issues. Thus, AI-driven systems are supposed to significantly

contribute to the optimal performance of networks with respect to threat detection and resource management, but security is a big concern. They are vulnerable to adversarial attacks and manipulations [7]. Adversarial attacks would comprise providing AI systems with incorrect or malicious inputs. This would cause the AI system to produce bad judgments or even classify items wrongly. A different scenario might see attackers manipulate the data being used by AI systems in an effort to try and identify threats. This means that there might be false positives or negatives that compromise network security [9]. Further, the ML models propelling AI in 6G networks are not impenetrable. The attackers can target such models using techniques like model inversion. The technique could potentially allow for an inference of the sensitive information from the model itself [6]. In model poisoning attacks, malicious data is injected into the dataset used to train the model. This could potentially degrade the AI model performance and improper network management decisions [7]. That is, such systems integrated within the very fabric of 6G will need to be secured against such attacks. After all, a network cannot afford to compromise on integrity and reliability.

3.3 Privacy Preservation in 6G Networks

3.3.1 Privacy Challenges in Hyper-Connected Ecosystems

Hyper-connected ecosystems are sure to go extremely well with 6G networks. This would exponentially generate and collect data. The hyper-connected landscape does pose great privacy issues. It means millions of devices, platforms, and tools will collect, track, and store sensitive and personal data. The rampant use of IoT devices, wearable technologies, and smart systems makes it easier for user profiles. The Information and Communication Technology in use can track behaviour, preferences, and activities [6]. User privacy is similarly threatened in the same environment. Data collection practice has no transparency at many times. It becomes hard for individuals to know how their data is used, shared, or monetized. One significant privacy issue in these hyper-connected spaces is the inability to obtain adequate informed user consent. Traditional consensus mechanisms for acquiring consent, for example, through opt-in agreements, are not suitable for the 6G context. Data harvesting is ubiquitous, and users might not have an idea of the magnitudes at which their data is being harvested [11].

The pervasive nature of 6G networks along with the complexity of data flow makes the management of user consent and control very cumbersome. In many scenarios, it will be impossible to manage user control over the

information flow; thus, it results in the loss of autonomy over personal information. In this respect, there is an increased need for mechanisms that are more sophisticated and allow users to regain control over their information. This is putting the requirements where there must be a mechanism whereby users can opt out of certain data collection processes without losing access to basic services. A further consideration needs to include the likelihood of data misuse and exploitation within the hyper-connected space. In networks for 6G, real-time exchange of data shall be possible from multiple devices on multiple platforms. Because of this, the chances of unauthorized access, breaches, and even profiling increase. Because attackers usually search for vulnerabilities in such systems to acquire unauthorized access to such sensitive information, privacy breach would be a concern alongside with the potential harm it may inflict on its users [3]. Moreover, even the vague regulations and standards used toward data privacy in 6G networks further complicate user privacy protection efforts. The different understandings of privacy by various stakeholders may also prevent the practice of protecting users' privacy.

3.3.2 Privacy in Massive IoT and Sensor Networks

6G networks will undoubtedly be large IoT devices and sensor networks. These technologies are part of how data is collected and processed in real time. They enjoy many benefits in terms of automation and efficiency but with a lot of risks on the side of privacy because of the volumes of data to generate. In fact, data leakage is a huge concern in IoT environments. Sensors may obtain some personal information that will be intercepted by malicious actors or misused for their gains. Examples can be smart home devices, health monitors, and wearable technologies. Its use can help infer lots of sensitive information about the individual, like daily routines, health status, or locations [8].

Re-identification is another critical danger in large IoT and sensor networks. Even when data is anonymized or pseudonymized, it can be still possible to identify individuals by adversaries. This is possible through correlations of multiple datasets [12]. This is especially dangerous in those environments where data from different sources are merged in order to be analyzed, such as smart cities or healthcare applications. The resultant power to track and re-identify individuals based on their data raises serious concerns for privacy as it might lead toward unwanted surveillance and profiling. Real-time data processing and privacy are great challenges for 6G networks, especially for IoT devices. Many IoT applications, like autonomous vehicles, industrial automation, and smart grids, strictly require real-time data processing for their proper operation.

In principle, it becomes difficult to maintain privacy with guaranteed speed efficiency of the systems. Most of the IoT devices may not possess the computational resources for accommodating conventional encryption techniques. Complex privacy-preserving techniques may become performance bottlenecks for the system [6]. So, new innovations in protecting privacy of IoT networks are required in high demand. The lightweight encryption techniques and decentralized architectures for privacy preserving fall in this category.

3.3.3 Managing Privacy in AI-Powered Applications

AI-based applications feature to be significantly informed by 6G networks. They will power services including smart cities, personalized healthcare, and predictive analytics. However, with the integration of AI, come some huge issues of privacy. These systems are dependent on big data in propounding their predictions and decisions. In healthcare, personalized services, and other sectors, AI models use some sensitive personal information. It gives personalized recommendations but raises problems of privacy if handled inappropriately [13]. For example, confidential medical information can be leaked due to data breaches or inappropriate use of algorithms applied in AI. Users may also be against their personal preferences being publicized. AI-based services are vulnerable to risks in terms of privacy because of the increasing call for access to large volumes of data. Such data often originates from several sources. The more data rich an AI model is, the greater performance it is able to provide. However, this process involves a higher possibility of privacy violation. For instance, a smart city environment reads data from surveillance cameras, sensors, and user devices to optimize traffic flow, energy consumption, and security measures through AI systems. However, this much collection of data may involve unwanted surveillance. But users will not know that their activity is being tracked and monitored [9]. To mitigate the risks, therefore, privacy-preserving AI techniques must be designed and implemented in 6G networks.

Federated learning is one such solution that has been employed to take care of the increased concerns of privacy in AI-based applications. Traditional ML models depend on centralized data, but AI models called federated learning are trained on decentralized data sources. This is a method that keeps the data to local devices, meaning there is less of an exposure risk [12]. It ensures that delicate information about the user never gets to the server. The updates on the model alone are shared with the central server. Federated learning can, therefore, benefit sectors most by healthcare, where patient data is very sensitive. Privacy must be the number one thing to consider. It must be implemented, like federated learning, with other privacy-enhancing techniques in 6G networks that will strike a balance between data-driven insights and protecting user privacy.

3.4 Emerging Technologies for Enhancing Security and Privacy in 6G

3.4.1 Next-Generation Encryption Techniques

With the development of 6G communication technology, new challenges and problems for security arise. 6G promises ultra-low latency, high-speed data transmission rates, as well as very high rise in number of connected devices. In this highly interconnected world, classical techniques of encryption may not suffice. Therefore, next-generation encryption methods are critical to ensure secure communication in 6G networks. Quantum-resistant cryptography is another promising development. Quantum-resistant cryptography is designed to stand against attacks from a quantum computer. Quantum computers are based on the principles of quantum mechanics. Quantum computers can also solve certain problems at least speedier than classical computers. This is a big threat for the currently used encryption algorithms. Algorithms, which rely on factoring large numbers or solving discrete logarithms, are vulnerable to this attack. For example, Shor's algorithm, a quantum algorithm, can break such encryption techniques [8]. This is the reason why quantum-resistant cryptographic algorithms are being developed.

Lattice-based cryptography, hash-based cryptography, among others, are what are being highlighted. These are believed to be quantum attack-resistant as well as not susceptible to classical attacks. This will ensure long-term security when maturity of quantum computing becomes a reality. The other important area of next-generation encryption is lightweight encryption. It is highly critical for IoT devices and other resource-constrained devices that will proliferate in 6G networks. One limitation of the above-mentioned devices is their device capacity. They often come with limited processing power and memory. Moreover, many have a limited battery life. This will essentially make traditional encryption methods inefficient or even impractical. Lightweight cryptography uses minimal computational resources and still ensures security. It is of essence for constrained-capacity devices. PRESENT, LED, and SIMON are some of the lightweight cryptography algorithms. They are less demanding in terms of energy and memory but strong enough to provide security. Lightweight cryptography algorithms support secure communication in IoT ecosystems without draining device resources [14]. With an increase in IoT dependency by 6G networks, essential data integrity and confidentiality will depend much on lightweight encryption techniques.

3.4.2 Decentralized Trust Models

Centralized trust models, as the scale and complexity of 6G networks begin to rise, may likely become a bottleneck in security. In contrast, there is steadily growing interest in decentralized trust models. Blockchain and Distributed Ledger Technologies (DLTs) are being examined. Of these, blockchain-based security solutions appear promising for managing trust and ensuring secure transactions in 6G networks. Blockchain is a decentralized, tamperproof ledger in which network participants can hold secure, clear-cut, and transparent transactions without a central authority. This occurs *via* consensus mechanisms. The consensus mechanisms validate and verify transactions across the network [15].

In 6G, blockchain would allow for secure data exchange. It would also mean proper control of access and that network infrastructure integrity had been properly safeguarded. For example, blockchain can facilitate safe communication between IoT devices. Here, the above-sensitive information will be accessed only by authorized devices. Moreover, blockchain is natively tamper-proof, which means it provides immunity to attacks that modify data or even destroy it. DLTs also introduce new opportunities for authentication and trust management within 6G networks. The DLT works similarly to blockchain but differs in consensus and even in storage.

DLTs will be helpful in decentralizing identity management in 6G environments. This means that the users will have sovereignty of personal data without having to necessarily rely on a central authority for trust. This strategy is helpful for privacy preservation. The users will be able to disclose selectively based on need without trusting a single entity with their data [7]. Thirdly, DLTs enhance the security of network infrastructures. DLTs provide a decentralized and secure mechanism for the verification of device identities, the management of network resources, and the reduction of threats associated with centralized server's attacks.

3.4.3 Privacy-Enhancing Technologies (PETs)

Another key aspect of safeguarding user privacy in 6G networks is the privacy-enhancing technologies (PETs) apart from encryption and decentralized trust models. PETs would enable data processing that does not cause harm to privacy and, hence, is an absolute requirement in high-volume data collection and analysis scenarios. One of the potential PETs is homomorphic encryption. Homomorphic encryption allows computation on any ciphertext and produces an encrypted result without revealing

what it originally hides. Such a characteristic is particularly well-suited in untrusted environments, like cloud computing.

Homomorphic encryption ensures the execution of all computations on sensitive data without deducing its secrecy. This is also the case when the environment is compromised [16]. It is envisioned at the 6G era to generate and process huge amounts of data in real time. Hence, the homomorphic encryption helps in preserving user privacy and enables big-data-driven services such as AI-based predictions and personalized recommendations. Another PET that is of utmost importance is secure multi-party computation. Secure multiparty computation (SMPC) refers to the development of technology that allows several parties to perform a collective function computation on inputs held private by each party. It would be particularly relevant in collaborative environments, like smart cities or healthcare systems. It involves bringing data from multiple sources for the purpose of analysis and, at the same time, protecting individual privacy. SMPC ensures that sensitive information remains confidential while being calculated and thus minimizing the leakage of data [6].

Another key PET in protecting user privacy in 6G networks includes differential privacy. Differential privacy determines whether the output of a computation does not say too much about an individual's data, even if a number of queries are made. Adding controlled noise to the data makes differential privacy achievable. This will prevent one from easily identifying specific individuals [17]. In the realm of 6G, differential privacy can be applied for the analysis of large-scale data. It supports the idea that insight can be extracted from the data without compromising individual privacy. This is especially beneficial in AI-driven applications, such as personalized healthcare or managing a smart city, where sensitive information needs to be made available for effective decision-making.

3.5 Regulatory Frameworks and Standards for 6G Security and Privacy

3.5.1 Overview of Existing Regulations

Therefore, security and privacy-related regulations must evolve with new challenges of the 6G generation. Table 3.1 highlights the current regulatory frameworks' relevance and limitations concerning the security and privacy challenges in 6G networks.

Table 3.1 Comparison of existing security and privacy regulations (GDPR and HIPAA) in the context of 6G networks.

Regulation	Key aspects	Relevance to 6G networks	Limitations in 6G context
General Data Protection Regulation (GDPR) (EU)	- Ensures personal data protection and user consent - Enforces data minimization, accuracy, and accountability - Requires transparency in data handling	- Provides a foundational framework for data security in 6G - Emphasizes user control over data, relevant for hyper-connected networks	- May not fully address AI-driven real-time data processing - Struggles with cross-border regulatory challenges in global 6G networks - Limited provisions for large-scale IoT and autonomous systems
Health Insurance Portability and Accountability Act (HIPAA) (U.S.)	- Protects confidential health information - Ensures healthcare organizations handle patient data securely - Imposes penalties for data breaches	- Important for healthcare applications in 6G, such as telemedicine and remote monitoring - Supports encryption and security protocols	- Not designed for massive real-time data transmission in 6G - Limited scope in handling AI-based predictive healthcare analytics
6G-specific regulatory needs	- Addresses ubiquitous data collection and hyper-connectivity - Focuses on mass IoT de-anonymization concerns - Introduces cross-border compliance mechanisms	- Ensures compliance with new security threats - Accounts for AI-driven data processing and automation	- Requires new legal frameworks that evolve with emerging technologies - Must balance innovation with privacy protection

Thus, the current data privacy and security guidelines as established by the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) will be very useful for incoming regulations to govern digital and healthcare systems. These rules ensure that personal data is kept safe and that sensitive information is private, at the same time ensuring that users granting access to their data have indeed consented to its processing [18]. The GDPR is one of the landmark regulations for the European Union, putting down strict guidelines related to data protection. Organizations must handle personal data responsibly and full transparency. It establishes principles of data minimization, data accuracy, and accountabilities, making it highly relevant to any network, including future 6G systems. On the same front, HIPAA in the U.S. enforces the management of confidential health information. It ensures that medical care providers and connected organizations keep personal patient data confidential and safe [19].

These existing frameworks form a basis for issues on security and privacy, but these have limitations as new technologies such as 6G come into the country, introducing new complexities to the technological sectors.

Vast volumes of data generation, real-time processing, and hyper-connectivity will characterize 6G networks. All these aspects present challenges that current regulations may not be able to adequately cater for. A consideration of the scale of data collection in 6G environments elucidates gaps in current frameworks. Data will be transmitted among billions of devices, including those in IoT ecosystems and autonomous systems. The current laws may not fully consider ubiquitous data collection or even more the AI-driven services that will be part of the envisioned 6G networks. There is a need for the consideration of new legal standards regarding issues of mass IoT de-anonymization, real-time processing that impacts privacy, and regulatory compliance without borders [13].

3.5.2 New Standards for 6G Security and Privacy

New standards and regulatory frameworks, therefore, ought to be envisaged in a quest to accommodate the unprecedented advancements and complexities of 6G networks. Table 3.2 highlights the key regulatory bodies, principles, and technologies essential for ensuring security and privacy in 6G networks, emphasizing global standards, encryption, AI-driven security, and privacy-preserving frameworks.

International regulatory bodies, such as the International Telecommunication Union (ITU) and the Institute of Electrical and Electronics Engineers (IEEE), therefore, have foundational roles to play in extrapolating global standards based upon these unique security and privacy issues of 6G. It will be guided toward creating protocols, policies, and technical standards that can help guide the fair implementation of emerging technologies. ITU is the organization that regulates telecommunication standards worldwide, and, because of this, it must steer and nudge the policies in matters concerning regulations of 6G. In terms of interest areas for ITU in this respect, some of these will be after cross-boundary data transfer policies, interoperability, and guidelines on protecting user privacy in ultra-dense and hyper-connected networks [20]. The IEEE can be of great contribution toward the establishment of security frameworks of 6G architecture. It entails protocols on quantum-safe encryption and secures network slicing. These endeavors will surely help counter the threats to data breaches, cyberattacks, and privacy violations based on AI-driven applications.

Table 3.2 Emerging regulatory frameworks for 6G security and privacy.

Regulatory body/ concept	Role in 6G security and privacy	Key considerations
International Telecommunication Union (ITU)	Regulates global telecommunication standards, including 6G security and privacy policies	- Cross-border data transfer policies - Interoperability guidelines - Protection of user privacy in ultra-dense networks
Institute of Electrical and Electronics Engineers (IEEE)	Develops security frameworks and technical protocols for 6G architecture	- Quantum-safe encryption - Secure network slicing - AI-driven security applications
Privacy by design	Integrates privacy safeguards at the initial stages of 6G development	- Proactive data protection - Minimization of data collection risks - Secure system architecture
Security by design	Embeds security features within the 6G network infrastructure	- Threat mitigation in real time - Secure authentication protocols - AI-driven threat detection
Quantum-resistant cryptography	Protects data from quantum computing-based cyber threats	- Strong encryption techniques - Secure key exchange mechanisms
Privacy-preserving AI	Ensures AI-driven services do not compromise user privacy	- Differential privacy techniques. - Homomorphic encryption for secure data processing.
Federated learning	Trains AI models without sharing raw data, enhancing privacy	- Decentralized AI training - Reduces risk of data breaches - Enables compliance with data protection laws
Government and industry collaboration	Develops adaptive regulations responsive to 6G advancements	- Industry-driven policy updates - Public-private partnerships for cybersecurity - Dynamic compliance strategies

In this regard, the regulatory frameworks must follow the privacy by design and security by design principles to keep in line with the emerging technologies. It refers to including necessary security and privacy safeguards during the development of a 6G system, which implies earlier adaptation in it.

Security paradigms such as quantum-resistant cryptography and privacy-preserving AI algorithms must also be included in new regulation. Governments and regulatory bodies should interact with industry stakeholders to make adaptive frameworks that are responsive to the changing ecosystem of 6G [3]. In addition, these kinds of privacy-preserving technologies such as differential privacy and homomorphic encryption should be further translated into regulations to be standardized in the 6G network. Similarly, the technique termed as federated learning where AI models can be trained without sharing raw data should also attract equal attention from regulation, considering it can ensure that privacy preservation occurs.

3.5.3 Compliance and Accountability in 6G Networks

Scaling the 6G networks around the world would itself be some kind of great challenge in the area of security and privacy compliance. In such complex systems, strategies for regulatory compliance need to be robust as well as scalable. Some promising approaches can include automation of checks powered by AI for ensuring compliance. AI systems can monitor the behaviour of the network in real time and flag a potential breach of security protocols or privacy breach. This could mean embedding compliance directly into the network fabric, which ensures a constant level of vigilance as data moves through 6G networks [21]. Transparency will also form the foundation of accountability in 6G networks. Users need to be in their right to know how their data is being used, processed, and shared. Regulations must ensure that service providers create accessible and understandable privacy policies. As is evident in the above, the possible role of empowering users would be as follows. The users must be given more control over their data. Some such control would include making it easy to be able to opt out from data collection or to a privacy setting. This tends to promote user trust concerning a service provider. In some other contexts, governments will make data portability obligations, which allow users to have their data transferred securely between two or more different kinds of service providers.

The role of user empowerment within 6G networks cannot be undervalued. As network infrastructure becomes increasingly decentralized, users should be given higher control over personal information; such solutions as self-sovereign identity frameworks will help this happen. It involves management of a user's digital identity by users themselves without central authorities. There is a potential for enabling users to have access to data with the possibility of having a higher degree of control through the application of blockchain technology as an accountable, decentralized mechanism for

identity management of users. It will provide tamper-proof records of data transactions and access permissions. Finally, multi-stakeholder collaboration will be vital to foster compliance in 6G environments. Governments, private industries, and international organizations must work together to build up a unified regulatory framework which delivers security and privacy. Continuous updates on regulations, which are sustained by the latest technological breakthroughs and case studies in real-life applications, will ensure the integrity of the networks of 6G.

3.6 Case Studies: Addressing Security and Privacy in 6G Networks

3.6.1 Case Study 1: Securing IoT Devices in a 6G Network

IoT devices are envisioned to be part of 6G networks, and, within them, billions of connected devices that, with them, require advanced security mechanisms. These billions of IoT devices create a large attack surface that hinders the objective of data confidentiality, integrity, and availability across the network. Securing resource-constrained devices is one of the biggest hurdles in advancing technology. Such devices are vulnerable to attacks because they have relatively low computational capabilities and memory storage. The threat of malware attacks, data breaches, and man-in-the-middle attacks is exploited because these devices are insecure [22]. Among several exemplars of going about this is pilot works, such as IoT-enhanced 6G smart grid systems. In those pilot projects, security is introduced with lightweight encryption algorithms designed for the IoT devices, guaranteeing integrity maintained without the strain of excessive consumption on device resources [23]. Another solution introduced to the IoT devices is the use of multi-factor authentication. Multi-factor authentication will prevent unauthorized access from biometric, password, and location-based verification processes.

The most important output of all these has been the success in minimizing the distributed denial-of-service attacks, which were a serious threat to IoT systems. Incorporating AI-based threats of detection mechanisms into 6G networks can monitor activities in real time and thus detect abnormal activity, which would allow one to diagnose and neutralize attacks before they compromise the network [9]. Best practices from these pilot projects highlight edge computing in securing IoT devices. Edge computing lets process data at the edge which decreases latency and increases security by the reduced need to send and receive sensitive data across networks.

3.6.2 Case Study 2: Privacy Preservation in AI-Driven Smart Cities

AI-driven smart cities are becoming a reality with the advent of 6G, which will enable the real-time processing of vast amounts of data from various sources, including surveillance systems, sensors, and citizen interactions. However, what seems to be the biggest concern in AI-led city infrastructure and services management is privacy over personal data collection and processing. It adopted the implementation of PETs in a pilot project in Barcelona, protecting the privacy of citizens while optimizing services. The PETs involved differential privacy and federated learning. Differential privacy ensures that personal data is anonymized before it is shared or analyzed. This allows for insights to be drawn without exposing identities. Federated learning enables AI models to be trained locally on devices. This approach avoids centralization of sensitive data, thus minimizing the threat of data breach [24].

The other major challenge when deploying these technologies was balancing between how granular data needed to ensure efficient AI decision-making and the level of privacy demanded by the respective regulation of data protection, such as GDPR. The Barcelona pilot project succeeded in showing how privacy-preserving AI enhances the management of a city without violating individualized personal privacy. For example, movement data was anonymized to make the public transport system more efficient. This increased the efficiency of the system with respect to privacy on the part of the users. The case study also puts forward the argument that privacy matters should always be brought into the design of smart city technologies at the very beginning [3].

3.6.3 Case Study 3: Blockchain-Based Security Solutions in 6G

Blockchain technology has been offered as promising solution to address security issues in 6G networks. Blockchain offers authentication and data integrity and will allow greater decentralization to enhance network security. It is, therefore, best suited for environments with highly complex stakeholders and devices in distributed scenarios. In the nascent stages of its deployment, blockchain has been applied to secure IoT ecosystems and 6G-enabled supply chain networks. One of the most studied cases dealt with is the deployment of blockchain-based security systems within a 6G smart logistics network. The system used DLTs to determine identity and verify data transactions within the network. Using blockchain's immutable ledger, each transaction could be traced through timestamps

and recording-meaning alterations or tampering of data could not be performed. In addition, the automation of security-related operations, such as authentication of IoT devices before they were allowed to communicate data over the network, was realized using smart contracts.

The most significant lesson learned from this deployment was that blockchain-based security systems are scalable and resilient in 6G complex environments. It provided the integrity of data together with a reduction in the needs for trusted central authorities, which are usually a single point of failure in a traditional network [25]. However, lessons learned from this project showed that it is essential to handle the high computational and energy costs related to blockchain. This motivates the development of lightweight versions of blockchain, which are referred to as blockchain for IoT or BIoT. Those variants aim to address some of the distinctive demands for 6G networks wherein efficiency and scalability become the ultimate concerns.

3.7 Future Directions and Opportunities

3.7.1 Emerging Threats and Security Challenges in 6G

As 6G technology becomes more advanced, the cybersecurity threat environment will be relatively challenging for the next-generation networks. The most common issue there will be that 6G networks need to be future-proofed against the ever-evolving and highly sophisticated cyber threats. For the first time, 6G will allow large-scale integration of IoT, autonomous systems, and AI-driven applications. This is going to highly expand the potential attack surface [4]. More and more devices connected to the network open up new vulnerabilities to be leveraged by the adversary. These new vulnerabilities will be zero-day attacks, breaches of data, and ransomware.

As quantum computing continues to grow, another characteristic of the threat landscape is the growth of quantum computing. Quantum computing is quite a double-edged sword with regard to encryption and potential threats [26]. On the positive side, quantum computing promises to enable the development of quantum-resistant cryptographic algorithms, thereby enhancing data protection in 6G networks. There is a need for post-quantum encryption methods in the face of threats from adversaries who may use their quantum computers to break classical encryption schemes. Conversely, the very quantum computing capability may allow decryption of sensitive data through attacks. This will severely put information

confidentiality at risk. More research and development in quantum-resistant encryption and advanced cybersecurity frameworks will mitigate the risks alone. Those frameworks, by necessity, must be strong enough to be immune to the power of quantum computers. Integration of AI-based threat detection systems will also play a pivotal role. Such a system of monitoring and mitigation of real-time cyberattacks will decrease the impact of such threats on 6G networks.

3.7.2 Innovations in Privacy-Preserving Technologies

One of the core concerns that privacy will face in the future as 6G emerges is the amount of personal and sensitive data handled by networks. Besides typical approaches, emerging approaches to achieve existing concerns in privacy-preserving technologies are required. For instance, differential privacy is promising to anonymize data while retaining utility for analysis. This approach already has potential in smart cities, healthcare, and even AI-driven service-oriented applications [24]. Another emerging technology relating to privacy is homomorphic encryption. Homomorphic encryption will let computations be carried out on the encrypted data itself, rather than requiring first decryption, thus ensuring sensitive information is kept private throughout the data processing cycle. This innovation indeed proves worthwhile especially in sectors such as healthcare and finance where privacy and security have to be paramount. Another is federated learning, which allows AI models to be trained on decentralized data. This approach is sure to maintain personal information with the user and contribute toward the development of global AI models [27].

PETs are one of the directions that future 6G privacy technologies are taking. PETs are now creating robust user data protections. With these PETs, new research and development opportunities lie in enhancing efficiency, scalability, and usability. Solutions in these areas must be developed further and deployed with the collaborations of governments, industries, and academic institutions. Privacy by design means that developers in this instance create systems not as afterthoughts but with embedded protections [28].

3.7.3 Collaborative Approaches to Security and Privacy in 6G

Considering that the networks of 6G are complex and interdependent, the issue of security and privacy requires collaboration. The cooperation between the sectors, including public and private, academia, and the regulatory body, during the 6G era, would thus be important. This collaboration is what will help make networks resilient and secure [7].

Collaborative efforts will also allow the actual development of common security standards and best practices. Common intelligence in terms of emergence or development of new threats also holds great importance. A good example of this collaboration is the establishment of public-private partnerships. Such partnerships can design security solutions for various industries. They pool their resources and expertise to design flexible cybersecurity frameworks that are powerful against new threats.

Academic bodies can add value by researching emerging security technologies. They can experiment with and validate novel solutions in real-world environments. In order to achieve resilience, 6G networks will need to be developed to be inter-operable across borders, and international standards for security and privacy will be foundational in this way [3]. Standards developed by organizations such as the ITU and the IEEE will ensure consistency on a global scale. It will address cross-border data flows along with differences in jurisdiction over data protection laws. Cross-industry collaboration may also be applied for the design of automated security solutions. The solutions come with AI and ML that is used to scan the networks in real-time so as to design a response to threats. They can reduce the time taken to respond to attacks, prevent breaches, and ensure strict adherence to privacy regulation compliance. Many stakeholders, including governments and private industry players will eventually allow for an all-rounded approach to cybersecurity governance on 6G networks [4].

3.8 Conclusion

Security and privacy exploration in 6G networks expose an area; both greater challenges are set and more solutions are expected. In the direction of promising unparalleled connectivity and data exchange, the technological development of 6G exacerbates manifold complexities related to security and privacy. These major challenges include the increased threat landscape due to proliferated IoT devices and sophistication of cyberattacks. The problem also presents other broad challenges in securing massive volumes of data and addressing vulnerabilities inherent in the network infrastructure, particularly considering the introduction of virtualization and AI. Technologies required for the mitigation of threats arising from these challenges include strong privacy preserving technologies, homomorphic encryption and differential privacy as well as AI-based threat detection and quantum-resistant cryptography. These need to be approached holistically to be dealt with well. This will involve integrating next-generation encryption techniques, decentralized trust models such

as blockchain, and PETs. Regulatory frameworks must further be adapted based on the very rapid trends of 6G technology, ensuring security and privacy together [7].

There are a number of actionable measures to take for network operators, policymakers, and technology developers.

- Network operators would have to invest in advanced security infrastructure. They should also adopt AI-driven monitoring systems to improve detection and response capabilities with threats.
- Policymakers will have to cooperate with international bodies. They must revise and formulate regulatory standards as per their exclusive needs in 6G networks.
- Technology developers will have to look at innovative solutions: quantum-resistant algorithms and privacy-preserving technologies among others to give their systems the most future-proof characteristics.
- Innovation should be continuous, and research is going to be continuous. Policy changes will have to be made according to the changing challenges 6G networks bring forth.
- Stakeholders need to develop a resilient 6G ecosystem by promoting collaboration and staying ahead of emerging threats. This ecosystem shall ensure and protect user data while delivering the transformative capability of next-generation connectivity [24, 26].

References

1. Saad, W., Bennis, M., Chen, M., A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Netw.*, *34*, 3, 134–142, 2019. https://doi.org/10.1109/MNET.001.1900287.
2. Latva-Aho, M. and Leppänen, K., *Key drivers and research challenges for 6G ubiquitous wireless intelligence*, Oulu University Research Repository, Finland, 2019, Retrieved from https://oulurepo.oulu.fi/handle/10024/36430.
3. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Fan, P., 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Veh. Technol. Mag.*, *14*, 3, 28–41, 2019. https://doi.org/10.1109/MVT.2019.2921208.
4. Dang, S., Amin, O., Shihada, B., Alouini, M.S., What should 6G be? *Nat. Electron.*, *3*, 1, 20–29, 2020. https://doi.org/10.1038/s41928-019-0355-6.

5. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., Zorzi, M., Toward 6G networks: Use cases and technologies. *IEEE Commun. Mag.*, *58*, 3, 55–61, 2020. https://doi.org/10.1109/MCOM.001.1900411.
6. Porambage, P., Gür, G., Osorio, D.P.M., Liyanage, M., Gurtov, A., Ylianttila, M., The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.*, 2, 1094–1122, 2021. https://doi.org/10.1109/OJCOMS.2021.3078081.
7. Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., Zhou, W., Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.*, *6*, 3, 281–291, 2020. https://doi.org/10.1016/j.dcan.2020.07.003.
8. Singh, M. and Malik, A., Multi-hop Routing Protocol in SDN-Based Wireless Sensor Network, in: *Software-Defined Network Frameworks*, pp. 121–141, CRC Press eBooks, London, 2024, https://doi.org/10.1201/9781003432869-8.
9. Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., AI and 6G security: Opportunities and challenges, in: *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 616–621, 2021, https://doi.org/10.1109/EuCNC/6GSummit51104.2021.948250.
10. Kumar, P.R., Raj, P.H., Jelciana, P., Exploring data security issues and solutions in cloud computing. *Procedia Comput. Sci.*, *125*, 691–697, 2018. https://doi.org/10.1016/j.procs.2017.12.089.
11. Nguyen, V.L., Lin, P.C., Cheng, B.C., Hwang, R.H., Lin, Y.D., Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Commun. Surv. Tutor.*, *23*, 4, 2384–2428, 2021. https://doi.org/10.1109/COMST.2021.3108618.
12. Alsabah, M., Naser, M.A., Mahmmod, B.M., Abdulhussain, S.H., Eissa, M.R., Al-Baidhani, A., Hashim, F., 6G wireless communications networks: A comprehensive survey. *IEEE Access*, 9, 148191–148243, 2021. https://doi.org/10.1109/ACCESS.2021.3124812.
13. Liu, X., Li, H., Xu, G., Lu, R., He, M., Adaptive privacy-preserving federated learning. *Peer-to-Peer Netw. Appl.*, 13, 2356–2366, 2020. https://doi.org/10.1007/s12083-019-00869-2.
14. Kazmi, S.H.A., Hassan, R., Qamar, F., Nisar, K., Ibrahim, A.A.A., Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques, and research directions. *Symmetry*, *15*, 6, 1147, 2023. https://doi.org/10.3390/sym15061147.
15. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., On blockchain and its integration with IoT: Challenges and opportunities. *Fut. Gener. Comput. Syst.*, 88, 173–190, 2018. https://doi.org/10.1016/j.future.2018.05.046.
16. Park, J. and Lim, H., Privacy-preserving federated learning using homomorphic encryption. *Appl. Sci.*, *12*, 2, 734, 2022. https://doi.org/10.3390/app12020734.
17. Dwork, C. and Roth, A., The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, *9*, 3–4, 211–407, 2014. https://doi.org/10.1561/0400000042.

18. Voigt, P. and Von dem Bussche, A., *The EU General Data Protection Regulation (GDPR): A practical guide*, 1st ed, Springer International Publishing, AG, Switzerland, 2017, https://doi.org/10.1007/978-3-319-57959-7.
19. Mbonihankuye, S., Nkunzimana, A., Ndagijimana, A., Healthcare data security technology: HIPAA compliance. *Wirel. Commun. Mobile Comput.*, 2019, 1927495, 2019. https://doi.org/10.1155/2019/1927495.
20. Strinati, E.C. and Barbarossa, S., 6G networks: Beyond Shannon towards semantic and goal-oriented communications. *Comput. Netw.*, 190, 107930, 2021. https://doi.org/10.1016/j.comnet.2021.107930.
21. Lim, C., Kim, K.J., Maglio, P.P., Smart cities with big data: Reference models, challenges, and considerations. *Cities*, 82, 86–99, 2018. https://doi.org/10.1016/j.cities.2018.04.011.
22. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., Security, privacy, and trust in the Internet of Things: The road ahead. *Comput. Netw.*, 76, 146–164, 2015. https://doi.org/10.1016/j.comnet.2014.11.008.
23. Singh, A. and Chatterjee, K., Edge computing-based secure health monitoring framework for electronic healthcare system. *Cluster Comput.*, *26*, 2, 1205–1220, 2023. https://doi.org/10.1007/s10586-022-03717-w.
24. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., Edge Computing-Based Design for IoT Security, in: *Network Optimization in Intelligent Internet of Things Applications*, pp. 298–309, Chapman and Hall/CRC eBooks, 2024, https://doi.org/10.1201/9781003405535-22.
25. Zafar, S., Bhatti, K.M., Shabbir, M., Hashmat, F., Akbar, A.H., Integration of blockchain and Internet of Things: Challenges and solutions. *Ann. Telecommun.*, *77*, 1, 13–32, 2022. https://doi.org/10.1007/s12243-021-00858-8.
26. McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B.A., Communication-efficient learning of deep networks from decentralized data, in: *Artificial Intelligence and Statistics*, pp. 1273–1282, PMLR, New York, April 2017.
27. Bernstein, D.J. and Lange, T., Post-quantum cryptography. *Nature*, *549*, 7671, 188–194, 2017. https://doi.org/10.1038/nature23461.
28. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., Blockchain applications for healthcare informaticn, in: *IoT and Blockchain Technology in 5G Smart Healthcare*, pp. 137–161, Elsevier eBooks, 2022, https://doi.org/10.1016/b978-0-323-90615-9.00004-9.

4

Enhancing Security and Privacy Frameworks in 6G Networks

Jaishree Jain[1]*, Rohit Kumar Goel[2], Updesh Kumar Jaiswal[1], Pawan Kumar[1] and Amit Singhal[3]

[1]Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad (U.P.), India
[2]Research Never Die, Ghaziabad (U.P.), India
[3]Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad (U. P.), India

Abstract

The 5G network age is still a way off, and, because of its limits, we need to start looking into sixth-generation (6G) networks right once. Therefore, we have produced a chapter on the current scenario of 6G security and privacy in order to compile and reinforce this basic research as a platform for further studies. This chapter gives an overview of basic networking techniques and how they affect the present 6G networking developments. We have discussed four main areas of 6G communication networks: three-dimensional (3D) intercoms, real-time intelligent edge computing, distributed artificial intelligence, and intelligent radio. We also cover some exciting new developments in each of these areas, including security concerns. Novel technology, an explosion of available user information, and a variety of threats in a space-air-ground integrated network environment are the challenges faced by 6G mobile networks. For the time being, 6G security and privacy concerns are still mostly theoretical and challenging. Informatics has advanced, changing our perception of accessibility and data processing to provide solutions. The survey starts with an overview of past networking technologies and their influence on the current developments in 6G networking. Next, we explore four critical components of 6G networks—real-time intelligent edge computing, distributed artificial intelligence, intelligent radio, and 3D intercoms—along with several innovative technologies emerging in each field and the associated security and privacy concerns. The survey wraps up with an analysis of the possible applications for 6G. To strengthen

**Corresponding author*: jaishree3112@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (81–106) © 2026 Scrivener Publishing LLC

and establish this foundational research as a groundwork for future studies, we have developed a survey regarding the current state of 6G security and privacy.

***Keywords*:** 3D intercoms, 5G network, 6G network, distributed AI, network generations, privacy, security

4.1 Introduction

A communication network refers to a system of interconnected devices and nodes that enable the exchange of data, voice, video, or other forms of information over various distances. Communication networks are essential for modern telecommunications, supporting services like the internet, telephone systems, and broadcasting. Here is an overview of communication networks, and their key components are discussed. The advent of sixth-generation (6G) communication networks marks a transformative era in global connectivity, promising unprecedented advancements in data speed, ultra-low latency, massive device connectivity, and intelligent automation. As the successor to 5G, 6G aims to integrate cutting-edge technologies such as artificial intelligence (AI), Internet of Things (IoT), pervasive sensing, and quantum computing to enable futuristic applications, including autonomous systems, immersive augmented reality, and smart cities. However, these technological leaps introduce significant challenges in maintaining robust security and safeguarding user privacy. The complexity of 6G networks, driven by their decentralized architectures, heterogeneous devices, and dynamic operational scenarios, expands the attack surface, exposing the ecosystem to new vulnerabilities. Furthermore, the integration of AI and machine learning (ML), while enhancing adaptability, poses risks such as adversarial attacks and data breaches. Similarly, the vast volumes of sensitive data generated in real-time by interconnected devices intensify privacy concerns, making the development of effective frameworks imperative.

This chapter explores the challenges associated with enhancing security and privacy in 6G networks and proposes solutions to address these issues. From leveraging AI-driven threat detection and post-quantum cryptography to implementing privacy-preserving techniques and zero-trust architectures, the discussion highlights the need for innovative and adaptive frameworks to ensure a secure 6G future. By addressing these challenges, we can build trust and resilience in a network that forms the backbone of tomorrow's digital society.

The rapid evolution of wireless communication technologies has brought humanity to the brink of the 6G of mobile networks, which promises to revolutionize connectivity and enable unprecedented applications. Building upon the foundations of 5G, 6G networks aim to deliver ultra-high-speed communication, latency on the order of microseconds, and seamless integration of billions of devices through the Internet of Everything (IoE). The envisioned applications of 6G include fully autonomous transportation systems, holographic telepresence, advanced smart cities, precision healthcare, and pervasive computing environments. These transformative capabilities, however, come with significant challenges in ensuring the security and privacy of users and systems. Unlike earlier generations, 6G networks are expected to feature highly decentralized and intelligent architectures, characterized by edge computing, AI-driven decision-making, and ultra-dense device deployment. This decentralization, while necessary for achieving performance goals, creates a vast and complex attack surface. The combination of massive machine-type communication, ultra-reliable low-latency communication, and enhanced mobile broadband (eMBB) adds layers of complexity to network management, making traditional security frameworks insufficient for addressing emerging threats.

Moreover, 6G's reliance on advanced technologies such as quantum computing, blockchain, and reconfigurable intelligent surfaces (RISs) introduces novel risks. For instance, quantum computers have the potential to break traditional encryption mechanisms, whereas blockchain-based systems could be susceptible to new types of attacks targeting consensus protocols. The increased connectivity of devices and the data-intensive nature of 6G networks further exacerbate privacy concerns, particularly regarding data ownership, sharing, and protection. In response to these challenges, the development of robust security and privacy frameworks for 6G is critical. Solutions must account for the unique features of 6G, including its reliance on AI for network orchestration, its integration with emerging technologies, and its unprecedented data-generation capabilities. AI-driven threat detection and response mechanisms, post-quantum cryptography, privacy-preserving data analytics, and zero-trust security architectures are among the promising approaches to securing 6G networks.

This chapter examines the multifaceted challenges of ensuring security and privacy in 6G communication networks and explores innovative solutions to address these issues. By delving into these aspects, the chapter aims to provide insights into designing a resilient 6G ecosystem that safeguards the integrity, confidentiality, and availability of data and services while fostering trust in the networks that will underpin the future of digital innovation.

The advent of 6G communication networks marks a paradigm shift in wireless technologies, promising to redefine how we interact with the digital world. As a successor to 5G, 6G aims to achieve unprecedented performance metrics such as terabits-per-second data rates, sub-millisecond latency, and seamless connectivity across terrestrial, aerial, and satellite networks. These advancements will facilitate revolutionary applications, including holographic communication, digital twins, autonomous systems, and ultra-smart cities. However, the integration of these capabilities comes with heightened challenges, particularly in ensuring the security and privacy of the networks and their users. Unlike previous generations, 6G networks will feature decentralized, intelligent, and dynamic architectures. Core technologies driving this evolution include AI, ML, quantum computing, blockchain, and RISs. While these innovations enable 6G to meet the demands of ultra-reliable and low-latency communication, massive device interconnectivity, and immersive user experiences, they also create novel vulnerabilities. For instance, the incorporation of AI and ML exposes networks to adversarial attacks, whereas the potential of quantum computing raises questions about the long-term viability of traditional cryptographic algorithms.

The increasing reliance on ultra-dense and interconnected devices heightens the complexity of safeguarding sensitive data. Privacy concerns are amplified by the vast amounts of data generated, transmitted, and analyzed in real time, often crossing geographical and regulatory boundaries. Existing security frameworks, designed for earlier generations of networks, fall short of addressing the dynamic and multidimensional threats posed by 6G environments. Addressing these issues requires a holistic approach to security and privacy that integrates cutting-edge technologies and innovative methodologies. Solutions must be tailored to 6G's unique characteristics, such as its reliance on AI for autonomous decision-making, its embrace of decentralized architectures, and its dependence on data-intensive applications. Promising strategies include the adoption of post-quantum cryptography, federated learning for privacy-preserving AI, zero-trust security models, and blockchain-based authentication mechanisms. Additionally, ethical considerations and regulatory frameworks must evolve to align with the technological complexities of 6G systems.

This chapter delves into the critical challenges and emerging solutions for enhancing security and privacy frameworks in 6G communication networks. It begins by exploring the transformative capabilities of 6G and the unique security and privacy risks that it introduces. Subsequently, it examines state-of-the-art solutions, focusing on their applicability to 6G's diverse use cases. By addressing these themes, the chapter aims to provide

a comprehensive understanding of how to build secure, resilient, and trustworthy 6G networks capable of supporting the next wave of digital innovation.

4.1.1 Challenges in Communication Networks

1) **Scalability**
   As the number of connected devices grows, networks need to scale efficiently without compromising performance.
2) **Security**
   Communication networks are vulnerable to cyberattacks such as hacking, Distributed Denial of Service attack (DDoS), and data breaches. Implementing encryption and secure protocols is critical.
3) **Latency and Bandwidth**
   Reducing latency (delay in data transmission) and increasing bandwidth (amount of data transmitted) are essential for real-time applications like video streaming and gaming.
4) **Interoperability**
   Ensuring that devices and systems from different manufacturers or platforms can work seamlessly together is crucial, especially with the rise of IoT and smart devices.

4.2 AI-Enabled 6G Networks

1) Privacy and Security
By employing ML models to identify patterns suggestive of cyberattacks, AI-driven systems are able to continually monitor 6G networks for indications of unusual behavior or security breaches. AI will improve security measures in real time by recognizing and eliminating threats more quickly than with conventional techniques. Adaptive Encryption: AI will be utilized to create security methods that adjust based on the kind of data being sent. For example, depending on real-time evaluations of possible risks, extremely sensitive data would immediately be encrypted with greater security.

2) Managing Massive Connectivity
As IoT devices proliferate, 6G will need AI to effectively manage enormous numbers of linked devices. AI will assist by ensuring that resources are deployed efficiently and prioritizing devices based on consumption patterns.

3) Assurance of Quality of Service
AI is able to predict traffic volumes in various areas, which enables the network to pre-allocate resources to ensure optimal performance during periods of heavy usage [9].

4) Advanced Applications of AI
AI will be crucial for handling the massive amount of data in holographic communications requirements of holographic communications, ensuring smooth transmission and minimal delays. AI-Driven Digital Twins: 6G networks will utilize digital twin technology, where AI creates real-time virtual models of physical objects or environments. This will enable remote monitoring, diagnostics, and even control of physical systems in fields like manufacturing, healthcare, and smart cities [10].

5) Context-Aware Networking
Personalized User Experience: AI can analyze the context in which a user is interacting with the network (e.g., location, device type, and application) and dynamically adjust the network settings to enhance the user experience. This could mean boosting bandwidth for immersive VR or lowering latency for real-time gaming.

The network energy efficiency for 6G must grow 10-fold over 5G and 100-fold over 4G [11]. It is anticipated to enable transmissions at extremely low power for devices with limited resources. At 1,000 km/h, swift movement will be possible thanks to sophisticated and proactive mobility management technology. The delay outcome of security procedures will be assessed in order to ensure that Extremely Reliable and Low Latency Communications (ERLLC) receives high-quality service. In a same vein, high standards necessitate extremely effective security solutions that ensure the availability of resources and services. The new security solutions utilizing distributed intelligent AI and ML include challenging to implement and run because of the IoE. Determining an essential component involves knowing how to provide additional security enablers to devices with constrained resources, as shown in Figure 4.1 [12].

This chapter highlights a thorough survey on privacy and 6G network security concerns. We provide a quick overview security evolution the first five generations of mobile radio technology, from 1G to 5G, with an emphasis security flaws identified current answers. The security of 6G issues several important domains looked into. Research also outlines the security needs and challenges for 6G technology and applications. Next, we suggest fixes for the new 6G apps. This research examines one of the earliest investigations that encompasses a comprehensive assessment for the prospective security solutions related to 6G new technology [13, 14] as shown in Figure 4.2. There are

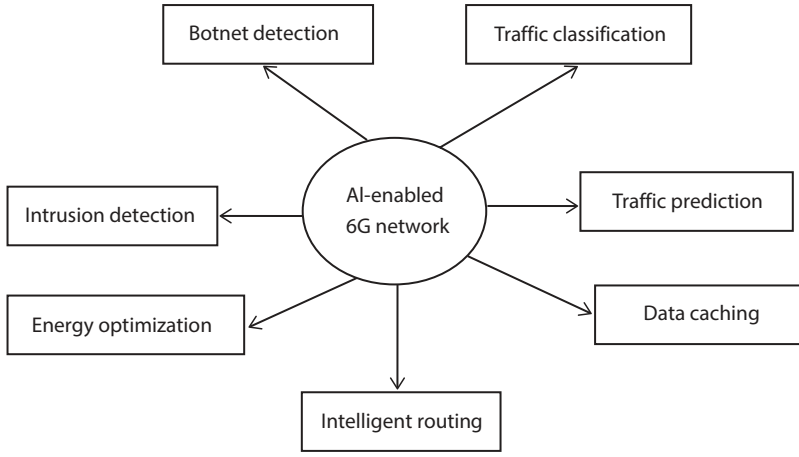

Figure 4.1 Applications of AI-enabled 6G network.

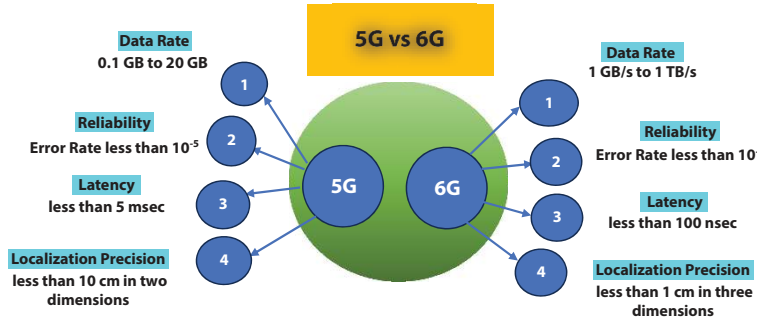

Figure 4.2 The 5G and 6G features comparison.

currently no standard features or requirements for the 6G network, just a multitude of options. Rather, it ought to offer complete coverage of the submerged area. Additionally, far greater AI capabilities should be available on the 6G network. Indeed, a lot of academics believe that the 6G network needs to be "AI-empowered," which means that AI will be both its main feature and its engine [2]. Its architecture should not be limited to using AI, like the 5G network does. The fully integrated use of presently developing AI in the 6G network is expected instruments and networking features. Furthermore, risk mitigation needs to be an essential component of the design, given the recent rise in relevance of privacy and network security issues [3].

These four domains comprise the most potent portion of the 6G research that is currently underway, which is why we selected them as our primary

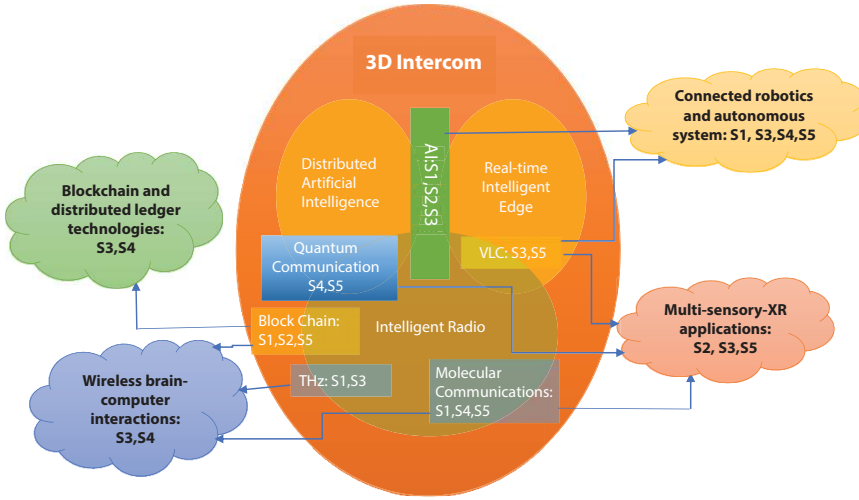

Figure 4.3 Security & Privacy Controls: S1: authentication; S2: access control; S3: malicious behaviors; S4: encryption; S5: communication.

emphasis [4]. They also face the greatest privacy and security risks shown in Figure 4.3. As a result, the following may be used to sum up this survey's primary contributions:

a. A list and examples of the primary privacy and security risks for 6G networks are provided.
b. The list of the most promising technologies for 6G networks is followed by a detailed investigation of the security and privacy concerns associated with these technologies.
c. New privacy and security issues unique to 6G networks are outlined and discussed.

Based on the above discussion, the following topics will be covered in the remaining sections of this chapter.

i. Outlining the most popular 6G technologies and investigating each one's unique security requirements.
ii. Investigating the requirements for 6G applications and services.
iii. Describe the security flaws in 6G apps and offer potential solutions.

4.3 Features and Drawbacks of 1G to 5G

1) **1G**
The "G" in 1G is used for "generation," and it refers to the generation of wireless mobile telecommunications technology [15]. Designed primarily for phone services, the 1G network was initially put to use analogy transmissions send data lacks any authorized wireless standards [5]. Intense handoffs as well as inadequate and no security and privacy guarantees are the negative effects of this, as shown in Figure 4.4.

2) **2G**
Making the Global system for mobile communications (GSM) aims to provide a system that is as safe as a Public Switched Telephone Network. 1) Privacy, 2) verification, 3) security of signals, and 4) protection of user information are some of its security and privacy offerings [8]. Anonymity is attained by using fictitious identifiers, making it challenging to determine the user's true identity. When the device is first turned on, though, the actual identity must be utilized; otherwise, a temporary identification is generated [6]. Network operators mostly employ authentication. Furthermore, end-to-end encryption is not used. Adversaries have a chance to launch an attack because just wireless channel is encrypted remains unencrypted [11].

3) **3G**
The 2G technologies provide the foundation of the 3G system's security. Furthermore, the Third-Generation Partnership Project offers a comprehensive security framework controlling access, which consists of two components [7].

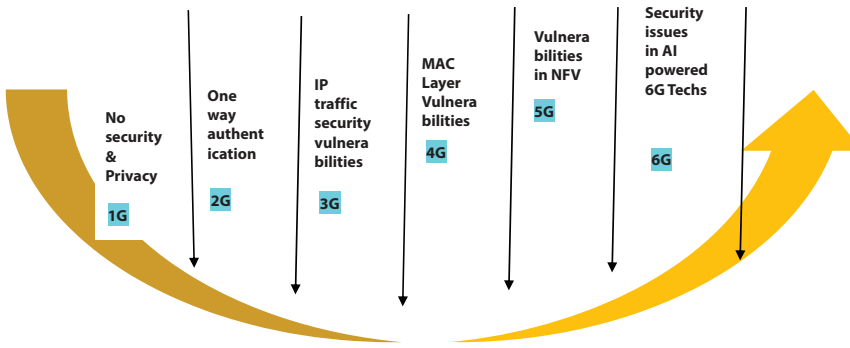

Figure 4.4 Evolving security and privacy concerns in wireless networks.

4) 4G
As 4G users become increasingly adept at interacting with one other and as executors of all wireless protocols, threats become more widespread [16]. Furthermore, more malicious software may be executed on mobile terminals as processing and storage capacity increase, possibly leading to greater harm. Common examples include malware, hardware platform interference, and weaknesses in operating systems.

5) 5G
Other devices, such as IoT equipment, could potentially be able to connect to the network in addition to smartphones [17, 18]. The network design of 5G networks, in particular its three tiers (access networks, backhaul networks, and core networks), may offer the most effective classification system for security and privacy issues [19].

4.4 Important Domains for 6G Networks

Numerous 5G network components and some network layer applications have already been built on AI [26]. Consequently, distributed AI and intelligent radio are unsupported as they are fully dependent on AI. Furthermore, latency makes it impossible to respond to emergency circumstances in "real-time," even in 5G networks that have already embraced real-time intelligent edge technologies like automobile networks [20, 21]. Additionally, 5G coverage is now restricted to the planet; at some three-dimensional (3D) intercom levels, communication in space or underwater is not feasible as shown in Table 4.1.

1) Real-Time Intelligent Edge
Real-time intelligence and extremely low network latency are required [22]. This is especially valid for networks of vehicles. Although autonomous driving is currently possible with the 5G network, and some of these capabilities are even being used by AI-powered cloud services, it is not possible to support network entities that possess self-awareness, self-adaptation, or prediction [28]. It is thus necessary to create a new network that is capable of doing these tasks [26]. Furthermore, vehicle-to-vehicle communications will benefit greatly from the usage of several emerging technologies, such as VideoLAN Client (VLC) [29]. A vehicle network should include both the physical and network environments, according to Tang *et al.* [30], because doing so may help lessen the threat provided by malicious automobiles. Group dynamics within parked automobiles need to be considered as well [23].

Table 4.1 A summary of key areas related to 6G.

Key areas	Summary	Characteristics	Relation to 6G
Real-time intelligent edge	Real-time intelligent edge technology might make it easier for autonomous vehicles to react quickly to new situations [25].	Real-time response	Capability of control
Distributed artificial intelligence	A sizable decentralized system with distributed artificial intelligence should be able to make intelligent decisions at many levels [27].	Make intelligent decision	Decision-making capacity
Intelligent radio	Within an intelligent radio system, hardware information may be used by receiver algorithms to dynamically configure and update themselves.	Self-adaptive	Be responsible for communication
3D intercoms	Services might be offered *via* 3D intercoms according to the needs of the moment and place. In addition to ground level, coverage extends to space and underwater levels [36, 38].	Full 3D cover	Be responsible for coverage

2) Distributed Artificial Intelligence

Beyond its handling as personal data, the shared data serves as a training set in this way. Correct implementation of this strategy may potentially enhance the network's security and privacy. Distributed AI security concerns have already been noted in some cases [43]. A malevolent user may, for instance, update a contaminated model to contaminate the training

model as a whole. Device security is another area with some concerns [32]. Furthermore, to guarantee data integrity, ML models should be enhanced [33], and enhancements to complete communication and control security are desirable [31]. Some distributed ledger technology (DLT) authentication problems should be resolved by blockchain-like techniques [34], but further research is required to enable machine-learning models to anticipate impending assaults [35].

3) Radio with Intelligence

Transceiver algorithms and devices were built in tandem hardware attribute networks, such that the number of antennae and the computation of decoders have been essentially unchanged [2]. But with to recent advancements in circuits and antennas, it is now feasible to isolate intelligent radio might function as a single system. According to Yang *et al.* [1], it is conceivable to exploit numerous high-frequency bands and dynamically employ different frequencies by combining software-defined radio with networking approaches. This would enable support for intelligent radio. An interface language and operating system have been presented by Huang *et al.* [2]. It is based on hardware data and AI techniques that allow for the reconfigurability of transceiver algorithms. Additionally, it has been suggested that intelligent radio assistance needs to meet a number of criteria. For instance, the frequency band should adjust to the hardware and surroundings [56].

4) Multimedia intercoms

Planning, analyzing, and optimizing networks skills in 6G networks will need to be upgraded from two dimensions to three in comparison to earlier network generations [37]. Therefore, in order to accommodate satellites, unmanned aerial vehicles, and underwater communications, 6G networks need to be able to enable communications in 3D space. For instance, because the fixed equipment connected to 4G and 5G networks cannot be moved, unmanned aerial vehicle (UAV) network setup and reaction during an emergency in a remote location are more economical than utilizing these networks [40]. Because satellites must operate in controlled frequency bands, terahertz (THz) bands are now being researched and tested at the space level [39]. Given its appropriateness for long-distance communication, communication and quantum communication might be used in this situation [29]. The Space-Terrestrial Integrated Network, as proposed by Yao *et al.* [41], is a system that combines mobile wireless networking, the internet, and satellite communications. Because of the complexity of the underwater environment,

there is ongoing debate on whether 6G networks might function underwater in terms of coverage. Grimmett [44], on the other hand, is leading the conversation on a few security concerns related to the methods used for transmission in wireless acoustic communication networks underwater. Therefore, further security concerns will undoubtedly surface in the future [42].

4.5 Contributions and Issues of Key Technologies with the Main 6G Technologies

Some important technologies are already showing to be secure and effective transmission services, high dependability, and low latency to 6G networks. But as was previously indicated in the part above, the majority of these technologies also bring with them new security and privacy risks. In this part, we talk about this that summarized in Table 4.2.

1) Terahertz (THz) Communication
High Data Rates: 6G will utilize THz frequencies (0.1–10 THz), enabling data rates up to 1 Tbps, far exceeding those of 5G. THz communication opens up enormous bandwidth for applications like immersive virtual reality (VR), holographic communication, and high-resolution imaging. The use of THz waves will enable extremely low-latency communication over short distances, essential for real-time applications like autonomous vehicles and AR. THz waves face significant propagation loss, meaning they cannot travel far or penetrate obstacles like walls, requiring a dense infrastructure of small cells. Power consumption and material limitations make it difficult to develop effective THz transceivers and antennas. The electronics of today are not entirely THz frequency optimized.

2) Machine Learning (ML) and Artificial Intelligence (AI)
Network Automation: AI will make it possible for networks to self-optimize (SON), allowing for automatic real-time modifications to traffic, resource allocation, and energy consumption. Predictive analytics powered by AI will improve spectrum management by cutting down on interference, optimizing bandwidth, and enhancing user experience. Real-time cyber threat detection and mitigation by AI-driven technologies enhances the 6G ecosystem's overall security. The integration of AI with 6G networks will significantly increase system complexity, making system management and troubleshooting more difficult. Using AI to make crucial network choices brings challenges regarding reliability, transparency, and accountability.

Table 4.2 Contribution and issues of key technologies with the main 6G technologies.

Key technology	Ref.	Security and privacy issues	Key technology contribution
AI	[33]	Access control	Detailed control procedures
	[37]	Malicious behavior	Seek for irregularities in the network and issue timely alerts
	[45]	Authentication	A technique for unsupervised learning that might be applied to the authentication procedure to improve the physical layers' security
	[46]	Communication	A machine learning–based antenna design that might be used to PHY layer communication to stop data leaks
Molecular communication	[47]	Encryption	Quantum encryption techniques and machine learning
	[48]	Malicious behavior	An enemy interfering with molecular communication or its mechanisms
	[49]	Encryption	A coding system that could improve data transmission security
	[50]	Authentication	Provide guidance for creating new methods of authentication
Quantum communication	[47]	Encryption	Protection mechanisms for quantum encryption keys
Blockchain	[52]	Authentication	A fresh conceptual framework for authorizing mobile services
	[53]	Access control	A technique to enhance access procedures
	[54]	Communication	Hashing power is used to verify transactions.
VLC	[57]	Communication	A safe procedure that is applicable to communication.
	[58]	Malicious behavior	Cooperating snoopers can make security less effective.

3) Reconfigurable Intelligent Surfaces (RISs)
Improved Signal Propagation: RISs are capable of modifying electromagnetic waves to increase the intensity and quality of the signal, particularly in places with inadequate coverage. By focusing and rerouting wireless signals, these surfaces eliminate the need for base stations that consume a lot of electricity. Integrated risk information system (IRIS), especially in urban settings, can assist reduce signal obstructions by reflecting and improving signal routes. It will be costly and logistically difficult to deploy RIS widely throughout buildings and infrastructure. Accurate alignment with signal routes and network optimization are essential to RIS performance, although these requirements may be challenging to uphold in practical settings. In places with a high population density and a large number of reflecting surfaces, improperly designed RIS may cause interference.

4) Quantum Communication and Computing
Virtually Unbreakable Encryption: With quantum cryptography, important communications on 6G networks might be protected from untraceable encryption. The processing power needed for intricate data analysis, optimization, and AI-driven applications might be significantly increased by quantum computing. Network Synchronization: By enabling incredibly accurate temporal synchronization throughout the network, quantum approaches may enhance cooperation between dispersed systems. The current scalability of quantum communication technologies is limited by their early development and need for extremely regulated conditions. The construction of quantum communication infrastructure is an expensive endeavor, as the technology is intricate and needs continuous research and development. There are compatibility issues when integrating quantum communication with conventional networking technology.

5) Non-Terrestrial Networks (NTNs) and Satellite Integration
Global Coverage: Remoting and underserved areas will be covered by satellite-based 6G networks, guaranteeing ubiquitous access even in rural areas and across seas. In times of emergency or natural catastrophe when terrestrial networks may collapse, NTNs provide resilience. NTNs will improve connectivity for use cases involving high mobility, such high-speed rail, aircraft, and maritime transportation.

6) Distributed ledger technologies (DLTs) and blockchain
Automated Contracts: Blockchain-driven smart contracts may make it possible for 6G networks to conduct safe, effective, and automated service-level agreements and transactions. Scalability is a problem for current

blockchain technology, especially when dealing with high transaction volumes or real-time data transfers. Because blockchain technology is decentralized, governments and other organizations may find it difficult to monitor and regulate blockchain-enabled systems.

Numerous cutting-edge technologies will be included into 6G networks, each of which will add to previously unheard-of levels of intelligence, speed, and connectedness. Although these technologies have great potential, they also present a number of difficult scalability, security, cost, and complexity issues. It will take ongoing study, technological advancement, and cooperation between governmental, corporate, and academic entities to overcome these problems. The next wave of digital revolution and the realization of 6G's full potential depend on the successful adoption of these crucial technologies, as shown in Figure 4.5.

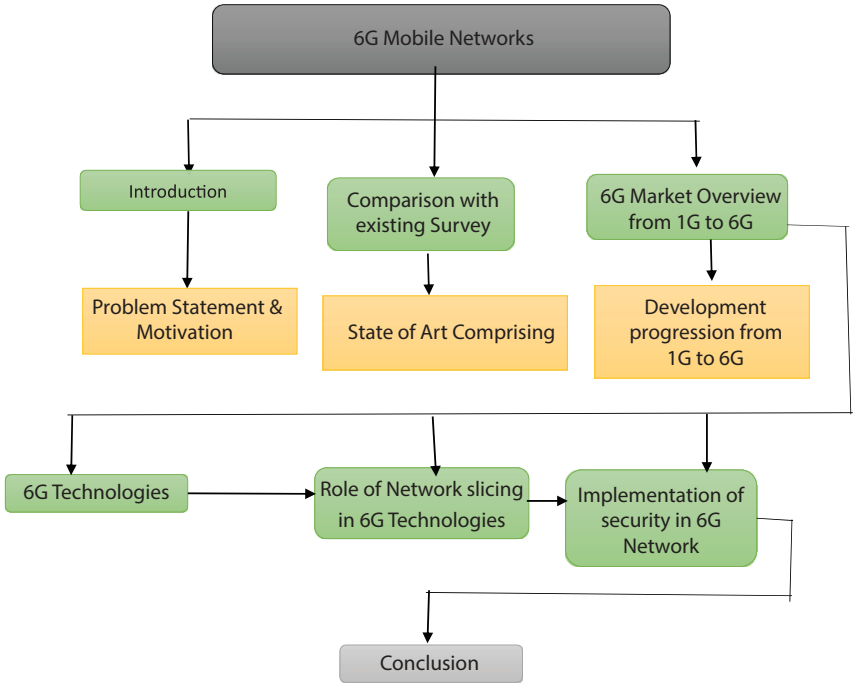

Figure 4.5 Key technologies in 6G mobile networks.

4.6 Upcoming Research Issues in 6G Technologies

Network technology is always changing, resulting in new and interesting applications. Even though 6G networks will still use several applications from previous network generations, the technology covered in Section 4.5 has a bright future. We will discuss these possible developments as well as the challenges that scientists are currently working to solve in this section as shown in Figure 4.6.

1) Applications of multisensory XR

However, Dang *et al.* [37] emphasize that greater focus has to be placed on the security, privacy, and secrecy of eMBB. Likewise, a 3D model of privacy risks in extended reality (XR) apps is described by Yamakami *et al.* [50] as a guide for the problems that need to be investigated by researchers. Additionally, Pilz *et al.* [1] point out that, in order to safeguard internal security, multisensory XR apps might regulate the verticals themselves.

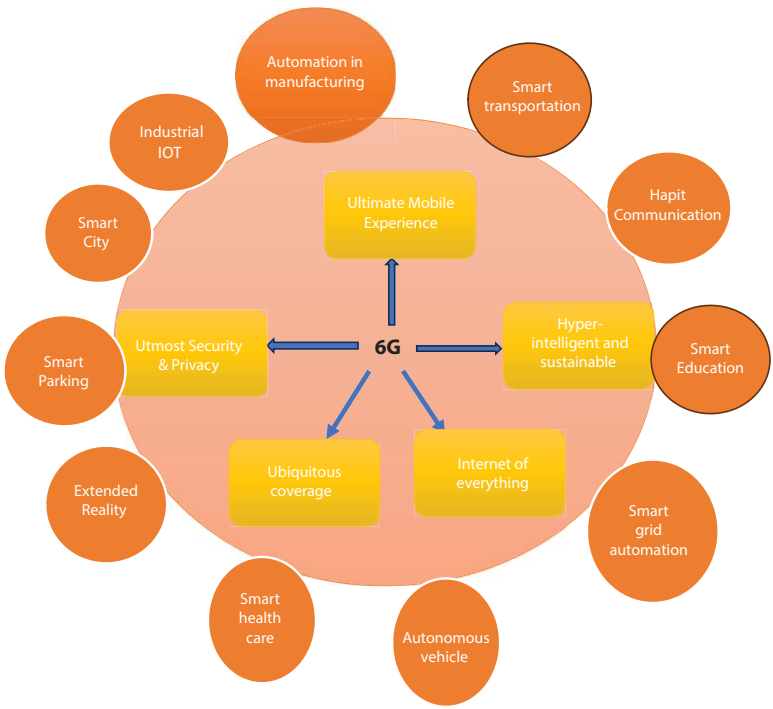

Figure 4.6 Upcoming issues in 6G technologies.

2) Autonomous Systems and Connected Robots

"Industry4.0," which refers to lowering human intervention in industrial processes through the use of automated control systems, is a concept discussed by Strianti *et al.* [34]. Additionally, these writers envisioned an automated factory that could manage a complete system's resource control, computations, caching, and communications automatically. The automated factory in this scenario is a fully autonomous system, equipped not just with actuators and mobile inspectors, but also with cloud services, databases, and UAV networks. These two applications' security and privacy concerns are covered separately below. But these systems are equally subject to some assaults. Li *et al.* [52] point out that UAV network management and control is done by software-defined networking (SDN) controllers are simple targets. A Tiro opponent may employ the WIFI-based attack. According to Fotouhi *et al.* [51], autonomous drone systems are susceptible to Denial of Service attack (DoS) assaults, spoofing attacks, hijacking attacks, and eavesdropping attacks. Consequently, relevant security safeguards must be in place.

3) Wireless Brain-Computer Connections

Over the course of two decades of study and development, wireless brain-computer interface (BCI), while not a new idea, has improved. The core idea of wireless BCI is the creation of a connection between the brain and an apparatus. The device might be inside, like the visual cortex, or external, like an artificial leg. This technique typically consists of four stages: signal capture, feature translation, feature extraction, and feedback. Until recently, helping the disabled utilize assistive technology was the main purpose of wireless brain stimulation (BCI) in the medical industry. However, Chen and colleagues [55] represented a new method for BCI in 2015 developed to use brain impulses to accelerate spelling.

4) Blockchain Technology and Distributed Ledgers

Blockchain technology is expected to be utilized for spectrum and data sharing, greatly boosting the security of 6G networks, as it exchanges data with all relevant stakeholders [24]. Some of these problems are still quite dangerous, though. Three categories of malevolent behavior attacks are listed by Nguyen *et al.* [58]: double-spending, transaction privacy leakage, and most vulnerability attacks. Additionally, they suggest a number of blockchain-based fixes, including incentive schemes and encryption algorithms, to address these problems in 6G networks.

4.7 Solutions of 6G Technological Issues

6G technology, expected to succeed 5G around 2030, presents numerous technological challenges. However, researchers and industries are actively working on solutions to address these issues. Below are some of the key challenges and their potential solutions:

1) Energy Efficiency
High-frequency 6G networks may require more power to operate, leading to greater energy consumption. Which improves battery technology and the creation of transmission protocols and hardware that use less energy. Techniques like energy harvesting from the environment (solar, motion, etc.) and AI-driven power management can help reduce power consumption.

2) Hardware Limitations
6G will rely on advanced hardware, such as THz transceivers, that currently face technological limitations. Materials science research is being done to create new semiconductors and components based on nanotechnology that can withstand extremely high frequencies with little power loss. Photonic devices are also being explored to improve data transmission efficiency.

3) Latency and Reliability
High reliability is required for critical applications like autonomous vehicles and remote surgeries. Use of edge, utilizing edge computing reduces latency by processing data closer to the source. To cut down on latency, AI and ML can further optimize data routing.

4) Security and Privacy
With more connected devices and higher data transmission rates, 6G networks will be more vulnerable to cyberattacks. Integration of quantum cryptography for unbreakable encryption, AI-based anomaly detection for real-time threat identification, and decentralized security models like blockchain to ensure data integrity.

5) Cost of Infrastructure
The deployment of 6G infrastructure, particularly in rural and underserved areas, can be prohibitively expensive. Using a network sharing approach in which several operators share a single piece of infrastructure. Satellite-based networks and integration of NTNs can also help extend coverage to remote areas.

6) Interoperability with Legacy Networks
6G will need to co-exist with 4G and 5G networks during the transition period. Network architecture that is backwards compatible and allows for smooth transitions between various network generations. SDN and network function virtualization (NFV) can facilitate easier integration across network types.

7) Sustainability and Environmental Impact
The environmental footprint of 6G infrastructure could be significant due to energy usage and materials. 6G networks will be powered by renewable energy sources, energy efficiency, and the use of sustainable materials in hardware manufacturing. Governments and industries may also work on carbon offset initiatives for 6G deployments.

8) Device Connectivity Density
Challenge: 6G networks will need to support a massive number of connected devices, far more than 5G.
Solution: Advanced multiple access techniques, such as Non-Orthogonal Multiple Access, can improve connectivity by enabling more devices to share the same resources. Intelligent beamforming and multiple-input, multiple-output antennas will enhance connection reliability and density.

By addressing these technological issues, 6G has the potential to revolutionize industries, enable new services like holographic communications, and support highly connected environments.

4.8 Conclusion

As 5G network development nears completion and is ready for deployment, researchers are starting to concentrate more on 6G networks. The 6G network will undoubtedly function better than earlier versions. As 6G technology evolves, it promises unprecedented advancements in communication speed, latency, and connectivity, opening doors to transformative applications such as holographic communication, immersive virtual environments, and autonomous systems. However, these benefits come with significant security and technological challenges. Security remains a critical concern, as 6G networks will introduce more devices, increased data traffic, and greater reliance on wireless communications. Emerging threats, such as advanced cyberattacks, data breaches, and privacy invasions,

will require robust security solutions, including quantum cryptography, AI-driven threat detection, and blockchain for decentralized security.

Challenges like spectrum management, energy efficiency, and infrastructure costs must be addressed to ensure seamless global deployment. Solutions such as advanced spectrum sharing, energy-efficient designs, and edge computing will help mitigate these challenges. Additionally, interoperability with legacy networks will be crucial during the transition period to 6G, requiring a balanced approach to innovation and backward compatibility. In summary, although 6G holds tremendous potential, overcoming its security risks and technological hurdles will be essential to unlocking its full capabilities. Collaboration among governments, industry leaders, and researchers will be key in building a secure, efficient, and inclusive 6G future.

References

1. Yang, P., Xiao, Y., Xiao, M., Li, S., 6g wireless communications: vision and potential techniques. *IEEE Netw.*, 33, 4, 70–75, 2019.
2. Letaief, K.B., Chen, W., Shi, Y., Zhang, J., Zhang, Y.-J.A., The roadmap to 6g: Ai empowered wireless networks. *IEEE Commun. Mag.*, 57, 8, 84–90, 2019.
3. Zhu, Tianqing, *et al.,* Differentially private model publishing in cyber physical systems. *Future Gener. Comput. Syst.,* 108, 1297–1306, 2020.
4. Chandra, P., Bensky, D., Bradley, T., Hurley, C., Rackley, S.A., Rittinghouse, J., Ransome, J.F., Cism, C., Stapko, T., Stefanek, G.L., *et al.*, *Wireless Security: Know it All*, Newnes, 2011.
5. Milovanovic, Dragorad A., Zoran S. Bojkovic, and Tulsi Pawan Fowdur. 5G-Advanced Mobile Communication: New Concepts and Research Challenges. *Driving 5G Mobile Communications with Artificial Intelligence towards 6G,* 3–81, 2023.
6. Gupta, L., Jain, R., Vaszkun, G., Survey of important issues in uav communication networks. *IEEE Commun. Surv. Tutor.*, 18, 2, 1123–1152, 2015.
7. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in renewable energy harvesting for EV charging infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 75–90, IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.
8. Brookson, C., Gsm security: a description of the reasons for security and the techniques. *IEEE Colloquium on Security and Cryptography Applications to Radio Systems*, 1994.
9. Gindraux, S., From 2G to 3G: a guide to mobile security. *Third International Conference on 3G Mobile Communication Technologies*, IET, pp. 308–311, 2002.
10. Cattaneo, G., De Maio, G., Petrillo, U.F., Security issues and attacks on the gsm standard: a review. *J. UCS*, 19, 16, 2437–2452, 2013.

11. Toorani, M. and Beheshti, A., Solutions to the gsm security weaknesses. *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, IEEE, pp. 576–581, 2008.
12. Gupta, M., Singh, M., Sharma, A., Sukhija, N., Aggarwal, P., Jain, P., Unification of machine learning and blockchain technology in the healthcare industry, in: *Institution of Engineering and Technology eBooks*, pp. 185–206, 2023, https://doi.org/10.1049/pbhe041e_ch6.
13. Sharma, P., Evolution of mobile wireless communication networks-1g to 5g as well as future prospective of next generation communication network. *Int. J. Comput. Sci. Mob. Comput.*, 2, 8, 47–53, 2013.
14. Saxena, P., Jain, P., Aggarwal, P., Singh, M., Goel, S., Batra, M., Communication requirements and performance metrics for electric vehicle charging: A comprehensive review, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 15–30, IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch002.
15. Cao, J., Ma, M., Li, H., Zhang, Y., Luo, Z., A survey on security aspects for lte and lte-a networks. *IEEE Commun. Surv. Tutor.*, 16, 1, 283–302, 2013.
16. Seddigh, N., Nandy, B., Makkar, R., Beaumont, J.-F., Security advances and challenges in 4g wireless networks. *2010 Eighth International Conference on Privacy, Security and Trust*, IEEE, pp. 62–71, 2010.
17. Mitra, R.N. and Agrawal, D.P., 5g mobile technology: a survey. *ICT Express*, 1, 3, 132–137, 2015.
18. Panwar, N., Sharma, S., Singh, A.K., A survey on 5g: the next generation of mobile communication. *Phys. Commun.*, 18, 64–84, 2016.
19. Jaber, M., Imran, M.A., Tafazolli, R., Tukmanov, A., 5g backhaul challenges and emerging research directions: a survey. *IEEE Access*, 4, 1743–1766, 2016.
20. Prados-Garzon, J., Adamuz-Hinojosa, O., Ameigeiras, P., Ramos-Munoz, J.J., Andres-Maldonado, P., Lopez-Soler, J.M., Handover implementation in a 5g sdn-based mobile network architecture. *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, IEEE, pp. 1–6, 2016.
21. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-Based wireless sensor network, pp. 121–141, CRC Press eBooks, 2024, https://doi.org/10.1201/9781003432869-8.
22. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., Edge Computing-Based design for IoT security, pp. 298–309, Chapman and Hall/CRC eBooks, 2024, https://doi.org/10.1201/9781003405535-22.
23. Bisson, P. and Waryet, J., 5G Ppp Phase1 Security Landscape, 5G PPP Security Group White Chapter.
24. Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., Ylianttila, M., Security for 5G and beyond. *IEEE Commun. Surv. Tutor.*, 21, 4, 3682–3722, 2019.

25. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., IoT and blockchain technology in 5G smart healthcare, pp. 137–161, Elsevier eBooks, 2022a, https://doi.org/10.1016/b978-0-323-90615-9.00004-9.
26. Singh, M., Sukhija, N., Sharma, A., Gupta, M., Aggarwal, P., Security and privacy requirements for IOMT-Based Smart Healthcare System, pp. 17–37, CRC Press eBooks, 2021, https://doi.org/10.1201/9781003032328-2.
27. Latva-aho, M. and Leppanen, K., Key Drivers and Research Chal-¨ Lenges for 6g Ubiquitous Wireless Intelligence (White Chapter), 6G Flagship Research Program, University of Oulu, Finland.
28. Kibria, M.G., Nguyen, K., Villardi, G.P., Zhao, O., Ishizu, K., Kojima, F., Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. *IEEE Access*, 6, 32328–32338, 2018.
29. Tariq, F., Khandaker, M., Wong, K.-K., Imran, M., Bennis, M., Debbah, M., A Speculative Study on 6g, arXiv Preprint arXiv:1902.06700.
30. Tang, Fengxiao, *et al.*, Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. *Proceedings of the IEEE,* 108, 2, 292–307, 2019.
31. Makar, K., Goel, S., Kaur, P., Singh, M., Jain, P., Aggarwal, P.K., Reliability of Mobile Applications: A Review and Some Perspectives. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, pp. 1–4, 2021, doi: 10.1109/ICRITO51393.2021.9596350.
32. McMahan, H.B., Moore, E., Ramage, D., Hampson, S., *et al.*, Communication-efficient learning of deep networks from decentralized data, *arXiv Preprint arXiv:1602.05629*.
33. Loven, L., Lepp´ anen, T., Peltonen, E., Partala, J., Harjula, E., Porambage, P., Ylianttila, M., Riekki, J., Edge Ai: A vision for distributed, edge-native artificial intelligence in future 6g networks. *The 1st 6G Wireless Summit*, pp. 1–2, 2019.
34. Strinati, E.C., Barbarossa, S., Gonzalez-Jimenez, J.L., Ktenas, D., Cassiau, N., Dehos, C., 6g: the Next Frontier, arXiv´ Preprint arXiv:1901.03239.
35. Gui, Guan, *et al.*, 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.,* 27, 5, 126–132, 2020.
36. Jiang, C., Zhang, H., Ren, Y., Han, Z., Chen, K.-C., Hanzo, L., Machine learning paradigms for next-generation wireless networks. *IEEE Wirel. Commun.*, 24, 2, 98–105, 2016.
37. Dang, S., Amin, O., Shihada, B., Alouini, M.-S., What should 6g be? *Nat. Electron.*, 3, 1, 20–29, 2020.
38. Saad, Walid, Mehdi Bennis, and Mingzhe Chen. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Netw.,* 34, 3, 134–142, 2019.
39. Katz, M., Pirinen, P., Posti, H., Towards 6g: getting ready for the next decade. *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, IEEE, pp. 714–718, 2019.

40. Wei, Y., Liu, H., Ma, J., Zhao, Y., Lu, H., He, G., Global voice chat over short message service of beidou navigation system. *2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, IEEE, pp. 1994–1997, 2019.
41. Yao, H., Wang, L., Wang, X., Lu, Z., Liu, Y., The space-terrestrial integrated network: an overview. *IEEE Commun. Mag.*, 56, 9, 178–185, 2018.
42. Zeng, Y., Zhang, R., Lim, T.J., Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Commun. Mag.*, 54, 5, 36–42, 2016.
43. Chen, X., Li, C., Wang, D., Wen, S., Zhang, J., Nepal, S., Xiang, Y., Ren, K., Android hiv: a study of repackaging malware for evading machine-learning detection. *IEEE Trans. Inf. Forensics Secur.*, 15, 987–1001, 2019.
44. Grimmett, D.J., Message routing criteria for undersea acoustic communication networks. *OCEANS 2007-Europe*, IEEE, pp. 1–6, 2007.
45. Sattiraju, R., Weinand, A., Schotten, H.D., Ai-assisted Phy Technologies for 6g and beyond Wireless Networks, arXiv Preprint arXiv:1908.09523.
46. Tao, H., Liu, C., Kadoch, M., Machine learning based antenna design for physical layer security in ambient backscatter communications. *Wirel. Commun. Mob. Comput*., 2019, 1, 4870656, 2019.
47. Nawaz, S.J., Sharma, S.K., Wyne, S., Patwary, M.N., Asaduzzaman, M., Quantum machine learning for 6g communication networks: state-of-the-art and vision for the fu-ture. *IEEE Access*, 7, 46317–46350, 2019.
48. Farsad, N., Yilmaz, H.B., Eckford, A., Chae, C.-B., Guo, W., A comprehensive survey of recent advancements in molecular communication. *IEEE Commun. Surv. Tutor.*, 18, 3, 1887–1919, 2016.
49. Lu, Y., Higgins, M.D., Leeson, M.S., Comparison of channel coding schemes for molecular communications systems. *IEEE Trans. Commun.*, 63, 11, 3991–4001, 2015.
50. Loscri, V., Marchal, C., Mitton, N., Fortino, G., Vasilakos, A.V., Security and privacy in molecular communication and networking: opportunities and challenges. *IEEE Trans. Nano Biosci.*, 13, 3, 198–207, 2014.
51. Hu, J.-Y., *et al*., Experimental quantum secure direct communication with single photons. *Light: Science & Applications,* 5, 9, e16144–e16144, 2016.
52. Kiyomoto, S., Basu, A., Rahman, M.S., Ruj, S., On blockchain-based authorization architecture for beyond-5g mobile services. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, pp. 136–141, 2017.
53. Kotobi, K. and Bilen, S.G., Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Veh. Technol. Mag.*, 13, 1, 32–39, 2018.
54. Ferraro, P., King, C., Shorten, R., Distributed ledger technology for smart cities, the sharing economy, and social compliance. *IEEE Access*, 6, 62728–62746, 2018.
55. Akyildiz, I.F., Jornet, J.M., Han, C., Terahertz band: next frontier for wireless communications. *Phys. Commun.*, 12, 16–32, 2014.

56. Ma, J., Shrestha, R., Adelberg, J., Yeh, C.-Y., Hossain, Z., Knightly, E., Jornet, J.M., Mittleman, D.M., Security and eavesdropping in terahertz wireless links. *Nature*, 563, 7729, 89–93, 2018.
57. Ucar, S., Coleri Ergen, S., Ozkasap, O., Tsonev, D., Burchardt, H., Secvlc: secure visible light communication for military vehicular networks. *Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access*, pp. 123–129, 2016.
58. Cho, S., Chen, G., Coon, J.P., Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems. *IEEE Trans. Inf. Forensics Secur.*, 14, 10, 2633–2648, 2019.

5

Adaptive Security Protocols for Dynamic 6G Environments

Pranshu Saxena[1], Mandeep Singh[1], Vikas Tyagi[3]* and Sanjay Kumar Singh[2]

[1]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
[2]University School of Automation & Robotics, Guru Gobind Singh Indraprastha University, East Delhi Campus, Delhi, India
[3]School of Computer Science Engineering, Galgotias University, Greater Noida, India

Abstract

This paper focuses on adaptive security protocols to secure sixth-generation (6G) networks and explains how the current and potential progressions may overcome unique challenges for securing the new next-generation technology. In its ability to offer unprecedented connectivity, speed, and integration with technologies such as artificial intelligence (AI), Internet of Things, and edge computing, 6G calls for more complex and dynamic environments than those traditionally dealt with by security models. It deals with proactive resilience at every level of 6G in terms of scale and complexity, designed by AI-driven threat detection, quantum-resistant encryption, and decentralized architectures. Multidimensional issues that include multi-layered security, context-aware protocols, and zero-trust models create protection against advanced cyberattacks as a comprehensive system and highlight the ethical and privacy considerations of monitoring data for automation in adaptive security architecture. It demands greater research and international standardization. In fact, it points out the need for adaptive security to offer a basis of a secure, resilient, and privacy-aware platform for 6G. Real-time threat anticipation as well as autonomous response capability in adaptive security will be the key for securing future digital landscapes.

***Keywords*:** Adaptive security protocols, 6G network security, quantum-resistant encryption, AI-driven threat detection, zero-trust architecture, context-aware security, self-healing networks

**Corresponding author*: itengg.vikas@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (107–128) © 2026 Scrivener Publishing LLC

5.1 Introduction

In many ways, it is incredible that the journey from third generation (3G) to sixth generation (6G) has been due to the acceleration of connectivity, speed, and capabilities transforming communication and interaction with digital technology.

Third generation (3G): The 3G technology was released in the early 2000s. It gave mobile internet access at much higher speed than the preceding generations, which made it possible to use essential data services like web browsing and multimedia applications on mobile devices. It supported speed up to 2 Mbps, and email, simple streaming, and web browsing were achievable [1]. Fourth generation (4G): Building on 3G, 4G was introduced around 2010 and increased data speed significantly, reaching up to 100 Mbps for mobile use and even faster in stationary conditions. 4G brought in the era of high-definition video streaming, advanced mobile applications, and low-latency communication, which made innovations like mobile HD video calls and cloud-based services possible. Fifth generation (5G): Currently, 5G is revolutionizing connectivity with ultra-low latency as low as 1 ms up to 10 Gbps and supporting massive Internet-of-Things (IoT) connectivity [2, 3]. This generation introduced network slicing, massive Multiple Input Multiple Output (MIMO), and edge computing, supporting high-demand applications such as autonomous vehicles, smart cities, and augmented reality/virtual reality (AR/VR). Finally, the 6G, set to be reached in the 2030s, is going to provide speed in the 100 Gbps to 1 Tbps, latency microsecond range, with virtually instantaneous communication [4]. It shall extend beyond the capabilities of 5G IoT

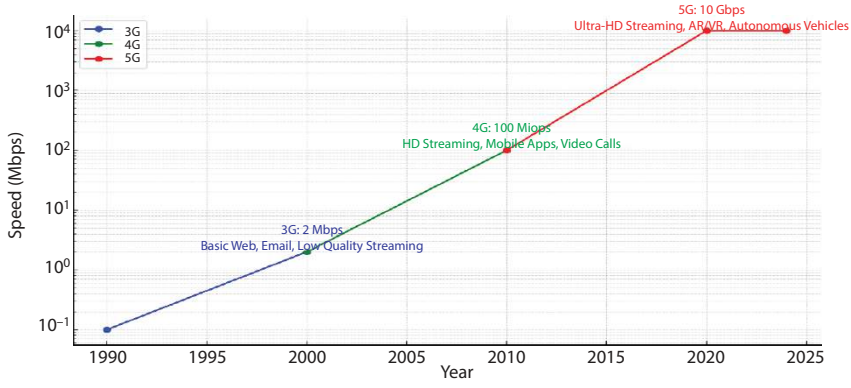

Figure 5.1 Journey of network evolution from 3G to 5G (1990–2024).

and reach breakthroughs in artificial intelligence (AI)–driven networks, quantum communication, and real-time holographic applications (Figure 5.1). It is a form of evolution that enables fully immersive extended reality, remote surgery, and interconnected, self-optimizing innovation ecosystems on a scale previously not possible, thus achieving unparalleled connectivity and digital integration in everyday life.

5.1.1 Emerging Security Challenges in 6G Technology

It represents transformative change in terms of the speed of such networks, connectivity, and technology integration into these 6G networks that make the security dynamic in nature and challenging (Figure 5.2). In this network, the handling of a huge amount of data can be done online, which can be transmitted through a rate up to 1 Tbps [5]. Seamless streaming of big data generates effective working in each sector. However, that also comes with vulnerability issues with respect to more mature cyber threats such as Distributed Denial of Service (DDoS) attacks, which overwhelm the network defenses with amounts of data of a different paradigm [6]. Furthermore, 6G will bring forth and support a never-seen-before density of connected entities such as IoT, sensor devices, and edge-based devices, creating a tremendous attack surface [7]. Even small vulnerabilities in these devices can compromise entire networks, especially in critical sectors such as healthcare, transportation, and smart cities, whose overall security depends on securing all devices across different kinds of environments.

AI will comprise a substantial part of 6G networks, thereby offering for intelligent management, predictive maintenance, and security monitoring. However, the increased reliance on AI brings in security risks that come with AI [8]. For example, an adverse attack can cause much damage

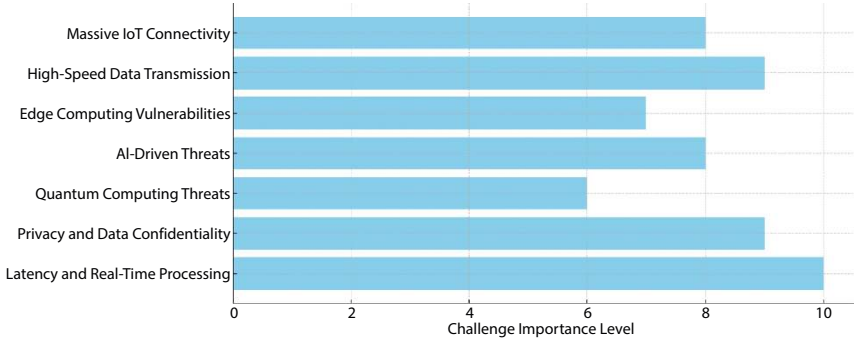

Figure 5.2 Emerging challenges in 6G technology.

if AI models embedded into network management are compromised. Such adverse attacks either cheat AI algorithms or data through poisoning attacks. Moreover, 6G will use edge computing in an effort to minimize latency, which is important for applications such as autonomous driving and remote surgery. The diffusion of processing power across devices used for edge computing increases the number of potential entry points for attacks, thus requiring stronger security controls to protect data integrity and prevent unauthorized access in these decentralized locations.

As the abilities of quantum computing advance, the new 6G networks should be prepared for such possible threats to traditional encryption, and, thus, the development of quantum-resistant security frameworks will become inevitable. This, aside from new privacy concerns that rise with the increased data for services like immersive AR and human–machine interactions, points out the need for good techniques of encryption and anonymization of data. Needless to say, all of this creates a huge need to implement adaptive, multi-layered security frameworks within the network of 6G while utilizing zero-trust architecture to continuously verify the user identity and permissions with the aid of AI-based threat detection to respond to evolving risks [9]. A proactive resilient approach to security in the current landscape will ensure 6G networks are safe and trusted.

5.1.2 Need for Adaptive Security

In the dynamic environment of 6G networks, with its vast scale, velocity, and complexity, such traditional static security protocols are very inadequate. Static protocols simply rely on predefined rules or signatures, which cannot stay abreast of the state-of-the-art sophistication of current cyber threats or respond well to the unique demands made by 6G in terms of high-speed as well as highly connected ecological demands [10]. As 6G integrates emerging technologies such as AI, IoT, and edge computing, it sees a significantly larger and constantly evolving attack surface where threats could arise in real time and change accordingly. This, therefore, poses an urgent need for adaptive security—a very fluid approach that would continuously be modified and strengthened to meet the most current threat landscape. Adaptive security uses AI and machine learning (ML) to identify anomalies, predict attacks, and respond proactively to emerging threats rather than relying on fixed defenses that sophisticated attackers can easily bypass. It is a method that helps the network remain resilient with regard to new attack vectors that arise and changes in behavior from devices, user patterns, and data flows, which maintain a robust security posture despite unpredictable cyber risks.

5.2 Overview of Security Challenges in 6G

6G networks introduce new security challenges, such as the massive proliferation of IoT devices, AI-based threats, and vulnerabilities caused by edge computing. Advanced adaptive security controls are, therefore, needed to protect complex, distributed attack surfaces [11, 12].

5.2.1 New Attack Vectors

The advent of 6G brings in new attack surfaces, increasing security challenges and requiring new protective strategies. With the massive proliferation of IoT devices, billions of sensors, smart appliances, and wearable devices would be connected through 6G networks, and any of them could be a pathway for cyber threats [13]. This highly dense network will open further possibilities of coordinated attacks wherein even one compromised IoT device can cause a cascade effect of vulnerabilities across interconnected systems. Moreover, the large-scale adoption of AI and ML in 6G networks is a double-edged sword as it enhances automated defenses; on the other hand, these can also be weaponized by the attackers. The adversary AI and data poisoning attacks can manipulate or mislead the critical ML models in the network security. In addition, decentralizing the processing using edge computing, which is a core aspect of 6G, aims to reduce latency [14, 15]. But such exposure of data outside the central security controls can be intercepted, tampered with, or accessed illegally for each node whether it is a smart city sensor, an autonomous vehicle, or a healthcare device. These emerging attack vectors indicate the need for an adaptive and holistic security framework that addresses the distributed as well as intelligent nature of 6G networks [16].

5.2.2 Privacy and Confidentiality

On the other hand, millions of IoT connections with all-time data exchange will throw significant concerns in 6G networks about user confidentiality and data confidentiality. That is, 6G networks will process unimaginably huge amounts of sensitive data coming from billions of devices in their lifetimes—smart homes and wearable health monitors. Such data typically comprise of confidential personal and location-based details, which can easily be intercepted, accessed without the authorized permission, or abused if not suitably safeguarded in 6G networks. The need to process data closer to the user in 6G due to real-time analytics, AI, and edge computing is going to expose more data to potential breaches [17]. With constant connectivity that maintains the flow of data across various devices, applications, and networks, it becomes tougher

to guarantee information is end-to-end secured [18]. Networks need to use advanced encryption methods, anonymize data, and impose strict access controls on user data. Transparency in policies about collection and usage of data and mechanisms for informed consent by users would, therefore, be crucial in this very connected ecosystem for generating trust and ensuring privacy [19].

5.2.3 Latency and Real-Time Processing

The most distinctive feature of 6G is low latency, being in the millisecond or almost instantaneous transmission times [20]. The 6G will, therefore, contribute to real-time processing-based application areas, such as vehicles, surgery, and the immersive experiences of AR and VR. Any delay, even small delay, will, thus, mean the serious failure and, hence, harm the safety effectiveness as well as user experiences [21]. This aspect calls upon the requirement of the tough yet agile security of the 6G that does not increase delays in processing malice and malicious actions at the processing level. Old security protocols that are so time-consuming may stall data flow, which cannot be tolerated for latency-sensitive applications. For this, 6G security has to depend on lightweight encryption methods, decentralized threat detection, and AI-based real-time anomaly detection. Adaptive and proactive security approaches like behavior-based threat detection at the edge will be able to ensure high security with speed without any compromise but balance protection and performance in such a way that 6G provides low-latency experiences that are both secure and seamless.

5.3 Core Concepts in Adaptive Security Protocols

Adaptive security protocols are dynamic systems that detect, respond, and evolve in real-time to emerging threats. Not like traditional security protocols with predefined rules, adaptive security uses real-time threat intelligence to adjust defences about new vulnerabilities and attack patterns. This approach relies on analytics, ML, and behavioral monitoring to identify anomalies and potential threats as they occur. Such protocols have been designed in the direction to respond appropriately and effectively toward sophisticated attacks and threats. Adaptive security anticipates the future threats, learns with every interaction, develops defenses, and keeps evolving to ensure resilience of the network [22]. Therefore, even before these threats can degrade the integrity of the network, adaptive security could counter the threats ahead. Thus, it is well suitable for this 6G complex, high-speed environment, beyond the reach of such outdated and static defenses [23].

The future of threat detection would likely rely on ML, where the application of the ML algorithms to security will enable adaptive systems that look at network patterns and behavior, detect anomalies, and even predict when potential threats are likely to arise. These algorithms have to learn normal network behavior patterns, varying from device, user, and application contexts. This baseline can then be used to detect the deviations, for example, uncharacteristic data transfers, logins from unknown places, or irregular device activities that may indicate a possible threat. The biggest advantage when ML is used in the detection of threats is its ability to detect subtle patterns, which might be evaded by traditional security systems. For example, it can detect multi-stage attacks, where the attacker may infiltrate a system over time, showing low activity to avoid being noticed. ML can alert the security systems to this gradual yet unusual behavior early in the process so that the security systems can respond before an attack gets too far along. Further, ML algorithms use predictive analytics to analyze the chances of future attacks by current data. These models of ML can identify directions that potential vulnerabilities may take. By analyzing trends in attempted intrusions or suspicious activities, the system can report areas of the network that are potentially at risk, enabling proactive threat mitigation. In predictive terms, this gives a chance for adaptive security systems to pre-empt, therefore making them stronger in the sense of countering emerging new threats that pop up now and then. Generally, learning, adapting, and predicting features of ML capabilities found it to make the network secure for 6G [24].

5.3.1 Multi-Layered Security

In 6G networks, a multi-layered security approach is essential due to the interconnected and distributed nature of devices, applications, and networks. With billions of endpoints, a single layer of security is insufficient to protect the vast and complex 6G ecosystem. Instead, a layered approach provides comprehensive coverage by addressing security at multiple levels: endpoints, networks, and applications [25].

A) Endpoint Security (Devices, Sensors): In a 6G network, billions of endpoints—including IoT devices, sensors, and personal devices—are constantly exchanging data. These endpoints are often vulnerable to tampering, malware, and unauthorized access, especially if they lack sufficient built-in security [26]. Endpoint security ensures that each device is protected, typically through device authentication, firmware updates, and secure configurations, to prevent compromised devices from becoming entry points for cyber threats.

B) Network-Level Security (Authentication and Data Encryption): Network-level security is the foundation for secure communication across the 6G infrastructure. Authentication protocols ensure that only authorized devices and users can access network resources, preventing unauthorized entry [27]. Data encryption protects the integrity and confidentiality of data as it travels across the network, safeguarding it from interception or tampering by malicious actors [28]. In a 6G environment, where data flows constantly and at high speed, robust network-level security is vital for maintaining secure, uninterrupted connectivity.

C) Application-Layer Security: Applications in 6G networks manage sensitive data and provide critical functions, especially with the rise of smart cities, autonomous systems, and health monitoring applications. Application-layer security protects data at its highest level, securing access to applications through methods like multi-factor authentication, role-based access control, and data privacy protocols [23]. This layer ensures that sensitive information remains confidential within the application, protecting it from unauthorized access or data leaks.

By implementing security at each of these layers, 6G networks can create a comprehensive, resilient defense against cyber threats. A multi-layered approach ensures that even if one layer is compromised, other layers continue to protect the network, reducing the risk of a widespread breach and maintaining robust security across all points of data exchange [26].

5.3.2 Proactive Defense Mechanisms

Consequently, proactive defense mechanisms are paramount when combating the rapidly evolving cyber threats in 6G networks. Predictive analytics, as well as automated response mechanisms, form the bedrock of this adaptive proactive strategy [29]. Predictive analytics analyze historical and real-time data to identify trends and patterns and early indicators that can be associated with new or emerging threats. The data is now processed *via* ML algorithms and thus enables predictive models to estimate probabilities of a particular attack vector: maybe unauthorized access attempts or possibly data exfiltration [26]. This permits security teams to prepare themselves and harden their defenses against possible threats even before such threats are fully manifested in the complex 6G landscape characterized by high speed of data and wide connectivity [30].

This completes the circle of responses in the sense that how responses can be offered immediately. Automated responses have provided instant reactions to emerging threats when such behaviors are identified-login

abnormalities, data transfer spikes, or network activities going beyond the standard patterns [31]. This may be done by cutting off infected devices, cutting off suspected IP addresses or restricting access to sensitive resources with minimal scope and impact such that this attack can occur. The integration of predictive analytics into automated response functions can be used in order to construct a proactive defence in 6G with the minimized vulnerabilities and high-speed responses, thus becoming a much more feasible proposition at the demand for high-speed high connectivity [32]. This adaptive proactive approach enhances network resilience by preventing damage before a particular attack is executed, thereby giving a stable base for advanced applications that would be built on the base of 6G.

5.4 Adaptive Security Frameworks for 6G

Adaptive security frameworks for 6G include real-time threat detection, self-healing, and continuous verification of threats as they continue to evolve in nature. It relies on AI and decentralized architecture for implementing a dynamic response for protecting this complex environment of 6G.

5.4.1 Self-Healing Networks

Self-healing capabilities in 6G networks introduce adaptive security frameworks that allow the network to autonomously detect, respond to, and recover from cyberattacks, which reduces downtime and disruption [33]. The self-healing network can use AI and machine learning to continuously monitor for unusual activities and identify vulnerabilities in real-time across the network. Adaptive protocols can automatically start recovery actions, isolate the affected components and redirect data to continue service should an attack be detected—such as a data breach, malware infiltration, or unauthorized device access [34].

Advanced diagnostics in self-healing networks assess the extent of damage and determine appropriate remedial measures to restore secure functionality. In the case where, for instance, one's IoT or edge node device is under attack, in such networks, this might be shut off, tested by security for patches, etc., after which all measures are followed to enable proper working without any potential insecurity. Adaptive algorithms, meanwhile, can adapt the security protocols of the entire network based on insights learned from the incident. It learns from the attack so that it will not happen again in the future. The proactive, learning-based adaptation is the key to making a resilient network that can handle security threats and improves continuously in response to them [35].

The self-healing nature of 6G networks reduces the level of manual intervention, an important aspect in high-speed, high-density environments in which human response alone is too slow. Self-healing networks automatically detect and contain the damage and subsequently remediate the problem, resulting in minimal service interruption and maintaining security and performance during complex cyber threats. This autonomous process of recovery forms the base of adaptive security frameworks within 6G, thereby creating a more resilient and secure digital infrastructure.

5.4.2 Decentralized Security Architectures

Decentralized security architectures like blockchain and distributed ledgers would increase data integrity and resilience in 6G networks through trust distribution and single points of failure elimination. Centralized architectures have data flow through a central hub, which is susceptible to attack where the whole network could be compromised. In decentralized approaches, data and verification processes are spread out in an independent node network. This distribution is such that in case of compromise of one or more nodes, the whole network stays secure and intact [36].

An example of a tamper-proof ledger is blockchain, in which each entry, or "block," is chained to the previous one and verified by multiple nodes. This makes it virtually impossible to change previously made records without being detected. Thus, the integrity and transparency of the data remain. Similarly, distributed ledgers will provide a real-time consensus on data validity over multiple nodes; thus, only authenticated and verified transactions would be recorded [37]. To ensure the large-scale data exchanges between IoT devices and between other connected elements, large-scale 6G scenario would be assured of having robust solutions with blockchain and distributed ledgers regarding the authenticity and reliability of data.

Consequently, decentralized security architectures reduce exposure to large DDoS attacks, for example, which can cripple a legacy system. In 6G networks, decentralized approaches handle data automatically and securely across thousands of devices and endpoints [23]. In this respect, 6G networks provide scalable, resilient, and trust-based security models that are appropriate for highly complex, high-density settings.

5.4.3 Context-Aware Security

Context-aware security protocols are flexible systems that adjust their mode of security in response to contextual factors, including physical environment, user behavior, and device roles. Static methods of security apply

uniform protections to everything, whereas context-aware systems continuously assess the context under which each interaction is established to provide tailored security based upon the current conditions and those risks. For example, if such access of classified information came from a network that had secured an office, a person may just experience usual authentication processes [24]. However, if such attempt came from any other location or device that was not recognized by the security system, then they might end up undergoing multi-factor authentications check processes.

In 6G networks, context-aware security will be very important because there will be a wide range of devices and applications from autonomous vehicles to wearable health monitors, each with its specific security requirements [27]. These protocols analyze real-time data—such as location, device type, recent user behavior, and network conditions—to determine appropriate security responses. For instance, a public wireless network could be risky and would necessitate stronger encryption or limit some functionalities. On the other hand, an environment that is trusted could be characterized by low risks, such as having the functionality work more seamlessly to enhance the experience for users [26].

By adapting to situational factors, context-aware security would enable 6G networks to respond to emerging risks in real-time while keeping unnecessary security hurdles out of the way without sacrificing safety. It would be able to keep that delicate balance between user convenience and robust protection such that security would be dynamically aligned with the demands of the network as well as the context of the user [30].

5.4.4 Zero-Trust Model

A zero-trust security model is, therefore, a forward-looking approach to ensure the assurance of security in dynamically changing environments as that associated with 6G networks, by making continuous validation at every point of access and irrespective of a user's or a device's location. Within traditional security frameworks, usually, devices and users within a network perimeter are given some implicit trust after initial authentication. However, for the complex, high-speed, and highly distributed nature of 6G with billions of devices constantly in interaction, a perimeter-based approach is not enough, but rather zero trust "never trust, always verify." [1].

Zero trust will require authentication, authorization, and encryption for every access request from a device, user, or application in the 6G environment. It means checking the identity of the users requesting access, the health of devices, location, and other contextual factors. This can happen if a device is logging into an unknown place or out of the typical behavior and would

still deny access or request more steps to authenticate regardless of whatever its former status in the trusted one was. It protects the system against more complex types of attacks that come through insider threats, malware such as those moving sideways, and devices that may be compromised [2].

This makes zero trust a highly viable solution for 6G's fast and unpredictable environment. Using AI and ML, zero-trust protocols can learn from each interaction to enhance verification processes continuously, thus creating a responsive security framework that may adjust to evolving threats and network conditions. Through the use of zero trust, 6G networks ensure only that authorized and verified entities access resources, so breach risks and exposure of sensitive data to the vast and complex interconnected infrastructure are limited.

5.5 Implementation of Adaptive Security Protocols in 6G

Implementing adaptive security protocols in 6G will integrate AI-driven threat analytics, quantum-resistant encryption, and context-aware security measures. This would ensure that there is protection in real-time, integrity of data, and functionality without a glitch across the highly connected and latency-sensitive network [5].

5.5.1 6G-Specific Protocols and Standards

Briefly outline any of the current or emerging security protocols and standards that are specific to 6G environments. As the technology advances in 6G, security protocols and standards emerge that focus on the challenges of this high-speed, highly connected environment. This includes quantum-resistant encryption for protecting sensitive data from potential quantum-powered attacks that might break traditional encryption methods. This forward-looking approach provides the means for 6G to be secure and future-proof against any forthcoming computational threats. AI-driven security standards also represent another important aspect which would be to govern the employment of AI in adaptive security and threat detection. Integrity, transparency, and the resilience of AI models need to be ensured to give a guarantee of reliable, secure AI functionality across the applications in 6G. Other decentralized identity management frameworks, often blockchain or distributed ledger based, come to ensure the security of device identities and interactions without a central authority to reduce points of failure and enhance transparency [6].

With the pervasive nature of edge computing in 6G networks, security protocols at the network edge are being developed with the use of lightweight encryption and local anomaly detection to maintain integrity and confidentiality of data being processed at the edge of the network. Zero Trust Network Access (ZTNA) standards take a "never trust, always verify" approach by continuously authenticating and assessing every device and data request in real time. ZTNA has effectively secured the network against intrusion and lateral attacks by checking everything at every level before the access is granted. Now, all these newly engineered protocols and standards are all interrelated with each other particularly for 6G super-complex infrastructure in advance, preparing a very strong, adaptive, and secured framework toward supporting the next generation [8].

5.5.2 Challenges in Implementation

There are numerous challenges attached (Table 5.1) to the implementation of adaptive security in 6G networks. This is attributed to the strict computational needs and real-time processing requirements, which also present data privacy issues with the advanced technology. The first is the high need for computational requirements because adaptive security heavily relies on AI-driven analytics and ML models that require massive processing power and storage. Most of these calculations are real-time threat detection and behavioral analysis. This type of computation cannot be supported by any device, especially those devices that form the basis of IoT resources in 6G [9].

Another challenge is posed by real-time processing requirements. To enable latency-sensitive applications such as autonomous driving, remote healthcare, and immersive AR/VR, security protocols must almost immediately detect and respond to threats. To realize such precision and speed, high-performance infrastructure and low-latency communication through devices, edge nodes, and cloud systems are needed. This involves coordination of these elements to provide smooth, real-time protection over a vast network and is complex and resource-intensive, often requiring highly efficient, distributed architectures to meet such expectations without sacrificing network performance [10].

Data privacy is the other major issue. Adaptive security systems always collect and process huge amounts of user data to identify unusual behavior so that they can proactively respond to threats. Thus, such constant monitoring again raises the question of what happens to the data while it is stored, processed, and protected, with much of the data of personal or potentially sensitive types. It can be a very challenging task to maintain an equilibrium between good security provisions and strong privacy protections as such a network is designed to restrict unauthorized access to a

Table 5.1 List of challenges along with implications for 6G security.

Challenge	Description	Implications for 6G security
Scalability	Traditional security protocols struggle to scale with the increased number of connected devices in 6G.	Overloads security systems, making it challenging to protect all devices in real time
Latency	High latency in current security systems impedes the responsiveness needed in real-time applications.	Affects applications requiring ultra-low latency (e.g., autonomous vehicles and real-time health monitoring)
Computational overhead	Security protocols often demand substantial processing power, which strains mobile and IoT devices.	Limits effectiveness on resource-constrained devices in 6G environments
Decentralized security management	Lack of uniform control and oversight in distributed networks like IoT ecosystems creates security vulnerabilities.	Challenges implementing secure and cohesive protocols across diverse networks
Privacy and data confidentiality	Existing protocols may not adequately protect user privacy, especially with pervasive data sharing in 6G.	Increases risk of personal data leakage across connected devices and applications
Context-aware security adaptation	Current systems lack mechanisms to adjust security levels based on real-time context changes.	Necessary to dynamically adjust security for various use cases (e.g., urban vs. rural).
Interoperability	Compatibility issues arise between legacy systems and new, adaptive 6G technologies.	Makes seamless security implementation difficult across heterogeneous devices
Energy consumption	Traditional security mechanisms consume substantial energy, which impacts battery life on mobile devices.	Poses a challenge for IoT and wearable devices expected in 6G
AI and ML limitations	Machine learning–based security models face challenges like data bias, adversarial attacks, and model drift.	Risks the reliability of AI-driven threat detection in adaptive protocols

user's data and, at the same time, make sure data is accessed quite well for analysis purposes relating to the security level. Both demand innovative solutions together that are made efficient enough to support adaptive security in 6G without affecting its performance and user confidentiality [8].

5.6 Future Directions in Adaptive Security for 6G

Quantum-resistant encryption will provide a focus for adaptive security of 6G: predictive analytics powered by AI, which would help identify threats beforehand; federated learning training of AI models on-device will also provide greater privacy than the traditional, centralized method of data processing; and, in this sense, networks with self-healing capability will automatically identify threats and isolate and eliminate them from within, so maintaining a degree of resilience. Last but not least, standards on ethical AI usage to provide a basis for greater transparency and fairness when deploying AI-based security mechanisms. These advancements look to create a secure, adaptable, and privacy-conscious foundation for 6G's highly connected and complex environment.

Integration of Quantum Security: Discuss the opportunity that quantum encryption presents to improve the strength of 6G encryption against a threat at the quantum level. Quantum encryption is believed to be a promising solution that 6G networks would adopt to prevent threats from becoming strong enough to break even traditionally encrypted systems. Of course, quantum key distribution (QKD) will be one of the approaches that is most applicable; it ensures secure exchange through quantum mechanics principles of keys, where any attempted eavesdropping could become immediately detectable. In a 6G network, QKD can be used to distribute encryption keys among devices and infrastructure so that any intercept attempt is detected right away.

A future solution could be post-quantum cryptography—algorithms that have been designed precisely to withstand quantum attacks. Such algorithms could be embedded in 6G, thus protecting data at the device and network levels with superior security in sensitive information. Hybrid models that integrate quantum encryption and classical methods may then emerge when the scale of 6G is attained, providing layered security while reaping the benefits of quantum techniques as well as of established cryptographic practices. Integrating quantum security into 6G networks will make data protection robust, capable of withstanding threats in the future based on a quantum model, and ensures that the security framework lasts for a long time.

5.6.1 AI Evolution and Threat Intelligence

The advancements in AI will greatly enhance adaptive security protocols for 6G by detecting and responding to risks with ever-increasing sharpness. Future AI's deeper learning algorithms and use of more complex data, which can recognize subtle pattern and correlation indicative of would-be security threats with unrivaled accuracy, provide an example. Advanced neural networks may analyze huge packets of network data in real-time, identifying anomalies and behaviors that traditional systems may miss out on.

AI-powered threat intelligence will evolve to predict emerging attack techniques through continuous learning based on global threat data, thereby allowing 6G networks to respond proactively before threats materialize. With the more adaptable AI models, responses will be automated and context-sensitive and specific to the nature and the severity of the threats under consideration. This will allow for very efficient autonomous security management. Therefore, the future AI-driven protocols would enhance adaptive security with a robust defense mechanism to battle sophisticated cyberattacks throughout 6G.

5.6.2 Ethics and Privacy Considerations

Adaptive security in 6G poses the most important ethics of surveillance, data utilization, and privacy. These systems are primarily monitoring huge masses of real-time data as they spot threats. Necessarily, it collects sensitive user behavior, locations, and what devices do about them. As a result, unchecked big data monitoring can cause alarms about surveillance and misuse of personal information because users perceive themselves being constantly observed even without a clear understanding and consent for such.

These ethical implications are based on data usage and privacy. Adaptive security has to ensure effective threat detection without allowing for over-collection or retention of data. The right to data protection should be ensured by making transparent policies regarding the use of data, ensuring minimal retention of data, and anonymization.

The data of the user should be controlled, enabling them to understand and set their own privacy settings, utilizing precise consent mechanisms. For AI-driven security systems which make decisions automatically, it is a must to have ethics in AI ensuring fairness and transparency in decision-making processes made with the use of automated intelligence. Such ethical AI would ensure that biases in detecting threats would not target one behavior or demographic over the other. Adaptive security in 6G must,

therefore, be designed with firm emphasis on user privacy, clear data governance, and fairness to ensure that robust protections do not come at the expense of individual rights.

5.6.3 Standardization and Global Policies

Hence, international standards and policies could be crucial for uniformity in security measures across the countries and regions when 6G networks are rolled out across the world. Otherwise, different types of security practices could raise vulnerabilities in the global network because inconsistent protection in some areas could open others up to vulnerabilities. International standards help give a uniform guideline through which best practice implementation should be carried on, with, therefore, uniform application of controls in security matters such as encryption, authentication, and response to threats.

Global policies also enable cross-border collaboration and the sharing of knowledge and facilitate nations acting together when emerging cyber threats start to appear and sharing threat intelligence. In adaptive security, such a unified approach is crucial as rapid detection of threats coupled with rapid response is the key in it. By creating universally accepted standards, international organizations can actually integrate those technologies, namely, quantum encryption, AI-based threat intelligence, and even privacy rules and regulations, toward a very secure, sound, and private 6G. These policies push the way for ethical use of data handling and guarantee protection toward the user as it provides a good number of bases in 6G worldwide.

5.7 Conclusion

In summary, 6G networks are a giant leap in connectivity that brings unprecedented speed, massive IoT integration, and seamless connectivity to revolutionize countless industries. These advances bring significant security challenges that need innovative solutions. All along, we have discussed how adaptive security protocols play a vital role in addressing such challenges and enable 6G to achieve its full potential. Unlike traditional static security, this adaptive security will be in action dynamically against the threat environment in real time and, accordingly, will fit into the highly fast, high volume of data and complex scenario like 6G. There will be a multi-layer defense at endpoints, networks, and applications, and this multi-layered defense creates resilient infrastructure as well, which is prepared with potential vulnerabilities in all of those levels.

Adaptive security in 6G shall integrate advanced technologies such as AI and quantum-resistant encryption. AI-driven threat detection with predictive analytics enables proactive responses to emerging threats, and self-healing capabilities allow networks to recover from attacks autonomously. As quantum computing advances, the implementation of quantum-resistant encryption will be critical for safeguarding data so that 6G will stay secure against future computational breakthroughs. Decentralized architectures of security, including blockchain and distributed ledger, will further allow the strengthening of data integrity by distributing trust across networks, providing real-time avoidance of single points of failure.

Ethics and privacy are the two aspects that make adaptive security successful in 6G. In 6G, data exchange is always going on, and there are enormous IoT networks; hence, it is essential to maintain robust security while keeping the user's privacy intact. Context-aware security, which adjusts measures according to the environment, user behavior, and device roles, will help in maintaining this balance by providing appropriate protections without violating the rights of the users. The zero-trust model, therefore, is able to reinforce security by doing verifications at all point accesses, which is something to be taken into greater measure in a network like that where billions of different devices and users will find an interface.

Because 6G is global, standardization and policies between nations need to be developed in unison for a coherent set of security practices. Regional consistency within countries leads to homogeneous protocol standards that enhance 6G networks and work seamlessly across the globe with low vulnerability points and facilitate knowledge dissemination across countries. As described, addressing the security-related challenges in 6G needs research, development, and policy-making continuously. To stay above this rising threat landscape surrounding such technological advances and to see this change in security practice accompany 6G development will require collaborative effort on the mentioned areas.

In the future, adaptive security will be the building block in protecting our digital ecosystems. This means that we will trust 6G networks, which will play a vital role in daily life and as part of critical infrastructure. Adaptive security will thus mark the pathway toward a secure and resilient digital future because of its capacity to dynamically respond to threats, prioritize user privacy, and incorporate the most advanced technologies. Adaptive security will not only safeguard networks but will also be an innovation-safe ecosystem as 6G matures; it will positively impact the users around the world without compromising safety and trust.

References

1. Chorti, Tomasin, S., Pappas, N., Context-Aware Security for 6G Wireless: The Role of Physical Layer Security. *IEEE Commun. Stand. Mag.*, 5, 1, 82–88, Mar. 2021.
2. Chen, X., Li, Y., Jin, D., Zero Trust Architecture for 6G Security. *IEEE Netw.*, 36, 1, 32–38, Jan. 2022.
3. Nguyen, L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., Lin, Y.-D., Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.*, 23, 4, 2384–2428, Fourthquarter 2021.
4. Singh, M. and Malik, A., Multi-hop Routing Protocol in SDN-Based Wireless Sensor Network, in: *Advances in Wireless and Mobile Communications*, pp. 121–141, CRC Press eBooks, 2024, https://doi.org/10.1201/9781003432869-8.
5. Letaief, K.B., Shi, Y., Lu, J., Lu, J., Edge Intelligence for 6G: Challenges and Opportunities. *IEEE Internet Things J.*, 7, 8, 6705–6720, Aug. 2020.
6. Singh, M., Gupta, M., Sharma, A., Jain, P., Aggarwal, P., Role of Deep Learning in the Healthcare Industry: Limitations, Challenges, and Future Scope, in: *Emerging Trends in Intelligent Healthcare Systems*, pp. 1–22, Bentham Science Publishers eBooks, 2023, https://doi.org/10.2174/9789815080230123020003.
7. Gaur, A., Singh, S.K., Saxena, P., Performance Analysis of Deepfake Text Detection Techniques on Social-media. *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, Bengaluru, India, pp. 1–6, 2024, doi: 10.1109/ICDCOT61034.2024.10515626.
8. Chowdhury, M.Z., *et al.*, 6G Wireless Communication Systems: Applications, Requirements, and Technology Enablers. *IEEE Commun. Surv. Tutor.*, 22, 4, 2444–2473, Fourthquarter 2020.
9. Gupta, M., Singh, M., Sharma, A., Sukhija, N., Aggarwal, P., Jain, P., Unification of Machine Learning and Blockchain Technology in the Healthcare Industry, in: *AI-Driven Applications for Smart Healthcare Solutions*, pp. 185–206, Institution of Engineering and Technology eBooks, 2023, https://doi.org/10.1049/pbhe041e_ch6.
10. Saxena, P., Jain, P., Aggarwal, P., Singh, M., Goel, S., Batra, M., Communication Requirements and Performance Metrics for Electric Vehicle Charging: A Comprehensive Review, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 15–30, IGI Global, Hershey, Pennsylvania, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch002.
11. Cui, Y., Xiao, J., Ding, L., Blockchain in 6G Networks: Security Challenges and Future Trends. *IEEE Netw.*, 35, 3, 187–193, June 2021.
12. Chen, S., *et al.*, Artificial Intelligence Enhanced 6G Networks: State of the Art and Vision for the Future. *IEEE Wirel. Commun.*, 28, 3, 56–63, June 2021.
13. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in Renewable Energy Harvesting for EV Charging Infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles,* pp. 75–90, IGI Global, Hershey, Pennsylvania, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.

14. Zhao, M., Lu, H., Zhang, Z., AI-Driven Security for Future 6G Networks: Opportunities and Challenges. *IEEE Wirel. Commun.*, 28, 6, 55–61, Dec. 2021.
15. You, X., *et al.*, AI in 6G Networks: Applications, Challenges, and Prospects. *IEEE Wirel. Commun.*, 28, 4, 112–120, Aug. 2021.
16. Chorti, A., Tomasin, S., Pappas, N., Physical Layer Security for 6G Systems: Why It Is Needed and How to Achieve It, arXiv preprint arXiv:2205.01552, May 2022.
17. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., IoT and Blockchain Technology in 5G Smart Healthcare, pp. 137–161, Elsevier eBooks, Amsterdam, Netherlands, 2022, https://doi.org/10.1016/b978-0-323-90615-9.00004-9
18. Singh, M., Sukhija, N., Sharma, A., Gupta, M., Aggarwal, P., Security and Privacy Requirements for IOMT-Based Smart Healthcare System, pp. 17–37, CRC Press eBooks, Boca Raton, Florida, 2021, https://doi.org/10.1201/9781003032328-2.
19. Saxena, P., Aggarwal, S.K., Sinha, A., Saxena, S., Singh, A.K., Review of computer-assisted diagnosis model to classify follicular lymphoma histology. *Cell Biochem. Funct.*, 42, 5, e4088, 2024 Jul. doi: 10.1002/cbf.4088. PMID: 38973163.
20. Jiang, T., Wang, Z., Wang, J., Trustworthy AI for 6G Networks. *IEEE Commun. Stand. Mag.*, 4, 1, 26–32, Mar. 2020.
21. Saxena, P. and Goyal, A., Study of Computerized Segmentation & Classification Techniques: An Application to Histopathological Imagery. *Informatica*, 43, 4, 561–572, 2019.
22. Ge, X., Wang, X., Andrews, A.G., Role of Artificial Intelligence in the Evolution of 6G Wireless Networks. *IEEE J. Sel. Areas Commun.*, 38, 12, 3051–3073, Dec. 2020.
23. Saxena, P. and Singh, S.K., Noble approach for texture classification of H&E-stained histopathological image by Gaussian wavelet. *2012 12th International Conference on Intelligent Systems Design and Applications (ISDA)*, Kochi, India, pp. 375–379, 2012, doi: 10.1109/ISDA.2012.6416567.
24. Shi, Y., Letaief, K.B., Lu, J., AI Empowered Communication Technologies in 6G: Challenges, Open Issues, and Research Directions. *IEEE Trans. Netw. Serv. Manage.*, 17, 2, 935–950, June 2020.
25. Saxena, P. and Goyal, A., Two-Stage Binary Classification of Follicular Histology Using Support Vector Machine. *Chin. J. Med. Genet.*, 31, 3, 258–268, Jul. 2022.
26. Demirkol, A.F., Subbalakshmi, K.P., Sharma, S.K., 6G and Next-Gen AI-Powered Network Security: Vision, Challenges, and Future Directions. *IEEE Internet Things J.*, 8, 7, 5091–5103, Apr. 2021.
27. Saxena, P. and Goyal, A., Computer-assisted grading of follicular lymphoma: a classification based on SVM, machine learning, and transfer learning approaches. *Imaging Sci. J.*, 70, 1, 30–45, 2022. https://doi.org/10.1080/13682199.2022.2162663.

28. Liu, Y., *et al.*, Decentralized Security Mechanisms for 6G Networks: Blockchain and Beyond. *IEEE Commun. Surv. Tutor.*, 23, 4, 2390–2412, Dec. 2021.
29. Saxena, P., Sinha, A., Singh, S.K., The outbreak of Corona Virus (2019-nCoV) in India: A Statistical case study. *Jour. Integr. Sci. Tech.*, 11, 4, 570, Jul. 2023.
30. Saxena, P., Goyal, A., Bivi, M.A., Singh, S.K., Rashid, M., Segmentation of Nucleus and Cytoplasm from H&E-Stained Follicular Lymphoma. *Electronics*, 12, 3, 651, 2023, https://doi.org/10.3390/electronics12030651.
31. Li, R., Hou, L., Zhang, L., Li, G.Y., Intelligent 5G: When Cellular Networks Meet AI. *IEEE Wirel. Commun.*, 24, 5, 175–183, Oct. 2020.
32. Saxena, P., Sinha, A., Singh, S.K., Computer-assisted interpretation, in-depth exploration and single cell type annotation of RNA sequence data using k-means clustering algorithm. *Computer Methods in Biomechanics and Biomedical Engineering,* 27, 5, pp. 561–578, 2024, https://doi.org/10.1080/10255842.2023.2300685.
33. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., Edge Computing-Based Design for IoT Security, pp. 298–309, Chapman and Hall/CRC eBooks, Boca Raton, Florida, 2024, https://doi.org/10.1201/9781003405535-22.
34. Saxena, P. and Goyal, A., Accurate demarcation of a biased nucleus from H&E-stained follicular lymphoma tissues samples. *Imaging Sci. J.*, 71, 8, 715–727, 2023, https://doi.org/10.1080/13682199.2023.2192550.
35. Pranshu, S,., Singh, S., Agrawal, P., Texture classification of biased cytoplasmic tissue sample from histopathological imagery by Gabor application. *J. Netw. Innov. Comput.*, 1, 248–259, 2013.
36. Singh, S.K., Rashid, M., Alshamrani, S.S., Alnfiai, M.M., Saxena, P., Khamparia, A., Efficient transfer learning approach for acute lymphoblastic leukemia diagnosis: Classification of lymphocytes and lymphoblastic cells. *Trait. du Signal*, 41, 4, 1749–1761, 2024, https://doi.org/10.18280/ts.410409.
37. Abdelhay, Z., Bello, Y., Refaey, A., Towards Zero-Trust 6GC: A Software Defined Perimeter Approach with Dynamic Moving Target Defense Mechanism, arXiv preprint arXiv:2312.17271, Dec. 2023.

6

BFL-IoV: Blockchain and Federated Learning for Secure 6G IoV Networks

Praneetha Surapaneni[1]*, Sailaja Chigurupati[2] and Sriramulu Bojjagani[1]

[1]IoT and Cyber Security Lab, Department of CSE, SRM University-AP, Andhra Pradesh, India
[2]Department of CSE, KL University, Andhra Pradesh, India

Abstract

6G communication is a revolutionary technology in wireless communication. It overtakes the 5G technology in terms of security. 6G opens its boundaries for the various Internet of Things applications in smart cities. Internet of Vehicles (IoV) sends and receives traffic-related data between various entities such as vehicles, pedestrians, roadside units (RSUs), mobiles, cloud servers, and other entities. This advancement in 6G ensures that communication between entities is more secure in an IoV environment. The increasing number of entities causes trust and privacy issues as it generates massive amounts of data with increased mobility. This chapter introduced the blockchain concept, which provides security and privacy in the IoV environment. Simultaneously, federated learning (FL) protects the user's privacy. FL reduces the attacks and ensures privacy by storing the information locally. In addition, blockchain provides immutability by allowing only trusted parties to participate. Integrating blockchain and FL provides more security among various entities in transportation systems. This chapter discusses the blockchain and FL challenges and 6G communication technology solutions. The simulation is performed using SUMO simulator to achieve the dynamic vehicular environment.

***Keywords*:** Blockchain, federated learning (FL), Internet of Vehicles (IoV), privacy, security, smart city, SUMO tool, 6G communications

**Corresponding author*: kilarupraneetha@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (129–146) © 2026 Scrivener Publishing LLC

6.1 Introduction

Nowadays, urban areas are converting into smart cities that use innovative technologies for the better life of people. Smart cities integrate Internet of Things (IoT) for smart infrastructure, smart governance, smart healthcare, and smart traffic mobility [1]. IoT contains a group of network connected entities that gather transfers and analyze the data that is generated from the surroundings [2]. The entities are connected one another using internet. IoV is the subdivision of IoT that mainly focus on the smart traffic management. Vehicles communicate to infrastructure (V2I), fog servers (V2F), cloud servers (V2C), mobiles (V2M), smart homes (V2H), and other vehicles (V2V) for safe and efficient communication [3]. As the number of IoT devices increases, CISCO assumes that, by the year 2030, the IoV vehicles will be around two billion [4]. Figure 6.1 shows the increase of connected vehicles by the year 2023.

As the number of vehicles increased, the data generation from the vehicles also increases. 6G communications is the new era in wireless communication that overcomes the deficiencies of 5G technology. 6G contains more advanced features and applications, even though; 5G highlights fast data transfer, low latency, and more entity communication [5]. 6G connects more entities and generates extensive data like 5G. These networks are more capable and adaptable for engaging more services effectively and optimize resources for various applications in real time [6].

Blockchain and artificial intelligence (AI) along with 6G integration in the IoV make more efficient and secure network for vehicles [4]. Blockchain provides a decentralized and tamper resistant communication in IoV.

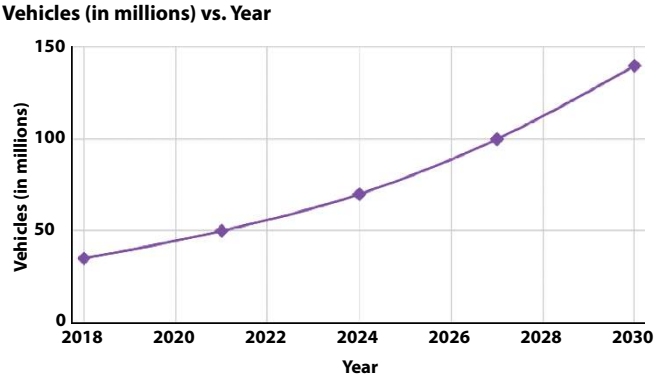

Figure 6.1 Year-wise connected vehicles growth.

It provides a unique identity for each vehicle that stores data in the blockchain network. The blockchain allows trusted vehicles to access the data to reduce various attacks. It also assures secured data transfer between vehicles and other entities ensuring authenticity and integrity among entities [7].

AI performs data processing and analysis of IoV data to avoid traffic collision and maintenance failures. AI collects data from various sensors and analyses for inter and intra communication for safe and comfort driving experience [8]. Federated learning (FL) is a crucial element of AI that minimizes the data centralization and secures data privacy using FL algorithms. Traditional algorithms perform data collection and processing at central servers, whereas, in FL, the data is stored in local entities and only attributes are shared [9]. As the data is stored locally, it ensures privacy of the sensitive data.

Regardless of their benefits, IoV devices are exposed to security threats, violation of privacy, and performance issues in real-time information sharing. As IoV expands, these hazards increase, making decentralized management, strong authentication, and secure data transfers necessary to maintain performance and confidence. By reducing data centralization and preserving privacy among IoV entities, FL tackles these issues. Sensitive information stays in the cars because data models are trained locally, lowering the dangers connected with centralized storage [9]. This decentralized strategy is further improved by blockchain, which offers safe data management. Blockchain consensus mechanisms, such Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), reduce the latency and computational expense of conventional Proof of Work (PoW) techniques by ensuring that only authenticated nodes exchange data [23]. In addition to enhancing security, this FL and blockchain integration in a 6G network streamlines the data management procedure in IoV systems.

Real-time communication between cars, pedestrians, roadside units (RSUs), and other entities is now possible because to the development of the IoV and the introduction of 6G communication technology, which has completely changed transportation networks. Although this development makes traffic management safer and more intelligent, it also poses serious problems with regard to scalability, privacy, trust, and data security.

- As vehicles, RSUs, and other connected devices are always exchanging information, IoV systems produce enormous volumes of data. This necessitates strong systems to manage and protect such enormous data streams.

- Because IoV is interconnected, it is critical to ensure safe connection and protect user data privacy. Malicious assaults including identity spoofing, eavesdropping, and data manipulation are frequently difficult to stop with current methods.
- The deployment of traditional security measures is made more difficult by the dynamic nature of vehicle networks, which are defined by high-speed mobility and frequent topological changes.
- IoV systems benefit greatly from 6G networks' extremely low latency and extensive connectivity. However, creative solutions that incorporate effective machine learning techniques and decentralized trust models are needed to fully realize these advantages.
- Single points of failure and scalability problems are common in centralized systems. By decentralizing data processing and storage while maintaining data privacy, the combination of blockchain technology with FL presents a viable remedy.

IoV security has advanced, yet there are still a number of important gaps that must be filled:

- Due to their significant computational burden and latency, traditional blockchain consensus algorithms such as PoW are not practical for IoV scenarios. In vehicular contexts, optimized techniques like PoS and PBFT require more research.
- In contexts with dynamic mobility, existing FL models—particularly those that use synchronous updates—perform poorly because cars might not always be connected. Although semi-synchronous FL offers a potential remedy, little is known about how to actually use it in IoV.
- Assessing trust between cars, RSUs, and other IoV entities is a challenging task, particularly when malicious nodes are present. Strong tools to dynamically evaluate and uphold trust in real time are absent from current systems.
- Although FL protects data privacy and blockchain offers immutability and decentralization, their integration for safe IoV apps is still in its infancy. To handle the particular difficulties of IoV, a thorough framework that integrates the advantages of both technologies is required.

- Energy-efficient solutions are essential because IoV devices have limited resources. An important consideration for practical application is energy consumption, which is frequently ignored by current blockchain and FL models.

In this chapter, we proposed an integration of blockchain and FL in the IoV environment that handles training models of the vehicles. The contributions of this chapter are listed below:

- Because high-speed mobility frequently interferes with data transfer, the suggested blockchain and federated learning (BFL)–IoV architecture is made to guarantee smooth communication and minimal latency in vehicle situations. The framework uses blockchain's immutable and decentralized design to include ways to improve trust between entities, such as vehicles, RSUs, and other IoV components.
- The system incorporates a strong consensus method, such PBFT, to verify the integrity and authenticity of locally trained models. This reduces the possibility of malicious data injection and manipulated training parameters by guaranteeing that only reliable data and models are added to the blockchain.
- By keeping raw data local to each entity and only sending trained models to aggregators, FL under the BFL-IoV framework preserves user privacy. This decentralized strategy promotes a safe learning environment in the IoV ecosystem by drastically lowering the danger of data breaches and illegal access.
- The suggested approach aggregates local models by using trustworthy entities, like RSUs, in place of centralized servers. Even in situations with considerable mobility, a dynamic aggregation mechanism guarantees the efficient and secure construction of the global model.
- Data manipulation, hostile assaults, and counterfeiting are only a few of the security issues in the IoV ecosystem that are addressed by the combination of blockchain and FL. By leveraging blockchain's distributed ledger technology, the suggested framework also eliminates single points of failure, guaranteeing resilience and dependability in crucial applications like traffic control and collision avoidance.

- Simulations employing SUMO (Simulation of Urban Mobility), a program created especially for traffic modelling, are used to verify the framework's performance. Evaluations of metrics including throughput, delay, trust, and anomaly detection demonstrate how well the suggested approach works in a dynamic vehicular environment.

Section 6.2 provides the literature survey of the previous works. Section 6.3 discusses about FL and blockchain in IoV environment where Section 6.4 elaborates the proposed system model. The simulation and discussion are given in Sections 6.5 and 6.6. Finally, Section 6.7 concludes the BFL-IoV framework, and Section 6.8 discusses the future directions.

6.2 Related Work

BFL is the workable approach to affirm security, privacy, and decentralization in IoV network. Numerous papers discussed the advantages and possibilities of BFL [10, 11]. BlockDeepNet [10] integrates the mutual learning and blockchain for IoT, where the edge entities categorizes its local attributes and performs deep learning algorithms for training the model. DeepChain [11] contains smart contracts for assuring the confidentiality and safety of the model using blockchain. The confidentiality of the data is provided using blockchain and FL [12]. The trained model ensures quality using new consensus mechanism. In IoV, the inadequacy of PoW, consensus delay, and latency issues are overcomes in [13]. Various consensuses for FL are used to overcome the delay. FL is utilized to predict the traffic on the road in DPBFT [14]. In [15], the blockchain contains two levels. One level contains the mobile devices and the other contains RSUs. All the entities are trained locally along PoK consensus mechanism.

To overcome the security attacks, blockchain is used in FL. To over the single point failure, blockchain is used in [15]. The vehicles use PBFT and save the data in cloud servers. Even though the edge devices are deficient, the trained data from the vehicles are transmitted to the cloud servers. The consensus mechanism in blockchain overcomes various security thefts in [14]. Masquerading, counterfeiting, and retro-engineering thefts in the IoV during FL are overcomes in [16].

In IoV, to secure FL blockchain is suggested to all frameworks that integrates MEC in 6G [17, 18]. To increase the scalability of FL in MEC, blockchain is used in [13].

6.3 BFL in IoV Environment

6.3.1 Roadblocks and Feasible Solutions

Synchronous and asynchronous are the two modes of FL [19]. In synchronous, the entities should upload the local models within the given time limit. Entities using asynchronous FL share their models at their convenience. The model gets updated whenever it is required, which results in better communication efficiency [20]. In contrast, as the vehicles move rapidly, the entities cannot upload the model in accurate time, as shown in Figures 6.2 and 6.3. This represents the drawback of the synchronous mode. The asynchronous mode cannot update the global model if the aggregator is disconnected due to the vehicle's dynamic nature. Figures 6.4 and 6.5 represent the asynchronous FL mode in IoV. To overcome the deficiencies of both modes, semi-synchronous FL is implemented in [20].

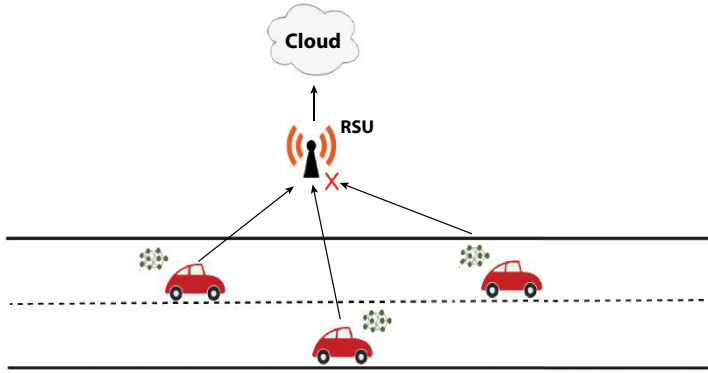

Figure 6.2 Synchronous FL where the data from every vehicle is sent within time.

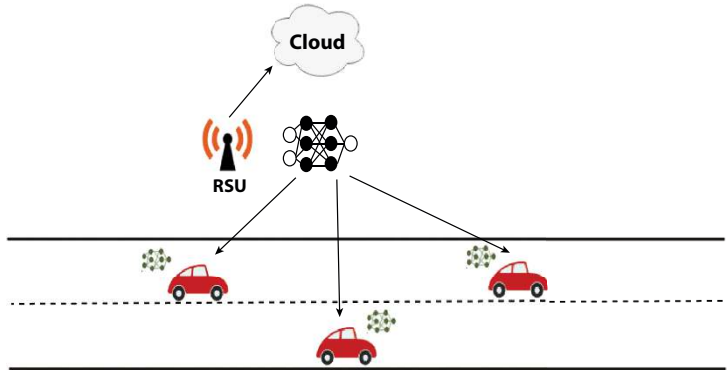

Figure 6.3 Synchronous FL where the global data from every vehicle is sent after time.

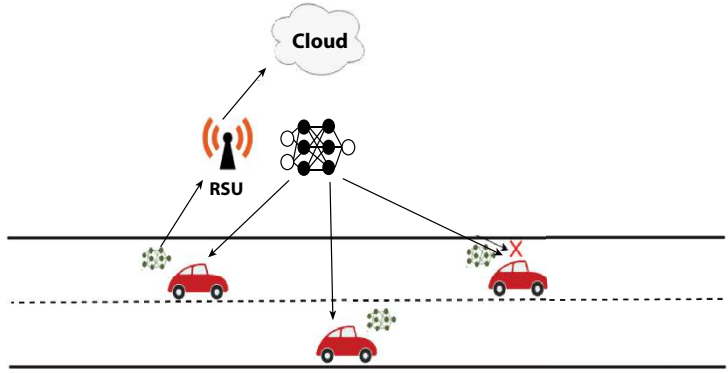

Figure 6.4 Asynchronous FL where aggregator updates and transfers the global model.

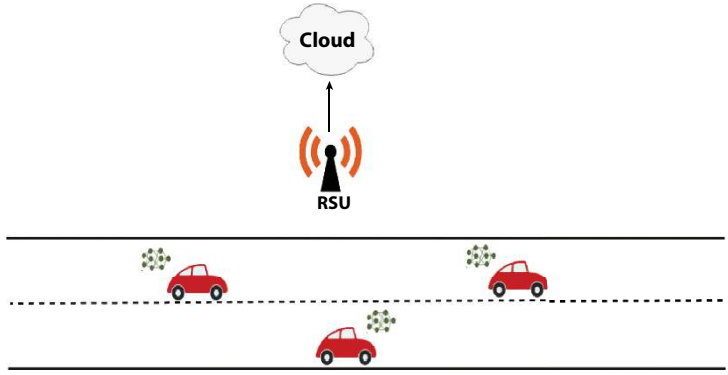

Figure 6.5 Asynchronous FL where vehicles train the global model that generates a fresh local model.

6.3.2 Blockchain

Blockchain contains connected blocks using hash function to store the data in the corresponding block [21]. IoV has recently adopted blockchain to overcome the security issues. To verify the data whether it comes from trusted nodes or untrusted node, blockchain is used to validate. To authenticate the message, PoS [22] and PoW [23] are used. The trust of each node is evaluated by using the distance between the nodes and the signal and noise ratio.

6.3.3 Roadblocks and Feasible Solutions

Number of adversary nodes, latency, and throughput are evaluated to check the performance of the blockchain network. Blockchain should contain low latency and high throughput for message distribution in IoV. As the vehicles move with high speed, PoW is not suitable. To overcome this PoS and PBFT are considered [24]. The probability of forks that occur in blockchain is another disadvantage. Fork is the block added to another in the chain. The legitimate blocks may get deleted due to the addition of fork blocks in a V2V communication. This drawback can be overcome by adding blocks using the authorized nodes in IoV network.

6.4 Proposed Framework

In this chapter, we analyzed a smart contract to achieve decentralization, automated process, and security. The suggested framework is analyzed for node selection using PBFT and message transmission. The following are the three steps for smart contract enabled FL. The proposed BFL framework is shown in Figure 6.6.

6.4.1 Collection of Data and Development of Local Models

- Vehicles, RSUs, and other linked IoV components are among the entities that collect environment-specific data, including weather, vehicle mobility patterns, traffic density, and vehicle crashes. For every entity, a localized dataset is created using this real-time data.
- Every entity uses its own private data to train a local machine learning model.

- Sensitive information is protected, and the likelihood of data breaches is decreased by the training process, which guarantees that the raw data stays local.
- The local models are regularly updated to take into account the shifting conditions of road traffic, vehicle density, and environmental elements because the IoV environment is so dynamic.
- This procedure improves the relevance of the local models and makes low-latency decision-making easier.

6.4.2 Transferring Data into the Blockchain Network

- Local models and their parameters are subjected to a PBFT consensus process prior to being uploaded to the blockchain.
- By doing this, the blockchain is guaranteed to include only validated and reliable data models.
- Local models are validated against pre-established criteria using smart contracts.
- In order to identify irregularities and discrepancies, these contracts contrast the actual performance of the local models with the anticipated outcomes (such as accuracy and loss metrics).
- When hostile entities try to alter training weights, parameters, or results, the smart contract and consensus mechanism work together to detect and isolate them.
- The framework preserves the integrity of the IoV network by guaranteeing that only verified data models are captured.
- To ensure immutability and tamper-proof storage, the local models are uploaded to the blockchain as separate data blocks after validation.
- The inclusion of local models into the blockchain is shown in Figure 6.6.

6.4.3 Generation of Global Model by Aggregating Local Models

- The trusted entities such as vehicles or RSUs acts like aggregator instead of using the centralized server.
- These aggregators create a single global model by combining the verified local models from the blockchain network.

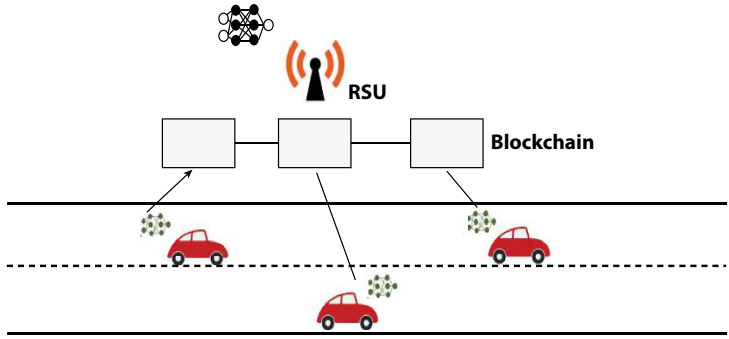

Figure 6.6 Proposed BFL framework.

- The most recent local models added to the blockchain are used by the aggregators to update the global model on a regular basis.
- The global model is updated to reflect the most recent data thanks to this iterative process.
- The global model, which ensures openness and trust in the model generation process, is uploaded into the blockchain as an upgrading key block after the local models have been aggregated.
- Until the global model fulfills a predetermined loss function or reaches the necessary performance indicators, the FL procedure is repeated.
- The global model is guaranteed to reach the highest level of accuracy and dependability thanks to this iterative process.

6.5 Simulation

The proposed BFL framework performance is evaluated using Python. SUMO is used for simulating the framework. SUMO is openly available software, more portable, and designed for traffic simulations. In this software, every vehicle can have its individual route without depending on the other. Traffic lights, pedestrians, and various types of vehicles can be inserted in the software. OpenStreetMap is used to download real-time maps that contain various roads and networks [24]. We considered a bidirectional road with a maximum speed of 60 to 70 kilometers. Vehicles speed, direction, and on-road vehicle density are used to train the local model. Figure 6.7 depicts the SUMO simulation environment.

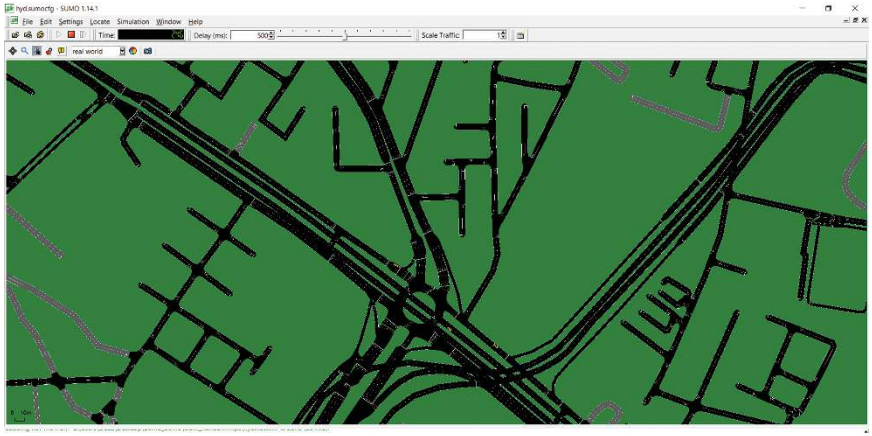

Figure 6.7 SUMO simulation environment.

6.6 Results and Discussion

6.6.1 Performance Evaluation of the BFL-IoV Framework

The simulation results show notable gains in computing efficiency, security, and privacy for IoV applications in a 6G-enabled setting. Throughput, privacy protection, trust assessment, and latency are the main performance parameters that are examined.

Reduced Latency: When compared to conventional centralized learning systems, the use of FL showed a significant decrease in latency. Communication overheads and processing delays were reduced by training local models inside of individual entities and only sharing aggregated models.

High Throughput: By cutting down on the amount of time needed for block validation, the blockchain consensus mechanism's application of PBFT increased throughput. In high-mobility settings like the Internet of Vehicles (IoV), this guaranteed effective message distribution.

Security and Privacy: FL and blockchain worked together to protect data privacy and guarantee safe communication between IoV entities. Blockchain offered tamper-proof data storage and validation, whereas FL permitted data to stay local, preventing the flow of critical information.

Evaluation of Trust: By using blockchain technology to authenticate and evaluate nodes according to their distance, signal-to-noise ratio, and past behavior, the framework successfully handled trust challenges. To further improve network dependability, participation was given preference to trustworthy nodes.

6.6.2 Evaluation against Current Frameworks

The BFL framework combined the advantages of blockchain with FL to exceed other IoV security methods. Single points of failure and increased privacy issues were problems with traditional centralized approaches. On the other hand, scalability problems prevented decentralized blockchain networks from managing high-speed vehicle settings alone. The suggested BFL architecture was a solid solution for 6G-enabled IoV because it struck a compromise between scalability, security, and computing efficiency.

6.6.3 Challenges and Limitations

The BFL framework faced a number of difficulties in spite of its benefits:

Dynamic Character of Vehicles: Occasionally, fast-moving vehicles interfered with FL's ability to synchronize local model updates. This problem was lessened but not completely resolved by semi-synchronous FL.

Energy Consumption: The computational resources needed to train local models and take part in blockchain consensus processes may have an effect on energy efficiency. A portion of this problem was resolved by lightweight consensus techniques like PBFT.

Forking in Blockchain: There was a chance of data loss when forks occurred during message validation in V2V communication. By limiting the ability of trusted nodes to contribute blocks to the blockchain, this was lessened.

6.6.4 Discussion on Simulation Results

Effectiveness of SUMO Simulation: The suggested framework's performance in urban traffic settings was realistically revealed by the SUMO simulation. Training local models was successfully accomplished using metrics including vehicle speed, density, and direction. With a top vehicle speed of 60–70 km/h, the bidirectional road scenario closely mirrored actual IoV environments.

Anomaly Detection: By utilizing the blockchain-based consensus mechanism, the BFL framework was able to successfully detect anomalies in local models. We identified and segregated malicious entities that were trying to change the training settings.

Scalability: By effectively managing growing data traffic and the inclusion of additional entities, the decentralized architecture of the framework proved its scalability. Smart contracts were included to further automate activities and guarantee smooth process execution.

6.7 Conclusion

This chapter offers a thorough examination of how to combine blockchain technology with FL to meet the crucial needs of data confidentiality, privacy, and security in the context of the IoV. The suggested BFL-IoV system makes use of FL's collaborative learning capabilities and blockchain's decentralized structure to enable safe and effective vehicle model training without jeopardizing sensitive data. The framework tackles a number of difficulties that arise when FL and blockchain are combined, including as scalability problems, consensus overhead, and latency. Adversarial assaults, model poisoning, and data tampering are all prevented by the suggested method's use of a strong consensus mechanism and secure communication protocols. Additionally, the approach improves the overall dependability of IoV networks by fostering trust among participating entities, such as cars and RSUs. Vehicles in the suggested system use FL to dynamically train and run local models, and blockchain verifies the models' validity and integrity prior to aggregation. By adding an unchangeable layer of security, blockchain makes sure that only verified data and models are included in the global aggregation process. In addition to improving security, this dual strategy fixes flaws in conventional systems such single-point failures and the possibility of centralized attacks. Through simulations conducted with the SUMO tool, the effectiveness of the framework was confirmed. The simulations show how well the framework adapts to real-world IoV scenarios by accurately simulating a dynamic vehicular environment. Reduced latency, improved security, and smooth model training are just a few of the key performance indicators that highlight the BFL-IoV framework's viability in next-generation transportation systems. All things considered, the suggested framework's integration of FL and blockchain technologies offers an IoV environment scalable, safe, and privacy-preserving solution.

By tackling important issues and laying the groundwork for upcoming developments in decentralized vehicular networks, this work advances intelligent transport systems.

6.8 Future Directions

In improving security, privacy, and efficiency in IoV environments, the suggested BFL-IoV framework shows encouraging results. To improve its scalability and usefulness, a few issues can be investigated further. The following are the areas of future research:

Federated learning's performance in dynamic IoV environments can be further optimized by incorporating cutting-edge AI techniques like generative adversarial networks and reinforcement learning. In high-mobility situations, these methods can be applied to adaptive learning, anomaly detection, and real-time decision-making. When implementing the BFL-IoV framework in extensive networks with thousands of vehicles and RSUs, scalability issues must be addressed through research. To preserve performance under high network loads, this entails optimizing communication protocols and consensus procedures.

References

1. Nastjuk, I., Trang, S., Papageorgiou, E., II, Smart cities and smart governance models for future cities: Current research and future directions. *Electron. Mark.*, 32, 4, 1917–1924, 2022, doi: 10.1007/s12525-022-00609-0.
2. Gupta, B.B. and Quamara, M., An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency Comput. Pract. Exper.*, 32, 21, e4946, 2020, doi: 10.1002/cpe.4946.
3. Surapaneni, P., Bojjagani, S., Bharathi, V.C., Morampudi, M.K., Maurya, A.K., Khan, M.K., A Systematic Review on Blockchain-enabled Internet of Vehicles (BIoV): Challenges, Defences and Future Research Directions. *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3453433.
4. Shah, K., Chadotra, S., Tanwar, S., Gupta, R., Kumar, N., Blockchain for IoV in 6G environment: Review solutions and challenges. *Cluster Comput.*, 25, 3, 1927–1955, 2022, doi: 10.1007/s10586-021-03492-0.
5. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in renewable energy harvesting for EV charging infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 75–90, IGI Global, Hershey, PA, USA, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.

6. Viswanathan, H. and Mogensen, P.E., Communications in the 6G era. *IEEE Access*, 8, 57063–57074, 2020, doi: 10.1109/ACCESS.2020.2981745.
7. Javed, M.U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N., Tahir, M., Blockchain-based secure data storage for distributed vehicular networks. *Appl. Sci.*, 10, 6, 2011, 2020, doi: 10.3390/app10062011.
8. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-Based wireless sensor network, in: *Advances in Wireless Sensor Networks and Applications*, pp. 121–141, CRC Press, Boca Raton, FL, USA, 2024, https://doi.org/10.1201/9781003432869-8.
9. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., Edge Computing-Based design for IoT security, in: *Edge and Fog Computing for Internet of Things Security*, pp. 298–309, Chapman and Hall/CRC, Boca Raton, FL, USA, 2024, https://doi.org/10.1201/9781003405535-22.
10. Rathore, S., Pan, Y., Park, J.H., BlockDeepNet: A blockchain-based secure deep learning for IoT network. *Sustainability*, 11, 14, 3974, 2019, doi: 10.3390/su11143974.
11. Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., Luo, W., Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Trans. Depend. Secure Comput.*, 18, 5, 2438–2455, 2019, doi: 10.1109/TDSC.2019.2952332.
12. Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y., Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inf.*, 16, 6, 4177–4186, 2019, doi: 10.1109/TII.2019.2942190.
13. Pokhrel, S.R. and Choi, J., Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Trans. Commun.*, 68, 8, 4734–4746, 2020, doi: 10.1109/TCOMM.2020.2990686.
14. Qi, Y., Hossain, M.S., Nie, J., Li, X., Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Gener. Comput. Syst.*, 117, 328–337, 2021, doi: 10.1016/j.future.2020.12.003.
15. Otoum, S., Al Ridhawi, I., Mouftah, H.T., Blockchain-supported federated learning for trustworthy vehicular networks, in: *GLOBECOM 2020-2020 IEEE Global Communications Conference*, IEEE, pp. 1–6, 2020, December, doi: 10.1109/GLOBECOM42002.2020.9322159.
16. Chen, J.H., Chen, M.R., Zeng, G.Q., Weng, J.S., BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle. *IEEE Trans. Veh. Technol.*, 70, 9, 8639–8652, 2021, doi: 10.1109/TVT.2021.3102121.
17. Nguyen, D.C., Ding, M., Pham, Q.V., Pathirana, P.N., Le, L.B., Seneviratne, A., Poor, H.V., Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet Things J.*, 8, 16, 12806–12825, 2021, doi: 10.1109/JIOT.2021.3072611.

18. Muscinelli, E., Shinde, S.S., Tarchi, D., Overview of distributed machine learning techniques for 6G networks. *Algorithms*, 15, 6, 210, 2022, doi: 10.3390/a15060210.
19. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y., Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Trans. Veh. Technol.*, 69, 4, 4298–4311, 2020, doi: 10.1109/TVT.2020.2973651.
20. Liang, F., Yang, Q., Liu, R., Wang, J., Sato, K., Guo, J., Semi-synchronous federated learning protocol with dynamic aggregation in internet of vehicles. *IEEE Trans. Veh. Technol.*, 71, 5, 4677–4691, 2022, doi: 10.1109/TVT.2022.3148872.
21. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile Ad Hoc Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019, https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
22. Han, Q., Yang, Y., Ma, Z., Li, J., Shi, Y., Zhang, J., Yang, S., CMBIoV: Consensus Mechanism for Blockchain on Internet of Vehicles, in: *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, Singapore, Springer, pp. 347–352, 2020, doi: https://link.springer.com/chapter/10.1007/978-981-15-9213-3_27.
23. Ayaz, F., Sheng, Z., Tian, D., Liang, G.Y., Leung, V., A voting blockchain based message dissemination in vehicular ad-hoc networks (VANETs), in: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, pp. 1–6, 2020, June, doi: 10.1109/ICC40277.2020.9148823.
24. Surapaneni, P., Bojjagani, S., Khan, M.K., VESecure: Verifiable authentication and efficient key exchange for secure intelligent transport systems deployment. *Veh. Commun.*, 49, 100822, 2024, doi: 10.1016/j.vehcom.2024.100822.

7

Leveraging Machine Learning for Enhanced 6G Security

Gnanasankaran Natarajan[1]*, Elakkiya Elango[2], Sundaravadivazhagan Balasubramanian[3] and Rakesh Gnanasekaran[1]

[1]Department of Computer Science, Thiagarajar College, Madurai, Tamil Nadu, India
[2]Department of Computer Science, Government College of Arts and Science for Women, Sivaganga, Tamil Nadu, India
[3]Department of Information Technology, University of Technology and Applied Sciences, AL Mussanah, Sultanate of Oman

Abstract

Network security is facing previously unheard-of possibilities and problems as the telecom sector prepares to begin the rollout of sixth-generation (6G) networks. The critical role that machine learning (ML) plays in bolstering the protection of 6G infrastructures is examined in this chapter. Revolutionary improvements in speed, capacity, and connection are anticipated with the transition from 5G to 6G, which will be fueled by the intricate interactions between innovations like enormous Multiple Input-Multiple Output (MIMO), Terahertz Interpersonal interaction, and artificial intelligence (AI)–driven networking orchestration. But new risks accompany these developments as well, calling for creative solutions to protect privacy of users and network integrity.

In this scenario, ML becomes a transformational tool with the ability to analyze massive volumes of heterogeneous data in real time, identify abnormalities, and continually modify defenses. This chapter examines a number of ML approaches that are relevant to 6G security, such as anomaly detection, AI-powered methods for authentication, systems for detecting and preventing intrusions, and advanced analytics for threat mitigation. Moreover, the amalgamation of ML with other cutting-edge technologies like as blockchain and quantum cryptography is scrutinized to enhance the robustness of 6G networks against intricate cyberattacks. The effectiveness of ML in strengthening the resilience and dependability of security

**Corresponding author*: sankarn.iisc@gmail.com; ORCID: 0000-0001-9486-6515

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (147–166) © 2026 Scrivener Publishing LLC

protocols in upcoming telecommunications networks is demonstrated *via* case studies and real-world applications.

This chapter concludes by emphasizing how crucial ML has been in forming the privacy paradigm of 6G networks. Stakeholders can maintain the reliability of next-generation telecommunications infrastructures, dynamically reduce risks, and guarantee data integrity by utilizing the capabilities of ML algorithms and frameworks.

***Keywords*:** 6G technology, machine learning, 6G security, cyber threats, cryptography, telecommunication

7.1 Introduction

Future advancements in mobile technology and network design are expected from sixth generation (6G). 6G technology has the potential to help companies globally and improve the well-being of people everywhere by delivering high-capacity connectivity at previously unheard-of bandwidth and low latency. Its ambitious goals include outpacing its predecessor and perhaps attaining a microsecond, latencies connectivity, along which would make it 1,000 times more rapid than 5G. 6G networks, which will utilize frequencies more powerful than 5G, will almost certainly enable mobile communications in future generations and enable major advancements in wireless technology. It is anticipated that 6G would transform wireless communication in ways that include better security, increased network capacity, location awareness, and imagery.

Alongside 6G technology are machine learning (ML) and artificial intelligence (AI). The decision-making process about IT infrastructure will be aided by 6G's utilization of AI and ML. Enhancing a network's speed and user experience may be achieved by determining the optimal locations for handling information, collaborating, and storing. 6G mobile technology and next cellular technologies are going to remain at the cutting edge as the globe moves toward the usage of autonomous vehicles, smart cities, and augmented and virtual reality [14, 23]. Although it is still in its early stages of development, 6G technologies has the potential to greatly expand the capabilities of wireless communications and increase global connectivity by creating more intelligent networks.

7.1.1 Recognizing 6G Technology

6G wireless technology represents the next technological step beyond the widely used 5G standard. Although 5G is still in its early phases of industry integration, technologists and researchers are currently establishing the foundation for its replacement [19]. Redefining the standards for speed, latency in addition to interconnectivity represents the fundamental goal of 6G technology. Seen as the foundation of the coming digital revolution, 6G promises to open up a world of possibilities, including continuous access even in the most remote parts of the world and blazingly fast data transfer rates.

7.1.2 Essential Elements of 6G Technology

The following notable characteristics of 6G technology open the door to its revolutionary potential:

- **Terabit Data Rates:** 6G offers transmission speeds higher than ten gigabits per second, making bandwidth-intensive applications possible and offering instantaneous data transfer.
- **Ultra-Low Latency:** 6G will enable real-time interactions that are essential for technologies like autonomous vehicles and remote medical care, with delay cut to a measly microsecond.
- **Massive Connectivity:** 6G promises to link an unprecedented number of things per square kilometre by utilizing cutting-edge antenna innovations, establishing the foundation for the global Internet-of-Things (IoT) ecosystems.
- **Energy Efficiency:** 6G strives to remain power-efficient considering its powerful abilities, using clever power management techniques to reduce its environmental impact.
- **AI Integration:** By forecasting network congestion, enhancing security procedures, and maximizing resource allocation, AI will have a critical role in 6G networks.
- **The Development of 6G:** Recognizing the fundamental technologies and functionalities

We will examine the essential features and technologies of 6G in this section, which will render it an innovative breakthrough for the telecom sector [9, 24]. 6G offers the power to completely change connections and make life-altering interactions possible with its faster speeds, reduced latency, and greater capacity.

Table 7.1 Comparison of key performance aspects of 6G with previous generations of wireless networks.

Generation	Speed	Latency	Capacity
2G	Upto 236 Kbps	150–4000 ms	Low
3G	Upto 42 Mbps	100–150 ms	Medium
4G	Upto 1 Gbps	10–20 ms	High
5G	Upto 10 Gbps	1 ms	Very High
6G	Upto 1 Tbps	Sub-1 ms	Ultra-High

7.1.3 6G's Potential

The benefits of 6G go beyond merely quicker speeds. 6G's inventiveness and revolutionary potential have the power to completely change a number of sectors and open up new markets for services and applications. With 6G, the possibilities are endless. 6G has the power to completely change our society, from facilitating autonomous vehicles and smart cities to improving distant experiences *via* both augmented and virtual reality [11]. We may start to see the fascinating future that lies ahead of us by comprehending the fundamental technologies and potential of 6G.

A comparison between 6G and earlier generations is displayed in Table 7.1.

7.1.4 How Will the 6G Technology Perform

The arrival of 6G networks is imminent. Thus, it is crucial to grasp how 6G technologies might work whether being a company looking to engage network experts on an hourly or a permanent basis or someone who might apply for network design positions in the coming years [4]. Researchers are unable to speculate about the functionality of the 6G technology because it is currently in its infancy of its development and is pending approval by the International Telecommunication Union (ITU). We are able to forecast with confidence whether 6G technology will perform based on the experiences of other wireless technology generations.

It is predicted that 6G the field of wireless technology will improve a free spectrum's efficiency. 6G technology could potentially be able to utilize sophisticated mathematics to facilitate simultaneous broadcasts and receives on the same band, in contrast to present technologies for wireless communication, which merely allow broadcasts and receives on a single frequency at the same time [5, 21]. A significant portion of 6G network research has

concentrated on data transmission at arbitrarily higher frequencies. To put things in perspective, 5G operates at up to 39 gigahertz (GHz), whereas hundreds of terahertz (THz) is anticipated to be supported by 6G technology. Although extremely high frequencies are brittle, using them could allow for far quicker data transfer rates. There is a chance that 6G technology would embrace mesh networking, in contrast to 5G networks, which generally employ hub-and-spoke design, in which end-user devices communicate to cell towers. By allowing objects to operate as emitters for one another's data, wireless network technology will be strengthened and expanded to allow for the participation of every device in data sending and receiving.

7.2 Implementing an Integrated 6G Security Platform by Combining Standardization and Threat Analysis

All privacy activity, including those related to 6G, must be grounded in a comprehensive threat analysis for specific use cases and technology. This type of work integrates mobile-specific techniques like Global System for Mobile Communications Association (GSMA) Multi-faceted Trustworthy Identity Framework (MOTIF), MITRE FIGHT, and the European Union Agency for Cybersecurity (ENISA) 5G matrixes with formal threat models including Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) and then refines them to handle additional 6G-specific risks [13, 17]. Early identification of the primary threats is necessary for establishing priority and direct standards and design, even though upstream threat analysis will never be completely comprehensive. Like 5G, 6G will also use open standards and technology, along with techniques and procedures used in the creation, implementation, and maintenance of mobile networks, as well as threat evaluations to inform its security architecture. The requirements for 6G security are presented along with five focal areas as shown in Figure 7.1.

7.2.1 Service Availability

In all its various guises, the 6G technology will provide a variety of services, with varying types of users having access to varying sets of those amenities. For users, these services' accessibility is essential, and it may even attract regulatory notice, especially when the service is thought to be essential to society's smooth operation [20]. The term "service availability" describes the capacity of users to depend on a service to operate under all circumstances, including unintentional or natural failures, network attacks, and

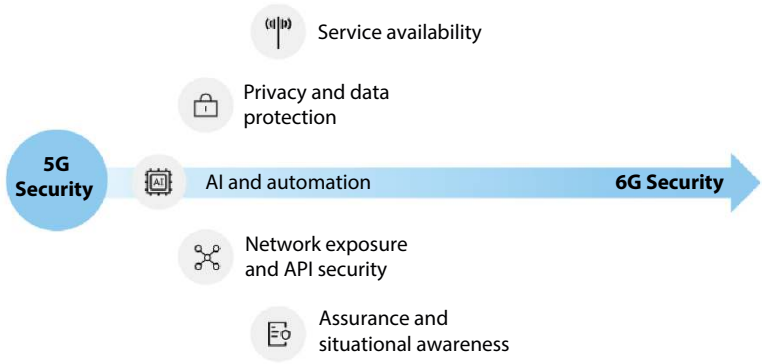

Figure 7.1 Priority areas for security in 6G.

normal operating conditions. The degree to which this reliance is satisfied is determined by how important the service is. In addition to offering a foundational level, the 6G platform will enable configuration to raise the amount of reliance as needed. This modification might be applied to a broader scope, to particular services, or to specified regions.

Oftentimes, rather than being included on as additional protection measures, robustness against deliberate assaults that impact availability can be achieved *via* concerns in design, protocols design, and network setup [10]. In order to lessen threats like denial of service attacks, signaling storms, and jamming, precautions are also taken with regard to operational networks. As we approach 6G, the importance of cyber threat intelligence—when applied to telecom use cases—will only grow.

7.2.2 Privacy and Data Protection

6G mobile networks must take into account the full safeguarding of integrity and confidentiality for information during transit, information being handled, as well as data idle, in addition to key creation, and management of keys, and logging, which is while earlier generations of mobile networks concentrated primarily on communications security [7, 22]. This means that the scope of 6G will expand from protecting data to securing wholesale delivery of services, which includes networking and data processing infrastructure protections. Through this, 6G will move the emphasis from data management to data ownership, encompassing features that guarantee the privacy and control of sensitive personally identifiable digital assets with respect to outside parties.

The importance of protected credentials and their administration is rising as a result of safe interactions, privacy of information, and API ownership [12]. Although a lot of contemporary virtual identities are utilized over the top, 6G will utilize identities to manage infrastructure and networking APIs, restrict network utilization, and regulate the utilization of edge compute APIs and network exposure. The prevailing eSIM pattern, the capability of delegate authentication, the potential to use authentication methods depending on the Extensible Authentication Protocol (EAP), and network connectivity are configurations that provide 5G and 6G with an extensive number of alternatives for industrial devices that will accommodate future 6G use cases, in addition to human-held devices and the Internet of Things.

A large portion of 5G security is predicated on widely acknowledged quantum-resistant symmetric-key cryptography elements. But several crucial components rely on asymmetric key cryptography, which makes them vulnerable to attacks from upcoming quantum computers. With the first launch of 6G, it is anticipated that novel quantum-resistant cryptography would be adopted, reducing such concerns. To provide quantum resistance, National Institute of Standards and Technology (NIST)-defined techniques will eventually be incorporated into 3GPP, frequently through modifications to IETF standards. The new NIST algorithms can be supported by a large number of Third Generation Partnership Project (3GPP)-defined interfaces, including those found in the 5G core Small Business Administration (SBA), with no impact on performance. However, one should consider the transmission overhead that comes with new public key methods, for instance, when considering radio access. Development of regulated high-performance security standards and algorithms, like high-speed 256-bit radio access methods, will also be prompted by rising throughput and data protection requirements.

In order to guarantee that user confidentiality and security standards are fulfilled, immersive communications and integrated sensors and communications (ISACs) will introduce extra efficiency and isolating demands. According to the intended use case, different technical approaches and safety measures will be used. For use in enclosed spaces, like a computerized industrial facility, or in situations where there exist no data identifying specific individuals, safety and confidentiality may probably be attained using current technologies and procedures [2]. More effort is required on public networks where data recognizing individuals may be obtained by combining data from multiple sources.

7.2.3 AI and Automation

AI is expected to have a big impact on both user services and platform management for 6G. AI and automation collaborate to maximize productivity, increase how they perform, and strengthen the mobile network's defence against cyberattacks. Mobile network attacks can be detected and handled by AI in a number of ways, such as identifying devices that are acting inappropriately, identifying fake base stations, and identifying and countering signaling attacks. AI and automation for cyber security—such as threat detection and adherence verification—will continue to grow as 6G adoption moves forward.

From a different angle, the increasing dependence on automation and AI places greater demands on AI to be reliable, transparent, secure, and protect security. In order to meet these needs, technological advancements must be complemented with a more thorough comprehension of the characteristics that are crucial for security in a particular application [1]. It also necessitates understanding the limitations of AI technology and how to apply it wisely in perhaps hostile environments. Because intent-based networking has been introduced, it is crucial to make certain that lower-level AI utilization and automated reconfiguration of networks accurately reflect higher-level intents.

AI is becoming more and more important in cyber security, but it cannot take the place of qualified human knowledge. Cyber security professionals will benefit from innovation by having better and more efficient ways to respond to cyberattacks on mobile networks. These mechanisms include identifying attacks, hunting for threats, and intelligence regarding threats. AI could support formalized security evaluation in the creation of security standards. Similarly, AI could be useful in systems development in identifying and clarifying bugs. In EU initiatives like Hexa-X, research is being done on security-preserving strategies for AI in a 6G context. Techniques like homomorphic encryption, differential security, and secure multi-party computational have all been studied.

7.2.4 Network Exposure and API Security

The ability to expose the network's capabilities in a flexible way *via* APIs will help 6G services expand transcend communication by giving applications and service designers more customization and adaptability options for how they utilize the network platform [18]. Although it will also require an emphasis on safeguarding the API usage, availability to network capabilities and information can improve gaming efficiency, drone management, or the broader use of extended reality (XR) in 6G.

Telecom standards-compliant 5G already has APIs, which allow internal and external exposure, with encryption. Authentication, then authorization, and audit logging are a few examples of this security. Application Programming Interface (API) security must be improved with proactive risk analysis, API posture the leadership team, and API performance surveillance as a result of the assumption that 6G will expose more network capabilities that will promote scenarios of use and encourage innovation. Mobile network services will incorporate certain safety concerns related to APIs, whereas others are going to be outlined in regulations. The management of security over the API life cycle generally shared responsibility by suppliers and manufacturers in mobile networks. Encouraging third parties to access network capabilities involves safeguarding subscriber privacy. Security protocols for APIs are not the only measures needed to protect privacy [16].

7.2.5 Assurance and Situational Awareness

Mobile networks have historically prioritized security assurance. Two results are the ongoing research by ENISA on a cyber security accreditation system and NESAS [6], a collaborative effort between 3GPP and GSMA. By ensuring compliance *via* required product testing, safe supply chains, and an efficient software development lifecycle, Network Equipment Security Assurance Scheme (NESAS) actually offers confidence. One may refer to this as preventive assurance. Moreover, functional security of deployed networks, which includes system monitoring and the use of reactive countermeasures, will be necessary for 6G.

In addition to providing security, sophisticated surveillance in 6G will provide management processes and security teams with a greater degree of acute awareness of the network's operating condition. This is a crucial component of zero-trust architecture. While they were not always clearly stated as such, 3GPP has previously implemented numerous of the zero-trust concepts as described by NIST in the frameworks of 3G, 4G, and 5G networks, and 6G standards will keep doing so. Robust identity utilization, secure communication throughout network operations, and authorization of API usage *via* exposure to specific data accessible by the network's base are a few examples.

Using strategies like those developed for a zero-trust framework will contribute to the establishment of an exhaustive structure for 6G security [6]. This architecture enables for adaptation to variations in operational conditions caused by network interactions, crimes, or network failures in some way in addition to demonstrating that protection mechanisms are in place (Figure 7.2). In addition to reducing subconscious confidence throughout entities, the idea of reinforcing procedures to maintain

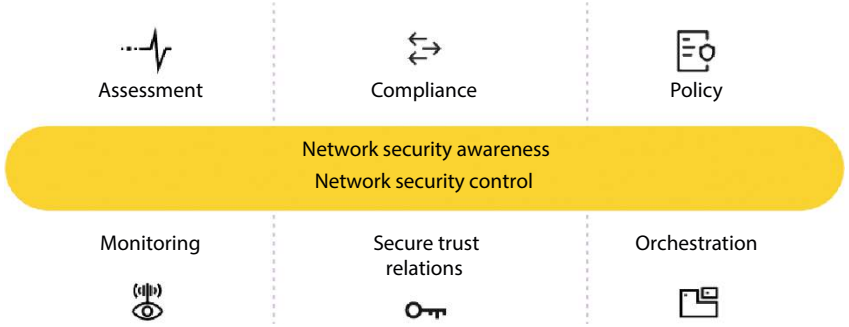

Figure 7.2 Integrating several strategies to create comprehensive security architecture for situational awareness and assurance in 6G.

some level security regardless of the instance of a preliminary intrusion also applies to reducing implicitly trusted between network layers. One instance of such an effort is the endeavor to integrate forward secrecy into the 3GPP authentication and key agreement process and network connection authentication.

7.3 Inspiration for New Technological Innovations

Another benefit of 6G technology that is notable is that it is expected to stimulate the creation of novel, optimized data centers and next-generation apps. These technical advancements are going to keep serving the increasing needs for networking technology and information across numerous industries by collaborating with AI and ML. The development of 6G wireless technology provides the promise to bring forth fresh abilities, sectors, and employment possibilities.

7.3.1 When Will 6G Be Released

"When will 6G come out?" is a common concern that businesses and prospective individuals in the field of network engineering should be asking. As we have mentioned, 6G technology remains being developed and has not been formally released yet. Important trade associations like the ITU, however, predict that 6G internet technology will launch between 2030 and 2035.

The following six wireless communications are being researched, developed, and launched with the help of global efforts:

- **Europe:** The world's initial 6G research initiative is the EU project called the 6G Flagship. Founded in 2018, the project investigates the core elements of 6G technologies throughout Europe, promoting substantial research in four different fields:
  - Wireless Connectivity
  - Devices and Circuit Technology
  - Distributed Intelligence
  - Services and Applications
- **Japan:** During the next few years, the Japanese government will be investing 50 billion yen ($482 million) in the development of 6G technology. By 2025, they hope to showcase cutting-edge mobile and wireless communication technologies.
- **United States:** The US and Japan have agreed to jointly invest $4.5 billion in the development of 6G technology, with the US contributing $2.5 billion and Japan contributing $2 billion.

Furthermore, the Next G Alliance, a 2020 industry project located in North America and backed by companies including Apple, AT&T, Google, T-Mobile, and Verizon, is concentrated on the advancement of 6G wireless technology [3]. The goal of having commercial 6G by the early 2030s is getting closer with continued R&D spending and international cooperation.

7.3.2 Addressing the Tasks of 6G Network Technology

6G technology is nearly set to completely transform cellular communications in the decades to come. It is anticipated to provide low latency, cutting-edge connectivity, and unmatched speeds. With the use of AI and ML and higher frequencies, 6G networks have the potential to greatly improve penetration, and protection, and performance. 6G is expected to elevate the capabilities of current wireless network technologies to new heights, spurring novel sectors, job possibilities, and inventions. It is projected to handle the growing needs of intelligent technologies and IoT devices. When 6G technology is formally introduced, we will be present to assist clients and applicants in adjusting to the changing network landscape.

7.3.2.1 Technologies Underpinning 6G Realization

The revolutionary technologies that will support the audacious 6G ambition are as follows:

- **Terahertz Communication:** The core of 6G networks will be terahertz frequencies, which will allow for fast data transfer over small distances.
- **Meta-Materials:** With the ability to operate at terahertz frequencies, meta-materials will change antenna design and allow for tiny, highly efficient antennas.
- **Unbreakable Encryption** is promised by quantum communication, providing strong security for 6G networks.
- **AI and ML:** AI algorithms will orchestrate and optimize networks, dynamically responding to changing user needs and network circumstances.
- **Edge Computing:** By decentralizing processing of data, edge computing will lower latency and improve 6G apps' responsiveness.

7.4 Machine Learning in the Sixth-Generation Wireless Technology Era

The combination of innovative algorithms using the sixth version of wireless technology is known as "machine learning with 6G" as shown in Figure 7.3. In a nutshell, it is teaching mobile networks and gadgets to become smarter and more effective by learning how to solve problems on their own. In 6G, ML is crucial for activities like maximizing network capacity, anticipating and averting problems, improving security, and tailoring services to the specific requirements of each user. This combination of technologies is meant to completely transform the way we engage with and experience wireless communication, making it faster, smarter, and more personalized.

ML, as used in the context of 6G, describes an effective technology that allows networks and devices to evolve and adapt. They may learn from experiences and arrive at judgments relying on information rather than becoming explicitly programmed. This feature enables 6G to become a smart and dynamic system, going beyond only data transmission.

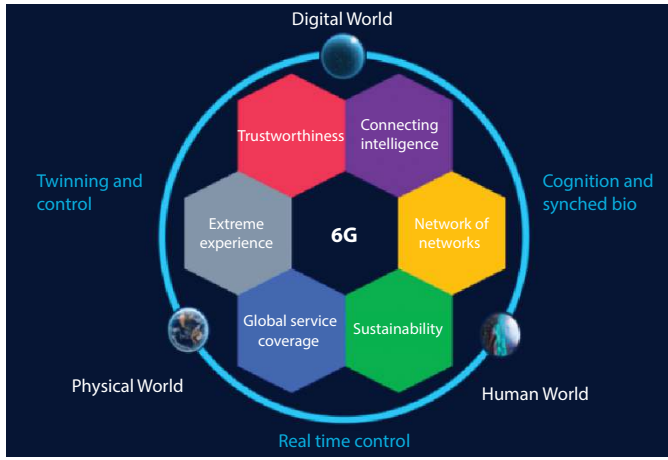

Figure 7.3 Enhancing 6G capabilities with machine learning.

ML dramatically expands 6G networks' potential. By maximizing the distribution of network resources, it guarantees effective utilization of bandwidth and minimizes latency. It also performs a predictive function by anticipating possible problems and averting them while they influence the network [8]. Robust safety measures are enhanced by ML, which recognizes and neutralizes threats instantly. Furthermore, it makes customized services possible by figuring out each user's unique requirements, resulting in an even more proactive and customized 6G experience. In summary, ML is integrated into 6G in order to render it not just quicker but additionally more intelligent and flexible.

7.4.1 Advantages of Machine Learning in 6G

- **Dynamic Resource Optimization:** 6G networks can now distribute resources more effectively, maximizing bandwidth and guaranteeing effective use, which lowers latency and improves efficiency. This is made possible by ML.
- **Better End-to-End Connection:** ML may contribute to better end-to-end connection, which will enable a more sustainable and connected society.
- **Advanced techniques:** Resource allocation, process offloading, and handover managerial issues may be resolved by utilizing cutting-edge ML techniques, such as unsupervised, supervised, and deep learning, reinforcement learning, and federated training.

- **Energy Efficiency:** By lowering latency and streamlining network operations, ML technologies may dramatically increase the energy effectiveness of 6G wireless networks.
- **Pervasive AI:** In an environment with a lot of interference, AI and ML will prove essential for optimization of networks, waveforms design, flexible allocation of resources, and traffic flow management.
- **Large-Scale Optimization:** Because of its accuracy, computational speed, flexibility, and generalizability, ML emerges as a potential approach for challenging large-scale optimization issues in 6G.
- **Smart Usage Scenarios:** Featuring the help of ML technology, the 6G industry will be able to create smart usage scenarios with vast data warehouses and all-encompassing services by utilizing advancements in imaging, being there, and location awareness.

7.4.2 Toward 6G: Imagining Applications of the Next Generation for 2030 and Afterward

A major advancement in system capacities transcend communication is anticipated with the 6G technology platform as shown in Figure 7.4. The first step toward this progress is outlined in the ITU-R–defined IMT-2030 framework, which provides a baseline for future wireless technologies by defining important use scenarios and performance indicators [15]. The development of these innovations is expected to bring about the convergence of the physical, digital, and virtual worlds into a new age with 6G, which will incorporate AI, advanced computing, and resilient system characteristics along with cutting-edge green technologies as well as ISAC.

Despite the fact that many contributor presentations focused on various sets of 6G use cases, we saw some distinct patterns regarding the main use cases that are under consideration. An indicative (i.e., non-exhaustive) list of the primary use cases covered in the workshop is provided below:

- Immersive Experiences: 6G will enable lightweight devices, which can be installed at the identical scale as current smartphones, therefore taking XR to entirely new heights. Hyper-realistic experiences, which include holographic teleportation, can be achieved with the help of novel capabilities including improved sensor fusion, brain-computer

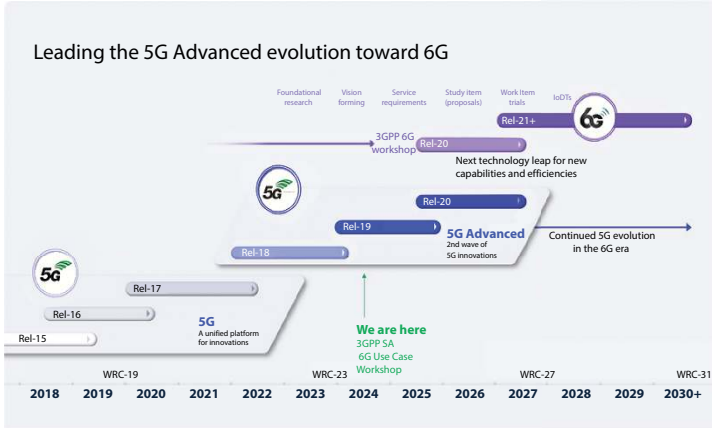

Figure 7.4 The ongoing advancement of 5G advanced technologies is part of the route to 6G.

interface, and digitalization of multisensory components (such as human emotions of touch, smell, sight, and taste). Enabling live and dynamic immersive content development and distribution is another field of concentration.

- **Digital Twins:** By simulating a physical system within the digital realm, new use cases and efficiency, such as communication networks, may be made possible. 6G digital twins are expected to deliver several new benefits, including improved safety and confidentiality, predicting and prescriptive insights, and quick advances in AI.
- **Robotics and Smart Industries:** 5G laid the technological groundwork for outstanding performance industrial IoT (such as TSN and URLLC), and 6G aims to fully realize the future potential of next-generation robotics, which includes delivery and customer service robots in addition to self-sufficient and cooperative robots capable of cooperate with people in this highly computerized and integrated setting.
- **Fixed Wireless Access:** 6G offers a chance to completely transform internet services. 6G may provide high network capacity and enhanced cost-efficiency by allocating additional wide-area spectrum (such as upper mid-band); expanding connectivity throughout urban, suburban, and rural areas equally; and promoting more inclusiveness and connectedness.

- **IoT of the Future Generation:** It is critical that 6G will be able to effectively support devices with less complexity right now. Low-power, wide-area (LPWA) and ambient IoT (i.e., powered by energy harvesting with or without storage) devices are among the several vertical services that 6G is expected to enable in the automotive, healthcare, agricultural, and other industries.
- **Connected Transportation:** 6G has the potential for unprecedented levels of safety and comfort. The 5GAA consortium envisaged the next-generation network to allow intelligent autonomous driving systems and real-time environmental modeling using new 6G capabilities like ISAC.
- **Critical Communications:** The goal of 6G is to provide mobile communications with an even higher degree of security, dependability, and trust. For use cases that are mission-critical, like public safety communications, this is extremely crucial. In order to achieve widespread coverage and beyond, 6G must take use of the deployment and learning from 5G.
- **Additional Developing Use Cases and Deployments:** Many of these 6G use cases are anticipated to supply services by utilizing seamless multi-connectivity technologies covering terrestrial and/or non-terrestrial communications. Of fact, the 6G technology cycle is still in its very early stages. We can clearly see that the future has use cases, which will be beyond our present ability to imagine as we remain on the cusp of these developments.

7.5 6G Technology's Future Reach and Its Effects on Business

As seen in Figure 7.5, businesses must adopt a proactive strategy that combines flexible implementation with strategic planning for the purpose to fully benefit from 6G technology. These are crucial strategies that businesses have to consider:

- **Invest in Research and Development:** Keep up with the most recent advancements in 6G technology and take part in research projects to understand how it will affect our business. Work together with research centers, business associations, and technology companies to investigate possible applications and create customized solutions.

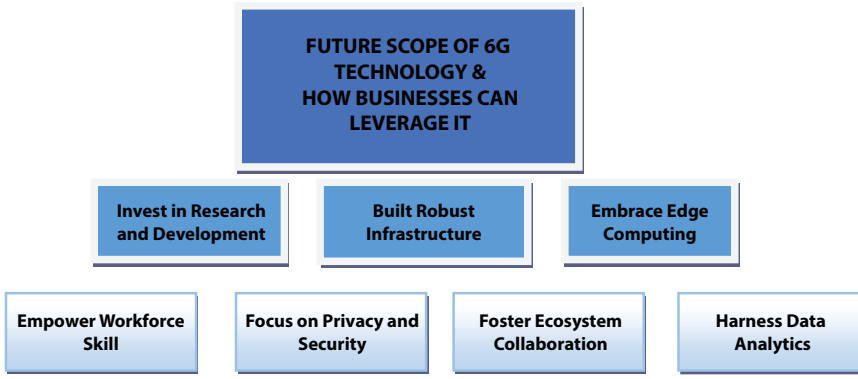

Figure 7.5 6G technology's future reach and its effects on business.

- **Build Robust Infrastructure:** Invest in a solid infrastructure that can handle the increased capabilities of 6G to set the stage for its adoption. Enhance the network design, implement cutting-edge antenna systems, and maximize the use of available spectrum to provide uninterrupted connectivity and optimal communication performance.
- **Embrace Edge Computing:** Use edge computing to improve responsiveness and reduce latency, especially for applications that are latency-sensitive like industrial automation and driverless cars. In order to process and make decisions in real time, transfer computer resources more closely to the location where the data is generated.
- **Utilize Data Analytics:** To gain useful insights, take advantage of the abundance of data produced by 6G-enabled devices and apps. Invest in AI-driven algorithms and sophisticated analytics tools for real-time data stream analysis. This will allow for targeted marketing, tailored services, and predictive maintenance.
- **Encourage Cooperation Among Ecosystems:** Develop strategic alliances inside the 6G ecosystem to jointly develop ground-breaking technologies and seize fresh market possibilities. Work together with colleagues in the industry, technology suppliers, and telecoms carriers to hasten the implementation of services provided by 6G.
- **Put Security and Privacy First:** To protect critical data in the 6G environment, put strong security protocols, encryption techniques, and access restrictions in place. Reduce hazards and make absolutely reliable online.

- **Enhance Workforce Skills:** Make investments in up skilling and training programs to provide our employees the skills they need to succeed in a 6G-enabled workplace. Encourage an innovative and perpetual learning culture to propel digital change throughout the company.

7.6 Conclusion

In order to adapt to a changing threat landscape, accommodate novel scenarios, changes in the environment and society, and comply with regulatory standards, 6G security will incorporate extra safeguards compared to 5G security. 6G securities will have to be built around an integrated approach, integrating various options and methods to gain situational awareness, as mobile networks become increasingly recognized as vital facilities and the cyber-physical combine emphasizes the significance of connection in daily life. The operational assurance, autonomous security and threat management, and zero-trust principle–based systems will all add to the situational awareness.

The foundation of mobile networks continues to be worldwide open standards, which guarantee interoperability, privacy, and transparency. Furthermore, there is a growing convergence of standards and implementation; hence, a major challenge in safely implementing and running 6G networks will involve combining free software, norms, and different implementation technologies. Although the 6G security perspective will need to be comprehensive, there are some specific issues that warrant further discussion, including network service accessibility; intriguing data protection and privacy regulations; ensuring that 6G is quantum-resistant; using protected AI and automation to improve network security, network exposition, and API safeguards; and operational privacy assurance.

References

1. Abasi, A.K., Aloqaily, M., Guizani, M., 6G mmWave Security: Next-Gen Protection with Federated Learning, in: *ICC 2024-IEEE International Conference on Communications*, IEEE, pp. 4281–4286, 2024, June.
2. Adil, M., Song, H., Khan, M.K., Farouk, A., Jin, Z., 5G/6G-enabled metaverse technologies: Taxonomy, applications, and open security challenges with future research directions. *J. Netw. Comput. Appl.*, 103828, 2024.

3. Ahad, A., Jiangbina, Z., Tahir, M., Shayea, I., Sheikh, M.A., Rasheed, F., 6G and Intelligent Healthcare: Taxonomy, technologies, open issues and future research directions. *Internet Things*, 25, 101068, 2024.
4. Alhammadi, A., Shayea, I., El-Saleh, A.A., Azmi, M.H., Ismail, Z.H., Kouhalvandi, L., Saad, S.A., Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges. *Int. J. Intell. Syst.*, 2024, 1, 8845070, 2024.
5. Alsharif, M.H., Jahid, A., Kannadasan, R., Kim, M.K., Unleashing the potential of sixth generation (6G) wireless networks in smart energy grid management: A comprehensive review. *Energy Rep.*, 11, 1376–1398, 2024.
6. Alshaer, N.A. and Ismail, T., II, AI-Driven Quantum Technology for Enhanced 6G networks: Opportunities, Challenges, and Future Directions. *J. Laser Sci. Appl.*, 1, 1, 21–30, 2024.
7. Alwahedi, F., Aldhaheri, A., Ferrag, M.A., Battah, A., Tihanyi, N., Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet Things Cyber-Phys. Syst.*, 4, 167–185, 2024.
8. Banik, S., Kothamali, P.R., Dandyala, S.S.M., Strengthening Cybersecurity in Edge Computing with Machine Learning. *Rev. Intel. Artif. Med.*, 15, 1, 332–364, 2024.
9. Blika, A., Palmos, S., Doukas, G., Lamprou, V., Pelekis, S., Kontoulis, M., Askounis, D., Federated Learning For Enhanced Cybersecurity And Trustworthiness In 5G and 6G Networks: A Comprehensive Survey. *IEEE Open J. Commun. Soc.*, 6, 3094–3130, 2024.
10. Chataut, R., Nankya, M., Akl, R., 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. *Sensors*, 24, 6, 1888, 2024.
11. Damaraju, A., The Future of Cybersecurity: 5G and 6G Networks and Their Implications. *Int. J. Adv. Eng. Technol. Innov.*, 1, 3, 359–386, 2024.
12. Hatim, J., Habiba, C., Chaimae, S., Evolving Security for 6G: Integrating Software-Defined Networking and Network Function Virtualization into Next-Generation Architectures. *Int. J. Adv. Comput. Sci. Appl.*, 15, 6, 909–914, 2024.
13. Ishteyaq, I., Muzaffar, K., Shafi, N., Alathbah, M.A., Unleashing the Power of Tomorrow: Exploration of Next Frontier with 6G Networks and Cutting Edge Technologies. *IEEE Access*, 12, 29445–29463, 2024.
14. Kaur, N., Kshetri, N., Pandey, P.S., 6AInets: Harnessing artificial intelligence for the 6G network security: Impacts and Challenges, *arXiv preprint arXiv:2404.08643*, 2024.
15. Khare, B.K., Sahu, D., Pandey, D., Tiwari, M., Kumar, H., Siddiqui, N., Exploring Machine Learning Solutions for Anomaly Detection in 6G Communication Systems, in: *Security Issues and Solutions in 6G Communications and Beyond*, pp. 230–250, IGI Global, 2024.

16. Mukherjee, S., Machine Learning Methodologies for Beyond 5G and 6G Heterogeneous Networks: Prediction, Automation, and Performance Analysis, Doctoral dissertation, University of Missouri-Kansas City, 2024.
17. Nair, M.M., Deshmukh, A., Tyagi, A.K., Artificial intelligence for cyber security: Current trends and future challenges, in: *Automated Secure Computing for Next-Generation Systems*, pp. 83–114, 2024.
18. Rojek, I., Kotlarz, P., Dorożyński, J., Mikołajewski, D., Sixth-Generation (6G) Networks for Improved Machine-to-Machine (M2M) Communication in Industry 4.0. *Electronics*, 13, 10, 1832, 2024.
19. Sabir, B., Yang, S., Nguyen, D., Wu, N., Abuadbba, A., Suzuki, H., Nepal, S., Systematic Literature Review of AI-enabled Spectrum Management in 6G and Future Networks. arXiv preprint arXiv:2407.10981, 2024.
20. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-Based wireless sensor network, in: *Software-Defined Network Frameworks*, pp. 121–141, CRC Press eBooks, Cornell University, Ithaca, New York, 2024, https://doi.org/10.1201/9781003432869-8.
21. Sun, M. and Sun, L., Harnessing the Power of 6G Connectivity for Advanced Big Data Analytics with Deep Learning. *Wirel. Pers. Commun.*, 24, 6, 1–18, 2024.
22. Valencia-Arias, A., González-Ruiz, J.D., Verde Flores, L., Vega-Mori, L., Rodríguez-Correa, P., Sánchez Santos, G., Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy. *Information*, 15, 1, 65, 2024.
23. Varadam, D., Shankar, S.P., Nidhi, N.P., Dubey, V., Jadwani, A., Taj, S.F., Bharadwaj, A., AI in 6G Network Security and Management, in: *Reshaping CyberSecurity With Generative AI Techniques*, pp. 173–200, IGI Global, 2025.
24. Zhu, X., Liu, J., Lu, L., Zhang, T., Qiu, T., Wang, C., Liu, Y., Enabling Intelligent Connectivity: A Survey of Secure ISAC in 6G Networks. *IEEE Commun. Surv. Tut.*, 27, 2, 748–781, 2024.

8

Applications of Machine Learning in Strengthening 6G Security

Gaganjot Kaur[1]*, Vineet Shrivastava[1], Surbhi Bhatia Khan[2] and Anshu Singh[3]

[1]Department of Computer Science & Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, India
[2]Data Science Department, University of Salford, Salford, United Kingdom
[3]MBA Department, ABES Business School, Ghaziabad, India

Abstract

With the introduction and rise in the wireless communication, sixth-generation (6G) technology scripts a trending and transformative era in today's world, especially defined by multiple benefits including ultra-low latency, more than a million-device connectivity, high and very-high data speeds, and advance technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and quantum computing integration. These advancements enable unparalleled capabilities across domains, including, but not limited to, the Internet of Things, ultra-modern smart cities, autonomous vehicles, and extended reality. However, the novel features of 6G also present significant security challenges, requiring robust strategies to ensure data integrity, privacy, and network reliability. Henceforth, focusing on this, the present research explores the vital and essential role of ML in enhancing security and highlighting its applications in dynamic threat detection, predictive maintenance, automated response systems, and anomaly detection. By employing the real time data analysis, the advanced ML algorithms deliver adaptive and intelligent responses to security breaches, optimizing network resilience and overall system efficiency. In addition to this, this present work also examines the integration of ML with other advanced technologies such as quantum-safe cryptography and decentralized authentication systems to strengthen the 6G security framework. Conclusively, considering the aspects and scope of 6G in the future, the comprehensive analysis presented in this paper highlights the essential role of ML in building resilient, adaptive, and secure communication infrastructures

**Corresponding author*: gaganjot28784@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (167–190) © 2026 Scrivener Publishing LLC

for the upcoming wireless technology generation, settling in the foundation for sustainable and reliable AI-driven 6G ecosystems.

***Keywords*:** 6G network, artificial intelligence (AI), Internet of Things (IoT), machine learning (ML), 6G network security

8.1 Introduction

Following the highly successful testing, development, and deployment of fifth-generation (5G) network all around the world, the advancements and requirement in the next generation, i.e., sixth-generation (6G) wireless communication networks, are critically significant as well as important. This is one of the key milestones in the history of wireless communication and/or telecommunications, confirming the rise in communication network while providing multiple benefits in various engineering sectors. While 5G networks have already introduced notable advancements, data speeds, and latency reduction, 6G is poised to exceed these achievements dramatically and reach newer heights. Anticipated to launch around 2030, 6G networks are expected to provide high data rates, i.e., at least a terabit-per-second and low latency, i.e., at a microsecond level, enabling near instantaneous data transmission. These advancements have the potential to power next-generation applications including, but not limited, to real-time holographic communication, immersive augmented and virtual reality (AR/VR) experiences, autonomous systems, remote surgeries, and ultra smart cities, fostering a fully connected and super-intelligent society.

However, such critical and essential capabilities and overall advantages/benefits also invites equally critical and significant security concerns. The scope of 6G includes not only a dramatic increase in device density potentially supporting more than a million devices per square kilometer but also a dependence on the recent and modern technologies like artificial intelligence (AI) and machine learning (ML) to manage, optimize, and protect networks. Therefore, these networks must operate in highly dynamic, complex environments populated with diverse connected devices, including, but not limited, to the Internet of Things (IoT) sensors, smart vehicles, such as autonomous and electric vehicles, and modern infrastructure. Ensuring security, integrity, and privacy of such an expansive ecosystem is a formidable challenge, as even one of the million connected devices can present a potential vulnerability threat and a point for abnormal or malicious activity. Henceforth, to address such an issue(s), this requires the development of a robust, adaptive, and intelligent security framework capable of evolving in real time to counter emerging threats.

While there are multiple advanced technologies with multiple benefits, ML proves to be a prominent solution for such security-related issues. It provides

intelligent, quick, and smart defense mechanism especially in view of the 6G networks. In contrast to the conventional and traditional algorithms, ML-based approach allows the operators and users to identify, analyze, and respond to all the critical threats, along with continuous monitoring capability from the network data. Along with this, it also adapts to novel attack patterns that differ in terms of their properties at all times. Besides, it also provides the capability of autonomous network optimization in view of the overall network performance. In view of this, the multiple ML applications include enhanced maintenance, automated system responses, abnormality detection, and better network robustness. In addition to this, ML also provides the capability to reduce the level of security concerns especially when integrated with other advance technologies like blockchain. It allows removing the issues related to single point of failure, etc. In view of this, Figure 8.1 presents the 6G security framework while mentioning the different aspects and features, including authentication and encryption.

Henceforth, taking into account the various aspects of 6G network and its benefits, this paper explores and presents the scope of advance technologies, especially ML in strengthening the overall network. This includes the scope of ML in various applications such as threat mitigation, reliable source allocation, and robust infrastructure. Therefore, through an in-depth analysis of all such aspects, the research highlights the role and scope of ML that how it contributes to the overall development of this

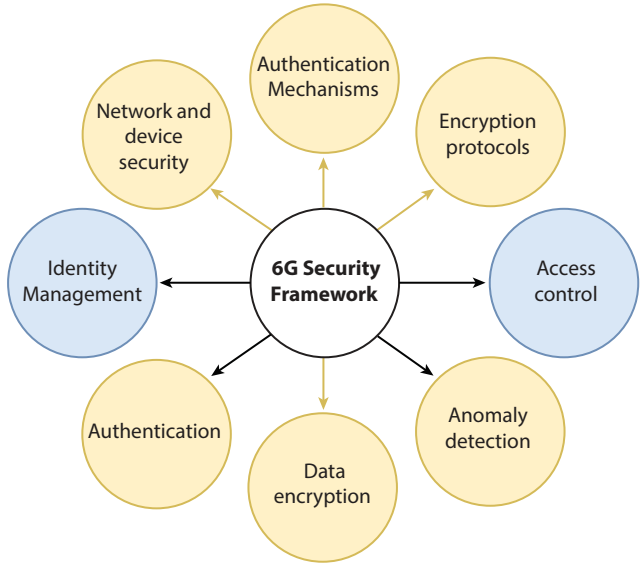

Figure 8.1 6G security framework.

trending technology, especially in view of safeguarding this technology, while the work also presents the other aspects of 6G network. By examining ML's integration with blockchain and quantum cryptography, this paper highlights the transformative potential of advanced approaches in establishing a secure, scalable, and sustainable 6G ecosystem.

8.1.1 Key Features and Innovations

Ultra-Low Latency: 6G aims to achieve latency in the microsecond range, enabling real-time applications, including, but not limited to, remote surgery, autonomous driving, and interactive holography.

Enhanced Data Rates: With data rates exceeding 1 terabit per second (Tbps), 6G supports high-definition content, AR/VR, and other bandwidth-intensive applications.

Massive Device Connectivity: These networks are projected to connect up to more than a million devices/square kilometer, powering smart cities, industrial automation, and/or extensive sensor networks.

Terahertz Communication: By utilizing terahertz (THz) frequencies, these network offers extremely high data rates and large bandwidths, despite challenges including the limited range and increased susceptibility to atmospheric absorption.

AI and ML: They play a crucial role in these networks by optimizing performance, managing resources, and addressing the possible and potential issues predictively, enabling self-optimizing networks.

Holographic Communication: These networks enable realistic 3D holographic communication, revolutionizing remote work, education, entertainment, and social interactions.

Integration with Satellites: Enhanced integration with satellite networks ensures seamless global coverage, critical for connecting rural and remote regions.

8.1.2 Potential 6G Applications

Ultra-Modern and Smart Cities: The 6G network is vital for the smart and ultra-modern cities by enabling seamless integration of multiple services including advanced traffic management, optimal and efficient energy

distribution, and smart environmental monitoring, especially using the smart sensors, such as IoT, etc.

Healthcare: These networks are ideal as well as vital for applications such as remote surgery, real-time monitoring, and telemedicine, significantly enhancing the access to medical healthcare services.

Industrial Automation: This network supports Industrial Internet of Things while enhancing manufacturing efficiency, minimizing downtime, and, besides, enabling predictive maintenance.

Entertainment and Media: These networks revolutionize entertainment through high definition streaming, especially live streaming as well as the highlights, along with immersive AR/VR experiences.

Transportation: Autonomous vehicles benefit from these networks real-time communication capabilities while enabling the coordinated traffic management, improved safety,and efficient route planning.

8.1.3 Emerging Security Challenges in 6G

The advantages and multiple benefits of the 6G networks come with significant security challenges. Its enhanced capabilities and widespread connectivity introduce multiple vulnerabilities that are concernful and, therefore, need to be essentially addressed while aiming optimal integrity and confidentiality of communication networks.

Increased Attack Surface
Device Proliferation: With over tens of millions of connected devices per square kilometer, the potential entry points for cyberattacks increase to new levels. Each device represents a vulnerability that attackers could exploit, necessitating robust and hardcore security measures across the network.
IoT Security: The multiple IoT devices have limited processing power and minimal security features. Securing these devices in such a network, where these devices play a key role and are essential to maintaining overall network security.

Data Privacy and Protection
Massive Data Generation: These networks generate vast amounts of sensitive data and safeguarding such information from unauthorized access while ensuring user privacy are currently the most critical priorities.

Data Integrity: Protecting the integrity of data as it travels through the network is very important as well as critical. Any tampering or corruption could lead to severe consequences, particularly in applications such as healthcare and/or autonomous driving.

Advanced Threats and Attack Vectors
Sophisticated Cyberattacks: As such networks grow in complexity, so do cyberattacks. Threats including, but not limited to, AI-driven malware, deepfakes, and multi-vector attacks require advanced, adaptive security mechanisms to mitigate and/or reduce the possible risks.
Quantum Computing: This ideology presents significant and critical challenges to current encryption methods. Implementing quantum-resistant encryption techniques is, therefore, most important and necessary to counteract these threats.

Network Infrastructure Security
Core Network Vulnerabilities: The core infrastructure of these networks including switches, routers, and data centers is a prime and key target for attackers. Therefore, the comprehensive and critical security for this infrastructure is important as well as essential.
Software-Defined Networking (SDN) and Network Function Virtualization (NFV): While SDN and NFV provide flexibility and scalability, they also introduce vulnerabilities, particularly in virtualized network functions and SDN controllers.

8.1.4 Challenges in Implementing Robust Security Measures

- Multiple devices, i.e., out of the million possible devices that can potentially connect within a 6G network, particularly, the IoT devices and/or sensors, have limited computational and energy resources. Therefore, it is important and noteworthy to take into account all their possible constraints while balancing the robust system security is a critical challenge and needs to be properly addressed.
- The multiple 6G applications need real-time processing and low latency. Security measures must operate effectively without introducing prominent delays.
- Ensuring only authorized multiple devices and many users accessing the 6G network is required and basically fundamental. Taking this into account, the advanced authentication

mechanisms, such as biometrics, through facial features, etc., and multi-factor authentication, are highly recommended.
- One of the most critical and important aspect is trust, i.e., developing trust among the multiple devices and diverse users in the network is crucial. For this purpose, the advanced technologies such as blockchain provide unmatchable records of transactions and interactions, confirming the transparency and overall trustworthiness within the given system.

8.1.5 Regulatory and Compliance Issues

Global Standards and Regulations: Harmonized worldwide standards and regulations are necessary to deploy the 6G networks successfully around the globe. This particularly includes that the multiple policymakers and various industry stakeholders must collaborate to develop these frameworks for the overall success and improved efficiency/performance of these networks.

Compliance with Data Protection Laws: As per the data, national/international protection laws are very critical, required, and, therefore, an essential step in developing and deploying the 6G networks. Therefore, all the related organizations must follow and thereby implement such reliable and robust measures to protect the data of more than a million users and ensure regular regulatory compliance.

8.2 Role of ML in Aspects of Security Challenges

ML is a vital, critical, essential, and one of the most trending technology for addressing the 6G network security challenges. With 6G's massive connectivity and high data throughput, the traditional security approaches struggle to keep up with the complexity and volume of potential threats and other issues. By leveraging ML algorithms, 6G networks incorporate advanced and adaptive security measures that protect networks from diverse and evolving cyber threats. Additionally, ML also empowers the development of intelligent, data-driven security solutions that proactively identify risks, streamline network management, and, lastly, enhance the overall robustness of network infrastructure.

Advanced Threat Detection: In the process, ML algorithms analyze large real time datasets, identifying different related patterns, anomalies, and irregularities that signal possible and potential security threats. This

capability enables the proactive detection of malicious activity, allowing the 6G networks to identify cyber threats much earlier than the multiple traditional and conventional methods. Techniques such as anomaly detection, clustering, and deep learning continuously refine the understanding of "normal" network behavior, and, therefore, as a result, these networks recognize subtle shifts in data patterns that indicate emerging threats, ensuring quick detection and response before any type of the security breaches escalate.

Predictive Maintenance: The extensive infrastructure of the 6G networks requires high levels of reliability and resilience. ML can effectively predict when specific network components, including, but not limited to, routers, IoT devices, and/or base stations, are likely to fail or experience performance degradation. In the process, by analyzing the historical performance data and environmental factors, the ML models have the capability to identify potential points of failure and alert network administrators to perform preemptive maintenance. This high end and crucial predictive capability minimizes the unplanned downtime and limited security vulnerabilities and, therefore, confirms the consistent and secure performance, particularly in mission-critical applications.

Automated Response Systems: ML-driven automated response systems are crucial for the 6G networks, which demand real-time and quick responses to security incidents within the overall system. This way, these systems enable quick and efficient actions by analyzing the received data and executing the pre-defined, data-driven response protocols for stable and performance oriented system.

Unlike the traditional and conventional methods, ML-based automated systems specifically learn and adapt to the conditions over time, enhancing their response strategies as they encounter newer challenges, in the form of potential threats. These systems have the capability to isolate compromised devices, update firewall rules, re-route device traffic, and activate specific defense mechanisms in an automated manner, aiming for efficient overall system performance. This behavior reduces the impact of the threats while confirming the robustness and integrity of the system.

Continuous Adaptation to Evolving Threats: The 6G networks face the time-to-time evolving threats. Concerning this, i.e., the potential threats, the advance and trending ML models used for threat detection and other benefits are dynamic in nature and adapt to the newer data quickly and

the different threat patterns. In addition to this, the multiple other similar techniques enable such models to update their system parameters in real time, aiming to improve their accuracy and overall effectiveness. This allows combatting complex attacks and AI-driven malware, providing efficient defence mechanism for high-density and high-speed networks.

Focusing on the above, this chapter provides a comprehensive analysis of the role and significance of ML in enhancing the 6G network security: Following this, Section 8.2 of this work comprehensive and detailed literature review related to the advancements in AI and ML within the wireless networks, especially focusing on 6G. Following this, Section 8.3 particularly explores the 6G security framework architecture showcasing its various aspects. In continuation, Section 8.4 discusses the factors such as performance metrics and regulatory compliance related to the 6G network. Then, Section 8.5 particularly highlights the various challenges and limitations of developing and, therefore, implementing the 6G security. Lastly, Section 8.6 concludes the work by presenting the critical insights while presenting the future research directions. Thus, through this work, the ideology is to offer a clear and in-depth understanding of how ML contributes to the concept of robust security in the 6G wireless Networks.

8.3 Literature Review

Wireless technologies are rapidly evolving day by day, with advancements in AI and ML playing a critical role in enhancing network performance. The AI/ML empowers the networks to make intelligent and quick decisions, automate processes, analyze large datasets, enable predictive capabilities, and, most important, adapt to dynamic conditions. Next-generation wireless networks require sophisticated AI for automated information delivery between smart applications.

Recent successes in ML and deep learning (DL) have spurred interest in AI-enabled wireless networks. This paper surveys AI technologies for various network applications, discusses AI-enabled uses, and addresses challenges and future research trends. It offers suggestions for making networks more intelligent and capable of handling complex problems, helping researchers understand AI-based designs and identify key research issues [1].

Explainable artificial intelligence (XAI) is crucial for enhancing the interpretability, transparency, and reliability of ML models, particularly in critical fields like cyber-security. Deshmukh *et al.* [2] discuss the approaches, structures, and evaluation criteria for implementing and comparing XAI techniques, offering a comprehensive understanding of XAI in adversarial ML.

Key aspects such as model-agnosticism, global/local explanations, adversarial resistance, interpretability, computational efficiency, and scalability are explored. As 5G is deployed, focus shifts to 6G that supports diverse applications and face numerous security threats due to open wireless channels and dynamic topology.

Traditional security mechanisms struggle against physical layer attacks, especially in IoT. Physical layer security (PLS) leverages channel randomness and hardware imperfections, enhanced by AI. Zhang *et al.* [3] review ML-empowered PLS techniques for 6G, covering key technologies and solutions for key generation, secure transmission, and attack detection, highlighting the future research opportunities.

The 6G communication network enhance the intelligent IoT, creating multiple possibilities such as Internet for Everything. Accordingly, the AI along with 6G is in the process to shift the current trend from connected things to a better version and as per the upcoming trend, i.e., connected intelligence. In continuation to this, the work in [4] explores AI's role in revolutionizing 6G, focusing on applications that address human needs and create value for new technologies. Likewise, to [4], the work in [5] presents the rise of AI applications is shaping the aspects of wireless networks, with 6G expected to transform to "connected intelligence." The existing AI systems based on DL and data analytics methodologies require large and complex computation and multiple communication sources, leading to latency, high and non-required energy consumption, high and inefficient network congestion, and a number of serious privacy issues. In view of this, the edge AI, integrating multiple characteristics such as sensing, better computation, and overall better intelligence at the network edge, provides an optimal solution to such problem in view of better efficiency, enhanced effectiveness, optimal and improved privacy, and, lastly, significant and essential 6G security.

Conclusively, reference [5] presents the aspects of edge AI in view of it being scalable and a reliable option while highlighting on the wireless communication strategies. In addition, this includes the decentralized ML algorithms, network design concepts and ideology, system architecture, standardization, platforms, resource allocation optimization, and multiple application scenarios for industrialization and commercialization to provide security for the same. Singh *et al.* [6] explore the AI integration along with the self-learning models for smart city ecosystems, addressing the evolving requirements of IoT, etc. Unlike existing studies focusing on either application requirements or network agility, this paper takes a holistic approach. It discusses the evolution from 1G to AI-driven 6G networks, offering taxonomy of technology-enabled smart city applications and

outlining future research directions. The deployment of 5G networks introduces novel features compared to 4G and sets the stage for the imminent rollout of the next generation, i.e., 6G wireless communication systems by the year 2030. Focusing on this, the present work explores the transformative potential of 6G, addressing challenges including, but not limited to, enhanced system capacity, better data rates, and improved service quality (QoS). It also presents the emerging technologies like AI and optical wireless, projecting 6G speeds of up to 1,000 Gbps and enabling innovations such as 3D holographic communication and extended reality (XR). The integration of AI and ML enhances 6G's capabilities in sub-mm wave technology while promising advancements in wireless sensing and mobile edge computing [7].

In the ultimate dynamic evolution of wireless communication, each generation from 1G's analog simplicity to 5G's digital prowess has driven transformative advancements in connectivity. With 5G laying the groundwork for global interconnectivity, the worldwide attention now turns to 6G networks. Chataut *et al.* [8] explore the foundational technologies and benefits of 6G networks, including terahertz communication, ultra-massive Multiple Input Multiple Output (MIMO), AI, ML, quantum communication, and reconfigurable intelligent surfaces. By integrating AI/ML, the 6G network promises unprecedented capabilities in mobile broadband and applications including smart cities and autonomous systems. Addressing challenges from technology to regulation, this study maps the future landscape of 6G networks, aiming to inspire the future research and innovation in this rapidly evolving field.

With 5G now deployed, focus shifts to designing the 6G system, which integrates space air-ground-sea platforms for diverse applications requiring stringent QoS and security standards. Given the open wireless channel and dynamic network topology, 6G network faces significant security challenges. Traditional cryptography struggles to counter physical layer attacks, especially in the IoT devices. PLS leverages wireless channel randomness and hardware imperfections to bolster security, further augmented by AI advancements.

Focusing on this, Zhang *et al.* [3] discussed a comprehensive overview of ML-driven PLS techniques for 6G networks, covering key technologies, security threats, ML methods, and recent advancements. It particularly concludes by highlighting future research opportunities for a more intelligent and secure 6G network. Following this state-of-the-art work, reference [9] presents the security of 6G technology as a concernful ideology for industry, governments, as well as academicians. To mitigate the specific cyber threats, new security approaches leveraging AI and Zero-Trust Architecture (ZTA) are proposed. This work analyzes current research in 6G network security, highlighting AI algorithms and ZTA while identifying

their limitations. Addressing these gaps, the work done in reference [9] proposes a new 6G security framework based on ZTA, incorporating adaptive AI algorithms implemented through hierarchical defense agents. These special measures aim to effectively bolster the security of 6G networks, their components, and overall services.

Additionally, the security management involves identifying and safeguarding company assets through various policies and multiple procedures. As AI applications thrive with trending and critical advancements in DL and cloud-edge computing, the IoT-related security challenges still persist. Thus, introducing 6G wireless communication assisted security management using AI aims to highlight and improve the overall system security. This framework integrates an energy-efficient 6G real-time communication system and a deep neural network-based security module to optimize network efficiency, reduce energy consumption, enhance privacy, ensure data integrity, and strengthen network security. Thus, Rekkas *et al.* [10] explore AI's role in enhancing 6G network security, addressing strategic challenges and proposing solutions.

AI, particularly ML, is pivotal in developing and optimizing 6G network applications. Noman [11] presents a concise overview of ML methods and a current ML application in 6G systems. These includes supervised, unsupervised, and reinforcement techniques. The work also examines unresolved challenges in ML for 6G networks and wireless communications, along with potential future trends to inspire ongoing research in this domain. 6G networks, as the next-generation communication standard, prioritize enhanced end-to-end connectivity for sustainability. AI advancements enable innovative technologies *via* ML models, vast datasets, and robust computing power. ML-driven intelligent resource management in 6G leverages parallel computing and autonomous decision-making to boost energy efficiency and computational capacity. Thus, Pandi [12] categorizes state-of-the-art ML algorithms in 6G, focusing on applications like Device-to-Device (D2D) networks, Vnet, and Fog Radio Access Networks (F-RANs). It addresses resource allocation, task offloading, handover management, energy efficiency, and latency reduction while outlining future research directions in ML-based 6G resource management.

The 6G of cellular transmission promises pervasive wireless connectivity for a fully connected world, supporting diverse smart devices and applications. This paper compares 6G with 5G technologies, highlighting security and privacy challenges. It proposes an authentication and identification approach for 6G security, emphasizing authentication and flexible position identification. The proposed architecture in [13] is evaluated for benefits and performance metrics with recommendations for future research in 6G

cellular network security. The future wireless networks (6G) aim to advance beyond the capabilities of 5G by enhancing broadband, supporting massive access, and ensuring ultra-reliable, low-latency services. These networks will be highly heterogeneous, densely deployed, and dynamic, challenging traditional operational methods. AI particularly ML, is critical and pivotal in achieving intelligent network orchestration and management. AI/ML-driven channel estimation and spectrum management promise to optimize ultra broadband techniques like terahertz communications. They also address ultra-massive access, energy efficiency, and security challenges while ensuring reliable, low latency service through intelligent mobility management and resource allocation. Thus, Bahl *et al.* [14] present the trending AI-ML techniques and its applications. 6G, the next generation in cellular technology, is presently in deployment stage for wireless systems. ML including DL has been increasingly applied across various sectors to enhance system performance, including in communication technologies for optimizing various parameters such as frequency spectrum usage and security.

However, with the level of advancement of ML techniques also raises security concerns, particularly regarding adversarial attacks that can compromise AI models. In view of this, the work in [15] proposes a mitigation approach against several types of attacks on 6G-ML models used for wave beam prediction. The work efficiently aims to bolster security by defending against fast gradient sign method attacks, demonstrating minimal impact on prediction accuracy compared to undefended models.

Wireless communication systems are pivotal in ultra-modern and smart society, such as smart cities, serving digital entertainment, business, health, safety, and more. Evolving from 5G, discussions on 6G systems emphasize the integration of smart algorithms such as AI across all system layers—physical, network, and application. Thus, Sankar Ganesh *et al.* [16] explore 6G concepts and the pervasive role of ML techniques like supervised learning. In addition to this, the multiple applications are also presented and well discussed in the work. As 6G wireless networks approach deployment, robust security is crucial. Identity and access management (IAM) provides authentication, whereas Zero-Trust Network Access (ZTNA) highlights continuous verification and access contributions.

Furthermore, the ideologies like secure network segmentation block threats. These multiple measures and ideologies confirm and provide the integrity and confidentiality of 6G networks with higher reliability. IAM provides better and reliable authentication, whereas ZTNA frameworks successfully achieve high detection rates of abnormal behaviors [17]. On the other side, whereas 5G networks introduced cloudification and microservices, the 6G network focuses on intelligent orchestration and

management. As discussed previously and by various researchers, AI, ML, and DL prove to be pivotal for proactive threat detection and the creation of automated, self-sustaining 6G networks. According to this, reference [18] explores AI's role in 6G security through the development of an anomaly detection system based on ensemble learning (EL), covering aspects such as pre-processing, feature selection, and intrusion detection.

In examining the evolution and transition toward the 6G wireless networks, it becomes clear that AI and ML are set to revolutionize every aspect of wireless communication. From enhancing network efficiency and security to enabling innovative applications across diverse sectors, 6G network promises development and advancements far beyond those of current 5G technologies. The integration of AI and ML techniques throughout the network architecture from the physical to the application layers highlights and signifies their indispensable and critical role in shaping the future and setting the trend of wireless connectivity. As the future research progresses with time, addressing challenges and exploring new applications will be crucial to unlocking the full potential of 6G networks across the globe.

8.4 6G Frameworks

As the development of trending 6G networks progresses, the need for robust security frameworks becomes increasingly critical and significant. The next generation of wireless communication promises transformative capabilities such as ultra-high data rates, ultra-low latency, and massive device connectivity, i.e., millions of devices, which introduce new security challenges and vulnerabilities. Therefore, this explores the various aspects of 6G security frameworks, including through examination of their core components, the recent and trending technological innovations, essential performance metrics, critical regulatory compliance, the possible challenges, and the required future directions [19–23].

8.4.1 Framework Components

To take into account and acknowledge the multi-faceted security challenges, a comprehensive framework with all aspects of security and robust components is essential and of high importance. The core elements for this purpose include advanced and smart authentication mechanisms, including biometrics, various encryption protocols, different access control methods, and unique as well as quick anomaly detection systems, each playing a vital role in securing the overall network integrity and protecting the user privacy, especially the user data.

Authentication Mechanisms:

1. Enhanced and much required security through a vital manner, i.e., multi-factor authentication using the trending biometrics methodology such as facial recognition and/or other ways such as fingerprint scanning is critical and, therefore, highly recommended.
2. Using the advanced blockchain technology to create secure and decentralized authentication systems that solely prevent the single points of failure can be well treated as another effective way for securing the user data under the authentication mechanism.

Encryption Protocols:

1. Implementing the trending cryptographic algorithms that are resistant to quantum computing attacks especially while ensuring the long-term user data security is highly recommended and required.
2. Encrypting data in the form of end-to-end-encryption, i.e., E2EE, as explained encryption from the source to a destination is important and highly recommended to secure the data from interception and spying.

Access Control Mechanisms:

1. Role-Based Access Control: Assigning a specific set of access rights to the users as per their dedicated roles, limiting and reducing the access to sensitive and critical information and the key functions is highly required and therefore, recommended for better system performance.
2. Attribute-Based Access Control: The variable and highly dynamic access control to the users based on particular attributes, characteristics, context, and, therefore, the environmental conditions are critical and very important.

Anomaly Detection Systems:

1. AI-Driven Detection: Utilizing AI- and ML-based algorithms to detect and respond to anomalies and potential security breaches in real-time is highly recommended and beneficial overall.
2. Behavioral Analysis: Monitoring user behavior to identify deviations from normal patterns, indicating possible security threats is an effective step and therefore recommended.

Technological Innovations

The security of trending and advance 6G networks relies on several advanced technological innovations designed to address emerging threats and enhance overall network resilience. The key innovations particularly include AI and ML, blockchain, quantum cryptography, and zero-trust network architectures, each contributing distinct capabilities to create a secure and specifically, adaptable 6G framework. Figure 8.2 shows the aspects of 6G security with quantum cryptography.

AI and Machine Learning:

1. Predictive Analytics: Using the AI-based algorithms to predict and mitigate security threats before they materialize, enhancing proactive security measures is highly recommended and is most effective approach.
2. Adaptive Security: ML algorithms that continuously adapt to evolving threats, providing dynamic security responses are effective and recommended based on their characteristics.

Blockchain:

1. Secure Transactions: Implementing blockchain for secure and transparent transactions and reducing the risk of fraud and tampering are great initiatives and effective steps.
2. Decentralized Identity Management: Ensuring the secure and verifiable user identities without entirely relying on centralized authorities improves the system's overall effectiveness.

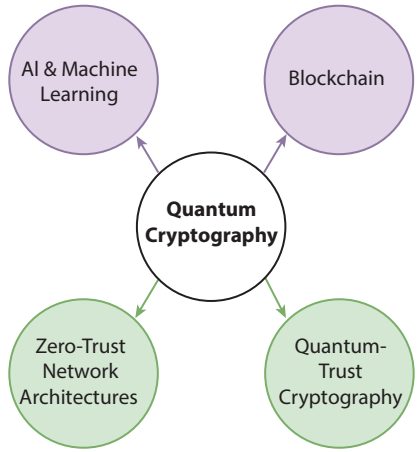

Figure 8.2 6G security and quantum cryptography.

Quantum Cryptography:

1. The initiation and process of using the quantum mechanics to privately and securely distribute encryption keys, ensuring continuous and uninterrupted communication channels, are recommended as per the overall effectiveness and efficiency of the developed approach.
2. Experimenting, developing, implementing, and thereby deploying the required set of cryptographic and advanced algorithms to withstand the possible quantum computing attacks are critical and, therefore, highly recommended and necessary.

Zero-Trust Network Architectures (ZTNA):

1. Micro-Segmentation: Dividing the more extensive networks into multiple smaller segments to ideally isolate and reduce and/or limit the number and level of security breaches is critical and, therefore, highly required, thus recommended for enhanced performance.
2. Continuous Verification: Developing and implementing the continuous verification of all the connected users and their corresponding multiple devices, regardless of their geographical location within and/or outside the network perimeter, help to enhance and, therefore, improve the overall system performance and efficiency.

8.4.2 Performance Metrics

To effectively evaluate and ensure the effectiveness of security frameworks in the 6G networks, it is essential and required to establish comprehensive performance metrics. These metrics assess the resilience, responsiveness, scalability, and adaptability of security measures, especially, ensuring that they can handle the dynamic and high-demand environment of the 6G networks. The key performance metrics include resilience to cyberattacks, response time, scalability, and adaptability, each providing insight into the robustness and flexibility of the 6G security frameworks.

Resilience to Cyberattacks:

1. Evaluating the security frameworks ability along with the advanced system algorithms to detect and prevent the unauthorized access into the system, and, thus, the attacks is an effective solution and an initiated step.

2. Measuring the overall robustness of security systems in maintaining functionalityduring and after attacks is critical aspect.

Response Time:

1. Assessing security frameworks' high speed and better efficiency in responding to and mitigating security incidents is a critical concern.
2. Evaluating the overall effectiveness of real-time system monitoring and threat detection capabilities is very important as well as an effective way of concurring the multiple system related issues.

Scalability:

1. Ensuring the overall security frameworks can scale with cumulative network size and complexity without compromising the overall system performance, which needs to be properly taken care of.
2. Supporting a growing number of connected devices, i.e., more than a million of devices, including IoT and edge devices, with constant security concerns and measures is also a significant concern and must be properly addressed.

Adaptability:

1. The ability and capability of the security frameworks to quickly and readily adapt to new system and security threats and variable network environments is recommended and highly significant.
2. While ensuring the overall system compatibility with traditional, i.e., existing and emerging technologies, national/international standards, and given protocols, it comprehensively improves the system efficiency, reliability, and performance.

8.4.3 Regulatory Compliance

The regulatory compliance is important and much essential as well as critical for maintaining the user data and trust, ensuring the user data privacy, and confirming the ethical and proper use of advanced technology such as AI and ML within the 6G networks. As the trending and advanced 6G

network, i.e., need of the hour technology expands connectivity and integrates more personal and sensitive user data, it is highly very important to establish and follow the regulatory frameworks that keeps into account and properly addresses the user data privacy concerns, national/international cybersecurity standards, and overall ethical considerations. Taking this into consideration and the importance of regulatory compliance, this section discussed the key aspects and compliance areas concerning the secure and trustworthy 6G networks for the users.

Data Privacy:

1. According to and following the data protection regulations is a critical and effective step toward system improvement, especially taking user privacy into consideration while ensuring the enhanced user experience.
2. Implementing multiple advance techniques such as AI and ML to analyze and protect the user data while focusing on to protect the user identities and other sensitive information is highly important and a much recommended step.

Security Standards:

1. According to and following the National Institute of Standards and Technology (NIST) guidelines for reliable, robust, and efficient cybersecurity practices are an important and much required initiative toward the overall effectiveness, system development, and effective deployment.
2. Complying with International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards is vital for the overall system, especially concerning the information security management and overall network security. This way, it improves the effectiveness and overall performance along with the reliability of the system.

Legal and Ethical Considerations:

1. Ethical AI: Ensuring that AI and ML applications in 6G networks follow the ethical guidelines and do not compromise user rights is significant and important.
2. Legal Compliance: Meeting legal requirements for data handling, storage, and transmission in different jurisdictions is important and highly recommended.

8.4.4 Challenges and Limitations

While the 6G networks offer transformative capabilities, implementing the corresponding comprehensive security frameworks presents several challenges and limitations. These particularly include interoperability issues, resource constraints, and overhead costs, which must be significantly and critically addressed to ensure that 6G security systems are effective and sustainable.

The various challenges and limitations are pictorially presented in Figure 8.3.

Interoperability Issues:

1. Legacy Systems: Integrating the new security frameworks with the existing and traditional legacy systems without causing disruptions is a critical and significant step of the overall process and, therefore, important.
2. Standardization: Lack of unified national and international standards for 6G security around the globe is of concern, as this leads to fragmentation along with a number of compatibility issues within the system.

Resource Constraints:

1. Computational Overhead: The very computational and complex system demands, especially considering the advanced security mechanisms, possibly affecting the overall network performance are very critical and essential and, therefore, need proper attention.

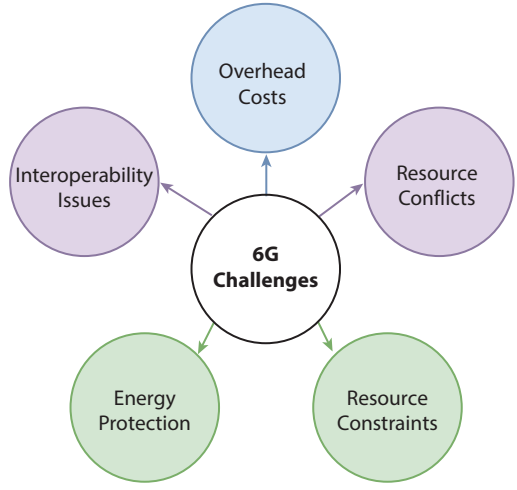

Figure 8.3 6G challenges and limitations.

2. Energy Consumption: Highly increased and oversized power energy consumption the system, especially the security measures, is a critical and highly significant concern that needs to be properly addressed and taken care of.

Overhead Costs:

1. Implementation Costs: The high initial capital costs associated with research, development, and deployment of the advanced security frameworks and technologies are important and key aspect and, therefore, must be properly considered.
2. Maintenance Costs: Accordingly, the maintenance cost for the overall system while confirming the system security is important and therefore needs proper attention.

Trade-Offs:

1. **Security vs. Performance:** A proper balance between the need for robust and reliable security with the efficient performance requirements of high data transmission speed and low-latency 6G networks is important, and therefore, needs proper attention.
2. **User Experience:** While confirming that the security measure do not reduce the user experience, is equally important and required for overall reliability and, therefore, needs to be properly addressed.

8.5 Conclusion

The various aspects and benefits of the next-generation telecommunication framework, i.e., 6G wireless communication technology, include multiple offerings over the current 5G framework. Particularly, its transformative potential and capabilities in communication is highly appreciable, especially in terms of number of devices, etc. However, with such benefits and overall advantages over the 5G framework, it also possesses a number of challenges and issues. This particularly includes the expanded threat zone, data privacy concerns, and threats from various types of cyberattacks. In view of this, ML possesses the capability to realize large dataset in real time to detect and further provide information related to potential issues, even before the threats are capable of impacting the network. This additionally includes the automated response system with quick decision-making and predictive and

efficient maintenance to ensure robust and efficient system performance. Moreover, ML also allows the system to integrate with blockchain and other, i.e., another advances technologies, to ensure additional features enhancing the overall system performance, including security aspects. Besides, this integration allows decentralized, reliable, and robust authentication methods and, thus, mitigates vulnerabilities across the complete network architecture.

Thus, based on the existing research, the future work will focus on developing the ML algorithms that are robust in nature and, besides, in integration with other advanced technologies. This will allow for additional resilience against attacks, better and safe reachability for the connected devices, and enhanced user trust. Besides, this can also incorporate AI and, therefore, compliance with global data protection standards in view of the trending 6G adoption. Conclusively, such approach with additional and advanced technologies will give extra space to the researchers to develop more robust structure while it also allows the stakeholders to come forward and thus establish a secure, resilient, and adaptable framework. Thus, it can be concluded with explicit conviction that the presence of ML will play a pivotal role in realizing secure and robust 6G ecosystem.

References

1. Yarali, A., Artificial Intelligence and Machine Learning in the Era of 5G and 6G Technology, in: *Artificial Intelligence and Machine Learning for Wireless Communications*, vol. 4, Wiley, Hoboken, NJ, USA, 2023.
2. Deshmukh, A. A., Hundekari, S., Dongre, Y., Wanjale, K., Maral, V. B., Bhaturkar, D., Explainable AI for Adversarial Machine Learning: Enhancing Transparency and Trust in Cyber Security. *J. Elect. Syst.*, 20, 1s, 2024–2024, 2024.
3. Zhang, S., Zhu, D., Liu, Y., Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities. *Comput. Netw.*, 242, 110255–110255, 2024.
4. Letaief, K.B., Shi, Y., Lu, J., Lu, J., Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications. *IEEE J. Sel. Areas Commun.*, 40, 1, 5–36, 2022.
5. Ismail, L., Buyya, R., Artificial Intelligence Applications and Self-Learning 6G Networks for Smart Cities Digital Ecosystems: Taxonomy, Challenges, and Future Directions. *Sensors*, 22, 15, 2022–2022, 2022.
6. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in renewable energy harvesting for EV charging infrastructure. in: *Optimized Energy Management Strategies for Electric Vehicles,* pp. 75–90. IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.

7. Periannasamy, S.M., Analysis of Artificial Intelligence Enabled Intelligent Sixth Generation (6G) Wireless Communication Networks, in: *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, pp. 1–8, 2022.
8. Chataut, R., Nankya, M., Akl, R., 6G Networks and the AI Revolution: Exploring Technologies, Applications, and Emerging Challenges. *Sensors*, 24, 6, 2024, 2024. https://doi.org/10.3390/s24062024.
9. Saxena, P., Jain, P., Aggarwal, P., Singh, M., Goel, S., Batra, M., Communication requirements and performance metrics for electric vehicle charging: A comprehensive review. in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 15–30, IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch002.
10. Rekkas, V. P., Sotiroudis, S., Sarigiannidis, P., Wan, S., Karagiannidis, G. K., Goudos, S. K., Machine Learning in Beyond 5G/6G Networks: State-of-the-Art and Future Trends. *Electronics,* 10, 22, 2782, 2021, https://doi.org/10.3390/electronics10222782.
11. Noman, H.M.F., Machine Learning Empowered Emerging Wireless Networks in 6G: Recent Advancements, Challenges and Future Trends. *IEEE Access*, 11, 83017–83051, 2023.
12. Pandi, S., Albert, A.J., Thapa, K.N.K., Prasanna, R.K., A novel enhanced security architecture for sixth generation (6G) cellular networks using authentication and acknowledgement (AA) approach. *Results Eng.*, 21, 101669–101669, 2024.
13. Du, J., Jiang, C., Wang, J., Ren, Y., Debbah, M., Machine Learning for 6G Wireless Networks: Carrying Forward Enhanced Bandwidth, Massive Access, and Ultrareliable/Low-Latency Service. *IEEE Veh. Technol. Mag.*, 15, 122–134, 2020.
14. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile Ad Hoc Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019. https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
15. Kaur, J., Khan, M.A., Iftikhar, M., Imran, M., Q, and Emad Ul Haq. Machine Learning Techniques for 5G and Beyond. *IEEE Access*, 9, 23472–23488, 2021.
16. Ganesh, S.S., Rajaram, G., Anusuya, V., Thirumalaikumari, T., Navaz, K., Sobia, M., Next-Generation Threat Detection and Mitigation in 6G Wireless Networks Using IAM, ZTNA and Advanced Security Mechanisms. *J. Electr. Syst.*, 20, 5s, 2034–2041, 2024.
17. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P. K., Singh, M., Edge Computing-Based Design for IoT Security, pp. 298–309, Chapman and Hall/CRC eBooks, 2024. https://doi.org/10.1201/9781003405535-22.
18. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., IoT and blockchain technology in 5G smart healthcare, pp. 137–161, Elsevier eBooks, 2022a, https://doi.org/10.1016/b978-0-323-90615-9.00004-9.
19. Porambage, P., Gür, G., Moya Osorio, D.P., Livanage, M., Ylianttila, M., 6G Security Challenges and Potential Solutions, in: *2021 Joint European*

Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), pp. 622–627, 2021.

20. Akhtar, M.W., Hassan, S.A., Ghaffar, R., The shift to 6G communications: Vision and requirements. *Human-centric Computing and Information Sciences*, 10, 53, 2020, https://doi.org/10.1186/s13673-020-00243-4.
21. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in Computer and Information Science*, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
22. Porambage, P., Gür, G., Osorio, D.P.M., Liyanage, M., Gurtov, A., Ylianttila, M., The Roadmap to 6G Security and Privacy. *IEEE Open J. Commun. Soc.*, 2, 1094–1122, 2021.
23. Singh, M., and Malik, A., Multi-Hop Routing Protocol in SDN-Based Wireless Sensor Network: A Comprehensive Survey. in: *Software-Defined Network Frameworks: Security Issues and Use Cases*, pp. 121–141, CRC Press, 2024, https://doi.org/10.1201/9781040018323-8.

9

Edge Computing and Privacy Challenges in 6G Networks

Mandeep Singh[1]*, Aruna Malik[2], Pawan Kumar[3], Megha Sharma[4] and Namrata Sukhija[5]

[1]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
[2]Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar, India
[3]Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad (U.P.), India
[4]SOET(CSE), K. R. Mangalam University, Gurugram, Haryana, India
[5]Department of Computer Science and Engineering, SRM University, Sonipat, Haryana, India

Abstract

Edge computing is set to play a vital role in the evolution of 6G networks by enabling real-time data processing closer to the source. This shift toward decentralized architectures significantly improves responsiveness and reduces latency, benefiting applications such as autonomous systems, smart healthcare, and industrial automation. However, moving computation to the network edge also introduces serious privacy and security concerns. This chapter investigates these challenges, focusing on issues like data exposure, inadequate access control, and regulatory compliance. It highlights promising approaches such as federated learning, differential privacy, blockchain-based identity verification, and secure multi-party computation, all tailored for edge environments. The discussion also considers the technical limitations of edge devices in handling complex cryptographic operations and suggests lightweight alternatives suitable for 6G scenarios. The chapter concludes with future directions emphasizing AI-enabled threat detection and standardized privacy models for globally distributed 6G infrastructures.

***Keywords*:** Edge computing, 6G, privacy, federated learning, blockchain, data security, differential privacy, secure computation

**Corresponding author*: mandeepsingh203@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (191–220) © 2026 Scrivener Publishing LLC

9.1 Introduction

The sixth generation, or 6G, of mobile networks is a promise toward revolutionizing the connectivity factor of today's world to unprecedented data speeds, ultra-low latency, and quality of service. This is set to take the leap by a giant margin over the network that currently exists in the form of 5G networks. The 6G is designed to support an expansive interconnected ecosystem of devices—from IoT-enabled sensors and autonomous systems to intelligent cities. Contrary to previous generations, 6G will erect a highly integrated network that supports, in addition to advanced telecommunications, sectors like healthcare, finance, and manufacturing by exchanging real-time data with high fidelity. Data rates are expected to be in the order of terabits per second, with a latency of just one millisecond, unlocking applications such as immersive extended reality and high-speed holographic communications.

Edge computing brings data processing closer to the sources of data. In this model, processing power is decentralized, enabling faster data handling and reducing the need to transmit data to central data centers. Edge computing in a 6G network minimizes latency and enhances reliability while reducing the load on the network's central resources. Processing at the edge enables near real-time decision-making, which is very critical for an application that needs to respond immediately. This is something that could be as simple as self-driving or healthcare applications or, in the industrial sense, real-time automation.

There are very big complexities and critical issues that arise in terms of privacy and security in 6G networks during this transition toward edge computing and massive numbers of connected devices. Data processing, transmission, and storage operations across the vast numbers of devices and edge nodes will become vulnerable to unauthorized access, breaches, and cyberattacks in 6G. Privacy would be a much larger issue as the networks process more sensitive data, including personal and financial information. Edge computing offers a decentralized topology to operate in an environment, which in itself makes traditional security mechanisms that often rely on centralized control less effective. Therefore, 6G networks require novel forms of solutions that protect data at various levels of the network while being compliant with privacy regulations.

Security breaches and privacy violations affect not only individual users but also industries and national infrastructures. Secure privacy and security solutions, therefore, become an absolute necessity in order to achieve the confidence of users to access 6G for sensitive data without compromising confidentiality, integrity, and availability. Therefore, advanced security protocols and privacy-preserving mechanisms can be integrated into the design of 6G networks.

9.1.1 Scope and Objectives of the Chapter

This chapter discusses the role that edge computing plays in 6G networks and talks about the innovative, unique challenges of privacy and security it brings with itself. It explores in-depth available and emergent risks related to processing data at the network's edge and discusses how innovations in security protocols and privacy-preserving technologies can mitigate those risks.

The primary objectives of this chapter are as follows:

- To provide an all-inclusive perspective of edge computing in the context of 6G
- Identification and analysis of the privacy and security issues related to edge computing of 6G
- Discussion of innovation and advanced solutions in responding to these issues by focusing on privacy-preserving techniques and robust security protocols
- Future work directions and possible solutions that will further improve the privacy and security framework for 6G edge computing

By focusing on these objectives, the chapter is expected to provide critical and valuable inputs to researchers, network designers, and stakeholders within the telecom operator domain who are working toward the secure and privacy-compliant implementation of edge computing in 6G networks.

9.2 Edge Computing in 6G Networks

Edge computing happens to be one of the fundamental technologies that meet the needs peculiar to 6G as the demand for connectivity continues to evolve with time. As compared to a classical centralized processing approach, edge computing leads to reduced latency and efficiency in doing things because computing resources are brought closer to where the data is generated. It continues by discussing a definition and the significant role of edge computing within 6G with components and an architectural framework that makes that possible while setting up a comparison to traditional cloud computing.

This includes the basic kind of distributed computing, which is that of edge computing that executes data processing near the generation site or even at such an event source and not as a solitary activity on the central server alone. Such an approach enables prompt responses by shifting the process closer to the "edge" of the network of sensors, smartphones, etc.,

and other IoT nodes. This is in contrast to the cloud because data needs to travel long distances to remote data centers for processing, and this normally incurs latency. In 6G networks, ultra-low latency and high bandwidth should be considered. Here again, edge computing would meet these better than cloud computing.

The concept of edge computing is critical in the 6G context, especially for real-time applications like autonomous driving, industrial automation, and augmented reality. For example, sensor data is processed in order to quickly make decisions on navigation and obstacles while driving. Processing at the edge allows almost instantaneous reaction times; therefore, safety is enormously critical. Huge inter-device communications that happen in real time for such applications are, therefore, the dependencies smart cities have for edge computing: traffic management and monitoring, environment, public safety, among others. In this framework, edge computing ensures a decentralized model with a minimum of delay and higher reliability; therefore, it is a cradle for 6G within the general context of overall vision in terms of connectivity and responsiveness.

9.2.1 Key Components and Architecture of Edge Computing in 6G

Edge computing architecture in 6G is a multi-layered system designed to support high-speed and low-latency data processing. Major components include edge nodes, edge servers, artificial intelligence (AI) and machine learning (ML), and the network layer.

This type of basic computing unit within edge computing is called an edge node, which encompasses sensors, devices associated with IoT, and all devices a customer utilizes that acquire data from its source. In some preliminary analysis, nodes would probably filter out data of low relevance so that reduced data volume is being transported up to higher levels of the network. Thus, only meaningful information will be transmitted and computed in the subsequent processing stages, thereby optimizing the usage of bandwidth. At the heart of contact with the core of a network are the edge nodes, which further come into play in the amalgamation of real-time information across all types of applications, from healthcare monitoring to industrial automation, smart infrastructure, and much more. Figure 9.1 illustrates the layered architecture of edge computing in 6G.

A sufficient number of nodes at that level are themselves edge servers that will form intermediate versions of data centers. Because it aggregates and analyses several nodes' data cannot be done by the edge nodes by themselves to perform higher-order processing tasks; smart manufacturing has

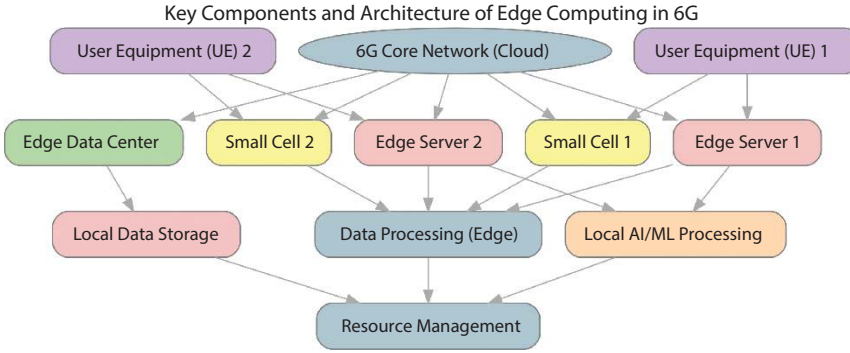

Figure 9.1 Key components and architecture of edge computing in 6G.

edge servers monitoring for anomalies of patterns or detection of patterns in one to a couple of sensors that would immediately report the anomaly in an effort to promptly react toward equipment failure. They provide faster data processing with increased network resiliency through the presence of localization processing nodes that can divide the load away from the central cloud server.

AI and ML capabilities are fundamental to the process of edge computing in 6G. These have offered the intelligent mechanisms essential to data processing management, resource distribution, and adaptability. In systems of edge computing, AI-based algorithms have the ability to learn data patterns and, sometimes, even make independent decisions on their own. This is going to be highly effective in the 6G network. The network might well end up dynamically managing resources without asking for a control system. But today, with ML at the edge, predictive maintenance falls into that category by predicting a failure even before an actual problem occurs based on information about machinery or infrastructure and cutting down unavailability time and costs.

The network layer can be termed as a backbone that connects these entities to ensure smooth communication from the edge nodes to edge servers and further on to the core network. In the network layer, design in 6G accounts for high data transfer rate with minimal delay. This aspect of applications would be quite important in real time response applications. Low-delay data transfer is applicable in remote healthcare scenarios where edge devices monitor the patient's vital signs so as to allow timely intervention. Ultra-reliable and low-latency communications is one of the key features in the 6G advanced network needed for the right functioning of applications at the edge.

9.2.2 Comparison with Traditional Cloud Computing and Its Limitations in 6G Scenarios

Central mass processing is the core of traditional cloud computing-housed in massive data centers and includes huge chunks of data coming from devices and applications to be processed and stored there. Despite cloud computing having done a lot to scale applications and make complex processing tasks, it does not look pretty usable for 6G applications requiring immediate responses with ultra-low latencies because of its centralized nature. This would leave only some potential of cloud computing for real-time fulfilment in 6G. Where data must travel a great distance to reach the central server, latency occurs, which is tolerated by some applications but not all.

One of the main drawbacks of cloud computing is latency, primarily when application demands meet the demands of 6G, which means that it requires almost instant data processing. For instance, for augmented reality, the delay may probably break down the whole user experience because data has to be processed in real time to overlay information digitally onto a physical environment. This is achieved through the edge computing mechanism where the processing of data happens locally at devices or immediately at the edge servers, which process the information almost in real-time. It does not introduce high latency and meets the strict requirements of low latency from application 6G applications that cannot be met through cloud computing. The latency in the transmission of data is reduced.

Another drawback in cloud computing is high bandwidth usage. In the central model, billions of devices have to transmit data back and forth to the cloud server. It will result in both network congestion as well as energy consumption. Thus, the 6G cannot be sustainable while serving millions of devices where device efficiency is required. This reduces the amount of bandwidth required in data transfer by edge computing as the processing is local. This local processing also has sustainability benefits because it consumes much less of the needed extensive data center resources besides being economical.

Table 9.1 compares traditional cloud computing with edge computing in 6G scenarios. Although the edge features of 6G networks are outlined, a great deal of complementary use still remains for 6G networks. Data, when stored in the cloud, spends more time, and there are substantial amounts of data in storage. Any level of analysis for large datasets fits well into the features that make the cloud relevant for analytics. The offloading and tasks requiring less response of a network are very well suited through cloud computing where the 6G network supports many devices as edge devices through the tasks requiring less response as an immediate reply

Table 9.1 Traditional cloud computing vs. edge computing in 6G scenarios.

Criteria	Traditional cloud computing	Edge computing in 6G
Core architecture	Centralized, with processing in large data centers	Decentralized, with processing closer to the data source
Latency	High latency due to data traveling long distances to the cloud	Ultra-low latency by processing data locally or at the edge
Bandwidth usage	High, requiring extensive data transfer between devices and cloud	Low, as local processing reduces the need for constant transfer
Real-time processing	Limited, unsuitable for real-time applications like AR/VR	Excellent, supports real-time applications like autonomous systems
Sustainability	Energy-intensive due to reliance on large-scale data centers	Energy-efficient, leveraging local and distributed resources
Suitability for 6G	Partial, useful for large-scale data storage and analysis	Ideal, designed for real-time, low-latency 6G applications
Security challenges	Secure but centralized, making it vulnerable to single-point attacks	Decentralized, offering improved security but increasing node-level risks
Scalability	Limited by central server capacity and network congestion	Highly scalable, leveraging distributed computing resources
Cost efficiency	Expensive for high-frequency real-time applications	Cost-effective by reducing reliance on centralized infrastructure

like analyzing the data at given periodicity or storage historical data. With the good balance of high speed and real-time processing at the edge and large-scale data management in the cloud with a hybrid of cloud computing and edge computing, 6G networks will be paving the future toward a truly connected world.

9.3 Privacy Challenges in 6G Edge Computing

The increased development of the 6G networks has edged computing into being one of the most powerful enablers in the real-time processing of data, which allows responses with very low latency. Although this shift toward edge computing is one of great popularity, it, on the other hand, raises a lot of privacy issues because of the distributed nature of the architecture with the movement of processing data away from the central servers to the edge of the network. Detailed key privacy issues on data ownership, control, data transmission vulnerabilities, user anonymity, data localization, and threats through data aggregation and AI/ML processing at the edge are outlined in the next sections.

9.3.1 Data Ownership and Control Issues at the Network Edge

In traditional centralized networks, data ownership and control normally lie with one organization or limited sets of entities. However, edge computing throws this in a complex web of issues regarding data ownership arising from the decentralized setup in which several stakeholders, like device manufacturers and service providers, along with end-users, are actively involved in generating, processing, and managing data. It makes it particularly challenging to issue clear guidelines with respect to data ownership in 6G networks because data is processed by different nodes in different jurisdictions.

The ownership of data is an especially relevant consideration when sensitive information, for example, health data or financial information or even location-tracked information, is involved. For example, in a medical context, edge devices might collect personal health metrics and perform simple preliminary analyses directly on the same device. The problem arises when there are several service providers in the same data processing chain, such that an individual can never be sure whether the system administrator, the parent firm, or the original data-generating person has the final authority over this data. In case of breach or misuse, who should be held accountable? This creates ambiguity and presents legal issues whenever sensitive data is mishandled because different jurisdictions have different regulations relating to data ownership rights.

Things get even more complicated when this is a matter of user consent. It might not be that users are fully aware of the amount of data shared and further processed at the edge of the network, thus losing control over their personal data. For 6G networks, this consent mechanism should be

brought up to promote even the same form of user consent to be given for the sharing and processing of data. Overall, ownership and control of data stand out as key concerns that stakeholders operating under 6G need to address to be transparent and accountable.

9.3.2 Vulnerabilities in Data Transmission and Storage

This results in high interactions among diverse nodes and edge servers and, sometimes, the core cloud infrastructure for data transmission. At every stage of such data transmission, there are potential vulnerabilities, most especially when such sensitive information has been transmitted between those different nodes. Data that is in motion between those edge devices and servers can actually be intercepted and used by anyone. Manipulation can also occur so that certain individuals gain unauthorized access to it, thereby breaching the privacy of that data. Secure data transfer is one of the essential aspects in 6G networks because these networks will have a wide range of sensitive data at the edge layer.

To minimize these vulnerabilities, encryption is broadly used to secure data while it is in transit. The problem is that most of these edge devices work with reduced processing power and energy. It becomes hard to implement strong encryption standards without hampering the performance of the devices. This limitation does create a compromise between security and performance, especially in resource-constrained environments such as those for an IoT-based smart home or wearable device. Furthermore, any data integrity compromise at the transmission level might have huge implications. For example, in autonomous vehicle networks, the compromised data might lead to decisions affecting the safety and security of passengers.

Storage vulnerabilities at the edge also contribute to risks related to privacy issues. Unlike centralized data centers, which have advanced security protocols, edge devices and servers have limited security controls. This makes them highly targeted for cyberattacks because it is easy to operate on those vulnerabilities in order to gain unauthorized access to the stored data, thus potentially leading to data breaches. This also means that data duplication is quite common in edge computing, whereby data is very widely spread across several devices in order to achieve high availability and redundancy. Although this approach enhances the robustness of systems, it expands the attack surface and creates new vulnerabilities based on these entry points into the system. Lightweight encryption solutions, secure mechanisms for access control, as well as timely security update distributions on the edge device can mitigate these challenges.

9.3.3 Challenges of User Anonymity, Data Localization, and Regulatory Compliance

Perhaps among the main challenges to user anonymity, data localization, and compliance with regulations that come from the decentralized nature of 6G edge computing is the widespread proliferation of IoT devices, sensors, and other edge technologies at the individual edge units' level. Because much personal data is so generated and processed close to the sources of data, localized data processing throws up important questions regarding the functions available for analysis and decision-making related to user anonymity.

While anonymization of user data is a requirement for privacy in edge computing, the kinds of differential and context-rich information that edge devices can capture pose a challenge. For instance, location-based services in smart cities capture the fullest profiles of movements and behavior of individuals, making it possible to identify particular users unless properly anonymized. With anonymous data, even advanced techniques such as the removal of identifiable information itself may not be very effective when more contextual clues are used to re-identify the data. Several privacy-preserving technologies, especially differential privacy, are still being researched. The integration of such techniques in edge computing environments still poses a challenge because of the limited processing power.

Data localization is another important problem, especially with 6G networks crossing international borders. For instance, some jurisdictions require that data about their citizens must stay within the country, making it difficult to deploy edge computing because the data could be processed across various locations. For instance, the General Data Protection Regulation (GDPR) of the European Union has strict rules on the transfer of data crossing more than one border country, which would be quite challenging in a 6G network with data being processed by nodes that are in other locations. Compliance with such regulation requires edge computing systems to implement data localization policies, which can be costly and operationally cumbersome, particularly while handling huge amounts of data across several regions.

Apart from the above factor, the regulatory compliance reaches user consent adequacy and respect also. For example, regulations like GDPR demand that the user must know how his data is processed and must be entitled to delete his data. Implementing such user rights in decentralized 6G edge networks can turn technically challenging, for example, as data will be stored in several devices and nodes with no clear path to deliver the results.

Such regulatory requirements further introduce new demands on mechanisms for compliance, weighing the user's right to privacy against the technical demands of edge computing.

9.3.4 Threats Related to Data Aggregation and AI/ML Processing at the Edge

Data aggregation in edge computing refers to data from multiple devices being aggregated for meaningful insights. While data aggregation allows for a more comprehensive analysis, it may compromise user privacy if data are not dealt with properly. Aggregated information about individuals or groups can be very sensitive and is further compromised when aggregated with powerful AI and ML algorithms. For instance, the data collected by smart home devices could reveal patterns of a household's routine, preferences, and behavior and, therefore, be abused for purposes such as targeted advertising or other invasive practices. Anonymization and aggregation methods should protect user privacy in collected data strongly, so individual data points are private.

The use of AI and ML models at the edge introduces another layer of complexity concerning privacy. Most of these models are trained on large quantities of data and improve with age, and when deployed at the edge, they can perform analysis directly on such data without needing to forward it to a central server for processing. AI and ML models themselves are exposed to a variety of attacks; one example is adversarial attacks, and the other one is model inversion attacks. Such adversarial attacks can force the model to misclassify data incorrectly, resulting in a wrongly produced output, and model inversion attacks recover private information that was used during the training of the model. Such vulnerabilities introduce serious privacy risks because an attacker might be able to infer sensitive information from AI and ML models deployed on the edge.

To respond to the new set of privacy concerns, researchers are working on novel privacy-preserving AI techniques where AI models learn from data without ever directly accessing them. These include federated learning, for instance, where models can be trained on the local device itself without transferring data to a central server, thereby protecting user privacy. However, these techniques require computational resources that may become a limitation for edge devices. The design of 6G networks is still a subject of conflicting computation demands on privacy-preserving AI with resource constraints at the edge.

9.4 Security Threats in Edge Computing for 6G Networks

As it has become prominent in 6G networks, edge computing promises not to have any equal competitors toward unparalleled advantages of reductions in latency, enhanced real-time data processing, and supportability for a large number of devices. This comes with considerable security challenges at their heels: edge computing moves data processing closer to end devices, effectively expanding the potential attack surface and increasing vulnerabilities. Security threats here range from vulnerabilities of network and device-specific nature to more advanced cyber threats that exploit decentralized, heterogeneous nodes. This section covers some of the key security threats in edge computing for 6G networks, which range from network vulnerabilities to different attack vectors, risks associated with decentralised nodes, and emerging malware and cybersecurity threats.

9.4.1 Network and Device Vulnerability 6G Specific

There are multiple points of vulnerability created in 6G networks with the infusion of edge computing, bringing more computations closer to the end-user. This change from a centralized to decentralized model of security also increases the number of potential targets that the attackers can exploit against the weak links in the network. In the traditional centralized system, the heart of the conventional centralized system tends to be the point of attack, whereas, in edge computing, attacks can target devices and nodes across a distributed network.

This is one of the major vulnerabilities of the network in 6G, related to the number of connected devices and sensors associated with them, many of which are resource-constrained IoT devices in terms of processing power and memory, respectively. This has meant that most of them lack advanced security features that put them in the hands of hackers. An attacker can use these weak spots to penetrate the network to launch subsequent attacks, including data intercept, device manipulation, and denial-of-service attacks. Even more so, with new 6G networks relying more on the high-frequency bands such as millimeter waves, new types of interference attacks and jamming will also arise to seize and jam those weak signals used in communication between the devices.

The firmware and software issues are also related to device vulnerabilities in 6G edge environments; most of the IoT devices run on obsolete firmware that has not been updated with the latest security patches.

Malicious code is injected into these vulnerabilities to gain control over the device by exploiting bugs in the firmware. These vulnerabilities can be very dangerous if they are in a critical application, like healthcare or autonomous driving, as compromised devices may cause significant safety risks. As the 6G networks expand, the needed effort will be to ensure that the devices are secure and have regular updates for edge nodes to avoid as many network and device-specific vulnerabilities as possible.

9.4.2 Threat Vectors: Physical Attacks, Network Attacks, and Data Tampering

Edge computing environments have several threat vectors across physical attacks, network-based attacks, data manipulation or tampering, and others.

a) Physical Attacks: Unlike centralized data centers that are benefited from a good physical security measure, the edge nodes, as the case, may be scattered at unmonitored or remote sites, making them susceptible to physical tampering. Such devices may also be accessed directly by attackers and changed or even exchanged to inject malicious information or erase the security elements. In a smart city, attackers can easily obtain physical access to edge devices installed on street lights or traffic light poles, and their network functionalities can be easily destroyed. Edge device physical protection becomes truly challenging in huge open areas. These risks can be mitigated by the implementation of tamper-resistant hardware and secure boot processes capable of detecting physical, unauthorized access.
b) Network-Based Threats: Network-based threats are a major threat in the 6G edge computing environment. One of the most common forms of network-based attacks is distributed denial of service (DDoS), where multiple compromised devices flood network traffic to servers, which, in turn, crashes the services being offered. The availability of thousands of IoT devices to be connected in edge computing results in very serious consequences of DDoS attacks and can potentially affect whole network segments. Spoofing is another kind of network attack during which the attackers pretend to be legitimate devices in the network and get access to data and services without permission.

c) Data Manipulation/Tampering: This threat becomes particularly potent in applications where data integrity matters, like financial transactions, health monitoring, or autonomous vehicles. A possible attack scenario is intercepting and manipulating data between edge devices and servers. The resulting corrupted data fed into the edge devices might then drive critical decisions. For example, in an autonomous network of vehicles, altered sensor data may cause incorrect calculation of routes or unsafe decisions for driving. Thus, along with the use of cryptographical techniques and data integrity checks, it is highly important to be assured that data was not modified while it was in transit across the network.
d) Advanced Persistent Threats (APTs): The APTs comprise advanced sophisticated attacks that are typically conducted by well-funded adversaries to target critical infrastructure. Therefore, APTs are essentially persistent surveillance and probing of vulnerabilities within a network that enables the attacker to exploit weak points for a long time. In 6G networks, where edge computing will play a very critical role in infrastructure application, the results of an APT can be disastrous if attackers can seize control over the edge nodes or sensors.

Different threat vectors necessitate robust multi-layered security measures; these include intrusion detection, encryption, and daily network scanning to identify possible attacks.

9.4.3 Security Risks Associated with Decentralized and Heterogeneous Nodes

This decentralized environment of edge computing threatens security severely, particularly when it comes to managing and securing nodes. Unlike the centralized network, in which the same security levels apply uniformly throughout the network, in the case of edge networks, different devices feature varying capacities and limitations. This heterogeneity makes it challenging to deploy security protocols consistently and sometimes provides weak links that attackers may exploit.

Nodes in a 6G edge environment could be from high-powered edge servers with sophisticated security attributes to low-powered IoT devices with hardly any computational ability. These latter will also be at the mercy of attackers because many IoT devices lack the resources to implement

complex encryption algorithms or even sophisticated security protocols. This contributes to a higher chance of security misconfigurations because various devices work with different versions of firmware or software, thus creating inconsistencies that prove challenging in monitoring.

Another challenge the decentralized architecture poses is how to effectively handle access control for the network. Each device needs to authenticate itself and communicate securely without relying on some central authority. This makes traditional models of centralized authentication less tenable and requires distributed identity management solutions like blockchain-based approaches, which can support distributed authentication and access control in edge environments. Thus, the approaches above look promising but demanding in terms of processing capability and are possibly out of the reach of some edge devices. Hence, secure identity management and access control in 6G edge networks are challenging at best.

9.4.4 Emerging Malware and Cybersecurity Threats in Edge Environments

With the growth of edge computing, new and more exotic forms of malware and cybersecurity threats are emerging directly at the particular weaknesses of decentralized networks. This might include traditional ones, such as ransomware and spyware, but will include advanced types, specifically developed for resource-constrained environments.

a) Ransomware. There have been increased attacks on ransomware and other malware from edge environments concerning IoT devices used with critical applications. In the event of ransomware, malware can lock up data on the device so that it becomes unavailable except to the holder of the device, who is made to pay a ransom. Given that many IoT devices have poor security, ransomware can easily proliferate through an edge network, in case all the devices share common security vulnerabilities. For example, in an industrial automation system, the attacks mentioned above could not only cause interruption to operations and financial loss but even lead to physical harm.
b) Botnets: Botnets are the network of compromised devices controlled by attackers away from the crime scene. An attacker can utilize vulnerable IoT devices in an edge computing environment to turn them into bots and form mass botnets.

Botnets are mainly used in DDoS attacks, data theft, or similar malicious acts. Because there would be vast deployment of devices in a 6G edge network, the scope for large botnets is potentially high, which is significant.

c) Edge-Specific Malware: Other cybercriminals have been designing edge-specific malware that exploits flaws of the edge appliances. Some malware kind utilizes the processing power of IoT devices for the purpose of cryptocurrency mining, infecting them. While an individual IoT device would not be capable of substantial computing power, thousands of compromised devices aggregated together could be valuable to attackers. This malware is difficult to detect because it does not interfere directly with device functions and can thereby run covertly.

d) AI-Driven Cyberattacks: The integration of AI and ML in 6G networks provides sophisticated tools for attackers to carry out attacks at the very edge of the environment. AI-driven malware analyzes network patterns and adjusts its behavior to evade detection. For instance, AI-based malware may be optimized to evade intrusion detection. Network administrators then face the challenge of finding it harder to identify and stop such malicious threats. AI-based cyberattacks then emerge as a new breed of attack that needs defence just as advanced or at least parallel with the level of sophistication as their AI-based counterparts, such as AI-based anomaly detection.

In fact, with emerging cybersecurity threats evolving, proactive defence mechanisms in 6G networks are becoming the need of the hour. All the above edge-specific cybersecurity solutions, such as lightweight intrusion detection systems, behavior-based anomaly detection systems, and regular security updates, help mitigate the risks posed by emerging malware and other cyber threats.

9.5 Innovations in Privacy and Security for Edge Computing in 6G

The deployment of edge computing in 6G networks introduces a number of privacy and security issues mainly because of the decentralized architecture and related real-time processing of data. Innovations in these privacy-preserving mechanisms, advanced security protocols, AI, and ML

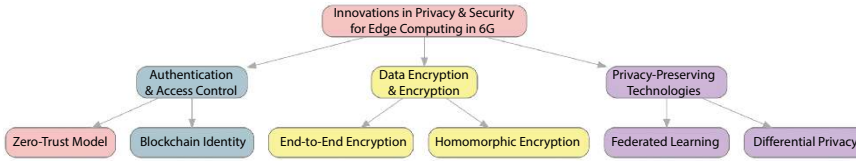

Figure 9.2 Innovations in privacy and security for edge computing in 6G.

applications are highly critical. This section looks into innovations where homomorphic encryption, secure multiparty computation, differential privacy, federated learning, blockchain-based security solutions, zero-trust architectures, and AI-driven anomaly detection will be investigated. Figure 9.2 highlights privacy and security innovations in 6G edge computing.

9.5.1 Privacy-Preserving Mechanisms

One of the root problems in 6G edge computing is maintaining private data processing efficiency. Edge computing does not centralize data at one location, unlike centralized systems, where all data remains contained within a single location; rather, edge computing processes data at the node level, moving through several nodes that are closer to the edge-user and, therefore, increase the exposure to potential privacy breaches. The mechanisms for privacy preservation may be required to protect such data as well as to ensure maintaining confidentiality among the users.

a) Homomorphic Encryption: It is a revolutionary technique whereby computations carried out on encrypted data do not have to be decrypted. It means that it can be processed in safely even if it is stored on an untrustworthy edge device. For instance, if health data is stored in encrypted form inside a device, homomorphic encryption will enable a remote server to analyse health trends without revealing the raw data itself. Homomorphic encryption could be viable in 6G networks where data is highly sensitive, particularly for applications such as health, finance, and personal communication. However, the technique requires high computational costs, making it difficult to be used in resource-constrained IoT devices. Current research attempts to make the homomorphic encryption technique more efficient, improving its usage within edge computing systems.

b) Secure Multi-Party Computation (SMPC): The SMPC is another privacy-preserving technology that allows different parties to perform computations over their data without having to reveal the individual inputs of each party involved. In edge computing, SMPC facilitates the collaborative work being done across distributed devices performing analysis on the data without compromising privacy. For example, sensors within a department could collaborate with one another to analyze pattern flows for smart cities. These results are then processed using schemes that ensure the nondisclosure of individual data sets. SMPC is, thus, highly applicable in use cases where devices of different organizations exchange sensitive information. Although SMPC offers privacy, it entails computational and communication overheads that may be quite demanding in high-frequency, low-latency 6G networks. Nevertheless, with the advance in SMPC, it is becoming increasingly feasible for use in edge computing, thus offering a powerful tool for collaborative analysis.
c) Differential Privacy: This is an approach that provides privacy for individual data points in the dataset as the noise is introduced to the data before conducting analysis. It provides statistical guarantees such that adding or omitting one single data point does not significantly alter the result obtained. Differential privacy is said to be implemented when it comes to differential anonymization of user data in 6G edge environments. Therefore, differential privacy may apply when users' information is anonymized before transmission over the network and also before processing by AI models in 6G edge environments. For instance, differential privacy may be applied when it comes to location information collected from mobile devices to allow service providers to analyze movement trends without revealing their identity. It is broadly adopted by tech companies and has shown great effectiveness in balancing data utility and protecting privacy, as a precious technique for 6G edge computing.
d) Privacy-Preserving Federated Learning Models: Federated learning is an emerging technique to enable AI models to learn from decentralized data sources without moving the data itself. In edge computing, federated learning enables devices to train, locally, a shared model on their own data. Only the model updates, not the data, are uploaded

to a central server. This ensures that sensitive data never leave the device, hence no direct risks of privacy breaches. Privacy-preserving federated learning adds encryption or differential privacy to model updates, hence protecting federated learning. Applications where data privacy is critical, such as healthcare or financial services, will benefit from this approach. Federated learning keeps the data local and preserves privacy, placing it well in the context of becoming an integral part of privacy-centric AI in 6G edge networks.

9.5.2 Advanced Security Protocols

As the nature of 6G's edge computing is decentralized and heterogeneous, most of the traditional security protocols are not sufficient. Advanced security protocols like blockchain-based solutions, zero-trust architectures, and secure access control mechanisms have emerged to address the weaknesses as described above and provide a more sophisticated security framework in 6G edge environments.

a) Blockchain-Based Security Solution Security Solutions: Because of its decentralized and tamper-resistant nature, blockchain technology is apt for securing the edge environments where trust can be distributed across multiple nodes. Blockchain can prevent the formidable threat of data tampering and unauthorized access by creating an immutable ledger of transactions. With this said, the application of blockchain technology can be made in numerous edge use cases over 6G networks that range from secure communication between IoT devices, data transaction authentication, and management of digital identity. For example, a connected car can establish the authenticity of data being shared through a vehicular network by using blockchain, making only verified data being acted upon for decision-making. While blockchain imposes computational overhead, light blockchain protocols are being developed to make the technology practical for use on resource-constrained edge devices.
b) Access Control Mechanisms and Zero-Trust Architectures: Zero-trust architecture is a security model that considers all devices and network components to be untrusted by default; therefore, continuous verification for every access request is conducted. Zero-trust is, in fact, especially relevant for use

in 6G edge networks because the devices are typically spread over an extensive area and lack central control. Mechanisms providing for access control to the environment securely form the core of zero-trust architectures of edge environments. multi-factor authentication (MFA) and behavior-based access will be examples in which a request for authentication will be made every time a device attempts to communicate with an edge server, thereby minimizing unauthorised access. Thirdly, behavior-based access control can track device behavior patterns and issue alerts on any deviating pattern from normal for further investigation. The two will, therefore, come together to form a dynamic security environment that continuously authenticates the authenticity of any device from invading the edge computing environment maliciously.

c) Token-Based Authentication: Token-based authentication is primarily used in edge computing environments to enable secure authentication of devices at scale. In token-based authentication, every device is authorized with a digital token to authenticate itself. The methodology is useful in edge networks consisting of a large number of devices where low-latency assured authentications are needed. In token-based systems, this additional security is provided by cryptographic tokens, and tokens can evaporate after some time or when suspicious activity is detected. This gives flexibility, which allows token-based authentication to be dynamically adapted according to changing conditions in the network and is, therefore, especially suitable for dynamic 6G edge networks.

9.5.3 AI and ML Applications for Privacy and Security

Although AI and ML are one of the main tools for adding value to privacy and security in edge computing, autonomous anomaly detection, threat assessment, and real-time adapted security measures can prevent cybersecurity breaches and a proactive approach to 6G networks.

1. AI-Driven Anomaly Detection and Threat Intelligence: AI-based anomaly detection systems can identify unusual patterns of network behavior, and this could provide an earlier indication of security incidents that may escalate from normal patterns. In a 6G edge environment, thousands of devices are constantly creating data streams; hence, no human

activity is possible to monitor all these streams. AI can process data flows analyze device behavior in real time and identify breaches or any deviation that may indicate malware, intrusions, or unauthorized access. An abnormality in the communication pattern of an IoT device within a smart city can be reported by the AI system for further scrutiny and isolation from the network. AI-driven threat intelligence could predict emerging threats through data analytics culled from previous attacks, thus enhancing stronger defences in the network.

2. Machine Learning Models for Adaptive Security at the Edge: These models adapt to give solutions such that they learn from past data, improving future security measures. For instance, in edge computing, ML models can analyze each of the behaviors exhibited by the devices and adapt security protocols to suit them. For example, an ML model can identify that a sensor from a smart grid uses which type of communication pattern and alerts on any deviation, identifying the same as a potential security threat. Adaptive security is critical in this regard because edge environments can vary so much as to location and device function, and adaptive security allows ML models to modify security protocols to the needs of each device and, thus, provide a more tailored defence system. Figure 9.3 shows layered privacy and security mechanisms in 6G edge computing.

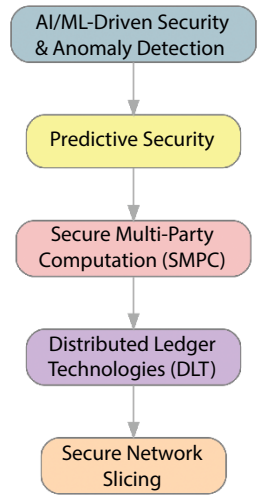

Figure 9.3 Classification of privacy and security mechanisms in 6G edge computing.

3. Federated Learning for Better Privacy and Security: Federated learning comes with privacy benefits along with much-needed security because it offers the chance for security models to be trained in a distributed manner without any loss of privacy. For instance, every edge device could build a model on the local edge device for threat data and share only model updates with a central server for the purpose of constructing a global model of threats. This implies the system learned from distributed data sources, improving its capacity in threat detection on the network. Federated learning is, therefore, the unification of two concepts, namely, the concept of privacy preservation and improved capabilities in threat detection; it is an excellent asset for 6G edge networks.
4. Behavioral Biometrics: This is a novel concept based on AI, which analyzes the various biometric details from users' behavioral patterns, such as typing speed, touch pressure, and gait, to authenticate them constantly. In 6G edge computing, it can enhance security with real-time, context-based user authentication without using passwords or PINs. The detection of anomalies in behavior patterns may enable the device to raise or reduce its security checks, limit access, or even avoid unauthorized use. This is a very effective approach, particularly in edge environments, where, given the constraints that a device might pose, traditional authentication practices may become impractical.

9.6 Future Directions and Open Research Challenges in 6G Edge Computing

The rapid evolution of 6G networks offers exciting opportunities as well as significant challenges, particularly with respect to privacy and security for edge computing. As edge computing appears as one of the basic features in 6G networks, researchers have recently explored new methods in the pursuit of resolving upcoming challenges concerning privacy and security arising from the use of network slicing and other characteristics of 6G networks. This section gives some future directions and open research challenges, a few of which are mapped to relevant topics in this book, including cross-layer security frameworks, finding the best balance between privacy and performance, investigation of quantum-resistant algorithms, and standardized protocols for privacy and security in 6G edge computing.

9.6.1 Potential for Cross-Layer Security Frameworks in 6G Edge Computing

Traditional security network approach often carries out each one of its layers, namely, physical, data link, network, transport, and application, in isolation. Sometimes, it may well ignore the possible variations in other layers. Conversely, cross-layer security provides an integrated defense that crosses more than one layer of a network. By doing so, it could well ensure uniform protection of the entire stack of communications.

Cross-layer security is very pertinent in the context of edge computing because of the heterogeneous nature of the network. The resultant edge environment of 6G will contain a highly diverse range of devices with different requirements and capabilities toward security. For example, IoT sensors, edge servers, and user devices all have unique vulnerabilities. Information about events could be shared across various layers within a network so a layered framework can coordinate a reaction to potential threats. For instance, if the physical layer detects an anomaly interference event that may be a signature of a jamming attack, then higher layers can be alerted to begin protection measures such as rerouting data.

Such a framework necessitates an understanding of how the security mechanisms function at various layers to complement each other in order to be effective. ML models can be quite handy for cross-layer security for analyzing data across various layers to detect patterns of possible threats and could be exploited as dynamic cross-layer frameworks that could eventually be implemented with significantly augmented 6G edge computing security, using a multi-layered adaptive, responsive, and all-encompassing defense system.

9.6.2 Balancing Privacy with Performance: Trade-Offs and Optimizations

Balancing privacy with performance is one of the greatest challenges with respect to the implementation of privacy in edge computing; indeed, privacy-preserving technologies such as encryption, homomorphic encryption, and differential privacy are all rather computationally expensive, and those can impact the processing performance, and so a trade-off will exist between the two, especially at the edge, where devices are endowed with even more limited resources.

Applications such as augmented reality, real-time health monitoring, and autonomous vehicles in 6G networks mandate near-real-time processing of data with no tolerance for latency. However, this comes at the cost of very

strong measures of privacy to ensure the safety of data and repute of users. Hence, optimization of privacy-preserving mechanisms to minimize the impact on system performance better remains a research area of key interest.

Lightweight encryption algorithms, especially developed for edge computing, are one promising method. These algorithms would provide constant privacy guarantees but decrease the computational costs as well. A more general version of selective privacy is to apply intense privacy-preserving techniques selectively only to those pieces of information that are most sensitive; generally, lighter protocols can be applied for less sensitive information. Edge-based AI may further aid by dynamically adjusting the balance of privacy efforts with regard to the type of data and application in order to optimize the competing ends of privacy and performance.

Future research will have to focus on the right spots at which privacy and performance could be mutually effective. For this purpose, new algorithms, hardware optimisations, and architectural innovations might enter the scene that will enhance privacy protection at a level that will not reduce efficiency as required for 6G applications. As research progresses, balancing between privacy and performance will become important for the full unleashing of 6G edge computing capabilities.

9.6.3 Exploring Quantum-Resistant Algorithms for Edge Security in 6G

Quantum computing is dangerous for traditional encryption algorithms; it could potentially break RSA and ECC, which are widely used in conventional cryptographic methods. With the lifespan of 6G networks lasting a considerable number of years, it is reasonable to foresee that the advent of quantum computing would also be possible, thus developing quantum-resistant algorithms to secure edge computing in 6G.

Quantum-resistant or post-quantum cryptography refers to developing cryptographic algorithms resistant to attacks by quantum computers, which is currently a rapidly evolving field of research. These algorithms have been designed to be resistant to both classical and quantum-based attacks, thus making sure that when quantum computing technologies become widespread, data would not become insecure. In this regard, implementing quantum-resistant algorithms at the edge is somewhat more challenging, as they are computationally expensive and need far more bytes than do legacy symmetric algorithms, so that may be a problem for resource-constrained devices.

While promising, it is also seen as a hope in the near future, with already-developed lightweight post-quantum algorithms that have been optimized for use in an edge environment with limited computational power. Thus, new types of post-quantum cryptography, such as lattice-based cryptography and hash-based signatures, may possibly bring an answer to solving the quantum threat at the 6G edge computing platform through further research in the future.

The other area of research focuses on hybrid cryptographic approaches, combining quantum-resistant algorithms with classical encryption. A dual-layer approach provides extra security value because it allows 6G networks to eventually utilize classical encryption in the short term while preparing for a quantum-safe future. Key to continued research is the quantum-resistant algorithms and hybrid cryptography for the life cycle and resilience of 6G edge computing security.

9.6.4 Opportunities for Standardization in 6G Edge Computing Privacy and Security

The decentralized and heterogeneous nature of 6G edge computing calls for standardization to achieve interoperability, security, and privacy across different devices and systems. As of now, the status of both edge computing and 6G is something in the emerging phase, and a universally accepted standard for privacy and security does not exist. Such standards are necessary to design a harmonious and security- and privacy-respecting 6G ecosystem.

Standardization can be applied to data handling practices, encryption protocols, authentication methods, and the secure communication frameworks of 6G edge computing. For example, there is a need to define standardized protocols for data encryption and anonymization so that an easy, lightweight means for seamless inter-networking is ensured using secure data sharing from one device to the other. Standards regarding the architectures of zero-trust for edge networks in 6G would indicate that every device, irrespective of the manufacturer or type, can follow the principles of uniform security measures in a way that diminishes the possibilities of vulnerabilities within a network.

Further, standardization should encompass compliance with regulations because 6G networks will definitely operate across international boundaries. Regulation on data privacy varies in different regions, such as GDPR in the European Union and CCPA in the United States. Standardized regulatory compliance frameworks will ensure that the 6G networks can be made operable in such diverse legal landscapes without losing any element

of user data privacy and other related issues. It would be based on cooperation involving the researchers, the regulatory bodies, and the industry stakeholders who would design these frameworks.

Beyond privacy and security, standardization in 6G edge computing will also usher in avenues for technological innovations. Standardization will facilitate having a uniform basis on which new technologies are built. As the companies would not have to worry about compatibility issues with uniform standards, there would be greater cooperation and openness in innovation to develop the 6G technology. Standardization would be an important milestone set in the early stages of developing 6G to deal with the overwhelming privacy and security problems that have been noticed.

9.7 Conclusion

As 6G networks get closer to reality, edge computing forms a front line of innovation, promising ultra-low latency, enhanced bandwidth, and real-time processing capabilities needed for next-generation applications. However, such a decentralized, edge-centric architecture also poses formidable privacy and security challenges. The challenges are problems of ownership of data, vulnerabilities of data transmissions and storage, threats from attacks in the physical and network setups, and risks from decentralized and heterogeneous nodes. These are very important challenges that need to be addressed so that edge computing can be rolled out in a secure and privacy-compliant manner that is reliable for users and industries. To address these challenges, various mechanisms and tools based on privacy-preserving mechanisms, advanced security protocols, and AI-driven tools are surfacing. Homomorphic encryption, secure multiparty computation, differential privacy, and federated learning provide strong architectures toward privacy preservation because the sensitivity in the cloud can now be manipulated without losing its confidentiality. Advanced security protocols are offered by blockchain-based solutions and zero-trust architectures that strengthen defences against unauthorized access and data tampering. Meanwhile, AI and ML introduce the possibility for an adaptive, real-time improvement of the capability of a network to identify and proactively act toward responding to threats and anomalies.

It is highly relevant to maintain user trust and ensure regulation in relation to the various issues of privacy and security in the 6G networks as more sensitive data is generated and processed toward the edge of the network. Privacy and security will be an essential requirement for successful 6G, operating not only with the underlying technical architecture of networks

but also with user adoption and industry confidence. Now, for 6G to live up to its promise, security and privacy need to become the focal point of stakeholders right from the start, offering a robust and reliable foundation that can seamlessly support the many applications of the future. There are many research areas that will require sustained development in the future. One such area will be cross-layer security frameworks, where cross-layer securities offer seamless, multi-layered protection across many network components. Balancing privacy with performance will require ongoing work to optimize privacy-preserving mechanisms for real-time edge applications. Further, quantum-resistant algorithms need to be worked on, with a view toward network protection against a future threat related to quantum computing. Finally, standardization efforts must be speeded up to produce clear, consistent, and interoperable privacy and security frameworks that can function effectively across international borders.

Thus, 6G edge computing promises transformative possibilities, but with such a journey comes the need to do it all under the banner of challenging complex privacy and security issues. Through collaborative innovation, industry-wide standards, and commitment to both privacy and security, 6G networks can be built to meet tomorrow's needs, protecting user's rights and their data across the globe. Overcoming these challenges will unlock the proper potential of 6G edge computing and lead to a world fit for all of us, which is more efficient, secure, and privacy-conscious.

Bibliography

1. Gür, G., Porambage, P., Osorio, D.M., Yavuz, A.A., Liyanage, M., 6G Security Vision: A Concise Update. *IEEE Future Networks World Forum (FNWF)*, Baltimore, MD, USA, Nov. 2023, [Online]. Available: https://cse.usf.edu/~attilaayavuz/article/23/6GSecurityFNWF2023.pdf.
2. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P. K., Singh, M., Edge computing-based design for IoT security, in: *Network Optimization in Intelligent Internet of Things Applications: Principles and Challenges,* pp. 298–309, CRC Press, 2024, https://doi.org/10.1201/9781003405535-22.
3. Peltonen, E., Bennis, M., Capobianco, M., Debbah, M., Ding, A., Gil-Castiñeira, F., Jurmu, M., Karvonen, T., Kelanti, M., Kliks, A., Leppänen, T., Lovén, L., Mikkonen, T., Rao, A., Samarakoon, S., Seppänen, K., Sroka, P., Tarkoma, S., Yang, T., 6G White Paper on Edge Intelligence, arXiv.org. https://arxiv.org/abs/2004.14850, 2020, April 30.
4. Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., Zhou, W., Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.*, 6, 3, 281–291, 2020, https://doi.org/10.1016/j.dcan.2020.07.003.

5. Liyanage, M., Odima, J.O., Sharma, S.K., Ahmad, T., AI and 6G Security: Opportunities and Challenges. *6G Network Communications*, vol. 2, pp. 1–10, Mar. 2022, [Online]. Available: https://oulurepo.oulu.fi/bitstream/handle/10024/30994/nbnfi-fe2021102051685.pdf?sequence=1.
6. Singh, M. and Malik, A., Multi-Hop Routing Protocol in SDN-Based Wireless Sensor Network: A Comprehensive Survey. in: *Software-Defined Network Frameworks: Security Issues and Use Cases,* pp. 121–141, CRC Press, 2024, https://doi.org/10.1201/9781040018323-8.
7. Saxena, P. and Goyal, A., Two-Stage Binary Classification of Follicular Histology Using Support Vector Machine. *Chin. J. Med. Genet.*, 31, 3, 258–268, Jul. 2022.
8. Mathew, A., Edge Computing and Its Convergence with Blockchain in 6G: Security Challenges. *Int. J. Comput. Sci. Mob. Comput.*, 10, 8, 8–14, 2021, https://doi.org/10.47760/ijcsmc.2021.v10i08.002.
9. Mao, B., Liu, J., Wu, Y., Kato, N., Security and Privacy on 6G Network Edge: A Survey, in: *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1095–1127, Secondquarter, 2023, doi: 10.1109/COMST.2023.3244674.
10. Gaur, A., Singh, S.K., Saxena, P., Performance Analysis of Deepfake Text Detection Techniques on Social-media. *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, Bengaluru, India, pp. 1–6, 2024, doi: 10.1109/ICDCOT61034.2024.10515626.
11. Singh, M., Sukhija, N., Sharma, A., Gupta, M., Aggarwal, P., Security and privacy requirements for IOMT-Based Smart Healthcare System, in: *Big Data Analysis for Green Computing: Concepts and Applications*, pp. 17–37, CRC Press eBooks, 2021, https://doi.org/10.1201/9781003032328-2.
12. Alawadhi, A. and Almogahed, A., Recent advances in edge computing for 6G, https://www.semanticscholar.org/paper/Recent-Advances-in-Edge-Computing-for-6G-Alawadhi-Almogahed/5dd2273903222b400e7b8d9a48473a01a465bb52, 2022.
13. Arastouei, N., 6G technologies: key features, challenges, security and privacy issues, in: *Communications in computer and information science*, pp. 94–109, 2023, https://doi.org/10.1007/978-3-031-36096-1_7.
14. Singh, M., Gupta, M., Sharma, A., Jain, P., Aggarwal, P., Role of deep learning in the healthcare industry: Limitations, challenges, and future scope, in: *Deep Learning for Healthcare Services*, pp. 1–22, Bentham Science Publishers eBooks, 2023, https://doi.org/10.2174/9789815080230123020003.
15. Saxena, P. and Goyal, A., Study of Computerized Segmentation & Classification Techniques: An Application to Histopathological Imagery. *Informatica*, 43, 4, 561–572, 2019.
16. Yang, M., Qu, Y., Ranbaduge, T., Thapa, C., Sultan, N., Ding, M., Suzuki, H., Ni, W., Abuadbba, S., Smith, D., Tyler, P., Pieprzyk, J., Rakotoarivelo, T., Guan, X., M'rabet, S., From 5G to 6G: A survey on security, privacy, and standardization pathways, arXiv.org. https://arxiv.org/abs/2410.21986, 2024, October 4.

17. Wang, Y., Kang, X., Li, T., Wang, H., Chu, C.-K., Lei, Z., SIX-Trust for 6G: Toward a Secure and Trustworthy Future Network, in: *IEEE Access*, vol. 11, pp. 107657–107668, 2023, doi: 10.1109/ACCESS.2023.3321114.
18. Hakeem, S.A., Hussein, H.H., Kim, H., Security requirements and challenges of 6G technologies and applications. *Sensors*, 22, 5, 1969, 2022, https://doi.org/10.3390/s22051969.
19. Akbar, M.S., Hussain, Z., Ikram, M., Sheng, Q.Z., Mukhopadhyay, S., 6G Survey on Challenges, Requirements, Applications, Key Enabling Technologies, Use Cases, AI integration issues and Security aspects, arXiv.org. https://arxiv.org/abs/2206.00868, 2022, June 2.
20. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile Ad Hoc Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019, https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
21. Sharma, A., Singh, M., Gupta, M., Sukhija, N., Aggarwal, P., IoT and blockchain technology in 5G smart healthcare, in: *Blockchain Applications for Healthcare Informatics: beyond 5G,* pp. 137–161, Elsevier eBooks, 2022a, https://doi.org/10.1016/b978-0-323-90615-9.00004-9.
22. Kelly, M., New AI and 5G Advancements Will Usher in the Era of Edge Computing on Smartphones, Autonomous Cars, and More, Business Insider, Mar. 2024, [Online]. Available: https://www.businessinsider.com/time-to-rethink-the-smartphone-ai-5g-mwc-2024-3.
23. Gupta, M., Singh, M., Sharma, A., Sukhija, N., Aggarwal, P., Jain, P., Unification of machine learning and blockchain technology in the healthcare industry, in: *Innovations in Healthcare Informatics: From interoperability to data analysis,* pp. 185–206, Institution of Engineering and Technology eBooks, 2023, https://doi.org/10.1049/pbhe041e_ch6.
24. Saxena, P., Goyal, A., Bivi, M.A., Singh, S.K., Rashid, M., Segmentation of Nucleus and Cytoplasm from H&E-Stained Follicular Lymphoma. *Electronics*, 12, 3, 651, 2023, https://doi.org/10.3390/electronics12030651.

10

Resilient Security Architectures for 6G-Enabled Smart Cities

Bikash Baruah[1], Shivangi Nigam[2] and Apeksha Koul[2]*

[1]Department of Computer Science and Engineering, The Assam Royal Global University, Guwahati, Assam, India
[2]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India

Abstract

Most of the security challenges for smart city design have grown in complexity with every new generation of network technology. Now, with the introduction of sixth-generation (6G) networks, smart city design faces its most challenging security issues. The chapter discusses four prominent security architectures: artificial intelligence–powered security architecture, quantum-resistant security architecture, blockchain-based security architecture, and adaptive security architecture. Each architecture is discussed on the basis of simple flow that depicts how they function; a short description of the layers associated with each such architecture is also provided. Besides architecture, the challenges pertaining to the implementation of those discussed architectures are explored. Such discussions will encourage researchers to propose techniques to overcome such problems or develop better solutions. However, this chapter provides a summary yet a clear overview of all state-of-the-art, powerful security systems designed for a 6G-enabled smart city in a very comprehensive and itemized manner. It is a useful resource for researchers and experts who are trying to build safer and smarter urban environments in the future.

***Keywords*:** Smart city, 6G network, resilient security architecture, blockchain, machine learning, quantum-resistant architecture

**Corresponding author*: apeksha.koul@bennett.edu.in; apekshakoulo9@gmail.com
Bikash Baruah: baruahbikash9@gmail.com
Shivangi Nigam: shivangi.nigam@bennett.edu.in

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (221–246) © 2026 Scrivener Publishing LLC

10.1 Introduction

Smart cities are the future of urban development where the technology will enhance different aspects of the urban life, such as digital technologies for governance, technical benefits, and real-time solutions to transportation, networking, healthcare, etc. With the advent of Internet of Things (IoT) [1], artificial intelligence (AI) [2], cloud computing [3], and sixth-generation (6G) wireless communication [4], these technologies will be useful for subjective addressal of the intricacies of modern urban societies. The advancements in wireless communication, along with IoT, have the potential to sustain a large-scale network infrastructure [5] with billions of devices connected. The latest 6G wireless standard basically uses high-frequency radio bands allowing wider frequency range and expanded bandwidth, capable for large-scale infrastructure with enhanced transmission rates. 6G-enabled IoT is a key component of the wider concept of smart cities. For instance, traffic monitoring systems [6] enabled by IoT, AI, and 6G will aid the traffic optimization in real time. Healthcare systems will be benefitted with intelligent and automated systems for surgeries, diagnostics, and real-time patient monitoring systems. Furthermore, disaster management systems [7], surveillance systems [8], and other life-saving systems will have warning systems and threat detection capabilities [9]. AI can be highly useful for governance by aiding the analysis and prediction of society needs of different age groups and suggesting age-appropriate facilities and real-time grievance addressal systems for personalized governance. Smart infrastructure is another major constituent of a smart city: sensor-enabled devices for monitoring different aspects like air quality, traffic, energy usage; smart grids for energy efficient distribution; smart office, market, and living spaces integrated with user-centric climate system and other energy efficient resources to reduce the carbon-footprint. With such collaboration of technology, governance, and innovations, the smart city would be enhancing the lifestyle quality allowing every citizen to innovate and grow [10].

The evolution of communication technologies [11] from 1G to 6G has been a long journey, which spans from analog communication with very basic and limited bandwidth and quality to advanced and intelligent systems today, like autonomous vehicles and IoT, and moving toward smarter cities. It was a digital revolution in 1990s, marking 2G communication, when global system for mobile communications (GSM) and code-division multiple access (CDMA) were introduced. It was a major shift from analog-to-digital devices where basic encryption algorithms like A5/1 for GSM were used. Since then, the technologies have been growing swiftly. Expanding to mobile broadband in early 2000s and providing internet access on

mobile devices, 3G communication brought more connectivity of device with improved encryption [12, 13] using authentication schemes between devices and networks. However, there were some vulnerabilities like man-in-the-middle attack (MITM) [14]. With the technologies like LTE and WiMAX, 4G communication introduced the high-speed internet, IoT support, HD video streaming, etc. Advancing the security system with Firewalls, end-to-end encryption systems, and intrusion detection systems, 4G communication ensured real-time anomaly detection with focus on secure key exchange. However, with the increased use of mobile apps, cloud, and IoT devices, the risk of privacy breach and other attacks has increased [15]. 5G communication brings intelligent connectivity with technologies like mmWave massive multiple input multiple output (MIMO) [16], which provide reliable ultra-low latency with enhanced security. Although schemes like AI-driven threat detection [17] and edge computing security frameworks [18] have minimized the risk of threats like MITM, impersonation attack, and distributed denial-of-service (DDoS), still, the supply chain, IoT devices, edge computing nodes, and AI systems are susceptible to attacks due to large-scale networks and complex-multi-scale architectures. With an aim to mitigate the limitations of 5G and create a network that is flexible, adaptable, autogenous healing to protect the devices, 6G communication technology is expected to provide resilient solution to the privacy concerns that all the above technologies have been facing till now. Figure 10.1 shows a brief overview of the evolution of communication technologies from 1G to 6G, depicting the growth of devices, security features, and applications.

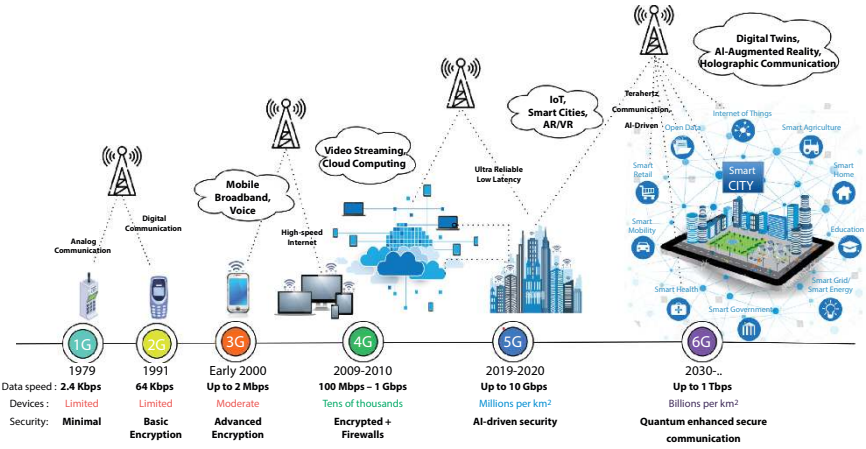

Figure 10.1 Evolution of communication technologies from 1G to 6G while depicting the evolution of basic devices with no internet in 1G and 2G to now having smart cities where everything is connected to each other.

The advancements of 5G have transformed the connectivity of devices providing low latency and ultra-high speeds, but the architecture of current IoT and AI-driven software is exposed to increased security risks. The vulnerabilities include security risk for IoT and autonomous devices due to their hyper-connectivity where not every point has proper security protocols, privacy risks due to non-uniformity of end-to-end encryption for every device, compatibility of 5G networks with quantum computing based encryption methods, and supply chain security risks. These shortcomings are a major setback for developing the smart cities. The current technologies face a significant security challenge in scalability to billions of devices, seamless connectivity for every device connected, energy demands that are very higher for these devices, delays in real-time communication, and, at last, huge amounts of data impacts the security. With 6G, it aims to mitigate the challenges posed here by revolutionizing the intelligence of devices and network. With the ultra-reliable low-latency communication [19], 6G networks are expected to provide ultra-high transmission speeds, which reaches up to 1 Tbps that aids real-time communication. The latency of 5G is as low as 0.1 ms, which is 1 ms in 5G network, which, in turn, can advance the technologies like autonomous vehicles, industry, and healthcare service automation with real-time decision-making. The AI/machine learning (ML) integration in the 6G network enables automation and optimization of network operations, aiding them with threat prediction capabilities. Advances in security schemes in 6G networks promote adaptive and scalable solutions, which are suitable for the large-scaled network with massive machine-type communication [20]. The 6G network has innovations like digital twin where the network has self-aware devices that are aware of their surrounding devices to interact with. 6G is well equipped and capable enough to handle the privacy and security concerns of future.

Security in architecture involves embedding protective measures within the structural design of a system to guard against unauthorized access, data breaches, cyberattacks, and other vulnerabilities. Security focuses on maintaining the confidentiality, integrity, and availability (CIA triad) of information and services. In a secure architecture, each component—be it a database, communication channel, or endpoint device—is designed to resist threats, detect anomalies, and recover from incidents. Techniques like encryption, firewalls, access control mechanisms, and secure coding practices are integral to embedding security into architecture. Beyond technical measures, security in architecture also encompasses policies, compliance standards, and user awareness to ensure comprehensive protection.

Resilience in security architecture refers to the system's ability to withstand, adapt to, and recover from security threats, failures, or attacks while

maintaining essential operations. In today's interconnected digital world, resilience is critical for several reasons:

- **Evolving Threat Landscape:** Cyber threats are becoming more sophisticated, ranging from ransomware and phishing to advanced persistent threats. A resilient security architecture can detect, respond to, and mitigate these threats effectively.
- **High Dependency on Digital Systems:** As organizations and cities become more reliant on digital infrastructure, even minor disruptions can lead to significant operational, financial, or reputational damage. Resilience ensures continuity during such disruptions.
- **Complex and Interconnected Systems:** Modern architectures often involve diverse and interconnected components, such as IoT devices, cloud systems, and AI-driven platforms. This complexity increases the attack surface, necessitating resilience to address vulnerabilities in real time.
- **Critical Services and Infrastructure:** In applications like smart cities, healthcare, and transportation, failures in security can jeopardize human lives, privacy, and public trust. Resilient systems ensure such critical services remain operational under adverse conditions.
- **Compliance and Trust:** Regulations and user expectations demand robust security measures. A resilient architecture ensures compliance with standards like general data protection regulation (GDPR), health insurance portability and accountability act (HIPAA), and national institute of standards and technology (NIST) while building trust among users and stakeholders.

A resilient security architecture is essential to create systems that are not only secure but also adaptable and reliable in the face of dynamic challenges. By integrating resilience into security design, organizations can proactively address potential threats, minimize downtime, and ensure the continued availability of critical services and data. This resilience lays the foundation for trust, innovation, and long-term sustainability in modern technological ecosystems.

The key features of this chapter are as follows:

1) The manuscript provides a detailed overview of the necessity of a security architecture in smart city design.

2) It discusses four prominent resilient security architectures.
3) It highlights key challenges associated with implementing security architectures in 6G-enabled smart cities.

The remaining sections of this chapter are organized as follows: Section 10.2 provides a detailed discussion of four prominent resilient security architectures, whereas Section 10.3 explores the various challenges associated with implementing these architectures and outlines potential future directions. Finally, Section 10.4 concludes the chapter with a summary.

10.2 Resilient Security Architectures for 6G-Enabled Smart Cities

Resilient security architectures are crucial for protecting 6G-enabled smart cities from growing cyber threats. Nowadays, different advanced technologies like AI, blockchain, and quantum-resistant cryptography are used to ensure data security and system reliability. These solutions help to maintain trust and safety in highly connected urban environments. This section discusses four prominent resilient architectures: AI-powered security architecture, quantum-resistant security architecture, blockchain-based security architecture, and adaptive security architecture.

10.2.1 AI-Powered Security Architecture for 6G-Enabled Smart Cities

The AI-powered security architecture [17, 21] includes different layers, namely, real-time, proactive, and autonomous security, which are used for the smart city 6G-enabled smart city structures. The architecture confirms a secure, flexible, and robust design for interconnected systems and sensitive information. The five main layers of AI-Powered security architecture are data layer, AI processing layer, security response layer, monitoring and feedback layer, and communication layer. The conceptual overview of this architecture is depicted in Figure 10.2.

10.2.1.1 Data Layer

The data layer collects the information from diverse sources within the smart city ecosystem. The devices that are used for data collection are different IoT gadgets like sensors, cameras, and autonomous vehicles. Generally, the information is critical infrastructure of industries like power grids and

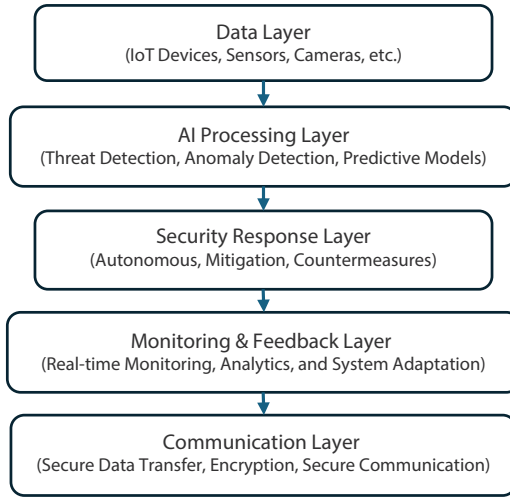

Figure 10.2 Conceptual overview of AI-powered security architecture for 6G-enabled smart cities.

transportation systems, citizen information, and public surveillance feeds. Algorithms implemented in data layer ensure the accuracy of the information gathered, so that it can be used for precise decision-making through data analysis. To protect this information, cryptanalytic methods are applied to ensure data security. Secure communication protocols ensure the confidentiality and reliability of the data while in transit. Basically, this layer provides a solid basis for the architecture so that it can be used for real-time decision-making and smooth operations within smart cities.

10.2.1.2 AI Processing Layer

The AI processing layer is the root of the architecture, which ensures real-time data processing along with threat detections. It uses ML algorithms to identify anomalies, like typical patterns of activities on devices and spikes in network traffic. Different prediction analysis algorithms are applied to enhance AI models that can foretell possible attacks, including DDoS, ransomware, and other data breaches, using available historical data and current forms of threat intelligence. It performs behavioral analysis to continuously monitor the devices, networks, and users that can identify anomalies and compromised devices. These AI models are consistently trained for real-time updates, ensuring high accuracy in catching new and emerging threats. This is the most critical reason why this layer is included for identifying and addressing risks in smart city systems.

10.2.1.3 Security Response Layer

The security response layer is designed to delete or modify the threats immediately upon detection, which ensures the interference of smart city functions as negligible as possible. Once a threat is identified, such as unauthorized access or malware, the automated systems get activated and isolate the affected devices to block malicious traffic, and, sometimes, such devices are disabled for a longer period. The architecture also deploys autonomous countermeasures, where emergency protocols like data rerouting or redundant service activation are enabled to maintain the continuity of smart city services during the time of attack also. Real-time decision-making processes allow the systems to act with low latency, hence acting on time against threats. Automating such responses by the architecture ensures the continuous protection of the critical services.

10.2.1.4 Monitoring and Feedback Layer

The monitoring and feedback layer keeps on monitoring the holistic security framework. This layer provides essential information for further improvement and modification. Non-stop monitoring provided by this layer tracks all the operations in the network so that no anomaly (or threat) can be left behind. The performance measurement evaluates the security protocols, AI models, and response mechanisms; and feedback layer provides additional information to enhance the AI algorithms, threat databases, and fine-tune predictive models. These are augmented by intrusion detection systems and log monitoring tools. The integration with external threat intelligence with intrusion detection system enhance the ability of this layer to adapt and improve the existing architecture to maintain its robustness against evolving threats.

10.2.1.5 Communication Layer

The communication layer ensures high-speed data transfer securely over the smart city framework. It uses advanced features of 6G networks. This layer provides interaction between IoT devices, AI models, and security response systems with advanced encryption techniques to protect data from unauthorized access or manipulation. In addition, different algorithms are implemented for designing zero-trust model that ensures the authenticity of every device's before granting the access in the smart city framework. This layer makes sure the compliance with privacy regulations and the security of sensitive information by isolating vital broadcasting data from private information. The communication layer becomes the responsible for continuous transfer of information within the smart cities while maintaining the security and reliability.

The AI-based architecture ensures that the smart cities designed for 6G technologies can enhance the quality of life to a next level without compromising security. With the implementation of AI, this security framework keeps on learning and adapting continuously using reinforcement ML models, which makes it more effective to the upcoming challenges and potential threats.

10.2.2 Quantum-Resistant Security Architecture for 6G-Enabled Smart Cities

Quantum-resistant security architecture [22, 23] is designed using quantum computing to protect smart city infrastructures from the potential threats. Quantum computers have the ability to break traditional cryptographic algorithms, such as digital signature algorithm (DSA), Rivest–Shamir–Adleman (RSA), and elliptic curve cryptography (ECC), because it relies on the discrete logarithms, which is very much powerful in solving large factors. Apart from that, quantum-resistant architecture adapts diverse cryptographic algorithms that are secured using the computational power of quantum machines. This architecture incorporates quantum-safe encryption, hybrid cryptographic schemes, secure key management, and quantum communication protocols to ensure robust security in the smart city infrastructure. The conceptual overview of this architecture is depicted in Figure 10.3.

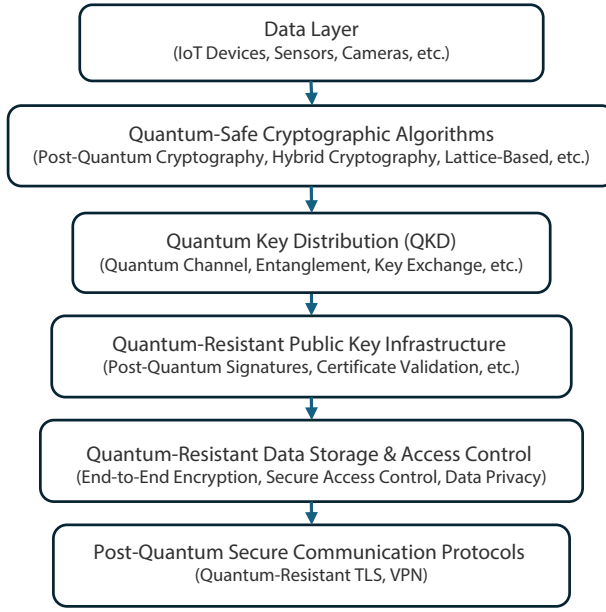

Figure 10.3 Conceptual overview of quantum-resistant security architecture for 6G-enabled smart cities.

10.2.2.1 Data Layer

The data layer is the foundation of this architecture. This layer collects the data generated by IoT devices, autonomous vehicles, smart grids, and communication networks. By employing quantum-resistant encryption protocols, the data layer ensures the confidentiality of the data at every stage: collection, transmission, and storage. This layer employs different algorithms to design advanced mechanisms to detect tampering and spying attempts involved in sensitive information like public surveillance feeds, healthcare data, and financial transactions.

10.2.2.2 Quantum-Safe Cryptographic Algorithms

This layer is the heart of this architecture. Quantum-safe cryptographic algorithms offer protection from the quantum computing, which is capable to crack conventional cryptosystems. The development of quantum-safe cryptographic algorithms incorporates discrete mathematics such as multivariate polynomial systems, lattice-based problems, and hash-based problems that are currently outside the capabilities of quantum computers. It allows us to confirm and believe in the security of such quantum-resistant architecture. Quantum-safe cryptography techniques, including post-quantum cryptography, hash-based signatures, and lattice-based encryption, are combined with discrete mathematics to design such a model. The hybrid cryptographic models, which provide a transition solution, are successfully designed by merging conventional discrete mathematics with quantum-safe cryptography. In addition, proactive strategies might increase the security level one step further for sensitive data exchange in big data.

10.2.2.3 Quantum Key Distribution (QKD)

Quantum key distribution (QKD) is a breakthrough technology designed to revolutionize cryptographic key exchanges using the principles of quantum mechanics. Its primary function is to detect and block any unauthorized attempts to intercept keys during transmission between a sender and receiver. In 6G-enabled smart cities, QKD plays a vital role in building quantum-resistant security architectures. By harnessing the behavior of photons and quantum entanglement, it provides a highly secure method of key distribution. Even advanced spying techniques powered by quantum computing cannot compromise the confidentiality of these keys. The combination of QKD with traditional communication systems ensures its practicality for real-world applications. This integration significantly

bolsters the security framework, making it highly resilient to sophisticated quantum-based cyberattacks.

10.2.2.4 Quantum-Resistant Public Key Infrastructure (PKI)

Quantum-resistant public key infrastructure (PKI) is a platform for communication where digital identities are empowered for quantum resistance. Quantum-resistant PKI replaces the classical algorithms by robust post-quantum models to maintain the integrity and authenticity of digital certificates. This architecture provides automated features for certificate creation, validation, and revocation. Additionally, the quantum secure environment is maintained through legacy systems for seamless transition. This ensures that the essential functions such as secure authentication, encrypted communication, and trust management remain reliable in a post-quantum world.

10.2.2.5 Quantum-Resistant Data Storage and Access Control

In smart cities, large amount of sensitive data is stored in different distributed systems, namely, cloud platforms and edge devices. The main challenge with distributed systems is its security issue, because all such data are stored in online platform. Hence, it requires robust protection. Quantum-resistant encryption ensures that the data remains inaccessible without the encryption keys. Additionally, access control algorithms are also used for post-quantum cryptographic authentication to prevent unauthorized access. Homomorphic encryption is a good example of quantum access control, where computations can be performed on encrypted data without exposing the raw information. These capabilities ensure that smart city data remains secure even though attackers are equipped with quantum-based decryption models.

10.2.2.6 Post-Quantum Secure Communication Protocols

Reliable high-speed networks along with appropriate protocols for secure communication are critical for smart city communications using 6G. The post-quantum safe communication protocol incorporates quantum-resistant cryptographic algorithms into the current framework like transport layer security (TLS) for safe data exchanges over the web and application channels. With integrated 6G infrastructure, it works securely on huge data communications even at low latency. Such protocols generally work by ensuring confidentiality and integrity in the data of the smart city infrastructure to assure secured data delivery against quantum-enabled attacks.

With these, the quantum-resistant security architecture offers comprehensive security for 6G-enabled smart cities against the power of quantum computing. It focuses on the inclusion of quantum-safe encryption, key exchange mechanisms, and secure communication protocols. Such architecture requires much development; hence, there are many loopholes present to date. However, with growing technology in security architecture, this platform is becoming more robust and feasible practically.

10.2.3 Blockchain-Based Security Architecture for 6G-Enabled Smart Cities

Blockchain technology [24, 25] is based on decentralization of control authorities and hence distributing the authority to multiple nodes across the network. With this decentralization, the security is enhanced by increasing the resistance to threats of the network. To address the security concerns in smart cities, blockchains ensure that the systems like traffic, healthcare, and autonomous industry operations are executed without any potential risks. Attacks such as DDoS, MITM, and tampering are avoided with blockchain due to the distributed nature of network authorities. Blockchain uses tamper-proof network where data is safe as it cannot be changed after it is written. This ensures that public records are safe, and the transparency is maintained, and, with robust verification systems, devices can be saved from various cyber threats. Blockchain also aids secure transactions, which can payments systems in smart city applications like billing of electricity, gas, transport etc. The conceptual overview of this architecture is depicted in Figure 10.4.

10.2.3.1 Data Layer

The smart cities would have billions of devices like sensors, IoT devices, vehicles, and electricity meters, which are connected for diverse applications. These connections are operated on data layer where the essential information to be communicated is generated, organized, and secured. With blockchain, the information is secured with the tamper-proof technology, restricting all unauthorized access. It also ensures the authenticity of devices. The resilient decentralization blocks the intrusion activities and is, hence, secure. For smart cities, the data layer helps in following ways:

a. The data storage in blockchains is immutable, providing vital support to applications like maintaining data integrity and transparency of public records, medical records, traffic information exchange.

b. In blockchain the data is tamper-proof as every data is stored with a timestamp, which cannot be altered. This feature can help in planning and tracing the smart city products.
c. It ensures and safeguards the systems from attacks by keeping decentralized system where is available even in case of failures on one or more control nodes. This can aid the smart city in maintaining failure-proof systems like smart grids.
d. Applications of data layer include smart transportation, energy management, smart governance, and healthcare systems.

With so many advantages, comes some challenges. Large volumes of data and devices in smart cities require scalable solutions like off-chain storage and distributed systems. Authorizing techniques need significant computational capabilities to authorize the data. The emergency systems in a smart city must have ultra-low latencies. Addressing these challenges combined with AI-driven technology, edge computing, etc., is essential.

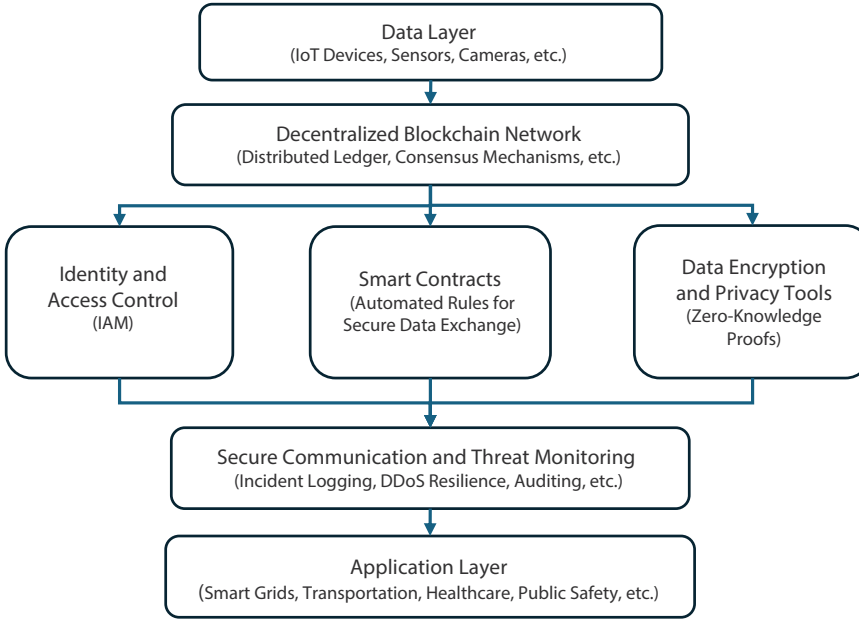

Figure 10.4 Conceptual overview of blockchain-based security architecture for 6G-enabled smart cities.

10.2.3.2 Decentralized Blockchain Network

The blockchains allow multiple distributed control nodes to manage the network. This feature allows the data to spread across a larger network, which, in turn, creates redundancy, promoting cyber threats to the network. To resolve this, consensus mechanisms like proof of stake or Byzantine fault tolerance are used to enforce transparency by having access to an immutable copy of the ledger. The access here to data is limited with some specific authorities, which balance the data sharing and transparency, thus creating a tolerant and reliable system. The benefits and challenges of decentralization for smart cities can be stated as follows:

a. The reliability of operational systems like power supply, water supply, and internet services are ensured to be remain operational even in case of any local issues.
b. The decentralization brings transparency to the system, which is essential for services like smart governance and public services.
c. Decentralization also provided distribution of resources for real-time optimization and balance in resource constrained applications such as energy production services.
d. It also provides integration with 6G communication to provide security to large-scale networks.
e. With the increased load of 6G network and smart city devices, there are some challenges that need to be addressed, as follows: cybersecurity risk like Sybil attacks and 51% attack; high infrastructure costs of decentralized systems; and coordination of large amount of devices.

10.2.3.3 Identity and Access Management (IAM)

Blockchain has a mechanism for ensuring secure access to data and applications, known as identity and access management (IAM). Using the cryptography techniques, the users and devices are allotted their unique identities and these saved on a tamper-proof ledger. Unlike the centralized systems, these systems are able to reduce the bottlenecks and vulnerabilities by maintaining the immutable ledger for authorization activities. The authorization and authentication of blockchain has strict entry points where cryptographic keys are used to access the information. It also has a single-sign-on feature through which the users and devices can log in on multiple platforms. With IAM, smart cities will be able to provide seamless

operations in applications such as healthcare, education, and public transport. IAM is capable to enhance security by making forgery harder, giving the ownership to user and providing trust by ensuring transparency. There are some challenges of IAM with the current infrastructure that needs to be address in 6G networks as in ensuring that all devices comply with the regional laws like GDPR, standardization, and integration with all devices, managing crypto keys where if the key is lost, then it could mean that identity is lost, etc.

10.2.3.4 Smart Contracts

Blockchains have an automatic process of applying terms and conditions of an agreement. If, at any time, the conditions are not met, then the agreement is revoked, providing security, trust, and transparency, without any manual operation. These agreements are termed as smart contracts, which have some pre-defined rules embedded in the system. Automatic execution, transparency, immutability, decentralization, and cost efficiency are some advantages of implementing these smart contracts. These are written in programmable languages like Solidity where they have all the rules and conditions to be met. On meeting the conditions, the agreement is invoked, and the transaction is recorded on blockchain. Accountability, security, and trust are some advantages of having smart contracts. However, there are some challenges, like vulnerabilities in smart contracts can allow breaches, regulatory rules are not fully developed for current systems, and inter-device operations need to be compatible. It can be useful for developing smart cities in following ways: automating the education and healthcare systems with these smart cards.

10.2.3.5 Data Encryption and Privacy

Smart cities development is incomplete without resilient data security and privacy services as the large amount of data shared is vulnerable to security breach. Encryption methods with blockchain, such as cryptographic methods (public-key cryptography), encryption methods, zero-knowledge proofs (ZKPs), and multi-party computation (MPC), ensure that privacy is preserved while data sharing. ZKPs are capable to authorize transactions without revealing the actual information useful for healthcare systems where medical records are sensitive information, in financial transactions and identity management. With these techniques of blockchain encryption, an immutable smart city system sustains. The key challenges of blockchain for encryption are as follows:

a. The increased number of devices and data is a major challenge as it would have large data storage and computation requirements.
b. Maintaining the keys is another concern for the owner, as, if lost, then they would lose their identity.
c. Once the data is recorded, it is there forever. The data should be correct; otherwise, it will not be useful and may conflict with the privacy rules.
d. The overall process of encryption and decryption is a computational overhead, which must be looked into.

10.2.3.6 Secure Data Exchange and Communication

The security is the first and foremost concern of a smart city. Blockchains are a great way to facilitate this within the whole ecosystem. Integration with technologies like IoT requires smart and immutable systems to handle the amount of data generated by the large-scale network. Blockchain techniques could automate the process and thereby ensure safe and secure network with minimal manual intervention. For most of the smart city operations, blockchain framework is available to address different needs of the system.

10.2.3.7 Secure Threat Monitoring

Smart cities have so many devices and applications connected, so they are all exposed to cyberthreats. With blockchain, real-time detection systems alleviate the DDoS attacks. Also, the immutable recording system of blockchain is open and transparent providing forensic capabilities such that the threats can be identified and resolved instantly. Thus, the trust and security of public are ensured in everyday operations of smart cities. The challenges with the monitoring systems include the following:

a. Maintaining common laws of regulation of rules for all devices lying under different regions serving different applications
b. Integrating with all the advancements in technologies like IoT and edge computing requires continuous improvements that are implements simultaneously
c. Maintaining low latency across all devices for real-time services
d. Balancing the need of transparency while keeping the sensitive information private

With future techniques like AI/ML integration, quantum computing–based blockchain rules, and compatibility of different communication technologies like 5G and 6G, smart cities would be safe and secure.

10.2.3.8 Application Layer

Application layer provides the deployment services for various applications, services, and functionalities of the smart cities, which are made to serve specific needs of smart urban operations. It has the advantage of blockchain features such as transparency and security across a wide range of domains of smart city. Different applications for a smart city could be a smart governance application sharing public services to its citizens and allowing data sharing with blockchain-enabled encryption techniques. Similarly, smart healthcare applications ensure secure maintenance of medical records and real-time emergency applications. This layer provides user-oriented customization of applications to cater a diverse range of customer issues.

The blockchain-based security architecture provides a comprehensive solution for securing 6G-enabled smart cities. By leveraging blockchain's decentralized, tamper-proof, and transparent properties, it addresses critical challenges such as data integrity, identity management, cyber resilience, and privacy preservation. This architecture not only safeguards urban infrastructure but also empowers innovation, collaboration, and sustainability, paving the way for a more secure and resilient urban future.

10.2.4 Adaptive Security Architecture for 6G-Enabled Smart Cities

Adaptive security architecture [26] is an ever-changing and actively engaged architecture of cybersecurity systems purposely building to tackle the continuously changing types and manifestations of security threats. This adaptive security is retroactively designed to protect systems against new data, vulnerabilities, or complex attack vectors in real time as opposed to traditional static security models that depend on a set of predefined, often algorithmic, rules. It uses real-time monitoring, predictive analytics, ML, and automation; as such, it can rapidly detect and respond to threats. Then, it becomes important for 6G-enabled smart cities, where all the IoT devices, automated systems, and critical infrastructures will be built and interconnected and, hence, proven susceptible to threats. Adaptation-resilient security architecture brings the necessary flexibility and robustness

to secure these systems and applications with room for seamless operation and ensures no interruption in critical services like smart grids, medical systems, or even transport. The conceptual overview of this architecture is depicted in Figure 10.5.

10.2.4.1 Data Sources and Systems

The adaptive security architecture includes all the data sources and systems as a bottom layer consisting of endpoint sites for the real-time information collected for smart city operations. It includes IoT devices, cloud platforms, edge devices, and specialized applications such as traffic management and healthcare applications. Such components are input to security analysis, providing the necessary information to help monitor threat detection and to inform decision-making in the security domain. Because the layer is made up of critical assets for city life, any compromise to the system would affect the availability of critical services. This, therefore, becomes needed to be secured for the purposes of integrity or availability for major operations including real-time control of traffic or emergency response in securing the whole urban ecosystem. In addition, it can improve the integrity of data against modification and lead toward more transparency through blockchains.

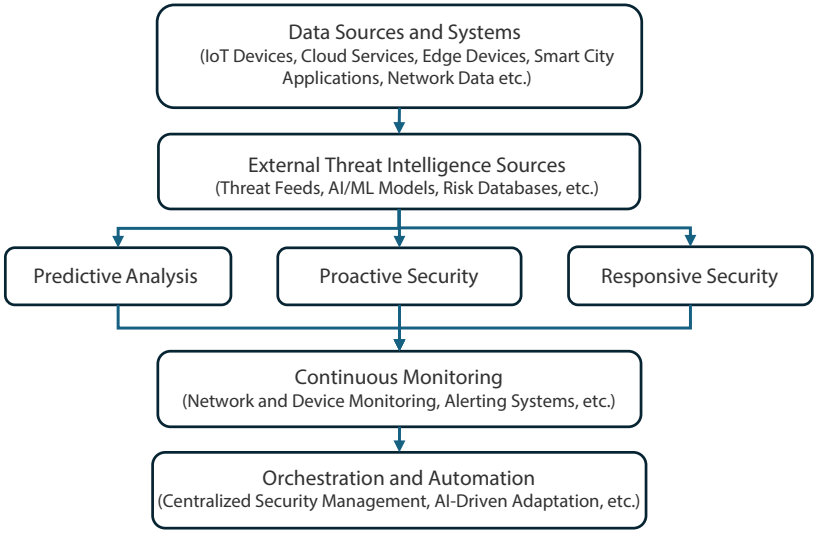

Figure 10.5 Conceptual overview of adaptive security architecture for 6G-enabled smart cities.

10.2.4.2 Predictive Analytics

Predictive analytics, being a major component of adaptive security, predicts latent risks before they manifest, through ML models for analysing patterns. Historical data is then supplemented by real-time inputs to deliver advanced algorithms for evaluating threat levels that enable prioritization of responses for scenarios that face higher risk. This layer is further strengthened by anomaly detection that identifies unusual behaviors ranging from ebbs and scuttle of network traffic to even unauthorized attempts of access—all of which might spell quite a lot of doom in cyber threat attacks. Ongoing real-time insight ensures that new risks are rapidly routed for remediation, limiting opportunity for exploit by malicious actors. For city governments, predictive analytics enables security teams not to wait for disruptive events or attacks and take timely action, which boosts their ability to prevent the impairment of urban service delivery. Predictive analytics provides better insights and statistics for security teams to proactively handle situations and improve the efficiency of the city government.

10.2.4.3 Proactive Security

Security proactive mechanism was designed for the prevention of incidents by addressing weaknesses and threats before they become problematic. Dynamic access control modifies user and device permissions in real time according to risk assessments, limiting access when suspicious behavior is detected to avoid attacks. Threat containment includes compromised systems and devices to contain the damage, providing the most vital and strongest defense before the onset of the organism in as early as possible early-stage threats. Firewalls and intrusion prevention systems are regularly updated to block malicious traffic and access unauthorized entry and remain ahead of developed vulnerabilities within the architecture. Using these proactive methods, the architecture reduces the chances of breaches to keep vital systems functional and secure against advanced threats.

10.2.4.4 Responsive Security

Real-time response secures rapid detection, containment, and remediation of threats, minimizing any potential harm. It allows you to automate incident response workflows that help you take actions such as isolating affected systems or notifying administrators, ensuring that security incidents are handled consistently and efficiently. Enabling instant recognition

of threats like malware or unauthorized access, it can isolate an incident in real-time before it compromises any sensitive data. Once the issue is contained, remediation involves restoring affected systems to their original state, ensuring that the business can operate with minimal disruption. The ability to deploy emergency protocols at a city-wide level is imperative, particularly in the context of smart cities where seamless service delivery and infrastructure resiliency is paramount. This includes both enabling downtime and preventing massive impacts from a cyberattack by supporting operational continuity through responsive security.

10.2.4.5 Continuous Monitoring

Continuous monitoring imparts the capability to understand in real-time the extent to which smart cities' systems are secure, assuring exhaustive protection against any threat. This layer captures suspicious activities, such as unauthorized logins or clues of data exfiltration, by constantly tracking network traffic, device activity, or even user interaction. It advanced alerting systems that notify the administrator of potential risks for further investigation and action. It enhances monitoring because access to global threat intelligence and discovery bases information collected from emerging vulnerabilities and attack trends, keeping security measures always in place with the latest threats. Continuous monitoring is needed because smart cities have multifaceted settings where device and system interconnectivity needs to be observed at an acute level to avoid a breach of continuity in services.

10.2.4.6 Orchestration and Automation

The orchestration and automation characteristics further enhance efficiency and scalability in security operations, especially when considering large environments, such as smart cities enabled by 6G telecommunication standards. Centralization of security management further streamlines the coordination of all the activities under which threat detection, response, and recovery take place within a singular platform. AI adaptation is dynamic in that it allows security policies to be modified from one point to another, based on real-time data-derived information, letting the architecture adapt quickly to constantly emerging threats. Automated workflows, such as patch management, alert escalation, and incident response, reduce the human side of these processes, reduce the chances for human error, and speed up reaction times. Altogether, orchestration and automation help keep security operations active, responsive, and ready for action, regardless of the scale at which cyberattacks may occur.

In 6G-enabled smart cities, the integration of IoT devices, autonomous systems, and real-time data processing creates a dynamic environment where traditional security models are inadequate. Adaptive security architecture addresses these challenges by providing a scalable, flexible, and responsive approach to cybersecurity. Through predictive analytics, proactive security measures, and automated responses, this architecture ensures that critical services remain secure and uninterrupted. By enabling real-time threat anticipation, swift mitigation, and continuous adaptation, adaptive security architecture plays a vital role in safeguarding the integrity, reliability, and resilience of next-generation urban systems.

10.3 Challenges and Future Scope

There exists a unique demand for rich and propounding security architectures owing to the seamless incorporation of 6G networks in smart cities. The first concern is to provide *ultra-low latency and reliability* in the most unassailable manner. Applications such as autonomous vehicles, smart healthcare systems, and industrial automation require ultra-low latency in the microsecond range, allowing minimal time for the use of traditional security solutions that consume great amounts of resource. In addition, the huge number of devices connected, and heterogeneous nature of smart cities will increase the difficulties involved. All these IoT devices are in billions, connecting the extremely capable edge servers to the very low resource sensors; however, achieving uniform security measures is becoming more and more complex. Moreover, the hyper-connected systems increase the attack surface significantly with vulnerabilities appearing at device, network, and application layers. Catastrophic impacts could result from cyberattacks, such as DDoS attack or ransomware, against critical services like transportation or energy grids. There is also the privacy issue, as smart cities will be using 6G-enabled AI applications in real-time decision-making that will involve heavy data gathering and processing. The challenges are to ensure secure sharing of data without letting users know who is sharing the data with whom, as well as compliance with privacy regulations. Finally, the dynamic and adaptive security frameworks would evolve with emerging technologies to deal with novel threats, including quantum computing attacks and sophisticated AI-driven adversarial methods.

As the integration of 6G networks with smart cities advances, there are several key future directions that can enhance the resilience and robustness of security architectures.

10.3.1 Integration of AI and Machine Learning

To a greater extent, the features of security systems can employ AI and ML. Automatic threat detection, anomaly detection, and predictive security are some uses of these technologies in real-time that allow the systems to autonomously respond to new threats instead of relying on humans to intervene. By using real AI models, for example, one would expose the system to patterns of attack in the past so that it might shape the future to predict and prevent attacks from happening, producing new proactive features in security systems within such a climate instead of the old reactive.

10.3.2 Blockchain for Data Integrity

Blockchain can be a good source for maintaining data integrity through the extensive interrelationships of 6G-enabled smart cities. It will ensure transparent and tamperproof data storage from IoT devices, proving them to be immutable and secure. Such conditions may be of paramount importance in areas demanding highly sensitive data, like smart healthcare or autonomous vehicles. It can enable 6G applications for secure smart contracts and for automated policy enforcement.

10.3.3 Decentralized Security Models

A decentralized security model promises to further improvement resilience, as opposed to a centralized control. In a decentralized model, security is distributed, instead of depending on a single point of control, across the entire network-reducing risk of a single point of failure. This can be realized with the help of several technologies, such as edge computing, fog computing, or any other method of taking security closer to the source of data (e.g., individual IoT devices), rather than directly linking it to a centralized cloud.

10.3.4 Quantum-Resistant Cryptography

As quantum computing technology keeps on evolving, all the traditional cryptographic techniques might be at risk. Hence, one crucial future direction toward security in the era of 6G will be implementing quantum-resistant cryptographic algorithms: post-quantum cryptography. These techniques would able to withstand assaults from classical and quantum computers alike, thereby securing the communication and data exchange across smart city infrastructure.

10.3.5 Security Automation and Orchestration

The growing demands of ever-increasing complexity for achieving 6G networks necessitate automation in security management across multiple layers. The automated responses to threats, continuous monitoring, and real-time policy updates are part of security automation tools and significantly reduce the need for manual participation. In addition, orchestration tools can also bring together security policies and responses from different network stemming and technology inputs, therefore securing consistent yet effective security management in the entire smart city infrastructure.

10.3.6 Interoperability Across Multiple Domains

Integration of technologies in energy management, intelligent transport, healthcare, public safety, etc., makes security in a smart city much dependent on the interoperability of those domains. Future initiatives should provide the means to create security standards and frameworks that cross domains and technologies for their integration into smart city fabric.

10.3.7 Human-Centric Security Solutions

Security in the 6G smart city should also include the human aspect, particularly in terms of privacy and user consent. Future security architectures should have a user-centric component and be equipped with privacy management provisions as well as user authentication and secure access control. User access can include biometrics, behavioral analytics, or identity management for safe and seamless user experience in all services offered by smart cities.

These key prospects will serve the purpose of advancing smart security frameworks to meet new challenges associated with 6G-built smart cities. Integrating technology with the cooperative, adaptive, and user-centric model would lend itself to these challenges and prepare the ground for smart cities of the future.

10.4 Conclusion

The paper gives an in-depth discussion justifying the huge necessity for resilient security architectures in smart cities transformed by 6G technologies. Increasing connectivity and automation levels keep pushing smart cities to depend more and more on such technologies as AI, quantum-resistant

cryptography, blockchain, and adaptive security systems. Each one is encapsulated in a customized framework, from AI-driven proactive layers to blockchain decentralized integrity, to address tough cyber threats. Several highlighted challenges that are scalability, interoperability, resource constraints, and ethical issues rose about solving them using advanced technologies, including quantum computing, alongside the development of global collaborations for standardized solutions. The paper highlights that security in smart cities in this case 6G is not only by having some technical mitigate measures; it is also about being assured trust and continuity for innovation using secured critical infrastructures in cities. In brief, the integration of adaptive and forward-thinking security measures ensures the alignment of technological advancement with societal needs, establishing a foundation for sustainable and secure urban ecosystems. This trajectory positions 6G-enabled smart cities as benchmarks for future intelligent urban environments.

References

1. Madakam, S., Ramaswamy, R., Tripathi, S., Internet of Things (IoT): A Literature Review. *J. Comput. Commun.*, 3, 5, May 2015, Art. no. 5, doi: 10.4236/jcc.2015.35021.
2. Zaman, M., Puryear, N., Abdelwahed, S., Zohrabi, N., A review of IoT-based smart city development and management. *Smart Cities*, 7, 3, 1462–1501, 2024.
3. Qian, L., Luo, Z., Du, Y., Guo, L., Cloud Computing: An Overview, in: *Cloud Computing*, M.G. Jaatun, G. Zhao, C. Rong (Eds.), pp. 626–631, Springer, Berlin, Heidelberg, 2009, doi: 10.1007/978-3-642-10665-1_63.
4. Bajpai, A. and Nigam, S., A Study on the Techniques of Computational Offloading from Mobile Devices to Cloud. *Res. India Publ.*, 10, 7, 2037–2060, 2017.
5. Dhurandher, S.K., Borah, S.J., Obaidat, M.S., Kr. Sharma, D., Gupta, S., Baruah, B., Probability-based controlled flooding in opportunistic networks, in: *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, Jul. 2015, IEEE, pp. 3–8.
6. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A., Enhancing Security and Privacy in Traffic-Monitoring Systems. *IEEE Pervasive Comput.*, 5, 4, 38–46, Oct. 2006, doi: 10.1109/MPRV.2006.69.
7. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-based wireless sensor network: a comprehensive survey, in: *Software-Defined Network Frameworks*, pp. 121–141, CRC Press eBooks, 2024.

8. Elharrouss, O., Almaadeed, N., Al-Maadeed, S., A review of video surveillance systems. *J. Vis. Commun. Image Represent.*, 77, 103116, May 2021, doi: 10.1016/j.jvcir.2021.103116.
9. Einstein, H.H. and Sousa, R., Warning systems for natural threats. *Georisk Assess. Manag. Risk Eng. Syst. Geohazards*, 1, 1, 3–20, Mar. 2007, doi: 10.1080/17499510601127087.
10. Angelidou, M., Smart city policies: A spatial approach. *Cities*, 41, S3–S11, Jul. 2014, doi: 10.1016/j.cities.2014.06.007.
11. V.C. *et al.*, Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.*, 7, 4, 529–539, Nov. 2011, doi: 10.1109/TII.2011.2166794.
12. Baruah, B. and Saikia, M., An FPGA implementation of chaos based image encryption and its performance analysis. *IJCSN-Int. J. Comput. Sci. Netw.*, 5, 5, 2016.
13. Saikia, M. and Baruah, B., Chaotic Map Based Image Encryption in Spatial Domain: A Brief Survey, in: *Proceedings of the First International Conference on Intelligent Computing and Communication, in Advances in Intelligent Systems and Computing*, Springer, Singapore, vol. 458, pp. 569–579, 2017.
14. Nigam, S., Bajpai, A., Kumar, N., Signal and Time Based Fuzzy Cluster Scheme to Detect Sybil Attack in VANET. *Int. J. Comput. Sci. Eng. IJCSE*, 9, 7, 2017.
15. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile Ad Hoc Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019, https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
16. Mumtaz, S., Rodriguez, J., Dai, L., Introduction to mmWave massive MIMO, in: *mmWave Massive MIMO*, pp. 1–18, Academic Press, 2017.
17. Mishra, S., Shukla, A., Arora, S., Kathuria, H., Singh, M., Controlling Weather Dependent Tasks Using Random Forest Algorithm, in: *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bengaluru, India, pp. 1–8, 2020, doi: 10.1109/ICAECC50550.2020.9339508.
18. Garg, S., *et al.*, Edge Computing-Based Security Framework for Big Data Analytics in VANETs. *IEEE Netw.*, 33, 2, 72–81, Mar. 2019, doi: 10.1109/MNET.2019.1800239.
19. Popovski, P., *et al.*, Wireless Access in Ultra-Reliable Low-Latency Communication (URLLC). *IEEE Trans. Commun.*, 67, 8, 5783–5801, Aug. 2019, doi: 10.1109/TCOMM.2019.2914652.
20. Bockelmann, C., *et al.*, Massive machine-type communications in 5g: physical and MAC-layer solutions. *IEEE Commun. Mag.*, 54, 9, 59–65, Sep. 2016, doi: 10.1109/MCOM.2016.7565189.
21. Awad, A., II, Babu, A., Barka, E., Shuaib, K., AI-powered biometrics for Internet of Things security: A review and future vision. *J. Inf. Secur. Appl.*, 82, 103748, May 2024, doi: 10.1016/j.jisa.2024.103748.

22. García, C.R., *et al.*, Quantum-resistant Transport Layer Security. *Comput. Commun.*, 213, 345–358, Jan. 2024, doi: 10.1016/j.comcom.2023.11.010.
23. Fernández-Caramés, T.M., From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet Things J.*, 7, 7, 6457–6480, Jul. 2020, doi: 10.1109/JIOT.2019.2958788.
24. Li, J., Liu, Z., Chen, L., Chen, P., Wu, J., Blockchain-Based Security Architecture for Distributed Cloud Storage, in: *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, Dec. 2017, pp. 408–411, doi: 10.1109/ISPA/IUCC.2017.00065.
25. Rathore, S., Wook Kwon, B., Park, J.H., BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.*, 143, 167–177, Oct. 2019, doi: 10.1016/j.jnca.2019.06.019.
26. Siddiqui, S., Hameed, S., Shah, S.A., Arshad, J., Ahmed, Y., Draheim, D., A smart-contract-based adaptive security governance architecture for smart city service interoperations. *Sustain. Cities Soc.*, 113, 105717, Oct. 2024, doi: 10.1016/j.scs.2024.105717.

11

Innovative Solutions for User Privacy in 6G Networks

Manisha Koranga[1]*, Tarun Kumar[2], Richa Pandey[1] and Sujata Negi Thakur[1]

[1]Department of Computer Science and Engineering, Graphic Era Hill University, Haldwani, Uttarakhand, India
[2]Department of Allied Sciences, Meerut Institute of Engineering & Technology Kumaun, Haldwani, Uttarakhand, India

Abstract

With the emergence of sixth-generation (6G) network technology, the highly interlinked surroundings and smart applications face significant privacy difficulties. The ubiquitous identity of the 6G, which features extremely minimal latency, significant artificial intelligence integration, and Internet of Things installations, increases the possibility of privacy infringement and unlawful information gathering. This research has investigated the major concerns about privacy in 6G networks, including the expansion of data collection, advanced tracking systems, and the decline in anonymity. Significant privacy concerns that have been recognized include manipulating information, identity theft, and aggressive observation, all of which could weaken user trust and inhibit using 6G technology. Eliminating these privacy risks involves the exploration of some innovative privacy-preserving solutions that are used to secure sensitive data. Decentralized methods for secure identity management and enhancing data transparency have also been identified. To promote the setting up of healthy, user-oriented 6G habitats that respect the basic entitlement to security, this paper offers a concise overview of privacy issues and solutions in 6G.

***Keywords*:** Sixth-generation (6G) networks, privacy-conserving, shielding, risks, hurdles, innovation

**Corresponding author*: ManishaKoranga@gehu.ac.in

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (247–262) © 2026 Scrivener Publishing LLC

11.1 Introduction

Building on the milestones of the fifth generation (5G), the forthcoming sixth-generation (6G) mobile technology promises revolutionary advancements in speed, capacity, and reliability to integrate artificial intelligence (AI), neural networks, and Internet of Things (IoT) into a seamless digital realm [18, 20]. Continuous assessment for smart towns and cities, ultra-reliable and minimal latency connections for autonomous systems, and improved wireless internet for engaging virtual reality and augmented experiences are all made achievable by 6G. In addition to optimizing IoT applications in homes with sensors, industrial automation, and monitoring the surroundings, it will assist cutting-edge healthcare solutions like telemedicine and remote surgery. The creation of cutting-edge applications like smart automation, holographic communication, and ubiquitous sensing is made easier by 6G's alluring qualities, which include incredibly low latency, increased data transmission capacity, wide device connectivity, and greater network intelligence. The introduction of 6G systems, anticipated to link numerous pieces of electronic equipment and enable the transfer of enormous volumes of data, poses serious problems in protecting user privacy [4, 7, 17, 30]. Significant privacy concerns are being brought about by the advanced characteristics of 6G technology, which comprises the possibility of enormous data procurement, advanced tracking techniques, and the misuse of private data. In this typical setting, maintaining user trust, following the law, and avoiding unwanted access and use of sensitive data all depend on protecting user privacy [4, 5, 26, 35].

11.2 Survey of Literature

The innovation in 6G networks was anticipated to bring its previously unattainable technology and connectivity. However, the major concern is to preserve privacy. This survey of previous literature looks at the state of privacy issues in 6G networks today, highlights major obstacles, and looks at creative fixes put forth in current studies and business advancements. A substantial exploration into 6G security due to advancements in network security hindered the worldwide debut of 5G.

This document examines the developing 6G communication framework, merging conventional security principles with advancements in the latest technologies. It highlights the threats associated with 6G and the corresponding cryptographic methods. Furthermore, it suggests avenues

for further research, highlighting various authentication methods [14]. As the shortcomings of 5G networks become apparent, the investigation into 6G as the forthcoming solution is gaining momentum, concentrating on essential security and privacy concerns. This survey examines the evolution of networking technologies throughout history, which have shaped contemporary 6G trends. It delves into prime components such as real-time smart edge computing, distributed AI, smart radio systems, and three-dimensional intercoms while focusing on critical issues, i.e., security and confidentiality. The survey concludes with an exploration of the prospective applications of 6G [32]. This paper addresses significant concerns such as security, confidentiality, and trust within 6G networks, outlining the standard technologies. It explains the 6G security framework, enhancements in 5G, and particular security difficulties encountered at both the physical and AI/machine learning (ML) layers.

After evaluating the safety developments in legacy wireless networks, important 6G application services, and safety standards, the inquiry concludes with a discussion of 6G network trust and solutions [9]. We look into how security affects hypothetical 6G systems, possible challenges, and ways to integrate privacy and security concerns in 6G networks. The authors describe the threat landscape, key performance indicators, and their vision for 6G security. Furthermore, the paper describes investigations and standardization efforts, addresses protection and security concerns in 6G technologies and applications, and supports technologies involving distributed record technology, physical level security, distributed AI/ML, visible light communication (VLC), and THz, quantum computing (QC). The paper took the initiative to standardize research projects to look at security and confidentiality issues in 6G technologies and applications.

With the advancement in 6G, privacy and security concerns become an important topic for research [24]. Blockchain technology has become a more secure and effective way to integrate with 6G networks. Blockchain technology is fruitful in 6G by specifying the safety measures required for encrypted communication and proposing an asynchronous agreement protocol based on directed acyclic graphs (DAG) for smooth integration. In addition to QC, we outline future research objectives and strategies for communication and storage optimization for this integration [19]. The present investigation examines 6G networks, emphasizing important aspects, enabling technologies, and technical developments. It explores the latest developments, possible uses, and AI's revolutionary role in upgrading 6G abilities, from wireless networks to smart cities and self-governing systems. The study explains deployment issues and thoroughly assesses 6G's future [5]. The authors of this paper examined new developments in xG security concerns (like 5G,

6G, etc.) brought on by important enabling technologies. They looked at ways to keep the network safe while meeting user needs, service requirements, and new services. The innovation of 6G technologies is the better way to reduce security risks enabling effective and safe interaction [26].

11.3 Stepwise Structure Framework of 6G Network

The steep growth to support upcoming technologies and applications is better than previous generations necessary to set up a stepwise structure framework on the multilayer framework [4, 7, 17–20, 26, 30, 35].

The 6G architectural framework is illustrated in Figure 11.1. The internal description of individual layers is described as follows:

A. Physical Layer (PHY)

- *Terahertz Communication*: 6G uses terahertz frequency slots for information transfer at very high speed.
- *Massive Multiple-Input Multiple Output (MIMO)*: Numerous antennae are used to increase signal strength and coverage.
- *Full Duplex Communication*: The same frequency bands for full-duplex communication enhance spectral efficiency.
- *Better Modulation and Coding*: Methods to increase dependability and data throughput.

B. Data Link Layer

- *Better Error Detection and Correction*: The 6G network uses better methods for dependable conveyance of information.
- *Robust Resource Distribution*: Implementing robust resource distribution methods into practice to meet user needs and obtain the most recent network circumstances.
- *Energy-efficient Protocols*: Efficient rules used to reduce power utilization while regulating performance.

C. Network Layer

- *Amalgamation of AI and ML*: It is used for intelligent routing, network administration, and optimization.
- *Enhanced Security Rules:* Quantum encryption methods and other enhanced security metrics to safeguard data integrity and confidentiality.
- *Network Slicing*: Constructing several virtual networks with distinct features for various services and applications.

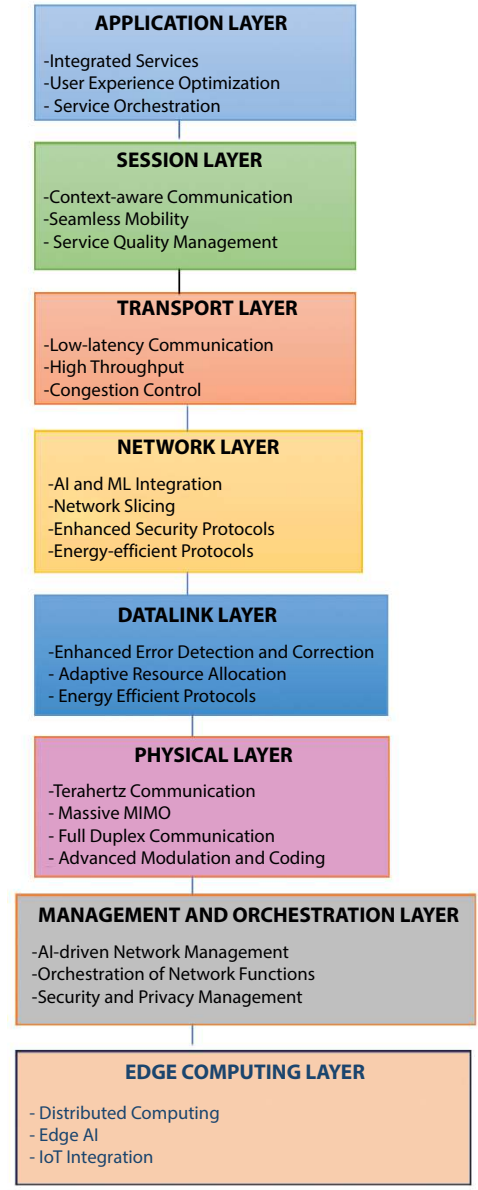

Figure 11.1 Layered framework of a sixth-generation network (6GN).

D. Transport Layer

- *Traffic Control:* Improved techniques for controlling network traffic and guaranteeing uninterrupted data transmission.
- *High Efficiency:* Able to handle extraordinarily high data speeds.
- *Low-Rate Communication:* The procedures and systems utilize extremely reliable and minimally delayed communication.

E. Session Layer

- *Circumstances-Aware Interaction:* Standards for session management that change according to the needs and context of applications.
- *Ensuring Unbroken Sessions*: When users travel across various network cells or regions.
- *Tracking and Regulating:* It helps to regulate the quality of services that satisfy various application requirements.

F. Application Layer

- *Consolidated Assistance:* Support for numerous applications including healthcare, smart cities, driverless cars, AR/VR, and the IoT.
- *Effective User Experience Optimization*: Tailored services and content according to the tastes and actions of the user.
- *Coordinating and Overseeing*: The provision of intricate services among several network tiers and slices.

G. Management and Orchestration Layer

- *Network Management Powered by AI:* Allows defect detection, network optimization, and predictive maintenance.
- *Network Function Structure*: Controlling and securing the smooth operation of virtualized network functions.
- *Privacy and Safety Management:* Putting in place thorough security procedures and guidelines to safeguard user information and the network.

H. Edge Computing Layer

- *Edge AI*: Using AI algorithms helps to make decisions more quickly and efficiently.
- *Distributed Computation*: To limit latency and better real-time processing, computation and data storage are placed close to the data point.
- *IoT Integration:* The effortless management and integration of IoT services and devices.

High performance, dependability, and security are guaranteed in 6G networks owing to the multi-layer architecture mentioned above, which is built to meet the many and exacting needs of future applications.

11.4 Key Technologies for 6G Networks

With a range of innovative technologies, the commencement of 6G connections is anticipated to transform telecommunications [1–4, 6, 8, 10–13, 15, 22, 25, 27–29, 31, 33]. Figure 11.2 lists the essential technologies anticipated to support 6G networks:

- ***Terahertz Communications:*** A frequency band of 0.1- to 10-THz transfers data in a wireless network at a very high speed and minimizes latency.
- ***Amalgamation of AI and ML:*** It will help optimize predictive upkeep, resource distribution, and network performance. By using intelligent information processing and decision-making, it enhances customer satisfaction.
- ***Massive MIMO:*** Many antennas are employed to increase signal intensity and capacity, improve spectral efficiency, and increase network dependability.
- ***Enhanced Network Slicing:*** The creation of many VPNs helps to provide on-demand services like the IoT, self-driving automobiles, and intelligent cities.

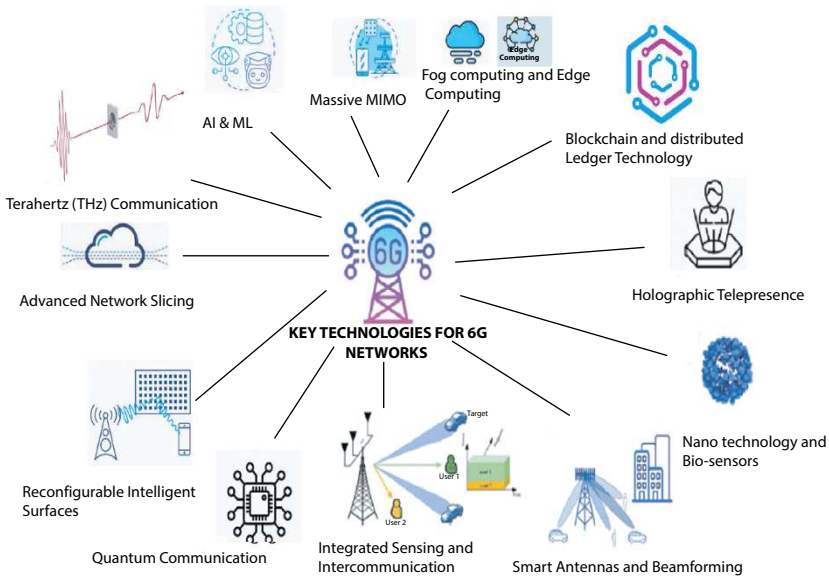

Figure 11.2 Essential technology for sixth-generation networks.

- ***Reconfigurable Intelligent Surfaces (RIS):*** By controlling electromagnetic waves with programmable surfaces, it enhances signal coverage and quality. Additionally, it improves spectrum and energy efficiency.
- ***Quantum Communication (QC):*** It is based on the theory of Quantum Mechanics (QM) to achieve highly secure communication. Advanced encryption and data security methods are used.
- ***Edge Computing and Fog Computing:*** Its functions are to process and store data close to the data source. It limits latency and network capacity consumption, and better real-time processing.
- ***Integrated Sensing and Intercommunication:*** It associates both characteristics such as communication and sensing to improve awareness of the network condition.
- ***Holographic Telepresence:*** Real-time holographic communication is made possible by holographic telepresence, boosting user immersion. It needs low latency and maximal data speeds to work properly.
- ***Blockchain and Distributed Record Technology:*** It facilitates safe and transparent network operations and improves security and trust.
- ***Nano-Technology and Bio-sensors:*** These two fields have been used in environmental monitoring and healthcare. They make it easier to create new devices and services.
- ***Intelligent Transmitters and Beamforming:*** These technologies accurately target communications where they are needed by using adaptable antennas. It lessens interference and boosts signal strength.

Multiple antennas are used in MIMO to increase signal strength and capacity, improve spectral efficiency, and increase network robustness [1, 4, 12, 31, 33, 34, 36].

11.5 Confidentiality Difficulties in Sixth-Generation Networks

As 6G networks advance, they provide unparalleled levels of speed, intelligence, and connectedness, but they also present serious privacy issues as shown in Figure 11.3 [3, 4, 16, 21, 23, 28, 29, 32]. It is essential to tackle these complexities to safeguard users' private data and uphold confidentiality in the 6G era.

- ***Enhanced Data Production and Acquisition:*** The endless information generated from smart devices and connected systems in these 6G networks is expected to dramatically increase the threat of privacy breaches. You have to make sure that you create solid data storage as well as privacy statistics in order not to allow an attack.
- ***Enhanced Location Tracking:*** Unlike 5G, in the era of 6G, location tracking in these networks will be more precise and granular, therefore enabling real-time material as well as human positioning. While it appears to support many advancements, this invention creates numerous privacy risks. Users' privacy gets harmed by illegal tracking, which

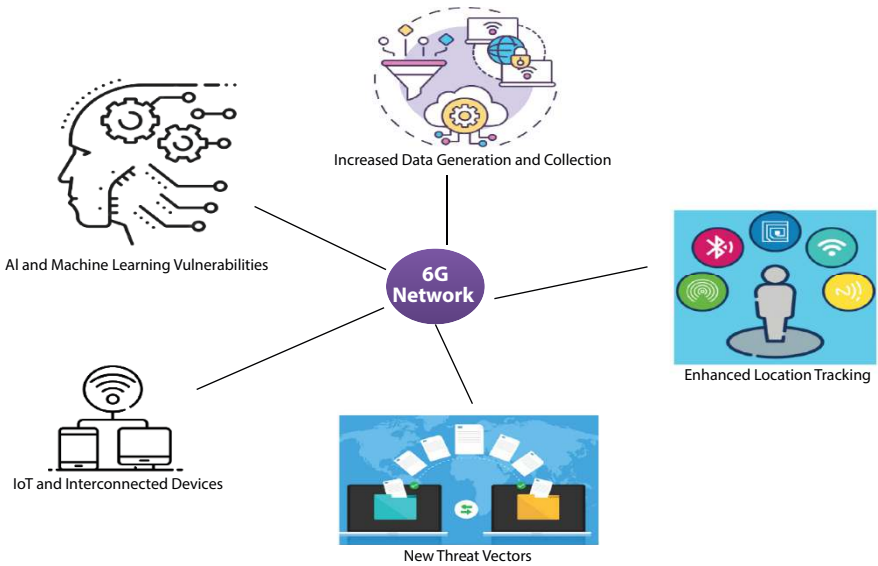

Figure 11.3 Confidentiality challenges in sixth-generation networks.

also facilitates unlawful monitoring and can even be abused by outside parties.

- ***Vulnerabilities in AI and ML:*** The efforts of combining AI and ML into 6G networks bring automation and intelligent decision-making capabilities. However, there are new concerns associated with this technology as well. The AI and ML systems use big data for analysis, and it is comprised of confidential and sensitive information.
- ***IoT and Interconnected Devices:*** IoT is a blessing for 6G networks that find application in various areas such as agriculture and health sector to industries. The increasing use of IoT poses data privacy threats. Protecting from these risks requires secure communication rules, efficient data encryption methods, and device authentication.
- ***Cross-Border Data Transfers:*** The attribute of seamless connectivity of 6G networks helps provide frequent cross-border data transfers. However, changing regulations for data protection pose data privacy challenges. It is important to implement a standardized privacy framework and policies for managing cross-border data transfers without any threat.
- ***New Threat Vectors:*** The use of QC introduces the threat to data privacy as it is capable of cracking conventional encryption methods. Long-term sensitive data is shielded *via* the use and deployment of quantum-resistant encryption methods.

11.6 Confidentiality Preserving Technologies and Methods

A variety of approaches, including differential confidentiality, homomorphic encryption, and decentralized framework, are included in the category of privacy-preserving technologies and strategies as illustrated in Figure 11.4 [2–4, 6, 21, 23, 28, 29, 32, 34].

- ***Differential Confidentiality:*** Differential confidentiality introduces random signals to data, so analysis results are not significantly affected by adding or removing a single data point. This prevents individual identification and preserves confidentiality while allowing valuable insights.

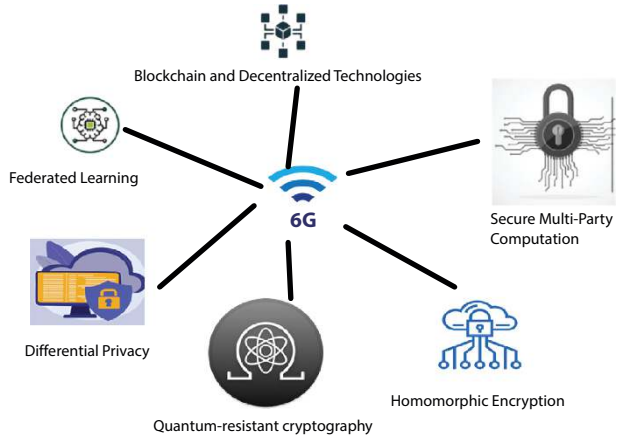

Figure 11.4 Confidentiality-preserving techniques in a sixth-generation network (6GN).

- ***Homomorphic Encryption:*** It allows the processing of encoded data except for decryption, ensuring confidentiality during processing. It is ideal for securely sharing data with external parties while preserving confidentiality. Various methods offer different levels of security and support for operations like addition and multiplication.
- ***Secure Multi-Party Computation (SMPC):*** SMPC allows one to calculate a function using their inputs by keeping the privacy of data.
- ***Federated Learning:*** Federated learning is used in various domains such as smart agriculture, healthcare, and mobile apps where the training of ML models on distributed equipment or servers with local data is performed while keeping the underlying data confidential and just disclosing model updates.
- ***Blockchain and Decentralized Technologies:*** When blockchain technology combined with cryptographic encryption methods, it offers perks including distributed, impermeable records to safeguard transactions and data transfers.
- ***Quantum-Resistant Cryptography*:** Encryption methods that are useful against the processing capability of quantum computers are used in quantum-resistant cryptography.

11.7 Ethics and Regulations in Practice

Following privacy regulations is important in 6G development to ensure user privacy, build trust, and reduce legal risks. Adherence to global privacy standards, the ethical deployment of AI, the provision of clear and transparent consent mechanisms, and the integration of privacy considerations from the outset are all essential for building trust and safeguarding user data in modern digital systems [4, 9, 11, 15, 25].

- ***Conformance to International Confidentiality Norms***
  With the motive to secure user data transparently and with rigorous usage obstacles, 6G networks must implement global privacy regulations. This lowers the potential for legal problems, safeguards user privacy, and promotes assurance.
- ***Ethics in AI and Data Handling***
  AI techniques employ legal measures, such as guaranteeing AI accountability, transparency, and equity and restricting the improper use of user data for illicit purposes.
- ***User Permission and Openness***
  User permission plays a critical role in maintaining privacy in 6G networks. Individuals require clear-cut information on how to procure data, manipulate it, and share it with others, by taking explicit consent for these processes. Openness data strategies build trust and enable users to use and share their personal information without fear.
- ***Privacy Integrated Design Strategies***
  Privacy-integrated technologies use various methods to protect user data. Employing regulatory and ethical principles, 6G networks will realize the following key benefits: enhanced user privacy; responsible data practices to ensure ethics in AI implementation; and uncompromised security levels complying with global standards bridging trust into a digital environment.

11.8 Novel Solutions for User Confidentiality

Ensuring strong individual security has become an urgent concern in the current era of fast-evolving digital connectedness. This paper highlights unique solutions to safeguard user confidentiality in various online platforms using AI-assisted technologies [4, 6, 11, 18, 20].

- ***Artificial Intelligence-Assisted Protection Tools***
  It improves the security and confidentiality of sensitive data identifying and reducing privacy threats. However, dynamic privacy helps to safeguard critical data.
- ***Agile Consent Management Frameworks***
  Agile consent management framework allows participants to grant and monitor permissions for large data processing tasks in real-time, offering transparent and flexible data control. Users can easily adjust preferences or withdraw consent, ensuring active participation and following confidentiality laws.
- ***Anonymization and Data Masking Methods***
  Falsification helps to identify information with false names under strict circumstances. The chance of risk associated with the privacy of individual data can be eliminated by eliminating the known information.
- ***Platforms to Share Data Safely***
  Safe sharing platforms enable creativity and collaboration by providing protected ways to share data without compromising privacy.
- ***Identity Management Systems for Enhancing Privacy***
  Identity management systems' advanced cryptographic algorithms and decentralized methods provide a safer path to preserve a digital repository to safeguard individual data. By maintaining a limit on data and limitations on user controls, these systems reduce the prospect of fraud and loss of identity.

In 6G networks, the aforementioned creative techniques can significantly increase user privacy in maintaining data security while permitting cutting-edge connectivity and services.

11.9 Conclusion

6G networks, new technologies, and privacy-preserving methods are needed to handle new threats and protect user confidentiality. Strict ordinances, industry standards, and cooperation between companies, researchers, and legislatures are important in addition to technical remedies. As 6G develops, privacy must be given higher priority, embedding security into the creation and application of technology.

References

1. Adhikary, A., Munir, M.S., Raha, A.D., Qiao, Y., Hong, S.H., Huh, E.-N., Hong, C.S., An artificial intelligence framework for holographic beamforming: coexistence of holographic MIMO and intelligent omni-surface. *2023 International Conference on Information Networking (ICOIN)*, IEEE, Bangkok, Thailand, pp. 19–24, doi:10.1109/ICOIN56518.2023.10048994.
2. Akbar, M.A., Khan, A.A., Hyrynsalmi, S., J.A., 6G secure quantum communication: a success probability prediction model. *Autom. Software Eng.*, 31, 1–40, 2024, doi: 10.1007/s10515-024-00427-y.
3. Anantrasirichai, N. and Bull, D., Artificial intelligence in the creative industries: review. *Artif. Intell. Rev.*, 55, 589–656, 2022, doi: 10.1007/s10462-021-10039-7.
4. Chowdhury, M.Z., Shahjalal, M., Ahmed, S., Jang, Y.M., 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions. *IEEE Open J. Commun. Soc.*, 1, 957–975, 2020, doi: 10.1109/OJCOMS.2020.3010270.
5. Chataut, R., Nankya, M., Akl, R., 6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges. *Sensors*, 24, 1888, 2024, doi: 10.3390/s24061 888.
6. Dangi, R., Choudhary, G., Dragoni, N., Lalwani, P., Khare, U., Kundu, S., 6G Mobile Networks: Key Technologies, Directions, and Advances. *Telecom*, 4, 836–876, 2023, doi: 10.3390/telecom4040037.
7. Domingo-Ferrer, J. and Blanco-Justicia, A., Privacy-Preserving Technologies, in: *The Ethics of Cybersecurity*, pp. 279–297, 2020, doi:10.1007/978-3-030-29053-5_14.
8. Farhad, A. and Pyun, J.-Y., Terahertz meets AI: the state-of-the-art. *Sensors*, 23, 11, 1–25, 2023, doi: 10.3390/s23115034.
9. Hakeem, S.A.A., Hussein, H.H., Kim, H., Security Requirements and Challenges of 6G Technologies and Applications. *Sens. (Basel)*, 22, 5, 1969, 2022a, doi: 10.3390/s22051969.
10. Hakeem, S.A.A., Hussein, H.H., Kim, H.-W., Vision and research directions of 6G technologies and applications. *J. King Saud Univ. Comput. Inf. Sci.*, 34, 6A, 2419–2442, 2022b, doi: 10.1016/j.jksuci.2022.03.019.
11. Hall, J., Jornet, J.M., Thawdar, N., Melodia, T., Restuccia, F., Deep learning at the physical layer for adaptive terahertz communications. *IEEE Trans. Terahertz Sci. Technol.*, 13, 2, 102–112, 2023, doi: 10.1109/tthz.2023.3237697.
12. Huang, Y., Zhu, Y., Qiao, X., Su, X., Dustdar, S., Zhang, P., Toward holographic video communications: a promising AI-driven solution. *IEEE Commun. Mag.*, 60, 11, 82–88, 2022, doi: 10.1109/mcom.001.220021.
13. Ji, B., Han, Y., Shuwen, L., Tao, F., Zhang, G., Fu, Z., Li, C., Several Key Technologies for 6G: Challenges and Opportunities. *IEEE Commun. Stand. Mag.*, 5, 2, 44–51, 2021, doi: 10.1109/MCOMSTD.001.2000038.

14. Kazmi, S.H.A., Hassan, R., Qamar, F., Nisar, K., Ibrahim, A.A.A., Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques, and Research Directions. *Symmetry*, 15, 1147, 2023, doi: 10.3390/sym15061147.
15. Kim, N., Kim, G., Shim, S., Jang, S., Song, J., Lee, B., Key Technologies for 6G-Enabled Smart Sustainable City. *Electronics*, 13, 268, 2024, doi: 10.3390/electronics13020268.
16. Kohli, P., Sharma, S., Matta, P., Secured Privacy Preserving Techniques Analysis of 6G Driven Vehicular Communication Network in Industry 5.0 Internet-of-Everything (IoE) Applications. *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, pp. 1–8, 2022, doi:10.1109/SMARTGENCON56628.2022.10084289.
17. Kumar, R., Gupta, S.K., Wang, H.-C., Kumari, C.S., Korlam, S.S.V.P., From Efficiency to Sustainability: Exploring the Potential of 6G for a Greener Future. *Sustainability*, 15, 16387, 2023, doi: 10.3390/su152316387.
18. Li, H., Li, S., Min, G., Lightweight privacy-preserving predictive maintenance in 6G enabled IOT. *J. Ind. Inf. Integr.*, 39, 100548, 2024, doi: 10.1016/j.jii.2023.100548.
19. Liu, Y., Peng, S., Zhang, M., Shi, S., Fu, J., Towards secure and efficient integration of blockchain and 6G network. *PLoS One*, 19, 4, e0302052, 2024, doi: 10.1371/journal.pone.0302052.
20. Mao, B., Liu, J., Wu, Y., Kato, N., Security and Privacy on 6G Network Edge: A Survey. *IEEE Commun. Surv. Tutor.*, 25, 2, 1095–1127, Secondquarter 2023, doi: 10.1109/COMST.2023.3244674.
21. Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., Lin, Y.-D., Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.*, 23, 4, 2384–2428, Fourthquarter 2021, doi: 10.1109/COMST.2021.3108618.
22. Ning, B., Tian, Z., Mei, W., Chen, Z., Li, C., Han, S., Yuan, J., Zhang, R., Beamforming technologies for ultra-massive MIMO in terahertz communications. *IEEE Open J. Commun. Soc.*, 4, 614–658, 2023, doi: 10.1109/ojcoms.2023.3245669.
23. Peng, T., Gong, B., Zhang, J., Towards Privacy Preserving in 6G Networks: Verifiable Searchable Symmetric Encryption Based on Blockchain. *Appl. Sci.*, 13, 10151, 2023, doi: 10.3390/app131810151.
24. Porambage, P., Gür, G., Osorio, D.P.M., Liyanage, M., Gurtov, A., Ylianttila, M., The roadmap to 6G Security and Privacy. *IEEE Open J. Commun. Soc.*, 2, 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.
25. Puspitasari, A.A., An, T.T., Alsharif, M.H., Lee, B.M., Emerging Technologies for 6G Communication Networks: Machine Learning Approaches. *Sens. (Basel)*, 23, 18, 7709, 2023, doi: 10.3390/s23187709.

26. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-Based wireless sensor network, in: *Software-Defined Network Frameworks,* pp. 121–141, CRC Press eBooks, 2024, https://doi.org/10.1201/9781003432869-8.
27. Shafie, A., Yang, N., Han, C., Jornet, J.M., Juntti, M., Kurner, T., Terahertz communications for 6G and beyond wireless networks: challenges, key advancements, and opportunities. *IEEE Netw.*, 37, 3, 162–169, 2023, doi: 10.1109/mnet.118.2200057.
28. Singh, S.K. and Park, J.H., TaLWaR: blockchain-based trust management scheme for smart enterprises with augmented intelligence. *IEEE Trans. Ind. Inf.*, 19, 1, 626–634, 2022a, doi: 10.1109/TII.2022.3204692.
29. Singh, S.K., Park, L., Park, J.H., Blockchain-based Federated Approach for Privacy-Preserved IoT-enabled Smart Vehicular Networks, in: *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, pp. 1995–1999, 2022b.
30. Srivastava, V., Mahara, T., Yadav, P., An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks. *Int. J. Cognit. Comput. Eng.*, 2, 171–179, 2021, doi: 10.1016/j.ijcce.2021.10.002.
31. Sun, Y., Peng, M., Zhang, S., Lin, G., Zhang, P., Integrated satellite-terrestrial networks: architectures, key techniques, and experimental progress. *IEEE Netw.*, 36, 6, 191–198, 2022, doi: 10.1109/mnet.106.2100622.
32. Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., Zhou, W., Security and privacy in 6G networks: new areas and new challenges. *Digit. Commun. Netw.*, 6, 3, 281–291, 2020, doi: 10.1016/j.dcan.2020.07.003.
33. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in computer and information science*, vol. pp, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
34. Wu, M., Cheng, G., Li, P., Yu, R., Wu, Y., Pan, M., Lu, R., Split learning with differential privacy for integrated terrestrial and non-terrestrial networks. *IEEE Wirel. Commun.*, 31, 3, 1–8, 2024, doi: 10.1109/mwc.015.2200462.
35. Zainuddin, A.A., Omar, N.F., Zakaria, N.N., Mbourou, C.N.A., Privacy-Preserving Techniques for IoT Data in 6G Networks with Blockchain Integration: A Review. *Int. J. Perceptive Cognit. Comput.*, 9, 2, 80–92, 2023, doi: 10.31436/ijpcc.v9i2.40.
36. Zhu, X. and Jiang, C., Creating efficient integrated satellite-terrestrial networks in the 6G era. *IEEE Wirel. Commun.*, 29, 4, 154–160, 2022, doi: 10.1109/mwc.011.2100643.

12

Analytic Study on Existing Communication Technologies for Smart Grid: Beyond the 5G and Extension Toward 6G

Mukta Jukaria[1]*, Sushil Kumar Singh[2] and Richa Pandey[1]

[1]Department of Computer Science and Engineering, Graphic Era Hill University, Haldwani, India
[2]Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India

Abstract

In recent scenario where every system needs to be smart, there are several downsides in our old power grid. This paper is looking forward to converting our old existing power grid into a smarter, automated, interactive, and communication-based power grid. Among the several elements, the smart meter is the most important component of smart grid having capability of performing various functions and integrating generation of distributed power (like solar power and wind power). Smart grid concept is gaining constant speedy responsiveness worldwide because of automated billing process, real-time monitoring, and energy management that requires a good communication infrastructure. In this research paper, we will discuss and analyze the status of existing communication technologies and the requirement of advancement for imminent Indian power sector with the extensive study of conditions of smart grid/meter along with intelligent communication infrastructure supporting fifth-generation and sixth-generation (6G) communication infrastructure. The paper will also provide a comprehensive investigation of the 6G network and fundamental security and privacy problems related to 6G communication technologies.

***Keywords*:** Intelligent energy networks (IENs), advanced metering infrastructure (AMI), Li-Fi, LoRa, 6G, centimeter wave (cmWave), sub-terahertz (sub-THz), mmWave

**Corresponding author*: muktajukaria@gehu.ac.in

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (263–286) © 2026 Scrivener Publishing LLC

12.1 Introduction

The power grid of any country is one of the important factors, which plays a very important role in the economic development of the nation. Nowadays, every developed and developing country is looking forward in the direction of implementing new era power grid equipped with bidirectional information and power flow capabilities, as old conventional power grid is only one directional and not very suitable to fulfill the future

Table 12.1 Key features of smart grid.

S. no.	Characteristics	Conventional grid	Smart grid
1.	Digital technology based	X	✓
2.	Bidirectional	X	✓
3.	Real-time monitoring/self-monitoring	X	✓
4.	Pervasive power flow control	X	✓
5.	Centralized and decentralized power generation	X	✓
6.	Self-healing capability	X	✓
7.	Remote monitoring, operation, and management	X	✓
8.	Pan-regional control system	X	✓
9.	Motivated active consumers.	X	✓
10.	Power quality for 21st century needs	X	✓
11.	Micro generation accommodation	X	✓
12.	Enables markets	X	✓
13.	Optimizes assets and operates efficiently	X	✓
14.	Emergency recovery	X	✓
15.	Smart price information	X	✓
16.	Customer choice optional function	X	✓
17.	Integration of AC-DC microgrids	X	✓

growing electric demand. The implementation of smart grid is one of the most inventing topics of research world widely because conventional grid is simple and simply involves generation, transmission, and distribution process of power in one direction from utility to consumer, but smart grid is a fully automated, smart, and very efficient system that comprises involvement of bidirectional flow of power as well as information from both utility and consumer side. Integration of various microgrids is also an important aspect of the smart grid. In short, our typical grid consists of 35 power generators, transmission lines/substations, distribution lines/substations, and various types of machinery and loads that supply only energy to customers daily [1], whereas smart grid is a modern power grid in which every element, appliances, devices, and even consumers are smart, intelligent, and much more efficient that supply energy as well as information to both utility and consumer [2]. Although there are enormous advantages/characteristics of smart grid over conventional grid, some of the key feature comparisons are shown in Table 12.1.

12.1.1 Component of Smart Grid

Nowadays, for any country, transforming an old electrical power grid into a progressive digital infrastructure-based energy grid with bidirectional flow capabilities for information exchange and equipment control is crucial. Intelligently using large number of sensors and integrating distributed energy resources are small-scale power-generating and storage solutions, ranging from 3 to 10,000 kW. The development of this information and communication system will be important for the reliability, efficiency, transmission and distribution (T&D) losses, security, and overall performance of the new smart grid infrastructure [5]. It is a big challenge and important topic of research for a couple of scientists and researchers all around the world to analyze and suggest an implementation possibility for the different components of a smart grid that integrate all the supplies. Advanced metering infrastructure (AMI) is the most important fragment of smart grid and consists of a massive number of sensors, various intelligent sensing and measuring devices, and advanced controllers with a good security arrangement [6]. Smart grids offer two-way communication between utilities and electrical consumers by incorporating crucial components such as smart meters, smart appliances, and smart measurement equipment into their premises, which are referred to as home area networks (HANs) [2]. Most of the conventional power grids based on the technology of 1970s look ill-suited for 21st century generation power

grid requirements, but modern/advanced grids require different areas that strappingly need to be explore, review, study, and identify the implementation possibility in the following areas:

- Automation and control system
- Asset management system
- Condition monitoring device
- Distribution management system and energy management system
- Decision support system and system integrity protection
- Power monitoring system
- Smart generation and consumption
- Smart meter and smart homes
- Building automation and control systems
- Substation automation and protection
- Information and communication technologies
- Microgrid generation
- Security system

All the above fields require expansion to perform various purposes so that its stability, reliability, efficiency, and security will increases and eventually accomplish to get more efficient advanced power grid in place of existing grid to make it 21st century new era power/energy grid. In this paper, we will explore and discuss the advancement requirement on a versatile concept called AMI consist of a very important device call smart meters whose analysis specially focused on information and communication technologies because integration of communication is a very vital, superior, and dynamic part of smart grid that will provide entryway for utility and consumers. The role of smart meters in order to encounter the customer's demands of energy consumption management through real-time monitoring and control is needed among smart meters and customer's equipment and appliances. A good communication infrastructure can communicate along different networks such as HAN, neighbor area network (NAN), and wide area network (WAN).

12.1.2 Advanced Metering Infrastructure (AMI)

The heart of smart grid is AMI, responsible for measuring and collecting data for analysis and transporting of energy *via* communication means among the metering devices. One of the four essential components of an

AMI is a smart meter with two-way communication capability for receiving and collecting data at exact time intervals for measuring, recording, displaying, and charging. The second component is an efficient communication medium/network that provides a home gateway to different networks to allow the dedicated data transmission among utility, meters, and consumers [7]. The third important components of AMI system is meter data acquisition system (MDAS), a software application used to obtain data from various meters using communication network, and the fourth element is meter data management system that receives, stores, and analyzes the data provided by MDAS.

Smart Meter: Existing AMR (automated meter reading) system utilized one-way communication for billing purpose, but, now, this is the time to replace it with a smart version having two-way communication based on fifth-generation (5G) communication technologies having capability enabling smart use of energy along with several functions from both consumer and customer. Smart meter systems are intelligent, automated electronic measurement radio devices that measure energy uses at different time intervals and communicate it *via* some communication media combined with two-way communication technology commonly acknowledged as AMI being deployed throughout the countries to improve the metering system activities by integrating the participation of both utility and customer. Smart meter is a very essential part of an overall smart power system that specifically requires an advanced and efficient wired (PLC/optical wire) and wireless communication (radio/microwave) infrastructure to monitor, control, and manage energy uses. It also supports time of use (TOU), critical peak pricing, and real-time pricing rate metering for demand response, which is based on smart grid standards from the ITU (International Telecommunication Union), IEC (International Electro technical Commission), IEEE (Institute of Electrical and Electronics Engineers), ETSI (European Telecommunication Standards), and CENELEC (European Committee for Electro technical Standardizations) for various networks [4]. A typical smart home area having dozens of individual home appliances such as washing machines, dishwashers, smart clocks, refrigerator, and smart printer needs a different communication technologies to send and receive information's *via* smart meters, whereas a NAN or WAN requires different communication technologies among smart meters (collector meters) to communicate information [6, 7]. Considering the 21st century, every home, hospitals, industries, institutes, and offices have a new wireless meter. This paper includes the use of different types of communication technologies for different types of networks and seeking future requirements or crucial needs to implementation and possibilities of integration

of new communication technologies. Although the deployment and use of smart meters started over more than last 15 years under the national system of standards like but the concept of smart grid joints partnership of both meters and communication technologies carry the top notch system available in the market today. Before installing and deploying smart meters, these devices must meet a few national standards, including American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), National Electrical Code (NEC), National Electrical Manufacturers Association (NEMA), Underwriters Laboratories (UL), National Electrical Safety Code (NESC), Federal Communications Commission (FCC), as well as state and municipal technical rules to assure correct functionality. Before we analyze and discuss different communication technologies, Figure 12.2 will give an idea about different networks and appropriate communication technologies for these networks within a power network.

12.1.3 Status of Smart Grid or Smart Meter in India

During 2010, the "India Smart Grid Task Force (ISGTF)," an inter-governmental body comprised of various government departments, initiated the implementation of smart grid, and the Ministry of Power (MOP) dealt with smart grid activities. The primary functions of the ISGTF are to raise awareness and integration of various activities, as well as to promote practices and services for R&D collaboration on an interoperability framework. In August 2013, the India Smart Grid Forum (ISGF) recommended the government on a potential smart grid implementation in the country, emphasizing the necessity of smart grid technology in the Indian power sector. In 2010, the MOP constituted the ISGF as an inter-ministerial task force having major objective of developing smart grid technologies in Indian power sector. National Smart Grid Mission is a government institutional system established in March 2015 for the planning, monitoring, and implementation of smart grid policies and programs, with an initial estimate of 980 Corers (Cr.) and budgetary support of ₹ 338 Cr during phase 1 (2014–2017). Throughout phase 2 from 2017 to 2020 [8], the Smart Grid Roadmap objectives are to enable access and availability of quality power, loss reduction, renewable integration, electric vehicles, and energy storage in smart projects and smart cities with an expected investment of ₹ 990 Cr., including budgetary support of ₹ 312 Cr. In conjunction with the United States Agency for International Development (USAID), the MOP and the Government of India (GOI) devised and conducted a nation-wide distribution reform training program. The primary goal of this program is to exhibit excellent commercial and technological practices that increase supply quality and power reliability in the country's urban and rural areas.

The Restructured Accelerated Power Development and Reforms Programme (R-APDRP) began in July 2008 as a 5-year plan focusing on actual demonstrable performance in terms of AT&C sustained loss reduction of 3% per year at the utility level and proposed covering urban areas with a population of more than 30,000 people. R-APDRP was established by the MOP and the GOI. Several government initiatives and regulations, including the R-APDRP and Central Electricity Authority recommendations, have addressed the country's intelligent smart metering mode. UDAY is a DISCOMS operational and financial turnaround project that is expected to install 35 million smart meters by 2019.

12.2 Generations of Communication Infrastructure

As discussed above, smart meters along with communication technologies make AMI concept complete so the best choice of communication technologies is a main task of a superlative communication infrastructure. Nowadays, numerous technologies have been proposed, developed, and deployed to enable this communication, with both wired and wireless options available having pros and cons for each. The deployments of smart meters within HAN is a major concept to manage smart home energy use, and investigating the best choice of communication technologies is a major task for the researchers as, over the during next few years, a very huge number of smart meters are expected to be deployed world widely. The success of smart metering infrastructure depends on efficient and reliable wired and wireless communication technology, although several types of communication technologies are available to get connectivity among different types of networks and topology such as HAN and other long range back haul networks (NAN and WAN) having their own advantages and limitations. In following section, we are going to discuss an overview of existing communication technologies used among smart meters and further discuss and recommend some suitable forthcoming communication technologies based on the concept of different communication environments and locations.

As foreseen, there are different generations of communication technologies; nowadays, 5G communication technologies are very popular in smart grid (SG) and include radio spectrum of sub–6 GHz and millimeter-wave (mmWave) bands. In recent decade, sixth generation (6G) is captivating large interest for more accurate and powerful radio sub-terahertz (sub-THz) and centimeter wave (cmWave), which we will discuss detailed further in upcoming sections.

12.3 Background of Existing Wireless Technologies

12.3.1 Zigbee

Zigbee is most popular unlicensed wireless communication technology that connects the widest range of devices in smart metering system within HANs used to transmit command and data between devices as a smart energy solution having self-healing networking capability, ensuring robust communication. A HAN is the computerization and automation of a small office/home office that connects digital devices within the house or office such as telephones, fax machines, televisions, computers, home security systems, video games, printers, scanners, and smart appliances. HAN is primarily used for demand-side management and is made up of four components: a gateway that connects the HAN to the NAN or WAN; an access point; a network operating system; and smart meters and appliances.

HAN technology provides the remote connection and control of a large number of interconnected digital devices within a networked region. Zigbee is a low-power, low-data-rate (20–250 Kbps) and short-range (approximately 10 m) communication system that operates on the IEEE802.15.4 standard at a frequency of 2.4 GHz, 868 MHz, and 928 MHz to facilitate the communication an interoperability among the digital devices. Zigbee has been recognized suitable for point-to-point or star-type network topology to provide correct measures of energy usage, log data real time, and TOU values between smart meter and appliances through Zigbee such as washer, dryers, washing machine, AC, water heater, and PC, but not found suitable for mesh-type communication network.

12.3.2 Wireless Mesh Network/Wireless Local Area Network (WMN/WLAN)

Mesh networks are critical enabling technologies for the deployment of dependable large-scale AMI networks, which are comprised of several wireless access points, mainly Wi-Fi and Wi-Max routers, to their clients, which include laptops, smartphones, RFID, smart meters, and sensors. Mesh networks are used to create a fully wireless communication network that serves both mobile and stationary users by connecting HANs and NANs that are plugged into a network gateway to access and connect to a utility's WAN. Wireless mesh accounts for around 96% of current smart grid network deployments, with an estimated 100 million households and billions of devices embedded with the grid.

12.3.3 Wi-Fi (Wireless Fidelity)

Wi-Fi communication technology IEEE 802.11 standard for wireless environment implements a variety of smart grid applications by effectively providing link between the smart meter network, utility, and smart device such as desktop, laptop, smart phones, video game, and smart appliances using 2.4-GHz and 5.8-GHz band especially useful for HAN and NAN.

12.3.4 Worldwide Interoperability for Microwave Access (Wi-Max)

Wi-Max is very attractive 802.16 IEEE standard 4G alliance technology for the AMI, providing meter-to-meter or M2M (machine-to-machine) communication platform for NAN and WAN. This communication technology can operate on a variety of frequency bands, depending on the speed and distance from whence the SG is located. In addition, 3.65 GHz and 5.8 GHz (unlicensed frequency) are utilized for fixed users, whereas 2.3 GHz, 2.5 GHz, 3.3 GHz, and 3.5 GHz are used for mobile users, with data rates up to 75 Mbps and a coverage radius of around 48 km. Wi-Max technology allows for multiple device connections, and its versatility allows for a wide range of devices to be compatible in a variety of environments, as well as distant connectivity to various types of smart devices between nodes. Wi-Max has the potential to be a major rival in AMI communication for distribution and monitoring.

12.3.5 Bluetooth

Bluetooth IEEE 802.15.1 is an open wireless technology that was developed to replace RS232 data wires connecting electronic equipment for exchanging data over short distances from fixed and mobile users.

Bluetooth operates in the unlicensed ISM band of 2.4 GHz as same range of Zigbee and Wi-Fi. Initially, there are some certain limitations of this wireless technology like short distance, interference, limitation to human interface devices, or audio headset with other frequencies, but to fulfill the requirements of smart grid environment, now, Bluetooth 5 is a potential use case in the smart grid space, which enables longer distance and high-speed communication by maintaining low power and better noise immunity. The presence of Bluetooth 5 could be a good link for smart meters to smart devices relationship including many new applications that will allow to track, monitor, and manage their energy on utility scale.

12.3.6 3G/4G Cellular

For the previous 20 years, the third generation (3G) of cellular network has been in use for wireless mobile telecommunications technology of data services, providing better internet speed than 2G and 2.5G GPRS networks greater than 3.1 Mbps and average speed range between 0.5 Mbps and 1.5 Mbps. The 3G network operates on a frequency band ranging from 1.8 GHz to 2.5 GHz, with an upload rate of 5 Mbps. 3G networks meet the IMT-2000 requirements for voice telephony, video calls and conferencing, and web access. Due to dedicated infrastructure, cellular systems have low time, solid security, cheap maintenance cost, wider coverage, and faster data speed.

4G Long Term Evolution (LTE) is the most recent type of broadband cellular network technology, with average ranges of 300 Mbps and upload speed of 75.4 Mbps. A 4G system must meet ITU-defined capabilities in IMT Advanced, with an operating frequency band of 2 GHz to 8 GHz and an upload rate of 500 Mbps. Currently, the download speed of LTE Advanced is up to 3.3 Gbps, with two primary applications in smart grids regulating and automating distribution systems and smart meters. 4G applications include a wide range of applications such as mobile online access, IP telephony, mobile video conferencing, gaming, HDTV, and 3D TV.

12.3.7 Z-Wave

A small range communication protocol useful for HAN is basically used for mesh type network for home automation up to 232 of nodes. Its data rate is about 100 Kbps within the range of 30 m. It uses low energy radio waves for M2M communication for home or office automation and can be controlled using smart phones.

12.4 Wired Communication Technology

12.4.1 Power Line Carriers (PLCs)

Power line communication or power line carrier (PLC) or power line digital subscriber line is well established and most widely used wired communication technology for data and power transmission especially used broadband networks or applications of smart grid applications like AMR/AMI because of low cost, reliability, and interference insensitivity.

There are many types of PLC systems, operating at a wide variety of frequencies. Power line technologies (PLCs) can be basically categorized into narrowband PLC (NB-PLC) and broadband PLC (BB-PLC) operating in different bandwidths. NB-PLC usually operates below 500 kHz in both low- and high-voltage transmission lines with bandwidth of up to 10 Kbps covering more than 150 km, whereas BB-PLC usually operates at frequency range of 2 MHz to 30 MHz (in some cases, 50 Hz even more), with bandwidth of up to 200 Mbps covering up to 1.5 km. PLCs are used to bring internet services to homes and smart meters at low operating and maintenance cost as already constructed wide communication infrastructure for NAN, WAN, HAN, and small-scale EMI structure (BB-PLC).

12.4.2 Digital Subscriber Line (DSL)

Digital subscriber line (DSL) is already constructed and widely distributed wire line technology for communicating great bandwidth information to home areas and minor businesses above copper wire telecommunication lines, aiming high speed internet transmission to the future smart grid applications. This technology shares network and telephone service at the same phone line without disrupting either your voice or network connections. DSL technology provides variety of DSL, such as ADSL (asymmetric DSL), SDSL (symmetric DSL), high-bit-rate digital subscriber line (HDSL), and rate-adaptive digital subscriber line (RADSL). The basic broadband DSL supports data downloading between 1.544 Mbps and 8.448 Mbps with the operating frequency band between 2 MHz and 30 MHz depending on the quality of line wire. SDSL preserves equal data rates for both uploads and downloads useful for business applications that need bulk amount of outgoing traffic, whereas ADSL are most used DSL technology that offers higher download speed than upload speed and is more useful for household applications up to 5 km or more in advanced versions covering NAN and HAN. Apart from the limitations noted above, DSL has the disadvantage of only working over a limited physical distance and being unavailable in regions where the local telephone infrastructure does not support this technology.

12.4.3 Optical Fiber

Fiber optic–based wired network can establish a more robust smart power grid opportunity by providing a communicating medium or infrastructure enabling very high-speed communications between smart devices

and power providers across the country. Initially, fiber optic–based smart grid project focus to interconnect substations and offices covering WAN to fulfil huge capacity, bandwidth, and countless benefits for collection and distribution of power system information and data in virtual real time. Upload speed and download speed of up to 1 Gbps are possible with fiber optic internet, which is more than 100 times quicker than existing internet. Several telecom firms, including Cisco, Alcatel-Lucent Verizon, and Tellabs ADVA Optical Networking, have promised and built fiber-to-the-home networks to promote economic prosperity in their regions by giving jobs and high-speed connections for industry and businesses. Electric power board, Chattanooga, TN, is one of America's largest publicly owned electric power provider company and teamed up with Tantalus to build a fiber-connected smart meter and applied for $111 million from the Department of Energy for a $226 million total project to extend the fiber network.

12.5 5G Technologies for Smart Grid

12.5.1 Sub-GHz

In a marketplace, Zigbee technology is extensively used in daily lives, especially popular in HAN, but, in a growing market, sub-GHz (sub–1 GHz) technology is a principal alternative for Zigbee technology used in smart grid, having further advantage of long range of kilometer with advantage of small power consumption. Several recent communication technologies targeted smart meter and recently proposed sub-GHz (sub–1 GHz) frequency bands of 433 MHz and 868/915 MHz.

There are numerous advantages to using sub-GHz wireless systems over 2.4-GHz technology for next-generation applications. For example, sub-GHz can operate unaided on battery power for 20 years, whereas a 2.4-GHz signal deteriorates or attenuates faster because as the frequency increases, so does the attenuation rate. One more advantage is that 2.4-GHz radio signals fade quickly in comparison to the sub-GHz signals because of the reflection of opaque surfaces, spatially in extremely congested situations. Sub-GHz signals are more suitable for urban environment because they propagate well than 2.4-GHz signals; being "bending property" around large structures, they are less prone to interference, and they are compatible to IEEE 802.15.4 [9]. Depending on network requirements, both 2.4-GHz and sub-GHz technologies are most widely employed in daily life,

although integrated circuit (IC) developed sub-GHz transreceivers. The EZ Radio and EZ Radio PRO from Silicon Labs are suited for power-sensitive and battery-powered applications. Because of the Friis formula for route loss, sub-GHz transmissions can travel longer distances for a given output power.

$$\mathrm{Pr} = PtGtGr\left(\frac{\lambda}{4\pi R}\right)^2$$

where Pr is the received power; Pt is the transmitted power; Gt and Gr are the transmitter and receiver antenna gains, respectively; R is the distance between antennas; and λ is the wavelength.

Several sub–1 GHz bands have been identified for new services such as low-cost internet deployments, and smart metering. Allotted licensed band in US for sub–1 GHz is 698 MHz to 806 MHz; in Europe 790 MHz to 862 MHz and 550 MHz to 606 MHz; and in India 585 MHz to 698 MHz and 698 MHz to 806 MHz. In December 2010, sub-GHz spectrum allocation in India is 890 MHz to 960 MHz for cellular services; 368 MHz to 380 MHz for fixed mobile band, 470 MHz to 520 MHz and 520 MHz to 585 MHz for fixed and mobile services, respectively; and 585 MHz to 806 MHz for broad casting services, which include mobile, TV, and smart meters. Sub-GHz technology is currently used in industrial automation, AMI and AMR, meter monitoring, home comfort, home healthcare, centralized building management, and other applications.

12.5.2 LoRa

Currently, all Zigbee devices are not capable of communicating to all other devices because of range, battery, and performance limitations. LoRa (long-range radio), a new transmission standard, is a game-changer and fastest growing technology similar to Zigbee for distributed devices and gateways, having the ability to handle millions of node and supporting smart metering applications with long battery life in excess of 10 years in the sub-GHz spectrum (ISM, 169 MHz and 433 MHZ; in North America, 866 MHz and 915 MHz; data rates in Europe range from 0.3 Kbps to 50 Kbps). LoRa standard IEEE 802.15.4g is a low-power, long-range communication protocol developed by Semtech company enabling M2M and Internet-of-Things (IoT) device communication possible up 2 to 5 km for urban and up to 15-km line of sight for suburban areas. LoRa corporation associates low-power WAN (LPWAN) extremely long-range and low-power wireless communication for IoT/M2M applications and has introduced various

Table 12.2 Parameters of different communication technology till 6G.

Type of technology	Name of technology	Operating frequency	Data rate	Range	Standard	SG field application
Wireless technology	Zigbee	2.4 GHz	20–250 Kbps	10 m	IEEE802.15.4	HAN
	WMN/ WLAN	900 MHz 2.4 GHz	1.5–300 Mbps	20–50 m	IEEE802.11 IEEE802.15 IEEE802.16	HAN NAN
	Wi-Fi	2.4 GHz 5.8 GHz	2–54 Mbps	50 km	IEEE802.11	HAN NAN
	Wi-Max	2.5 GHz 3.5 GHz 5.8 GHz	Up to 75 Mbps 15 Mbps	10–100 m	IEEE802.16	NAN WAN
	Bluetooth	2.4 GHz	Up to 25 Mbps	up to 60 m	IEEE802.15.1	HAN
	3G/4G/ Cellular	1.8–2.5 GHz	5–14.7 Mbps (3G) 300 Mbps (4G)		UMTS CDMA 2000 EDGE	NAN WAN
	Sub-GHz (long-range IoT)	433 MHz 868 MHz 915 MHz	500 Kbps	13-tens km	IEEE802.15.4	HAN NAN

(*Continued*)

Table 12.2 Parameters of different communication technology till 6G. (*Continued*)

Type of technology	Name of technology	Operating frequency	Data rate	Range	Standard	SG field application
	LORA/ LPWAN/ HPWAN	137–960 MHz 860–1,000 MHz	0.3–50 Kbps	2–5 km >15 km	IEEE802.15.g	HAN NAN
	Z Wave	800–900 MHz	100 Kbps	up to 30 m	G.9959	HAN
5G/6G spectrum	Sub-THz Wave	0.3–10 THz	100 Gbps to 1 Tbps	Approx. 20–100 m	IEEE Std. 802.15.3d–2017	Holographic communication (HAN, NAN, and WAN)
	Li-Fi (infrared light)	Approx. 400–800 THz	9.6–224 Gbps	Approx. 10 m	IEEE 802.11bb	HAN Underwater
	cmWave	3–30 GHz	100 Mbps to 1 Gbps	Few 100 m	IEEE 802.11ad and IEEE 802.11ay	HAN NAN WAN

(*Continued*)

Table 12.2 Parameters of different communication technology till 6G. (*Continued*)

Type of technology	Name of technology	Operating frequency	Data rate	Range	Standard	SG field application
Wired technology	PLC 1. Narrow band 2. Broad band	<500 KHz (1.6 to 80 MHz	100 Kbps 256 Kbps to 135 Mbps	Hundreds of km	Federal Communication Commission (FCC) International electro technical Commission (ISO) IEEE 1901.2 ITU-T	HAN NAN WAN
	DSL	25 KHz to 1 MHz	256 Kbps to over 100 Mbps	Up to 3.5 km	ITU G.992.1,3,5 ITU G.993.1,2	HAN NAN
	Optical fiber	180–330 THz	Gbps to 2.56 Tbps	Few km to thousand km	ITU-T G.651 ITU-T G.651	HAN NAN WAN

LoRa modules like SX127X family operated between 860 MHz and 1,000 MHz and between 137 MHz and 960 MHz.

Although there are several communication technologies, this paper discussed some of the most useful and appropriate communication technologies especially related to smart meter communication for HAN, NAN, and WAN. Table 12.2 gives a complete knowledge and comparison of different characteristic parameters of wired and wireless technology from first generation to sixth generation.

12.6 Next Generation of Communication Technology (6G)

In previous sections, we have discussed the available communication technologies required for 1G to 5G communication systems. These days, 5G communication technologies are at their rapid advancement, but, now, researchers have seeking for a new era communication infrastructure by considering a milestone of robust network having a massive number of integrated devices with minimum requirements. Considering smart grid 5G is underway with ITUR-2015 standardization.

6G is the upcoming generation of wireless technology considered as successor of 5G technology with very high speed (approximately 1,000 times more than 5G), higher radio spectrum, together with integration of artificial intelligence (AI) and machine learning (ML), more advanced IoT, and automation. As a successor of 5G technologies, 6G communication technology harnesses advanced communication techniques using higher radio spectrum such as mmWave and THz frequency bands (30–300 GHz) and THz (300–3000 GHz), respectively, so that ultra-speedy, highly reliable, and secure communication infrastructure can be realized for smart grid. We are aware that 5G is designed to operate at the data rate around 50 Gbps, whereas 6G aimed to reach data rate upto1,000 Gbps so that a higher connectivity required in various fields can be achieved such as in ultimate multimedia like hologram. Here, we are mentioning some key performance indicators of 6G communication.

- Peak data rate with mobility, massive and limitless connectivity, and energy efficiency
- Communication in space and deep sea
- Existence of variable radio access technologies
- Integration of new radio spectrum

- Involvement of ML and AI
- Digitalized programmable physical world
- Fully automated self-learning/self-healing IoT (cognitive network)
- Integration of alternative energy technologies
- Involvement of smart materials and network compute fabric
- Ultra-dense and secure communication
- Integrated sensing and communication

12.6.1 Road Map of 6G

Till now, there is not yet a detailed road map for 6G. Being a successor of 5G, 6G will define new vision and standard of technology, and it is expected around 2030 under ITU-R-6G vision. Realization of 6G spectrum requires deeper evolution of the spectrum blueprint. New frequency band in cmWave and sub-THz range along with microwave and infrared light spectrum is explored.

Talking about a new power infrastructure (smart grid) wireless communication is an essential part, which provides two-way communication among the customers, consumers, and devices (M2M communication). Involvement of cognitive technology requires a more powerful and enhanced version of communication technology. 6G aims to revolutionize wireless communication by providing faster, limitless, and improved connectivity and advanced features. The following section will explore and discuss the characteristics and possible opportunities for cmWave and sub-THz spectrum within smart grid as key radio enablers.

As we have already discussed, the 6G wireless communication is seeking a new radio spectrum to take over the pros and discard the cons of sub-6 GHz, mmWave, and sub-THz bands, as shown in Figure 12.1.

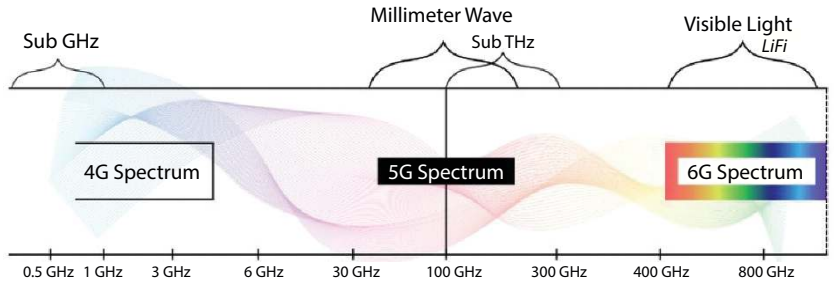

Figure 12.1 5G/6G frequency spectrum.

12.6.1.1 Sub-THz Band

The THz frequency range for 6G gains attention because of the reason that these waves penetrate lossless through a few materials as well as non-materials like plastics, wood, paper, and fabrics. Although the energy of THz radio can disrupt chemical bonds and damage electronic transitions in a medium, still, it has a wide range of applications because of unique transmission properties such as telecommunication, diagnostics, spectroscopy, sensing, quality control, and imaging, which become very attractive. These waves are located in between microwave frequency spectrum and optical wave spectrum ranging from 100 GHz to 300 GHz; some key features of sub-THz frequency spectrum are its abundant bandwidth that tends to data rate ranging from 100 Gbps to 1 Tbsp. The integration of sub-THz waves in 6G networks promises to revolutionize wireless communication and open up new possibilities for various industries. Some key features of 6G as follows.

S. no.	Key features	Applications
1	Very high data rate	➢ AI and ML ➢ Drone swarming ➢ Blockchain ➢ Remote surgery ➢ Smart homes and smart grid ➢ IoT (Internet of Things) ➢ IoE (Internet of Everything) ➢ Semantic Communication ➢ More secure transactions ➢ Smart cities ➢ Radar imaging ➢ Holography (3D communication) ➢ Intelligent robotics ➢ Autonomous driving ➢ Immersive experience extended reality (XR)
2	Advanced applications	
3	New frequency spectrum	
4	Involvement of advanced sensors	
5	Advanced communication technologies	
6	More secure	

12.6.1.2 Millimeter Waves (mmWaves)

We already discussed that sub-GHz wave and mmWave are expected to play an important role in the development of 6G technology. Differences between both the technologies can be understand by just looking at the radio spectrum given below; if we consider 5G, then mmWave operates at 30- to 300-GHz (wavelength of 1 mm to 10 mm) frequency band, but, now,

we are extending our research into the range of 300 GHz to 3 THz that will exhibit unique characteristics such as extremely high data rates, very high capacity enhanced precision, and more secure infrastructure better suited for real-time applications, location-based services, smart grid communication, industrial automation, smart cities, satellite communication, and so on.

12.6.1.3 Li-Fi Technology (Infrared Light)

Apart of the above communication technologies, nowadays, Li-Fi "light facility" technology is attracting researchers as a great transaction of alternative of radio wave communication that can be considered as an important communication tool of 5G and 6G. Li-Fi is a wireless communication technology based on the principle of visible light communication that uses visible light and infrared frequency spectrum for data communication.

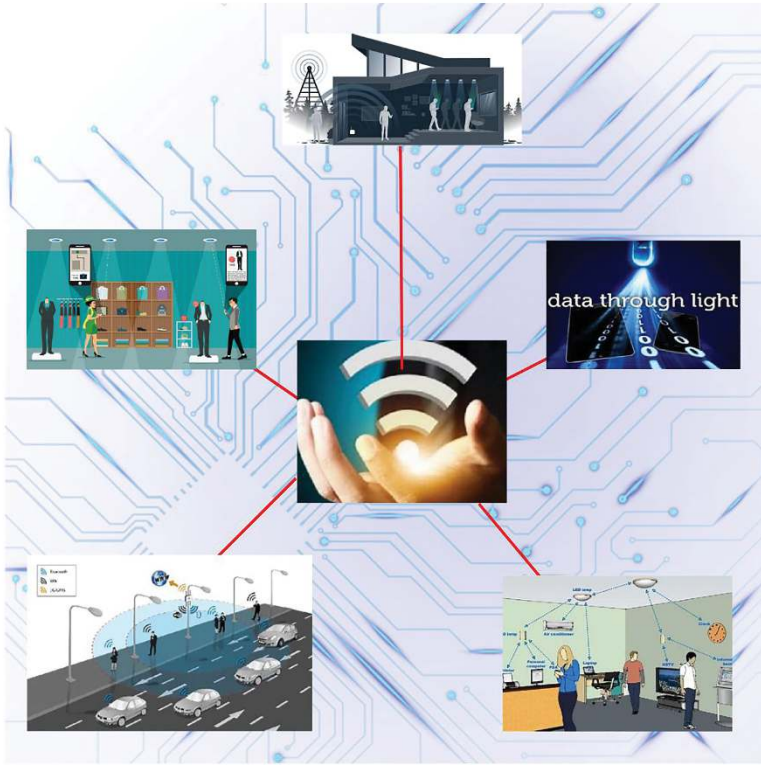

Figure 12.2 Lighting the way to connectivity: Li-Fi.

Li-Fi is an outlet of optical wireless communication as an emerging technology for the 21st century wireless communication, especially for indoor applications within a HAN. Li-Fi operates in the range of visible light spectrum ranging from 400 THz to 800 THz and because of its enormous capacity and very high-speed (>Gbps) data transfer by light by removing wired fiber connections and then wirelessly through LED light. Li-Fi is a worthy substitute for Wi-Fi technology and competent for other existing and emerging technologies for future applications. It is the forthcoming and growing technology looking forward for a brighter future of communication technology for interior applications, as, in the future, every bulb in our work area will work as a Wi-Fi spot. Very soon in the future, every light bulb will be available as a Wi-Fi spot followed by 5G and 6G communication technology [25]. Presently, Li-Fi—also referred to as Gi-Fi in some contexts—is gaining attention especially for smart cities and premises, offering a promising alternative to traditional radio-based communication that are extended to various areas and applications like industries, medical, education, smart grid, military, airlines, and robotics—traffic everywhere and a light bulb that is available, as shown in Figure 12.2. Nowadays, Li-Fi technology can achieve data rate up to 224 Gbps but looking forward to getting speed up to 1 Tbps that can be an eminent part of 6G communication. This technology will play a crucial role where radio frequencies are restricted such as airplanes, laboratories, and hospitals.

12.7 Conclusion

Being the backbone of the new power grid, selection of appropriate, efficient, and cost-effective communication technology for different parts of smart grid spatially for smart meter is very important and mandatory. As we know, every technology has its own advantages and drawbacks. This paper gives knowledge to choose the proper existing wired and wireless communication technologies in smart metering system for different purposes like transmission, collection, management, and measurement of data, as well as real-time monitoring and billing. This paper compares various communication technologies keeping different characteristics in mind. Furthermore, this paper discusses and reviews the requirement of modification and integration of some new technologies for 5G followed by 6G along with its beneficial characteristics so that the teething troubles facing in using the existing technologies within the grid can be overcome. Furthermore, it will be always required to research favorable and beneficial new technologies for the 21st century power systems. Advancement in

technology tends to have a necessary impact on the lifestyle of a person. Wireless communication technologies play a crucial role in the living standards of human beings to provide M2M communication in 6G. Integration of AI, blockchain, and ML will provide a very efficient self-optimizing and self-organizing communication infrastructure in smart grid architecture. Continuous advancement in communication infrastructure that evolved from different generations (1G to 5G) and now looking for 6G of communication technologies and ITU sector (ITU-R) require providing the standardization of 6G by the end of this decade.

Bibliography

1. Azari, A., Survey of Smart Grid from Power and Communication Aspects. *Middle East J. Sci. Res.*, 21, 1512–1519, 2014.
2. Mohsenian, D.H., *Introduction to Smart Grid*, Springer, Department of Electrical & Computer Engineering Texas Tech University, 2012.
3. Bouhafs, F., Mackay, M., Merabti, M., Links to the Future: Communication Requirements and Challenges in the Smart Grid, in: *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 24–32, Jan.-Feb. 2012, doi: 10.1109/MPE.2011.943134.
4. Jukaria, M., Singh, K.B., Kumar, A., A Comprehensive Review on Smart Meter Communication Systems in Smart Grid for Indian Scenario. *Int. J. Adv. Res. Ideas Innov. Technol.*, 3, 1, 559–566, 2017.
5. Karandikar, A. and Shetty, S., *Opportunities for India in sub-1GHz Spectrum and International Standardization*, TICET, IIT Bombay, 2010.
6. Fang, X., Misra, S., Xue, G., Yang, D., Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surveys Tutor.*, 14, 4, 944–980, 2011.
7. Central Electricity Authority. *Functional requirements of Advanced Metering Infrastructure (AMI) in India*. Ministry of Power, Government of India. 2016, August, https://www.nsgm.gov.in/sites/default/files/CEA-AMI-Functional-Requirements-August-2016.pdf.
8. *Advanced Metering Infrastructure Analytics -A Case Study*, Smart Grid PGCIL, Gurgaon, India, IEEE, Gurgaon, India, ISBN: 978-1-4799-5141, 2014.
9. India Smart Grid Bulletin, Technical paper. *India Smart Grid Forum*, May 2016.
10. Sabolcik, R., *Key priorities for Sub-GHz wireless deployment*. DigiKey. 2010, December 22, https://www.digikey.in/en/articles/key-priorities-for-sub-ghz-wireless-deployment.
11. Kuzlu, M., Pipattanasomporn, M., Rahman, S., Communication network requirements for major smart grid requirements in HAN, NAN and WAN. *Comput. Netw.*, 67, 74–88, 2014.

12. Daoud, M., On the Communication Requirements for Smart grid, Scientific. *Energy Power Eng.*, Feb 2011.
13. Abid, M.R., Khallaayoun, A., Harroud, H., Harroud, R.L., Lghoul, R., Boulmalf, M., A Wireless Mesh Architecture for the Advanced Metering Infrastructure in Residential Smart Grids. *IEEE Green Technologies Conference*, doi: DOI 10.1109/GreenTech.2013.
14. Ducrot, N., Ray, D., Saadani, A., Hersent, O., Pop, G., Remond, G., LoRa device developer guide. Orange Connected Objects & Partnerships, *Actility*, 4–24, 2016.
15. Mishra, S., Shukla, A., Arora, S., Kathuria, H., Singh, M., Controlling Weather Dependent Tasks Using Random Forest Algorithm. *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bengaluru, India, pp. 1–8, 2020, doi: 10.1109/ICAECC50550.2020.9339508.
16. *SG Communication assessment criteria among RF mesh, PLC and Cellular technology*, TRILLENT White Paper, June 2013.
17. Singh, M. and Malik, A., Multi-hop routing protocol in SDN-based wireless sensor network: a comprehensive survey. *Software-Defined Network Frameworks*, pp. 121–141, 2024.
18. Gungor, Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., Hancke, G., Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inf.*, 7, 4, Nov. 2011.
19. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile *Ad Hoc* Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019. https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
20. Fang, X., Misra, S., Xue, G., Yang, D., Smart Grid— The New and Improved Power Grid: A Survey. *Int. J. IEEE Commun. Surv. Tutor.*, 14, 4, 2011.
21. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., *Edge Computing-Based design for IoT security*, pp. 298–309, Chapman and Hall/CRC eBooks, 2024, https://doi.org/10.1201/9781003405535-22.
22. Relan, Y.H. and Shinde, V.D., Vision and Strategy for India's Electricity Metering Infrastructure of the future. *Int. J. Eng. Res. Appl.*, ISSN: 2248-9622, 5, 12(Part-1), December 2015. www.ijera.com.
23. Fan, Z., Kalogridis, G., Efthymiou, C., Sooriya Bandara, M., Serizawa, M., McGeehan, J., The new frontier of communications research: Smart grid and smart metering. *ACM e-Energy*, 2010.
24. Aftab, F., Ulfat khan, M.N., Ali, S., Light Fidelity (Li-Fi) Based Indoor Communication System. *Int. J. Comput. Netw. Commun.*, May 2016.
25. Alao O.D Joshua, J.V., Franklyn, A.S., Komolafe, O., Light Fidelity (Li-Fi): An Emerging Technology for The Future. *IOSR J. Mob. Comput. Appl.*, May-Jun. 2016.
26. Hadi, M.A., Wireless Communication tends to Smart Technology Li-Fi and its comparison with Wi-Fi. *Am. J. Eng. Res.*, 2016.

27. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in Computer And Information Science*, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
28. Haas, H., LiFi is a paradigm-shifting 5G technology, LiFi Research and Development Centre, The University of Edinburgh, King's Buildings, Edinburgh, EH9 3JL, UK, Elsevier B.V 2405–4283, © 2017.
29. Akhtar, M.W., *et al.*, The shift to 6G communications: vision and requirements. *Hum.-Centric Comput. Inf. Sci.*, 10, Article number: 53 2020.
30. Cengiz, A., *et al.*, *6th Global Power, Energy and Communication Conference (GPECOM),The Next Generation in Communication Technology: Roadmap to 6G*, July 5, 2024, IEEE Xplore, 2024.
31. Katwe, M.V., *et al.*, Cm Wave and Sub-THz: Key Radio Enablers and Complementary Spectrum for 6G, Xiv:2406.18391v1 [eess.SP], Jun 26, 2024.

13

Power-Efficient Techniques for Sustainable 6G Networks

Pramod Kumar Sagar[1]* and Arnika Jain[2]

[1]Department of Computer Science & Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India
[2]Department of Computer Science and Technology, Manav Rachna University, Faridabad, Haryana, India

Abstract

Sixth-generation (6G) network is a new-generation technology that increases the connectivity and raises the various issues of usage of energy and sustainability. Due to the high power consumption of base stations, network infrastructure, and end-user devices, telecommunication systems rank among the world's biggest energy consumers. In order to ensure that 6G networks fulfill global technological, financial, and environmental objectives, this chapter examines the critical need for power-efficient techniques. It looks at crucial elements like device longevity, environmental sustainability, and economic viability that emphasize the need for energy-efficient solutions. Energy-conscious network protocols, green hardware design, artificial intelligence for energy optimization, and the integration of renewable energies are some of the creative ways to reach an energy-hungry minimum without sacrificing transmission quality, which are covered in this chapter. This chapter offers a thorough roadmap for creating sustainable and financially feasible 6G networks by tackling issues like high costs, interoperability, and computational complexity. This chapter emphasizes the importance of power-efficient methods as a pillar for the future of telecommunication, providing guidance to scholars, business partners, and legislators seeking to strike a balance between sustainability and performance.

***Keywords*:** High-performance computing, environmental sustainability, energy-aware scheduling, energy optimization, green technology

**Corresponding author*: pksagar1975@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.) Security and Privacy in 6G Communication Technology, (287–314) © 2026 Scrivener Publishing LLC

13.1 Introduction

The sixth generation of mobile networks—the 6G—indicates the next step of the wireless communication revolution and has been set as an unprecedented goal for achieving seamless worldwide connectivity and ultra-reliable low-latency communication (URLLC). These are supposed to help realize the most demanding futuristic applications, such as holographic communication, digital twins, and massive-scale Internet-of-Things (IoT) deployment. But, it faces substantial challenges, mainly related to energy consumption.

Telecommunication systems are among the largest consumers of energy globally, with base stations, network infrastructure, and end-user devices consuming large amounts of power [1]. By shifting from 5G network to 6G network with the increased in communication [in terahertz (THz)], connectivity of the devices are dense, increased in computing power, and expected to increase in the energy consumption.

The transition from 5G to 6G, with its focus on THz communication, dense device connectivity, and high-performance computing, is expected to further increase energy consumption [2, 3]. This increase presents a critical environmental concern as, in many regions, energy production remains heavily dependent on fossil fuels, thereby contributing to the emission of greenhouse gases and to climate change.

To overcome these challenges, energy-efficient methods for 6G networks must be taken into account. This chapter discusses the need for energy efficiency in 6G networks, which include some of the key challenges:

- High energy demands of ultra-dense networks
- Energy-intensive nature of massive multiple-input–multiple-output systems
- Increasing computational requirements for artificial intelligence (AI)–driven network management

The chapter also examines opportunities presented by technological advancements, such as green hardware designs, AI-optimized network operations, and the integration of renewable energy sources.

13.1.1 Motivation of the Chapter

With the fast progression of remote correspondence advancements, 6G organizations have turned into the future, promising exceptional degrees

of network, speed, and unwavering quality. Be that as it may, this improvement accompanies an exceptionally high expansion in energy requests, which is related with a great deal of natural and monetary difficulties. Considering the worldwide issues concerning environmental change and expanded fossil fuel byproducts, it is important that power-productive arrangements are put on the top plan so the organization of 6G organizations does not abuse the maintainability targets. The part examines novel methods in tending to the requirement for developing energy proficiency without forfeiting the elite exhibition of cutting edge organizations.

Further, underlining the significance of energy-productive 6G organizations are monetary contemplations. Following expanding requests for information administrations and with additional associated gadgets, there is a heightening expense for energy by telecom administrators. This can be viewed as a likely wellspring of diminishing functional expenses and, furthermore, helps specialist organizations in offering reasonable answers for buyers. Also, with the ascent of sun oriented and other sustainable power sources, utilizing these sources to control network foundation turns into a financially feasible yet ecologically dependable procedure.

Notwithstanding manageability and financial reasonability, life span in associated gadgets is one of the primary drivers for advancement in energy-productive 6G organizations. The dramatic development of the Web of Things and brilliant gadgets requires arrangements that will assist with broadening battery duration and give steady execution after some time. This part gives an all-encompassing outline of the different strategies that offers its execution and its advantages.

13.2 Literature Review

Gururaj [4] defines the efficient communication in wireless sensor network (WSNs) in terms of energy use if it is to last over time. Higher energy consumption might result from the higher data rates and greater complexity of 5G/6G networks. Energy-efficient communication protocol design and algorithm optimization are vital to lowering energy usage without compromising on performance. WSNs are notorious for making do with little power supplies, processor speed, memory, and network throughput. Higher data speeds and more traffic on 5G/6G networks might strain these systems. Sustainable communication in the face of resource restrictions requires the development of resource allocation and management techniques that consider the specific needs of WSNs.

Strinati [5] narrated various visions of the forthcoming 6G networks pointing toward flexible connect-and-compute technologies to support future innovative services and the corresponding use cases. 6G can accommodate diverse applications, regulations, and user requirements. The reconfigurable intelligent surface (RIS) is crucial for smart and energy sustainable wireless systems. In this paper, two new concepts were introduced as wireless environment such as service and performance-boosted areas. The article discusses key enablers, research challenges, and the role of RISs in Open Radio Access Network architecture.

Mahmood [6] stated that the 5G network systems are about to be deployed, which creates the opportunity to realize massive connectivity with high throughput, low latency, high energy efficiency, and security. Additionally, it prioritizes the provision of extensive IoT network connectivity, health services, large-scale industrial and agricultural production, intelligent traffic control, and transmission and distribution systems for electricity generation. The growing number of user devices, however, is pushing researchers to look at systems that go beyond 5G in order to provide these devices with more bandwidth. Higher bandwidth availability for densely connected, larger network devices with quality-of-service (QoS) assurance is already being investigated for 6G wireless network systems. In order to improve future IoT network operations and services, researchers are utilizing machine learning (ML) and AI.

The study done by Maiti [7] delves into strategies for enhancing energy efficiency in 5G and 6G networks, focusing on network optimization, radio access techniques, and management. It looks at research papers to identify key tactics. Notable optimizations include resource allocation strategies for wireless energy transmission, dynamic base station napping to conserve power during low traffic, and a comparison of the energy efficiency of deploying small cells in different microcell topologies. Adaptive sectorization and hybrid beamforming are proposed as methods to increase network capacity and decrease energy consumption. Network topology management strategies, such as route diversity and inactive base station modes, are being researched in order to reduce energy consumption and boost throughput. Even though these techniques could greatly lower energy usage and enhance network performance, more research and development is required to optimize the advantages of energy-efficient wireless communications in the future.

Liu [8] explores computation offloading within blockchain-integrated IoT, focusing on securing the data uploading link from sensors to a base station using intelligent reflecting surface (IRS)–assisted physical-layer security. Because current schemes frequently overlook gas fees, which

causes dissatisfaction among high gas providers, the study attempts to improve energy efficiency while taking gas fees into account when computation offloading. Based on Ethereum's decentralized platform, it presents a gas-oriented computation offloading scheme that guarantees low sensor dissatisfaction, lowers energy consumption, and improves computational resource allocation. The system uses Ethereum's core layers for task data transmission, contract creation, result computing, and blockchain-based transaction synchronization. It also uses an IRS-assisted uplink communication model. The integration of sensors' limited computational capabilities with computational resources from mobile-edge computing servers is the focus of this study.

Ahmad [9] stated that sustainability has become inevitable due to the strain on natural resources including materials and energy and increase in greenhouse emissions. There will be significant concern over the energy usage and the ensuing carbon emissions into the atmosphere. Because of the fundamental limits of nature, we cannot expect the current exponential development to continue. We start by providing a succinct overview of system-level guidelines for upcoming networks. Feedback loops that are nearly isolated from one another, suggesting loose coupling and quick convergence, will be used to implement intelligence. Next, we concentrate on sustainability issues, such as network hardware, security, and management. Regarding the goal-directed distributed network management viewpoints of 6G sustainability, a number of strategies and algorithms are highlighted. Enabling sleep mode during idle periods, switching to software-based security features rather than hardware-based systems, and reconsidering encryption methods can all help reduce resource consumption in network security.

According to Taneja [10], a massive IoT network involves information flow between a massive number of connected devices for varied IoT application verticals. The primary issues with this battery-limited digital network are its high power consumption and massive energy overhead. In order to meet the energy demands of these networks, network service providers are searching for sustainable energy solutions. A workable power-allocation model that maximizes power resources and boosts network efficiency is presented in this paper. There are two suggested user-scheduling algorithms that choose which users each access point (AP) will serve. Parametric changes in the number of antennas at the AP, AP deployment, channel state information (CSI) availability, and spatial correlation for various precoding schemes are used to assess the performance of the suggested model. APs with multiple antennas that are deployed less densely have been found to produce higher spectral efficiency.

Yrjölä [11] aimed at developing future scenarios for sustainable 6G business strategies and (b) analyzing the scenarios from a sustainable business model perspective. There are two options to think about in this. First, this study examines business models as a viewpoint on ecosystemic activity, as opposed to the single focal firm that is typical in traditional business model research. Second, because this study is about the future, it focuses on investigating different future scenarios between 2030 and 2035. This study employs the scenario planning process, business modeling viewpoint, and anticipatory action learning method to achieve this goal. The data used in this study comes from a series of virtual strategy workshops held in 2020 by the Faculty of Information Technology and Electrical Engineering at the University of Oulu, Finland, and a series of virtual future-focused white paper expert group workshops hosted by the 6G Flagship.

Carayannis [12] said that the assets of the education segment are related to human competencies stemming from the propagation of knowledge and research. The business segment includes governmental entities, businesses, legal and financial actors, and other components of a society's economic capital and structure. Intellectual property, capital, materials, and manufacturing processes are among its assets. Materials and substances found in nature that can be exploited for financial benefit are the source of natural assets. They consist of air, water, flora, fauna, minerals, forests, and fertile land. The social culture helix discusses associated resources like information and social capital and integrates media and civil society. The political and legal sphere represents the accumulation of resources and authority by stakeholders and within their systems, which is reflected in laws and regulations.

According to Matinmikko-Blue [13], communal assets and public funding in a 6G context relate particularly to network infrastructure and radio spectrum. Public-private partnerships (PPPs) that cover various aspects of smart communities, including logistics, transportation, health, public safety, and utilities, are now receiving funding and support for deployment programs for telecommunication networks, which were previously focused on rural areas and other underserved areas. Sustainable development and the use of wireless telecommunication infrastructure as a general-purpose digital platform are highlighted in innovative PPP funding models. Because there are many different spectrum access concepts, including shared spectrum and local licensing, and a rapidly expanding number of frequency bands, radio spectrum policy, regulation, and management will become more complex. Localized spectrum licensing will make it possible for different network deployments and make it easier for a number of new

stakeholders to enter the market. To deal with this, more dynamic spectrum access management will be required.

Matinmikko-Blue [14] stated that the trends related to urbanization build on the 85% of gross domestic product globally created in urban areas today, and future mega-cities will be the powerhouses of the global economy. According to projections, there will be 5 billion urban dwellers by 2030, making up 3% of the world's population, yet they will use 80% of energy and produce 75% of carbon dioxide. In the developing world, rapid urbanization is putting increasing strain on the environment, public utilities, and public health. According to demographic projections, the 9 billion people in 2030 will be split into two groups. While the population of Europe, Russia, and China will continue to grow, Sub-Saharan Africa and South Asia will experience an explosion. Cities with unique identities and social and economic values will become more independent. With the help of widely available, reasonably priced connections, 6G will enable internet and mobility for the next billion people. Applications and digital services will be provided in native languages to both rural and urban areas at a never-before-seen level.

Kantola [15] stated that the data regulation and net neutrality require of internet service providers to treat all traffic equally. However, as networks advance toward 6G, they are becoming entirely service-driven platforms with connectivity customized for each tenant, use case, and application through the use of virtualized resources between cloud providers and mobile operators. Laws create uncertainty about convergent edge cloud services and technologies, especially in the area of cybersecurity.

13.3 Key Drivers for Power Efficiency in 6G

Demand for the energy increases with the evolution of 6G networks. With the revolution in 6G network, it increases environmental, economic, and technical challenges; so to handle these types of issue, it is required to make power efficiently environment on top priorities [2].

A large number of energy drivers, as shown in Figure 13.1, emphasize the requirement energy-efficient 6G networks so that it will fit not only to achieve the goal of sustainability but also to make it economically and operationally feasible.

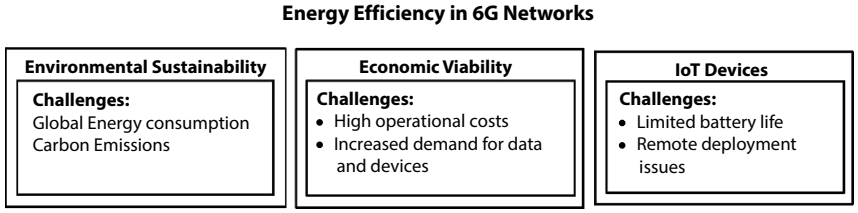

Figure 13.1 Energy drivers.

13.3.1 Environmental Sustainability

With the impact of growing telecommunication network on the environment, the sector contributes to global energy consumption and carbon emissions. Various base stations, data centers, and network infrastructure consume large amounts of electricity, out of large section is derived from fossil fuels.

With the establishment of the United Nations' Sustainable Development Goals and Paris Agreement, a law was formed to reduce the greenhouse gas emission across industries of different countries [16]. It involves designing greener hardware, optimizing network operations to minimize energy wastage, and leveraging renewable energy sources such as solar and wind to power network components.

By giving priorities to the environmental sustainability, 6G networks can play a pivotal role in reducing the carbon effect of the telecommunications industry and thus contributing to a greener planet.

13.3.2 Economic Viability

With the increased in the demand for the energy consumptions, it increases the operational cost of the telecommunication networks. Because the networks increase to fulfill the requirements of the user demands for the data and with the uses of the devices connected with each other, it increases the financial burden for the service providers.

Requirement of power-efficient 6G network provides the solution by reducing energy costs associated with base stations, core networks, and end-user devices [17]. Various techniques like dynamically allocation of the resources, energy-aware protocols, and network virtualization can optimize energy use and reduce the operational expenses.

Other than this, by using energy-efficient practices, we can enhance the economic sustainability of 6G networks, which allows operators to allocate resources as per the requirements and service improvement instead of excessive energy costs.

13.3.3 IoT Devices

The rapid growth of the IoT has led to the deployment of billions of connected devices, ranging from sensors to smart appliances [18]. Many of these devices are battery-powered and operate in environments where frequent recharging or battery replacement is impractical.

Energy-efficient 6G networks can significantly enhance the battery life of IoT devices by minimizing power consumption during data transmission and enabling low-power communication modes. This is particularly important for IoT applications in remote or inaccessible areas, such as environmental monitoring and smart agriculture.

Improved device longevity not only reduces maintenance costs but also promotes the scalability and adoption of IoT applications. It aligns with the overarching goal of 6G networks to provide sustainable and user-centric solutions for the connected world.

13.4 Techniques for Power Efficiency in 6G

To meet the growing demand for energy efficiency while maintaining high performance, 6G networks must adopt a multifaceted approach to reduce energy consumption across devices, infrastructure, and network operations.

As shown in Figure 13.2, the key techniques that enable power-efficient 6G networks are as follows,

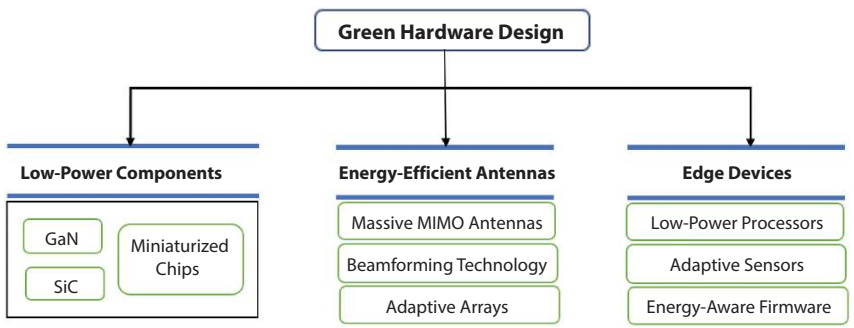

Figure 13.2 Green hardware design.

13.4.1 Green Hardware Design

The foundation of energy efficiency in 6G networks begins with the design and deployment of hardware optimized for minimal power consumption. As the physical components of the network directly impact energy usage, advancements in materials, architecture, and functionality are critical for achieving sustainable operations. Key strategies for green hardware design are low-power components, energy-efficient antennas, and edge devices with energy optimization.

Material innovations such as those in gallium nitride (GaN) and silicon carbide (SiC) have led the way for energy efficiency breakthroughs in hardware. Whereas GaN-based transistors and RF components exhibit a higher power density and lesser thermal losses compared with their silicon-based counterparts, SiC finds considerable application in high-voltage applications where substantial energy gains are achievable in power converters and amplifiers.

IoT device proliferation requires power-efficient solutions to limit power consumption throughout the network. Low-power processors, for example, ARM Cortex-M, are designed to exhibit ultra-low–power performance to suit IoT and edge computing applications. Adaptive sensors provide power-saving modes and also support energy harvesting to significantly reduce dependence on frequent replacement of batteries. Furthermore, energy-aware firmware supports a seamless transition between low-power states when in an idle state to high-performance states when actually in use, thus supporting both efficiency and reliability.

13.4.2 Energy-Aware Network Protocols

In 6G networks, energy efficiency cannot be solely achieved through hardware improvements; the network protocols governing how resources are managed and utilized play a pivotal role in reducing power consumption. Energy-aware protocols are designed to optimize the use of network resources while ensuring high performance. Sleep mode for base stations, energy-aware scheduling, and optimized routing are critical methods for developing energy-efficient network protocols.

As the backbone of cellular networks, base stations consume significant amounts of power, especially when there is low traffic. Dynamic sleep modes can really reduce such energy consumption. For example, idle base stations or even transmitters and processors can be turned off or put into low-power states when there is low demand for traffic. Like all base stations, on-demand activation facilitates using all base stations in low power

until there is a call for full capacity, avoiding minimal disruptions. In small cells, such as in the examples used above, femtocell and picocell usage can also be dynamically matched to local demand, raising its global efficiency.

Energy-aware scheduling techniques are essential for efficient resource allocation in networks, balancing load while minimizing power consumption. Dynamic load balancing evenly distributes traffic across network nodes, preventing excessive power usage by any single base station or server. Traffic prediction and optimization algorithms allocate resources more effectively based on traffic patterns, eliminating idle or redundant network components. Scheduling algorithms also consider saving energy and still ensure QoS constraints for such critical applications that will not degrade their performance. The green routing and power control protocols adjust transmission power in accordance with network demand, reducing the wastage of energy.

Optimized routing is very critical to minimize energy usage in 6G networks, where data transmission has multiple hops between devices and base stations. The efficient path selection ensures that routing algorithms choose paths that consume the least amount of power, with link quality, distance, and device power consumption considered. Multi-hop communication reduces the energy demand of long-range transmissions by utilizing intermediate nodes. Energy-aware forwarding algorithms dynamically determine the best route for transmission, based on real-time network conditions, power consumption, and traffic load. Proactive routing adjustments are used to reroute traffic from congested or high-power-consuming paths to more efficient alternatives to ensure adaptive and energy-efficient network performance.

13.4.3 Dynamic Resource Allocation

Dynamic resource allocation techniques allow real-time adaptation of network slices according to data traffic and energy consumption patterns, thus minimizing power wastage and maximizing overall network efficiency. Technologies such as software-defined networking (SDN) and network functions virtualization (NFV) allow for dynamic allocation or deallocation of resources according to demand, so that non-critical slices can scale down when traffic is low while the critical slices remain fully operational. Continuous monitoring of traffic and energy usage will allow for energy-aware traffic management, where virtualized resources are adjusted to balance power efficiency with service quality, allocating additional resources to busy slices and scaling back unused ones. Load balancing ensures that resources are optimally distributed across slices so that some slices do not

become congested while others remain underutilized. In addition, inter-slice coordination ensures that virtualized components within inactive slices either migrate toward active slices or are powered off completely, thus allowing energy savings and overall more efficient network infrastructure.

Network slicing offers the ability to create tailored network segments optimized for specific use cases, significantly reducing power consumption by aligning slices with the unique energy requirements of various applications. For low-energy use cases like IoT devices, which require minimal bandwidth and frequent low-power operations, slices can be designed to allocate only the necessary resources, avoiding over-provisioning and minimizing energy usage. Similarly, for URLLCs, slices supporting mission-critical services can activate power-intensive network resources only when absolutely necessary. This ensures that energy-intensive components are utilized solely during peak demand, meeting the stringent latency and reliability requirements of critical applications while conserving energy during periods of low activity.

13.5 Artificial Intelligence (AI) for Energy Optimization

AI and ML are two powerful tools used to optimized uses of energy in 6G networks [6]. With the help of AI algorithms, networks can dynamically adjusted to dynamic conditions because it can predict energy demands, and, based on the demand, it can efficiently allocate resources to minimize power consumption. Network operations become smarter, and, when data is provided in real-time environment and decisions are taken when data is derived, these two modes of operations help in enhancing energy efficiency. Some AI-driven techniques for energy optimization in 6G are traffic prediction, energy optimization algorithms, and fault detection.

Traffic Prediction: The optimization of energy consumption using predictive network traffic patterns can be done at a minimal cost by using AI models that analyze historical data and identify trends in data movement. These models can, therefore, enable proactive energy management through the prediction of future traffic demands. Predictive traffic models rely on AI algorithms to analyze user behavior, application usage, and network load so that resources can be allocated before the demand arises. This ensures optimal energy use during high-demand periods while conserving power during low-traffic intervals. Additionally, energy-aware traffic shaping adjusts transmission rates and prioritizes energy-efficient routes

by predicting traffic flows. For instance, during an anticipated traffic peak, AI can pre-emptively allocate additional resources, ensuring smooth data flow without overburdening network components. Adaptive resource scaling also improves efficiency because AI-driven systems dynamically scale network resources based on predicted demand while maintaining performance at optimal energy levels.

Energy Optimization Algorithms: AI and ML are pivotal in driving the optimization of energy strategies, particularly in terms of resource allocation, load balancing, and device handovers. AI algorithms can predict the optimal point for a device to transition between base stations, which results in minimum energy usage in the process. The method selects the most energy-efficient paths and times and, therefore, reduces the consumption of power by devices and network infrastructure. In load balancing, AI dynamically distributes traffic across network nodes. This prevents overburdening of individual stations and reduces power usage. For example, traffic can be offloaded from an overburdened base station to nearby stations, ensuring that no single node consumes excessive energy. Dynamic power control predicts the transmission power requirement based on the current network demand, whereas energy-efficient scheduling ensures that high-energy operations are executed only when necessary and are distributed across the network for maximum efficiency.

Fault Detection: AI improves network reliability through detection of inefficiencies or malfunctions that cause energy wastage. ML algorithms are able to identify anomalies in the behavior of the network, for example, sudden increases in power usage due to hardware failure, software bugs, or misconfigurations. These anomalies prompt automated alerts or responses, allowing network operators to correct the issue before energy waste becomes a significant problem. This proactive approach not only saves energy but also avoids disruptions, hence ensuring the smooth and efficient operation of the network. AI contributes to sustainable energy management in modern network systems by identifying faults and correcting them early on.

13.6 Blockchain for Energy Management

Blockchain technology, widely recognized for its applications in secure transactions and decentralized networks, holds significant potential in the management of energy within 6G networks. By offering transparency,

Table 13.1 Blockchain for energy management in 6G networks.

Aspect	Description	Benefits	Challenges
Energy trading	Decentralized trading of surplus energy between devices, base stations, and grids	Optimizes energy use across the network, reduces wastage, and encourages renewable adoption	Requires secure and scalable blockchain infrastructure for real-time transactions
Transparent energy auditing	Blockchain maintains a tamper-proof ledger of energy usage records.	Enables accountability, ensures fairness in energy distribution, and prevents fraud	High computational power needed for maintaining an immutable ledger in large-scale systems
Dynamic resource allocation	Smart contracts automate energy allocation based on real-time demand and supply	Increases efficiency by eliminating manual intervention and supports adaptive network needs	Complexity in creating and deploying efficient smart contracts for diverse energy needs
Grid decentralization	Decentralized control of energy distribution within the network	Reduces reliance on centralized grids, enhancing network resilience and scalability	Integration challenges with legacy power systems and existing centralized networks

(*Continued*)

Table 13.1 Blockchain for energy management in 6G networks. (*Continued*)

Aspect	Description	Benefits	Challenges
Incentive mechanisms	Reward systems for nodes contributing to energy efficiency or providing surplus	Encourages participation in energy-saving initiatives and renewable energy production	Designing fair and effective reward mechanisms is technically and economically challenging
Data privacy and security	Securing energy data through blockchain encryption and decentralized storage	Protects sensitive energy data and ensures only authorized access to energy records	Potential vulnerabilities in poorly implemented blockchain networks

security, and efficiency, blockchain can play a pivotal role in optimizing energy usage, tracking energy consumption, and facilitating energy trading between different network components [19].

Table 13.1 describes the different roles that can be played by blockchain in energy management for 6G networks:

Energy Trading: Blockchain would enable smooth energy trading, thus efficiently using available renewable energy.
Transparency and Accountability: A blockchain ledger ensures clear and auditable records of energy usage, thus minimizing disputes.
Smart Contracts: Automation through smart contracts eradicates human errors in resource allocation, which makes operations adaptive and efficient.
Decentralization: By reducing dependence on centralized grids, the network gains resilience, particularly in rural or remote areas.
Incentives: Gamification or rewards promote energy-saving behaviors and contributions to the grid.

The decentralized nature of blockchain allows for a more efficient, transparent, and secure system of energy management, addressing challenges in 6G networks such as energy wastage, high operational costs, and inefficient resource allocation. Energy trading systems, efficient record keeping, and energy demand response and load balancing are key ways in which blockchain can be integrated into energy management for sustainable 6G networks.

Blockchain technology enables peer-to-peer energy trading. Network components, such as base stations, edge devices, and IoT sensors, can trade excess energy generated by them. This enhances the overall utilization of energy and reduces wastage. Peer-to-peer energy trading enables low-energy nodes or remote devices that need additional power to receive surplus energy from the solar-powered base stations without any fear of fraud and with full transparency due to the fact that transactions are recorded on a blockchain. Smart contracts automatically execute these energy transactions based on pre-defined conditions, for example, transferring excess solar power from a base station to nearby IoT devices in need of charging, with minimal need for manual intervention. Moreover, blockchain enables the integration of DERs, including solar panels and wind turbines, into decentralized energy grids, thus facilitating flexible and reliable energy sharing across network components.

Blockchain's ability to maintain immutable and transparent records provides secure, real-time tracking of energy usage, ensuring a consistent energy supply and reducing waste. Transparent energy usage tracking records consumption and generation on a decentralized ledger, allowing easy identification of inefficiencies or discrepancies in energy flow. Real-time monitoring ensures the energy data is constantly updated, thus providing network operators with a comprehensive and real-time view of power consumption across the network for more informed decisions. Auditable transactions, securely recorded on the blockchain, help in verifying compliance with sustainability goals and regulatory requirements. Also, through identification of areas of energy waste, such as idle nodes or inefficient routing, blockchain supports the optimization of energy usage across the network.

It will support energy demand response systems because it allows for the dynamic adjustment of energy usage in accordance with real-time network demands. Decentralized load balancing enables each component of the network to automatically respond to the shifting needs of energy, including turning on energy-saving modes when consumption peaks or task reallocation to energy-efficient parts of the network. Blockchain can also promote energy efficiency as credits, tokens, or any blockchain-based

rewards motivate components to use less energy or trade effectively in energy. This system not only promotes sustainability but also maintains that the network operates smoothly while maintaining optimal energy use.

13.7 Role of Renewable Energy in 6G Networks

As the speed of 6G network increases, it provides more connectivity, and many advance services are added; it increases the sustainability and environmental impact also reduces with the increase in efficiency [20]. One of the best ways to achieve these goals is by integrating the sources of renewable energy into network infrastructure. By using renewable energy, dependency on fossil fuels is reduced, helping to meet the increased energy demand of 6G networks and maintain a sustainable balance. There are some key roles of renewable energy to maintain the sustainability and power efficiency of 6G networks given below:

13.7.1 Integration with Smart Grids

Smart grids are used to provide the solution to maintain and to optimize the generation, distribution, and consumption of energy. There are many benefits of renewable energy sources when we integrate it with 6G networks in association with smart grids:

Dynamic Energy Distribution: Because smart grids uses the data generated in real-time environment and advanced analytics are used to manage the energy distribution, renewable energy will be allocated when it is required. In case of huge amount of energy generation (like when solar panels are producing excess power), the smart grid can direct the excess energy to various base stations or other components of the network when power is required and thus minimizing the waste of energy.
Load Balancing and Demand Response: With the policy of supply based on the demand, smart grid dynamically maintain energy based on the real-time demand. Thus, dependency on the conventional grid power during the peak demand is decreased, and renewable resources are used more efficiently. Other than this, smart grid also helps in preventing network consumptions and maintaining the balance in distribution of power across various network components.
Real-Time Monitoring and Control: With the help of smart grid technology, 6G networks work in real-time monitoring environment, and it controls the usages of energy. Real-time monitoring helps in identifying

various areas where energy saving can be achieved and optimal solution can be used for the deployment of the resources to maintain network sustainability.

13.7.2 Localized Renewable Energy Systems

Incorporating localized renewable energy systems is an essential strategy for reducing the carbon footprint of 6G networks. With the integration of solar panels, wind turbines, and other renewable energy sources at network components (like base stations), efficiency of 6G networks can be increased by clean energy, thus reducing the dependency over the traditional grid power [21]:

Solar-Powered Base Stations: One of the richest sources of energy solution in 6G network is obtained from the solar power. At the roof of the home/buildings or nearby locations, solar panels can be implemented to provide the direct energy source. Solar energy is more beneficial in remote areas or rural areas where reachability of traditional grid is limited or un available. With the help of solar power, base stations can operate independently and provide uninterrupted service with the low cost of operation.
Wind-Powered Base Stations: In the remote areas where wind flow is high, wind turbines can be installed and large amount of renewable energy can be generated for the 6G infrastructure. Like solar energy, wind energy is also having low impact of energy consumption and providing a reliable and consistent source of power.
Microgrids for Remote Locations: In rural areas or areas located at distant location where reachability of conventional power grids are not reachable, microgrids powered by renewable energy systems like solar and wind can provide a constant supply of energy to the 6G base stations. These microgrids work as a local power station and ensure the operational reliability of the network in where these grids are located.

13.7.3 Energy Storage Solutions

While renewable energy sources like solar and wind provide a sustainable and clean power supply, their intermittent nature (solar energy being available during the day, and wind energy being variable) poses a challenge for consistent power supply. This is where energy storage solutions come into play:

Advanced Battery Systems: Energy storage systems, such as lithium-ion batteries, flow batteries, and solid-state batteries, can store excess renewable energy generated during periods of low demand or high energy production. These systems ensure that renewable energy is available when needed, even during periods of low sunlight or when wind speeds are low. Energy storage is crucial for maintaining the continuous operation of 6G networks without relying on fossil fuel–based backup power.
Grid-Scale Storage: With the increase in requirement of 6G network deployments, grid-scale energy storage systems can be used to store renewable energy at the grid level. It helps in providing the aggregation of renewable power from multiple sources (e.g., solar farms and wind turbines) and ensures that energy can be redistributed to different network components as needed, thus it enhancing grid stability and reducing the impact of power generation on environment.
Reducing Battery Costs and Improving Efficiency: With the innovations and researches in energy technology, it focuses on improving the efficiency and cost-effectiveness of energy storage systems. This includes innovations in battery chemistry, charge/discharge cycles, and integration with smart grids, which will further reduce the operational costs of 6G networks and enhance their sustainability.

13.7.4 Integration with Other Renewable Technologies

Renewable energy systems in 6G networks can be combined with other emerging technologies for optimal energy efficiency and sustainability.

Hybrid Energy Systems: The combination of solar power, wind energy, and traditional grid power through hybrid energy systems offers a flexible and resilient power solution for 6G networks. Hybrid systems ensure that there is steady energy supply, as these compensate for the intermittency of individual renewable sources of energy, thereby allowing for uninterrupted power supply in the entire network. This means that wind energy can supply power even when sunlight does not get through.
Energy-Efficient Infrastructure: This would be further optimized in integrating renewable energy systems into energy-efficient infrastructure designs. The integration of low-power components, energy-saving algorithms, and AI-based management systems should ensure that energy is consumed efficiently. Renewable energy in combination with energy-efficient infrastructure can help 6G networks significantly reduce their environmental footprint while improving network performance.

13.7.5 Environmental and Economic Benefits

Environmental as well as economic benefits accrue through the integration of renewable energy into 6G networks [22].

Reduction in Carbon Emissions: The 6G network can significantly reduce its carbon emission by using renewable energy sources thereby helping meet global sustainability objectives and combat climate change while aligning with international endeavors to transition into a low-carbon economy and reduce the environmental footprint of the telecommunications industry.
Cost Savings: While investment in renewable energy infrastructure and energy storage systems may be heavy in the beginning, savings during operation from reduced energy cost may be huge. As the time progresses, renewable energy systems will reduce the overall cost of ownership for 6G network operators and create a more financially viable model for network operation.
Energy Independence: As the 6G network depends on local renewable energy sources, it will have more independence and less dependency on the conventional power grid. Energy security is improved, and services in the network will remain active even in cases of grid failures or power shortages.

13.8 Challenges in Achieving Power Efficiency

Even though transition to 6G networks with a focus on power efficiency opens so many possibilities toward sustainability and cost reduction, there are several significant challenges in that. Overcoming such significant obstacles requires creative solutions as well as meticulous planning. Here are a few major challenges in power efficiency toward 6G networks:

13.8.1 High Cost of Green Technology

One of the biggest barriers to achieving the wide-scale use of power-efficient technologies is the hefty initial cost of implementing green infrastructure and renewable energy systems, such as the following:

Investment in Renewable Energy: Solar panels, wind turbines, and hybrid energy systems for 6G base stations require a lot of up-front capital. Although they are very beneficial in the long run, installation cost and maintenance costs are sometimes very high. Integration of renewable

energy systems into an existing network infrastructure is costly, especially in areas that have scarce renewable energy sources.
Energy-Efficient Hardware: High-performance, low-power components such as GaN semiconductors and energy-efficient antennas significantly cut power consumption. They also are expensive to procure; hence, they can act as a cost barrier to entry, especially in cost-sensitive regions or to an organization with a constrained budget.
Energy Storage Systems: Advanced energy storage technologies, such as lithium-ion and solid-state batteries, which are critical to ensuring a stable energy supply from intermittent renewable sources, can also be expensive. In addition to the high cost of storage systems themselves, ensuring their efficient operation and integration into the broader network infrastructure requires ongoing investment in research and development.

These high initial costs hinder the rate of adoption in power-efficient technologies, especially when budgetary constraints are an issue in the region or marketplace. Once the technology matures and economies of scale have been realized, renewable energy systems and energy-efficient equipment are likely to decrease cost, becoming more affordable in the long run.

13.8.2 Interoperability Issues

The integration of energy-efficient solutions and renewable energy sources into existing 5G and legacy network infrastructures poses interoperability issues, such as the following:

Legacy Compatibility: Much of the existing network elements and base stations were designed without considering power efficiency and renewable energy integration. These older systems are hard to upgrade for new technologies of saving power or renewable sources of energy. Integration of efficient hardware and renewable sources with an older network setup might require significant redesigning or overhauling in many places.
Standardization Issues: Incompatible standardization of renewable integration and energy-saving techniques also creates problems in deploying high power-efficient technologies smoothly. Various energy systems like the solar panel or the wind turbine operate at different levels of voltage or on completely different communication protocols. Energy-saving techniques, implemented under 6G, can be incompatible with standard, existing network management systems; the same can be said about adherence

to specific industry standards on energy-saving techniques that, as of yet, might not be fully developed and adopted.

Integration of NFV and SDN: NFV and SDN provide flexibility in creating virtual networks customized for specific applications. Integration of these technologies with energy-efficient strategies can be very challenging. Energy optimization of virtualized network functions must be achieved without performance and reliability degradation. Advanced algorithms and coordination among the layers of software involved in these technologies may not always be compatible with current network management systems.

Toward this end, the industry needs to work toward formulating universal standards for integrating energy-efficient technologies and renewable energy that would enable a smoother transition from legacy networks to sustainable 6G infrastructure.

13.8.3 Complexity of AI and ML Deployment

AI and ML are crucial in optimizing energy efficiency in 6G through traffic pattern prediction, managing resources, and discovering ineffectiveness [23]. Nevertheless, their deployment brings new challenges:

Computational Power Requirements: AI and ML algorithms, especially those that are deployed for real-time optimization and predictive maintenance, require significant computational resources to process large volumes of data quickly. Such computational power often involves high-performance computing systems that can consume substantial energy themselves. In some cases, the energy required to run AI algorithms may offset the power savings achieved through their implementation, especially when running on traditional hardware that is not optimized for energy efficiency.

Complexity of Real-Time AI Models: Real-time AI and ML models working to analyze the network traffic, energy use, or even device behaviors need to be highly responsive and adaptable. However, developing such models in both energy efficiencies and rapid decisions can require a considerable amount of computationally-intensive resources. Maintaining this will be complex because keeping these AI models from burning energy while having to maintain speed in this network system can be incredibly challenging and must be optimized adequately.

Data Transmission and Processing: In AI-driven energy optimization systems, the data that needs to be constantly transmitted between devices, base stations, and data centers in order to train and fine-tune algorithms requires significant energy consumption. This constant flow of data and the need to store vast datasets for model training add to the overall energy consumption of the network. Balancing the energy demand of data transmission, processing, and AI operations is a complex issue that needs to be addressed to ensure that AI-based systems lead to overall power savings.

Research in energy-efficient AI and ML algorithms and the use of specialized hardware for AI acceleration, like edge computing devices with AI capabilities, will be necessary to overcome these challenges. This can be a key to reduce the computational power required for real-time analysis and minimizing the energy footprint of AI models.

13.8.4 Reliability of Renewable Energy Sources

The challenge associated with renewable energy sources like solar and wind power, for the deployment of sustainable 6G networks, lies in their unpredictable and reliability aspects:

Weather Dependence: Solar power is weather dependent, while wind power is dependent on the wind speed. In areas of unpredictable weather patterns or seasons when sunlight or wind is less, the renewable energy generated may not be adequate to fulfill the network's energy requirements. This might require reliance on backup sources of energy such as traditional grid power or fossil fuels, which would defeat the purpose of incorporating renewable energy into the grid.
Energy Storage Limitation: The storage capacity for ensuring energy from renewable sources can be limited, even with most advanced energy storage systems. At low renewable energy generation points, the stored energy might not even be sufficient to meet a continuous demand for power until other alternative sources of supply can be found. Second, the energy storage devices have degradation characteristics, especially with time, and have their efficiencies and reliability degrading.
Infrastructure Costs of Energy Harvesting: There are some locations, the energy-harvesting renewable energy system installation and maintenance costs outmatch the benefit, especially for the remote areas or locations with limited energy use and fluctuation in the demand for energy. This makes the case for renewable energy less economically viable in certain circumstances, posing a challenge to its widespread adoption.

To mitigate the impact of these challenges, hybrid energy systems that combine multiple renewable energy sources and incorporate energy storage solutions can help ensure more consistent and reliable power supply for 6G networks.

13.9 Future Directions: A Roadmap for Power-Efficient 6G Networks

The future of power-efficient 6G networks would depend on the smooth integration of emerging technologies that now offer a transformative potential. A clear roadmap is necessary for such integration while considering the feasibility and encouraging collaboration among the researchers, industry leaders, and policymakers.

Nanoscale ultra-low-power component development is promising for improving energy efficiency in 6G devices and infrastructure. Scalable manufacturing techniques for nanomaterials, such as graphene and carbon nanotubes, should be explored to create energy-efficient transistors and sensors. The involvement of academia and semiconductor industries can hasten the design and commercialization of these components. Standards on nano-electronics integration in 6G networks will ensure interoperability and streamline deployment. Quantum technologies have the potential to transform energy optimization in 6G networks with high-speed data processing and advanced resource allocation algorithms. Short-term feasibility will be found in hybrid systems combining quantum and classical computing to solve computationally intensive tasks, such as traffic prediction and network optimization. PPPs and international collaborations will be essential in developing the infrastructure and expertise required for the adoption of quantum computing in 6G.

Wireless power transfer (WPT) is likely to cater to the burgeoning energy requirements of IoT devices and sensors by replacing the frequent requirement of battery recharging. In this regard, research should be focused on long-range power transfer mechanisms, like resonant inductive coupling and RF-based charging. Pilot projects on WPT-enabled IoT networks in smart cities and industrial automation can be undertaken to provide important insights into practical challenges and scalability. Building WPT ecosystems will require collaborative efforts between energy solution providers and telecommunication companies.

13.10 Conclusion

6G networks present unique opportunities for connecting and innovating in ways previously unavailable yet call for a critical leap toward sustainable practices. It is, therefore, pertinent that this chapter outlines the significant contribution of power-efficient techniques in realizing the environmental, economic, and operational feasibility of future networks. As 6G networks will embed green hardware, renewable energy sources, energy-aware protocols, and advanced optimization techniques, the future networks are able to save substantially on energy expenditure while preserving extraordinary performance. These solutions do not only mitigate challenges such as carbon emissions and growing energy costs but also create an opportunity for even more durable and efficient IoT systems. This chapter calls for a continuous need to conduct further research, encourage collaborations from industry participants, and implement policies in an effort to accomplish these goals. With 6G set to be the main framework for the future's communications systems, a sustainable approach is key in constructing a greener, resilient, and inclusive digital future.

References

1. Lambert, S., Van Heddeghem, W., Vereecken, W., Lannoo, B., Colle, D., Pickavet, M., Worldwide electricity consumption of communication networks. *Opt. Express*, 20, 26, 513–524, 2012.
2. Banafaa, M., Shayea, I., Din, J., Azmi, M.H., Alashbi, A., Daradkeh, Y., II, Alhammadi, A., 6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities. *Alex. Eng. J.*, 64, 245–274, 2023.
3. Alsharif, M.H., Kelechi, A.H., Albreem, M.A., Chaudhry, S.A., Zia, M.S., Kim, S., Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions. *Symmetry*, 12, 4, 676, 2020.
4. Gururaj, H.L., Natarajan, R., Almujally, N.A., Flammini, F., Krishna, S., Gupta, S.K., Collaborative energy-efficient routing protocol for sustainable communication in 5G/6G wireless sensor networks. *IEEE Open J. Commun. Soc.*, 2050–2061, 2023.
5. Strinati, E.C., Alexandropoulos, G.C., Wymeersch, H., Denis, B., Sciancalepore, V., D'Errico, R., Reconfigurable, intelligent, and sustainable wireless environments for 6G smart connectivity. *IEEE Commun. Mag.*, 59, 10, 99–105, 2021.

6. Mahmood, M.R., Matin, M.A., Sarigiannidis, P., Goudos, S.K., A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. *IEEE Access*, 10, 87535–87562, 2022.
7. Maiti, S. and Juneja, S., Energy Efficiency Techniques in 5G/6G Networks: Green Communication Solutions. *International Conference on Advances in Data-driven Computing and Intelligent Systems*, Springer Nature Singapore, Singapore, 2023.
8. Liu, Y., Su, Z., Wang, Y., Energy-efficient and physical-layer secure computation offloading in blockchain-empowered internet of things. *IEEE Internet Things J.*, 10, 8, 6598–6610, 2022.
9. Ahmad, I., Mämmelä, A., Mowla, M.M., Flizikowski, A., Abbasi, M.A.B., Zelenchuk, D., Sustainability in 6G networks: Vision and directions. *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2023.
10. Taneja, A., Saluja, N., Taneja, N., Alqahtani, A., Elmagzoub, M.A., Shaikh, A., Koundal, D., Power optimization model for energy sustainability in 6G wireless networks. *Sustainability*, 14, 12, 7310, 2022.
11. Yrjölä, S., Ahokangas, P., Matinmikko-Blue, M., Sustainability as a challenge and driver for novel ecosystemic 6G business scenarios. *Sustainability*, 12, 21, 8951, 2020.
12. Carayannis, E.G. and Campbell, D.FJ., *Smart quintuple helix innovation systems: How social ecology and environmental protection are driving innovation, sustainable development and economic growth*, pp. 31–37, Springer, 2018.
13. Matinmikko-Blue, M., Yrjölä, S., Ahokangas, P., Spectrum management in the 6G era: The role of regulation and spectrum sharing. *2nd 6G Wireless Summit (6G SUMMIT)*, IEEE, 2020.
14. Matinmikko-Blue, M., Aalto, S., Asghar, M.I., Berndt, H., Chen, Y., Dixit, S., Jurva, R., Karppinen, P., Kekkonen, M., Kinnula, M., *et al.*, *6G Research Visions, No. 2*, M. Matinmikko-Blue, S. Aalto, M. Asghar II, H. Berndt, Y. Chen, S. Dixit, R. Jurva, P. Karppinen, M. Kekkonen, M. Kinnula, P. Kostakos, J. Lindberg, E. Mutafungwa, K. Ojutkangas, E. Rossi, S. Yrjola, A. Oorni, P. Ahokangas, M.-Z. Asghar, F. Chen, N. Iivari, M. Katz, A. Kinnula, J. Noll, H. Oinas-Kukkonen, I. Oppermann, E. Peltonen, H. Saarela, H. Saarnisaari, A. Suorsa, G. Wikstrom, V. Ziegler (Eds.), University of Oulu, Oulu, Finland, 2020.
15. Kantola, R., *Net Neutrality Under EU Law–a Hindrance to 5G Success*, 2019.
16. Banerjee, S.B., Jermier, J.M., Peredo, A.M., Perey, R., Reichel, A., Theoretical perspectives on organizations and organizing in a post-growth era. *Organization*, 28, 3, 337–357, 2021.
17. Wikström, G., Peisa, J., Rugeland, P., Johansson, N., Parkvall, S., Girnyk, M., Mildh, G., Da Silva, I.L., *Challenges and technologies for 6G 2020 2nd 6G wireless summit (6G SUMMIT)*, IEEE, 2020.

18. Georgakopoulos, D. and Jayaraman, P.P., Internet of things: from internet scale sensing to smart services. *Computing*, 98, 1041–1058, 2016.
19. Miglani, A., Kumar, N., Chamola, V., Zeadally, S., Blockchain for Internet of Energy management: Review, solutions, and challenges. *Comput. Commun.*, 151, 395–418, 2020.
20. Dhillon, H.S., Huang, H., Viswanathan, H., Wide-area wireless communication challenges for the Internet of Things. *IEEE Commun. Mag.*, 55, 2, 168–174, 2017.
21. Bhat, J.R. and Alqahtani, S.A., 6G ecosystem: Current status and future perspective. *IEEE Access*, 9, 43134–43167, 2021.
22. Yap, K.Y., Chin, H.H., Klemeš, J.J., Future outlook on 6G technology for renewable energy sources (RES). *Renew. Sustain. Energy Rev.*, 167, 112722, 2022.
23. Yaacoub, E. and Alouini, M.-S., A key 6G challenge and opportunity-Connecting the base of the pyramid: A survey on rural connectivity. *Proc. IEEE*, 108, 4, 533–582, 2020.

14

Cybersecurity in 6G: Challenges and Future Directions

Shikha Aggarwal[1]*, Deepti Mehrotra[2], Anchal Garg[3] and Sanjeev Thakur[1]

[1]Department of Computer Science and Engineering, Amity University, Noida, India
[2]Department of Information Technology, Amity University, Noida, India
[3]Department of Computing, University of Bolton, Greater Manchester, England, UK

Abstract

While the fifth-generation (5G) wireless networks are still being studied, there is already speculation about sixth-generation (6G) echo systems. We understand that 5G is still new to the world, under proper implementation, and might have numerous problems. However, we must continue moving toward the better and the issues faced by 5G can be addressed while working with the 6G technology.

To increase security and privacy in 6G networks, we investigated the possible impact of security on wireless systems, found concerns with different technologies, and provided remedies. The limitations of 5G networks have been realized as more and more 5G networks have been deployed, which surely encourages additional research into 6G networks as the next-generation answer. More and more 5G networks are being deployed. The global deployment of 5G communication has been delayed owing to network security issues. As a result, research into 6G security analysis is critically required.

The 6G of wireless technology is the successor of 5G. This technology is still in development at various scientific and educational institutions. The 6G technology works on untapped radio frequencies and uses multiple cognitive technologies like artificial intelligence (AI) for implementation. The 6G technology is an upgrade, not only to the technological world but also to the standard of living for people. That is why many countries have shown interest in this wireless technology.

**Corresponding author*: shikhaagl03@gmail.com

Parita Jain, Puneet Kumar Aggarwal, Mandeep Singh, Sushil Kumar Singh and Amit Singhal (eds.)
Security and Privacy in 6G Communication Technology, (315–342) © 2026 Scrivener Publishing LLC

This article analyzes potential cyber-defense options for 5G and upcoming 6G networks. After thoroughly reviewing existing literature and industry practices, we discuss proactive approaches such as network segmentation, encryption protocols, intrusion detection systems, and AI-powered threat intelligence.

***Keywords*:** AI integration, attacks, edge computing, IoT security, zero-trust model

14.1 Introduction

Future systems will be automated with intelligent connections, allowing rapid, efficient, and thoughtful service delivery. The need for intelligent cybersecurity features is increasing, with a focus on attaining optimum security at a low cost. Although fifth generation (5G) is still in its early stages of commercialization, it is crucial to anticipate future communication needs and research technology for the next generation of mobile communication. This includes further enhancing technical features and investigating business models for the Internet of Things (IoT) and vertical industry applications [1]. A sixth-generation (6G) mobile network system must provide high speeds, increased capacity, and non-proximity support for new applications such as medicine, catastrophe prediction, and virtual reality. Our everyday lives and social interactions are fundamentally reliant on wireless communication. Applications of humans and machines are driving rapid expansion. There might be 59 times as many linked gadgets as people on the planet. Every 10 years, there are frequently generational shifts in the mobile industry. Work is continuing to study and standardize 6G (IMT 2030) wireless technologies, which are expected to be used starting in 2030, whereas 5G is being implemented and 5G Advanced is being developed [2].

Cybersecurity in 6G communication is on safeguarding ultra-fast, low-latency networks against new attacks. As 6G combines modern technologies such as artificial intelligence (AI), IoT, and edge computing, it faces increased risks of data breaches, cyberattacks, and privacy violations. Ensuring safe data transfer, strong encryption, and resilient network topologies is crucial. 6G's worldwide connection needs stronger security mechanisms to protect key infrastructure and personal data from sophisticated cyber-attacks.

14.2 Literature Survey

S. no.	Title	Authors/ year of publication	Focus area	Key findings	Methodology
1	Securing 6G: Challenges and Research Directions [1]	X. Zhang *et al.* (2021)	Security challenges and countermeasures	Proposed AI-driven security frameworks, including blockchain integration for enhanced security in 6G	Conceptual framework and simulation
2	Cybersecurity Threats in 6G Networks: A Survey [2]	M. Hussain *et al.* (2022)	Threats and challenges	Identified AI-driven attacks, quantum computing threats, and the need for zero-trust architectures	Literature review and expert analysis
3	Blockchain for 6G: Applications and Security Challenges [3]	L. Wang *et al.* (2023)	Blockchain in 6G	Explored the use of blockchain to enhance security and privacy in 6G networks; identified scalability and energy consumption as key challenges	Analytical Study and use-case analysis
4	Quantum Security in 6G Networks: Opportunities and Challenges [4]	A. Kumar (2021)	Quantum security	Discussed the role of quantum cryptography in securing 6G networks, emphasizing its potential to counter quantum computing threats	Theoretical study and simulation

(*Continued*)

(*Continued*)

S. no.	Title	Authors/ year of publication	Focus area	Key findings	Methodology
5	AI-Powered Security for 6G Networks: A Comprehensive Survey [5]	Y. Liu *et al.* (2022)	AI in 6G security	Surveyed the integration of AI in 6G security, highlighting its dual role in both enhancing and threatening network security	Survey and case study analysis
6	Privacy and Security in 6G: Emerging Issues and Research Directions [6]	S. Patel *et al.* (2023)	Privacy and security in 6G	Discussed the implications of new technologies like massive IoT and AI on privacy and security, proposing new privacy-preserving mechanisms for 6G	Literature review and future directions proposal

14.3 Cybersecurity Challenges in 6G Networks

6G communication is the next generation of wireless technology, expected to succeed 5G and offer significant advancements in speed, capacity, and connectivity. However, with these advancements come new cybersecurity challenges and considerations. Here are some key points regarding cybersecurity in 6G communication.

14.3.1 Emerging Threat Topography in 6G Networks

The introduction of 6G is anticipated to introduce new attack vectors due to its increased dependence on AI, IoT, and unmanned aerial vehicle (UAV) networks. Proactive measures are necessary to identify and mitigate risks in this broader threat landscape [7].

- **AI Integration:** AI raises security and privacy concerns, such as software vulnerabilities, illegal use of AI technology,

and security difficulties with data, models, and algorithms. To train the AI model for data security, service providers need to collect a lot of data, yet this data may contain sensitive user information like location, trajectory, and identity. Sensitive data may leak rather fast during data processing and transport. Attacks using "white-box" techniques provide the attacker access to safe AI models and algorithms. Even if the architecture and parameters of the AI model are unknown, the attacker may still approach the model through input and output, identifying the model's weak points and potential attack areas. Under these circumstances, the dynamic protection of AI models including flow monitoring and model output is very essential.

- **IoT Integration:** With more devices connected, including IoT devices, the potential entry points for cyber-attacks increase, necessitating robust security measures. It is easy to create a signaling storm while accessing and controlling low-power, large-scale IoT devices. It is necessary to build effective authentication methods for large-scale IoT deployments. A standardized security protocol is essential to prevent hackers from exploiting interconnection protocols for malicious intent, as IoT devices often communicate with one another.

  Conventional security methods involving encryption and decryption need both processing power and key management systems. IoT devices' limited battery life, storage capacity, and computing power limit how secure they can be. A lightweight security mechanism has to be created in order to give low-power IoT devices access that is energy-efficient. However, because device connections are so widespread, the attack surface of IoT networks has expanded. Consequently, 6G is expected to enhance the security of network infrastructure as well as the dispersed defense mechanism against a multitude of IoT devices.
- **UAV Networks:** UAVs cannot support the complex cryptographic methods that terrestrial base stations can because of their stringent weight and power restrictions. UAVs are, therefore, more vulnerable to security flaws. UAVs should be designed with lightweight encryption techniques in mind.

  Because of the way they operate, UAVs can be taken over by an enemy. UAVs should include internal attack protection

measures that stop physical intrusion from allowing access to the internal workings of the operating system in order to prevent physical manipulation.

14.3.2 Advanced Threats and Attack Vectors

The foundation of 6G technology development is the emergence of contemporary network communication regime innovations including network function virtualization, software-defined networking, and fog computing [8]. Because of the symmetry in wireless technologies, network users in a 6G environment will be able to seamlessly transition between several service providers and technologies while maintaining a high degree of quality of service, quick 3D switching, cognitive networking, and universal openness. Cyber dangers provide a significant obstacle to this 6G multidimensional development [9, 10]. As a result, in a 6G-based unconventional communication environment, there will be a number of fundamental security challenges pertaining to the CIA triad: secrecy, integrity, and availability.

The recent publications published cover various issues, including 6G communication networking enhancements, applications, and security. With the advancement of technology and the various degrees of research publications during the last 3 years, computer communication is expanding toward 6G networks.

14.3.3 Enhanced Privacy and Data Protection

Research will be primarily focused on improved privacy and data protection in 6G communication as we move toward the next generation of wireless technology.

Quantum-immune techniques: With quantum technology on the horizon, 6G systems will need encryption techniques immune to quantum attacks. This includes lattice-based cryptography as well as post-quantum cryptographic methods [11].
Completely Encryption: To prevent unwanted access, data is encrypted from the source to the destination without the need for an intermediate to decrypt it.

The technique of using AI to find odd patterns or behaviors that can point to a security issue is known as anomaly detection. Machine learning (ML) algorithms are used in predictive analytics to identify and stop

potential security threats. Patching entails ensuring that software and firmware are regularly updated to address vulnerabilities. Methods for ensuring security, strict procedures for securely distributing and verifying methods are used to prevent tampering.

14.4 New Security Paradigms and Technologies

The ever-evolving technical landscape and new cyber dangers have prompted the development of new security paradigms and solutions. The following are some of the newest ideas and innovations influencing cybersecurity:

a) Quantum-Safe Cryptography
With a lengthy history, cryptography has been important to human culture from the beginning of civilization. Many people consider Claude Shannon's 1945 article "A mathematical theory of cryptography" to be the foundation of modern cryptography as a separate field of study. Shannon established the field of information theory with the publication of "A mathematical theory of communication," another seminal work, in 1949. Shannon himself pointed out the tight relationship between information theory and encryption. Information theory is mostly concerned with information transmission, whereas cryptography is the discipline of hiding information. As a result, the two topics can gain from one another. In actuality, Shannon's creation of information theory was greatly aided by the understanding what he gained from studying cryptography. Up until the development of public-key cryptography, it appeared as though the two subjects would live happily ever after because they have many similar ideas and formulations. The seminal work "New directions in cryptography" by Diffie and Hellman was published in the IEEE Transactions on Information Theory in 1976. Strangely, this study led to the reduction of information theory's impact on cryptography, even though the field of cryptography has grown significantly over the preceding few decades. This is due to the fact that, although information-theoretic security as developed by Shannon still plays a (very limited) part in cryptography, computational security is the foundation of most modern encryption [27].

b) AI and Machine Learning in 6G Cybersecurity
With their incredibly fast speeds, extremely low latency, and extensive connection, 6G networks provide cybersecurity opportunities and problems never seen before. AI and ML are becoming crucial technologies to

properly handle these difficulties. Now, let us elaborate about main uses of ML and AI in the 6G cybersecurity environment [28].

- **Threat Detection and Prevention:**
  Anomaly Detection: Thus, predictive AI systems can analyze the flow of traffic within the computer networks and learn patterns that can be subsequently used to spot typical scenarios that can indicate that something malicious is happening. This process is known as deviation detection.
  Malware Detection: Many live ML training examples may be prescriptive for training a model that should be capable of distinguishing and categorizing hundreds of most common classes of threats such as ransomware, viruses, and phishing.
  Intrusion Detection: This is admitted on the basis that because of the incorporation of AI into the systems, for the task of monitoring the browser traffic for the existence of security threats and updating the managers on the outcomes obtained in relation to breaches.

c) Privacy and Data Protection in 6G
With low latency, faster than the 5G networks, 6G networks when in place present both great opportunities and risks such as invasion of privacy and data theft. 6G networks have inherently improved traffic, versatility, and privacy than previous networks making necessary measures to protect consumer's privacy and security from cyberattacks. Main challenges and issues that this paper will explore include the following [29].

Data Volume and Variety: In its new version, called 6G, the networks will generate large amounts of data geographical, biometric, personal and specific health data. The overwhelming amount and types of data are out there that are difficult to protect.
Data Sharing and Interoperability: 6G networks will also be applied into the regulation of the information exchange and integration between different technologies and apps. While this improves the users' experience, it also exposes a system to more cases of getting data and illicit access.
Emerging Technologies: It will bring next gen technologies such as ML, AI, and IoT in to 6G network and these and these technologies would pose a more severe threat to privacy and security of the users.
Cross-Border Data Transfers: Ninety percent of 6G networks would often involve cross-border data transfers, which makes it extremely difficult to adhere to various data protection standards.

User Consent and Control: A digital era privacy entails ensuring that users give meaningful consent for their data to be collected and utilized as per the planned utilization, and the users are given effective solutions to control their data.

Strategies for Enhancing Privacy and Data Protection:
Strong Privacy Frameworks: Governments and business groups should call for privacy legislation that covers the exact challenges posed by 6G networks.
Data Minimization: Collection and preservation of information should be done to the extent necessary for achieving the goal of data usage. Anonymization and pseudonymization are procedures aimed at minimization of recognizable data.
Encryption: Data should always be encrypted both when in transit and when at rest to avoid getting into wrong hands.
Access Controls: For purposes of restricting the access granted to particular individuals, sound access controls should be installed.
User Education and Understanding: Perhaps to help the users prevent these particular threats or reduce their chances, clinicians should explain what kind of risks they are likely to face and how their privacy is being protected.
International Cooperation: The studies contained in this work can help establish international norms and recommendations for the protection of data in 6G networks, which, in turn, will help the formation of a unified approach to the elimination of regulatory fragmentation in the field of communication.

The privacy and protection of the data that runs through 6G networks is not an easy task and thus requires a multilayered approach. Privacy and trust in the context of the 6G ecosystem can be safeguarded provided the right security mechanisms are instituted, users and others educated, and multiplicity of international cooperation employed.

d) Blockchain and Decentralized Identity

- **Concept:** Toward a system where people own their data: Distributed data ownership for health informatics. A Science Information Journalistic introduces personal data and identity credentials, which help to minimize reliance on central bodies [3].

- **Technologies:** Circulating the details through blockchain makes the transactions safe, and transparent. Distributed ledger technology (DLTs) also allow decentralized authentication and data management systems [30].

e) Secure Multi-Party Computation (SMPC)

- **Concept:** SMPC enables two or more parties to compute a function simultaneously with their inputs and at the same time provide for the protection of their data in the process.
- **Technologies:** Security protocols are used to maintain confidentiality and integrity of data exchanged between terminal equipment transformations, which provide the basis for preserving high levels of privacy during joint work in case information is involved [12].

f) Edge Computing and IoT Security

- **Concept:** As IoT devices are introduced to today's market, edge computing allows processing, introduces security measures closer to the devices, and minimizes the usage of security in the cloud.
- **Technologies:** Edge security solutions, together with lightweight cryptography, guard devices on the periphery of the network, where other methods of protection can be ineffective.

g) Zero-Trust Security Model

- **Concept:** The principle is to "never trust, always verify." Instead of assuming users inside the network are safe, it requires continuous authentication and authorization, no matter where the users or devices are.
- **Technologies:** Core components include identity verification, endpoint security, multi-factor authentication (MFA), and network segmentation at a granular level [23].

h) Confidential Computing

- **Concept:** Confidential computing ensures that sensitive data remains protected not only when stored or during transit but also while being processed, offering complete data privacy.
- **Technologies:** This paradigm employs pocket hardware-based environment like trusted solutions like Intel's SGX and AMD's SEV that they refer to as execution environments to protect the data isolated during processing.

i) Secure Access Service Edge

- **Concept:** This family cog consolidates both networking and security services functionalities software framework, to be run from the cloud.
- **Technologies:** You will often use a combination of solutions that include cloud firewall and webs secure gateway (shadows, gateways, portals, or secure web gateway (SWG)), virtual private networks and cloud access security brokers. Cloud access security brokers extend that same security to support remote working.

j) Extended Detection and Response (XDR)

- **Concept:** With an integration of collection and correlation for a broad security solution, information across networks, endpoints, servers, and the cloud allows bigger visibility and quicker threat identification compared to solution-based models.
- **Technologies:** XDR platforms use real AI and ML algorithms to enable designers to decipher activity from multiple points of an organization structure, enhancing central threat detection effectiveness.

14.5 Interoperability, Regulatory, and Standardization Efforts

Interoperability:

- 6G networks will have to connect many technologies and networks seamlessly. A huge challenge is everything surrounding interoperable security across diverse systems.
- There are efforts underway for interconnecting 6G components and subsystems through standard security interfaces and protocols.
- The ATIS Next G Alliance develops compatible security architectures for 6G.

Regulatory:

- Regulatory authorities such as the Federal Communications Commission (FCC), European Telecommunications Standards Institute (ETSI), and International Telecommunication Union (ITU) are starting to look into 6G security and privacy regulations.
- There is a push for "security by design" legislation to ensure that 6G systems are built with cybersecurity from the ground up.
- There are continuous discussions concerning data protection, encryption standards, and security evaluations for 6G networks.
- Some proposed constraints are centered on supply chain security to avoid compromised hardware and software in 6G infrastructure.

Standardization Efforts:

- Standards organizations such as 3rd Generation Partnership Project (3GPP), Institute of Electrical and Electronics Engineers (IEEE), and Internet Engineering Task Force (IETF) are in the early stages of producing 6G security specifications.

- Quantum-resistant encryption, AI-enabled security, distributed ledger technologies, and 6G zero-trust architectures are all topics of focus.
- The ITU-T Focus Group on Network Technologies for 2030 is creating security rules for 6G.
- Industry consortiums, such as the Next G Alliance and the 6G Flagship effort, are developing security recommendations to assist create standards [26].

14.6 User Awareness and Education

- **Understanding 6G Technology:** Customers should be informed on the primary advantages of 6G technology, such as ultra-low latency, increased capacity, and improved connection. Explain how these functions may introduce new vulnerabilities, such as those seen in IoT devices and edge computing [24].
- **Importance of Cyber Hygiene**: Encourage the use of strong, unique passwords and password managers. Emphasize the need of updating devices and applications to reduce vulnerabilities.
- **Phishing and Social Engineering Awareness:** Train customers on scams commonly used in phishing techniques; fortunately, as with 6G, they can also bring in more complex social engineering attacks. Build clear procedures for reporting inappropriate messages.
- **Continuous Learning and Resources:** Promote ongoing training and workshops on changing cybersecurity threats and means to eliminate them. Allow individuals to obtain up-to-date 6G cybersecurity knowledge from authoritative resources.
- **Instilling a Security Culture:** Create a place in which security should be embraced by all. Facilitate open discussions regarding security policies. The organization might also consider proposing a recognition program for those employees displaying outstanding cybersecurity procedures.
- **Data Privacy and Protection:** Provide information to people about their rights to the collection and usage of their data, more so in a hyperconnected world. Encourage good practices related to encryption and safe data sharing [25].

14.7 Security Architecture for 6G

The security architecture of the 6G networks requires solid credence toward some of the more complex hindrances associated with this new technology. A standpoint taken is to use zero trust: no devices and no users should be trusted; that is, network access is allowed to those strictly verified by authorization process.

Some kind of post-quantum cryptography, such as lattice-based or code-based encryption, should be established to combat the potential threat of quantum computers. Threat detection and response systems will be to stabilize and detect with respect to new cyber threats in real time; that is, with AI being the technology used. Ultimately, these developments will allow blockchain techniques to record activities within the network on an immutable basis, thereby promoting transparency and accountability. Coupled with the abided notion of dealing with a variety of devices and numerous applications connecting through 6G networks, the solution is to implement a multilayered security design approach targeted at network, device, and application levels. Special concerns will need to be raised on providing secure boot processes, intrusion detection systems, and encryption protocols. It will also be equally essential to monitor- constantly and in real-time the conditions and actions taken to maintain a certain level of privacy and the integrity of the data being tunneled through 6G, as depicted in Figure 14.1.

a) Zero-Trust Security Models for 6G

Hence, considering their high-speed performance, low latency, and massive connectivity, 6G networks provide security challenges and opportunities never seen before. Because the 6G networks will not have a static perimeter and will rather have a dynamic network, traditional perimeter-based security methods will not be good enough. In such a situation, Figure 14.2 shows zero-trust models appear to be promising solutions.

Understanding Zero Trust

Zero-trust security is a concept that does not rely on trust in the accessibility of the network. Authentication of the device, user, or application is the bedrock for accessing resources. It changes from perimeter defense to direct facilitation of security for transactions between interactions that take place over the network [18].

Key Principles of Zero Trust for 6G

- Continuous Verification: Every entity seeking access, regardless of location, must be continuously verified and authorized before being granted access to resources.

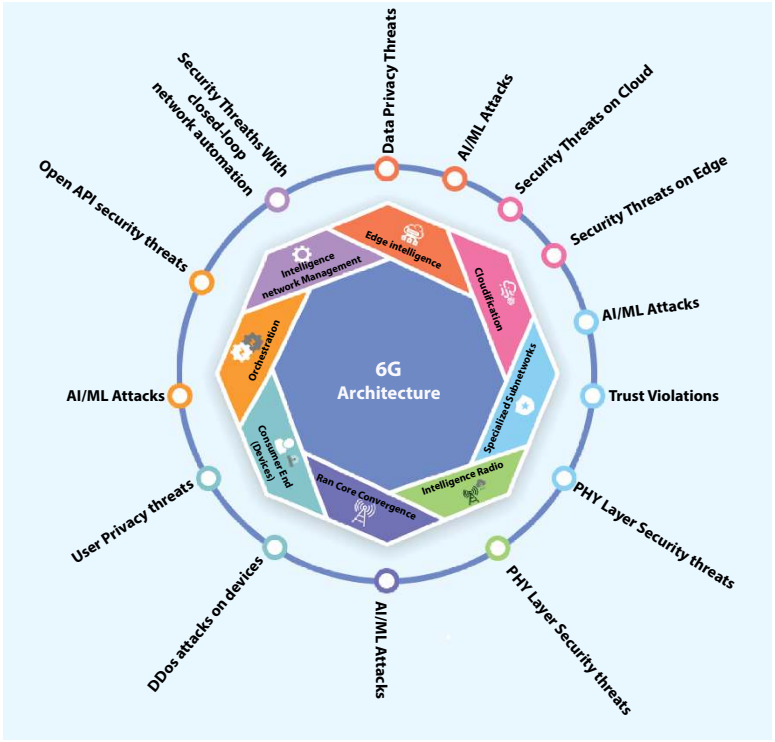

Figure 14.1 6G security architecture.

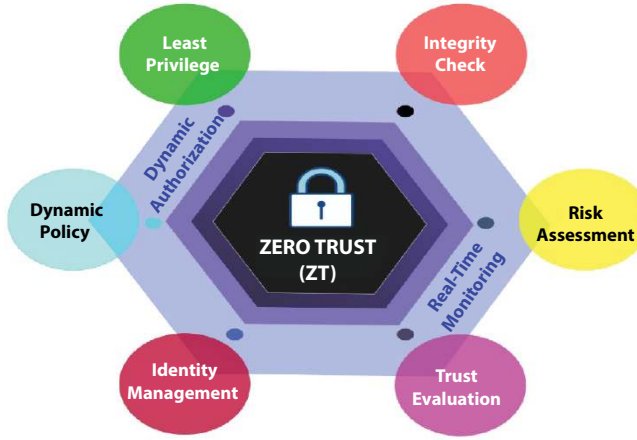

Figure 14.2 Zero-trust security model.

- Least Privilege: Access is granted only on a need-to-know basis, ensuring that entities have the minimum privileges necessary to perform their functions.
- Micro-Segmentation: Networks are divided into smaller segments or micro-segments, limiting the lateral movement of threats within the network.
- Data-Centric Security: Protection is focused on data rather than the network perimeter. Data is encrypted and protected throughout its lifecycle.
- Adaptive Policies: Security policies are dynamic and adapt to changing network conditions and threat landscapes.

Applications of Zero Trust in 6G

Device authentication: Every mobile phone and other IoT device, with the express intention of shielding unauthorized peoples from any sort of access, should undergo strong authentication.

Identity Access Management: A well-deserving software will invariably allow only the legitimate persons into the network [23].

Application Control: Continuous monitoring and control over applications prevent malicious acts and data breaches.

- Data Encryption: Sensitive data is encrypted at rest and in transit to protect it from unauthorized access.
- Network Segmentation: Network segmentation isolates critical resources and limits the spread of threats.
- Complexity: Implementing zero trust in 6G networks can be complex, requiring significant planning and investment.
- Performance Overhead: Additional security measures can introduce performance overhead, especially in latency-sensitive applications.
- Scalability: Zero-trust architectures must be scalable to accommodate the massive number of devices and connections in 6G networks.

Zero-trust security models provide a strong yet flexible means of securing 6G networks. In this way, network security against the growing challenges and scale of modern networks may be achieved by shifting the focus from a perimeter defense model to a continuous verification and micro-segmentation model. In tandem with the evolution of 6G networks, Zero-trust tenets will tend to become critical in ensuring security and privacy concerning highly sensitive data.

b) Resilience and Incident Response in 6G

The revolutionary features of 6G networks include ultra-high speeds and massive interconnected networks, which create a mushrooming number of choices and challenges for security. Resilience and involuntary restoration of 6G networks must be enough for their reliability or safeguarding sensitive data [22].

Key Challenges in 6G Resilience and Incident Response:

- Much More Complex: 6G is many folds more complex compared with earlier generations, as it includes a large number of interrelated devices and services. These phenomena become complicated enough that discovering vulnerabilities for addressing will be challenging [17].
- Distributed Architecture: In most cases, 6G networks are bound to operate with a distributed architecture; numerous nodes may have spread functions. Such architectures lead to complexities in isolating and containing incidents.
- Real-Time Requirements: The 6G network applications are likely to be highly demanding on the real-time requirement, leaving less time to respond to incidents.
- Emerging Threats: New threats and vulnerabilities arise on a day-to-day basis, thus making it overwhelming to keep up with the threat actors' capacity to find new attack vectors.

Strategies for Enhancing Resilience and Incident Response:

- Regular Risk Assessments: Adopting frequent risk assessments will help in identifying possible weaknesses and threats [16].
- Segmentation of the Network: Segmenting the network into smaller units restricts the incidence to a smaller extent.
- Redundancy: Critical components must be implemented with redundancy in order to continue operations in case of failure.
- Automation: All the mundane tasks, including vulnerability scanning and patch management, need to be automated in order to enhance efficiency and reduce the likelihood of human error.

- Incident Response Planning: Develop a comprehensive incident response plan explaining exactly how to behave in the event of an attack or breach. Maintaining awareness of emerging threats and vulnerabilities by operating with threat intelligence feeds.
- Monitoring in Real Time: Increasingly using more advanced tools for monitoring so that this phase can be recognized in time before it becomes a threat, either as anomalies or as threats.
- AI and ML: Integrating AI/ML with the organization to carry out live anomaly/potential threats identification and corresponding responses.

Resilience combined with effective response of an incident is crucial for a 6G network. The execution of these strategies would not only reduce the risk to the operator but to an extent minimize downtime and guard sensitive data. As the technology of 6G advances, so do emerging threats and thus the importance to stay ahead of emerging threats while adapting security measures becomes paramount.

c) Security of Internet of Everything (IoE) in 6G

The security environment of the Internet of Everything (IoE) in the context of the 6G network is lined with new fears as well as tremendous prospects. IoE expands upon the conventional IoT, taking it one notch higher by adding a myriad of devices, systems, and humans to allow for more purposeful and wise interactions. Against this background, the extremely high number of connected devices also increases the risks of cyberattacks and unauthorized access, thus calling for stronger security measures [21].

If security is concerned, then one of the essential elements positively influencing security is authentication mechanisms. Access to a device itself must be based on MFA so that only genuine users can interact with the IoE devices. Furthermore, a decentralized identity system enables securing the identities of billions of other devices and thus helps reduce the risks posed by credential compromise.

Data confidentiality as well as integrity is a built-in requirement within the purview of IoE security in 6G architecture. In an end-to-end encrypted arrangement, transmission of data from one device to another cannot be interfered with, allowing secure access. Besides, cryptographic hash algorithms can check for integrity and ascertain that data are not modified while in transmission [20].

Network security mechanisms should conform to the unique challenges of IoE. A zero-trust architecture can ensure that irrespective of the location of devices and users on the network, proper identity and access controls are instituted. In addition, network segmentation can curtail the extent of the breach and the attack surface as a whole, thus enhancing the roadmap for security.

The ability to detect and respond to threats in real time is the bedrock for overall security in a fluid IoE environment. Employing AI and ML will assist in the ongoing inspection of the network data to identify anomalies and possible threats. Further, incident automation tools provide the organization with the ability to investigate security incidents quickly, thus reducing the potential for further damage due to time loss.

Hardened device security and management are key to maintaining the integrity of the IoE ecosystem. Devices must have secure boot processes, and firmware should be regularly updated as protection against vulnerabilities. Further strong device-life-cycle management practices ranging from secure provisioning to proper decommissioning are important for securing devices for the length of their operational life.

Collaborative security strategies are inherently interwoven with the sound completion of the IoE's security fabric. Maturity in the scope of cyber-vulnerability provides an opportunity for developers of security-related products and partnered service providers to foster interactions where special reporting for all constituent actors is requested. Agencies further collaborate with each other in an information-sharing environment to identify changing threats and IoE vulnerabilities.

Finally, it is also crucial to come up with security measures that are future proof continually. Adaptive security solutions that can cater to the growing number of IoE devices within the 6G environment would guarantee resilience. Frequent reviews and revisions to cybersecurity guidelines would help make responses robust to evolving threats and technology developments and hence enable seamless protection of the IoE ecosystem.

14.8 Regulatory and Legal Considerations

In summary, it indicates heavy consideration has to be placed on cybersecurity with 6G. It should be very holistic in orientation toward regulatory and legal aspects with a view toward improving user privacy, protecting networks, and hence building some degree of public trust. Some key regulatory and legal issues of cybersecurity in the context of 6G include:

a) Data Privacy and Protection:

- **EU General Data Protection Regulation (GDPR) and Other Data Protection Laws:** The user data protection laws like the GDPR and other laws around the world need to be adhered to very strictly. Because 6G will create data that varies in modality from other technologies, including certain sensitive personal information, there is a certain assurance that its privacy is preserved.
- **New Types of Data:** 6G will generate some new categories of data, such as biometrics and health information. Such data is likely to be much more sensitive and may very well construe questions about an enhanced form of protection.
- **Cross-Border Data Transfers:** Transnational data transfers raise specific problems because of their global collaborations and international processing. Indeed, it is essential for all the jurisdictions to ensure compliance with all such data transfer laws and protections for data privacy.

b) Network Security and Resilience:

- **Critical Infrastructure:** 6G networks are anticipated to be critical infrastructure and therefore will require strict security measures to prevent any kind of disruption or attacks. As they consolidate various sectors, their security is becoming all the more important [17].
- **Supply Chain Security:** Supply chain security, including hardware, software, and services, is essential in ensuring no weak links instantiate vulnerabilities supply chain security, either internally or externally, poses a threat to the security design of the entire service.
- **Emergency Response:** A stricter and systematic approach to emergency response could be ordered by the government for 6G should accidents that range from cyberattacks to natural disasters illustrate their nastiness. Such protocols allow for quick recovery after the event and could soften the blow for the occurrences.
- **AI and ML:** The employment of AI and ML within the 6G networks raises inherent questions about accountability, bias, and transparency. Although these technologies could

help to proactively address security edge cases, they can also, if badly managed, introduce extreme risks.

- **IoT and Edge Computing:** The pervasive growth of IoT devices and edge computing has expanded the spectrum of threats and new legal challenges. These technologies inescapably demand some degree of security measures in addition to introducing newer vulnerabilities with attendant expansion of the attack surface.
- **Autonomous Systems:** The deployment of autonomous systems, such as self-driving cars, requires robust cybersecurity measures to prevent accidents and misuse. Ensuring the security of autonomous systems is critical for public safety and preventing malicious actions [16].

c) Numerous worldwide cooperative corporations that tackle network security exist:

- **Harmonization of Standards:** Developing harmonized international standards for 6G cybersecurity can facilitate global cooperation and reduce regulatory fragmentation. Consistent standards can help ensure interoperability and prevent regulatory arbitrage.
- **Cross-Border Investigations:** Establishing mechanisms for cross-border cooperation between law enforcement agencies is essential for investigating and addressing cybercrimes. International collaboration can help address threats that transcend national borders.

d) National Legislation on Cybersecurity: To meet modern challenges and to secure critical infrastructure, many nations have developed *stricto sensu* laws for cyberspace. These basic laws were set to legally regulate any cybersecurity activities and address violations with corresponding penalties.

- **Global Organizations:** The OECD and the ITU, among others, are among the largest in terms of developing international standards and recommendations. Such organizations ought to provide recommendations and best practice for 6G in cybersecurity.

- **Industry Standards:** Industry organizations, such as the GSMA and 3GPP, are developing standards in the area of security for 6G networks. These standards will need to establish the needed requirements for regulatory compliance.

The legal and regulatory aspects around 6G cybersecurity grow in much faster pace. The international organizations, governments, and the industry must work together to come up with complete frameworks that would cover specific issues raised by this new technology. Thus, with these considerations, we could finally assure ourselves of the safe and responsible implementation of the 6G networks.

14.9 Ethical Implications of 6G Cybersecurity

Some ethical issues with the emergence of 6G networks in cybersecurity emerge which offer ultra-high speed, low latency, and immense interconnectivity. Almost instantaneous networking and real-time connectivity will resolve a majority of beneficial hacks. Nevertheless, major ethical considerations regarding fast-paced integration of 6G technology in the world necessitate proper investigations [12].

a) Privacy and Surveillance:

- **Collection and Storage of Data:** Networks with 6G systems will generate loads of data, from location data, biometrics, and personal data drawn from other aspects of human interactions. All these complex data generation techniques earn a serious question about the whole concept of privacy-which it is going-and a fresh debate on the monitoring of data storage will cut in. Positions of individuals could be tracked easily and continuously against their viability and freedom of movement [13].
- **Government Surveillance:** That is the thing that the government would carve the mass surveillance on the network, and may even infringe individual rights to privacy, thus again creating a catch 22 situation: national security versus personal freedoms [14].

b) Digital Divide:

- **Accessibility and Affordability:** However, with the wide deployment of 6G on the horizon, a wider digital divide is anticipated in such a way that access to it would only be catered for those fortunate enough to afford it—such a situation could further widen the discrepancies and disparities in socioeconomic status.
- **Discrimination:** The various levels of access to 6G technology could engender discrimination and thus create social exclusion; people in the rural areas or with ill-portioned economic cupboards within the range of these networks might limit this factor in education, employment opportunities, and basic services.

c) Autonomous Systems and Decision-Making:

- **Bias and Discrimination:** Unless appropriate checks are kept, autonomous systems powered by 6G technology could propagate the very biases and discriminations that, in fact, compromise value in development. For instance, if the database setting up the autonomous system gives considerable weight to a particular demographic, then the autonomous system is again going to discriminate.
- **Accountability:** One of those difficult questions becomes the assessment of responsibility for the actions of all the autonomous systems. Where some injury or wrongful act is concerned, one would imply the so-called "accountability" and perhaps one will add: who is held responsible for the decisions made.

d) Cyber Warfare and State-Sponsored Attacks:

- **Escalation of Conflict:** The late dependence on the 6G network for business-critical investment in infrastructure could expose them to cyber warfare and state-sponsored attacks. This could very easily lead to the factionalization of the state and a new bout of conflict in an already volatile part of the world and could spiral up the conflict between the nations [19].

- **Collateral Damage:** Business interruption and loss of life might be the negative impacts' penalties to targets on 6G networks. For instance, assaults that target any of the key sectors in the nation's economy for instance power and transportation systems could have devastating effects.

e) Environmental Impact:

- **Energy Consumption:** The development will be done in stages successively with a contribution to the generation of high power greenhouse gasses thus causing climate change in the environment. The relatively high demand exploitation of energy resources could tap the available and may further compound environmental hitches [15].
- **Resource Depletion:** Devices and facilities for the 6G networks can also harm natural resources in a way that it tends to deplete it or use them up. They can also be used with the following adverse effects on the community, its surroundings, and the future generations of the society.

f) Ethical Frameworks and Principles:

- **Human Rights Framework:** Making sure that human rights include liberties like freedom of speech, privacy, and equality are protected by 6G technology. By implication, the interests of human rights should be taken into account in the development and deployment of 6G technology.
- **Beneficence and Non-Maleficence:** Addressing the evidence of how the projected gains in 6g technology are likely to be harmful but at the same time applying it in the right manner that will enable improvement of the society. It implies balancing between the benefits of the new technology, which are enhanced connection and economic development in this case at the disposal of the 6G network against the liabilities of the 6G.
- **Justice:** Fair distribution of the potential gains and losses that this new technology will bring in full implementation of 6G technology. This implies that the advantages of 6G should not be "captured" by few individuals while most of the negatives are experienced by other persons.

- **Autonomy:** Respecting personal freedom and people's right to make informed decisions that concern how 6G can be harnessed. This occurs by ensuring that the ownership of data is with the individuals who timely produce it such that they make decisions of how that specific data should be employed.

14.10 Conclusion and Future Scope

The epical consequences of cybersecurity in 6G are numerous and have several ethical considerations. To be able to handle these problems, governments, businesses, and civil society need to establish relationships. It is feasible to ensure that 6G technology is built and implemented in an ethical manner and will be advantageous using ethical principles.

Coming with the slogan of bringing ultra-low latency, ultra-high speed, and enormous interconnectivity, 6G communication will undoubtedly bring shocking cultural transformation and a large number of enterprises. But thanks to technological advancement, that has brought about some new challenges, especially in the area of security. Some of the important research areas that should be of future concern include: IoT security, quantum-safe cryptographic algorithms, AI security and threat detection and response mechanisms, network slicing security, blockchain security, privacy-preserving data analysis techniques, and human–machine interface integration into security frameworks. Scholars and stakeholders might support the construction of a safe and strong 6G communication system ready to address future challenges by focusing on these areas.

References

1. Zhang, X., *et al.*, Securing 6G: Challenges and Research Directions. *IEEE Commun. Surv. Tutor.*, 23, 3, 234–250, 2021.
2. Hussain, M., *et al.*, Cybersecurity Threats in 6G Networks: A Survey. *J. Netw. Secur.*, 10, 2, 12–28, 2022.
3. Wang, L. and Chen, J., Blockchain for 6G: Applications and Security Challenges. *IEEE Trans. Netw. Serv. Manage.*, 20, 1, 112–120, 2023.
4. Kumar, A. and Rathi, S., Quantum Security in 6G Networks: Opportunities and Challenges. *IEEE Access*, 29, 4, 300–315, 2021.
5. Liu, Y., *et al.*, AI-Powered Security for 6G Networks: A Comprehensive Survey. *IEEE Internet Things J.*, 9, 1, 1–14, 2022.

6. Patel, S. and Singh, R., Privacy and Security in 6G: Emerging Issues and Research Directions. *Int. J. Netw. Secur.*, 25, 3, 67–81, 2023.
7. A.You, X., Wang, C.X., Huang, J., Gao, X., Zhang, Z., Wang, M., Huang, Y., Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Sci. China Inf. Sci.*, 64, 1–74, 2021, DOI:10.1007/s11432-020-2955-6.
8. Snehi, J., Snehi, M., Prasad, D., Simaiya, S., Kansal, I., Baggan, V., SDN-Based Cloud Combining Edge Computing for IoT Infrastructure, in: *Software Defined Networks: Architecture and Applications*, pp. 497–540, Wiley-Scrivener Publishing, Beverly, MA, USA, 2022.
9. Wang, J., Wang, C.-X., Huang, J., Chen, Y., 6G THz Propagation Channel Characteristics and Modeling: Recent Developments and Future Challenges. *Comm. Mag*., 62, 2, 56–62, February 2024. https://doi.org/10.1109/MCOM.001.2200403.
10. Qamar, F., Siddiqui, M.U.A., Hindia, M.N., Hassan, R., Nguyen, Q.N., Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks. *Electronics*, 9, 14–16, 2020.
11. *Privacy and Data Protection in 6G Networks: Challenges and Opportunities*, Huawei, https://forum.huawei.com/enterprise/en/6G-and-Huawei-s-Vision/thread/738886544024027136-667213872962088960.
12. Gür, G. and Alagöz, F., Security implications of spectrum sharing in cognitive radio networks. *IEEE Wirel. Commun.*, 18, 4, 32–39, 2011, DOI:10.1109/MWC.2011.5999753.
13. Singh, M. and Malik, A., Multi-Hop Routing Protocol in SDN-Based Wireless Sensor Network: A Comprehensive Survey, in: *Software-Defined Network Frameworks: Security Issues and Use Cases*, pp. 121–141, CRC Press, 2024, https://doi.org/10.1201/9781040018323-8.
14. Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., AI and 6G Security: Opportunities and Challenges. *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Porto, Portugal, pp. 616–621, 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.
15. Jain, A.K., Nandakumar, K., Ross, A., 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognit. Lett.*, 79, 80–105, 2016, DOI:10.1016/j.patrec.2015.12.013.
16. Belkhir, L. and Elmeligi, A., Assessing ICT global emissions footprint: Trends to 2040 & recommendations. *J. Clean. Prod.*, 177, 448–463, 2018, DOI:10.1016/j.jclepro.2017.12.239.
17. Chen, Y., Ho, P.-H., Wen, H., Chang, S., Real, S., On Physical-Layer Authentication *via* Online Transfer Learning. *IEEE Internet Things J.*, 1–1, 2021, doi: 10.1109/JIOT.2021.3086581.
18. Manan, A., Min, Z., Mahmoudi, C., Formicola, V., Extending 5G services with Zero Trust security pillars: a modular approach. *2022 IEEE/ACS 19th*

International Conference on Computer Systems and Applications (AICCSA), pp. 1–6, 2022.

19. Laaroussi, Z., Soykan, E.U., Liljenstam, M., Gulen, U., Karacay, L., Tomur, E., On the security of 6G use cases: Threat Analysis of "All-Senses Meeting." *Proceedings - IEEE Consumer Communications and Networking Conference, CCNC*, 2022. https://doi.org/10.1109/CCNC49033.2022.9700673.
20. Bahl, G., Dawar, A., Singh, M., Research Analysis of Different Routing Protocols of Mobile *Ad Hoc* Network (MANET). *Int. J. Comput. Sci. Technol.*, 10, 1, 48–53, 2019. https://www.ijcst.com/vol10/issue1/9-amit-dawar.pdf.
21. Perera, C., Liu, C.H., Jayawardena, S., The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Trans. Emerg. Top. Comput.*, 3, 4, 585–598, 2015, DOI:10.1109/TETC.2015.2390034.
22. Dutton, W.H. and Dubois, E., Cyber resilience: A necessary and sufficient condition for digital security? *Cyber Def. Rev.*, 1, 1, 53–64, 2015, DOI:10.2139/ssrn.2757105.
23. Bertino, E. and Sandhu, R., Database security-Concepts, approaches, and challenges. *IEEE Trans. Dependable Secure Comput.*, 2, 1, 2–19, 2005, DOI:10.1109/TDSC.2005.9.
24. Singh, R., Sharma, R., Kumar, K., Singh, M., Vajpayee, P., Securing lives and assets: IoT-Based earthquake and fire detection for Real-Time monitoring and safety, in: *Communications in Computer and Information Science*, pp. 15–25, 2024, https://doi.org/10.1007/978-3-031-56703-2_2.
25. Jain, P., Sharma, S., Arora, S., Shokeen, V., Aggarwal, P.K., Singh, M., Edge computing-based design for IoT security, in: *Network Optimization in Intelligent Internet of Things Applications: Principles and Challenges*, pp. 298–309, CRC Press, 2024, https://doi.org/10.1201/9781003405535-22.
26. Mishra, S., Shukla, A., Arora, S., Kathuria, H., Singh, M., Controlling Weather Dependent Tasks Using Random Forest Algorithm. *2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bengaluru, India, pp. 1–8, 2020, doi: 10.1109/ICAECC50550.2020.9339508.
27. Mosca, M., Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Privacy*, 16, 5, 38–41, 2018, DOI:10.1109/MSP.2018.3761723.
28. Park, J. and Pan, S., Artificial intelligence in 6G technology: Challenges and future directions. *IEEE Access*, 9, 43150–43157, 2021, DOI:10.1109/ACCESS.2021.3062737.
29. Ziegeldorf, J.H., Morchon, O.G., Wehrle, K., Privacy in the Internet of Things: Threats and challenges. *Secur. Commun. Netw.*, 7, 12, 2728–2742, 2014, DOI:10.1002/sec.795.
30. Singh, M., Sharma, R., Singh, R., Malik, A., Aggarwal, P., Advancements in renewable energy harvesting for EV charging infrastructure, in: *Optimized Energy Management Strategies for Electric Vehicles*, pp. 75–90, IGI Global, USA, 2024, https://doi.org/10.4018/979-8-3693-6844-2.ch005.

About the Editors

Parita Jain, PhD is an Assistant Professor of Research and Assistant Dean of Academics in the Department of Computer Science and Engineering at the KIET Group of Institutions. She has authored numerous research papers published in reputable national and international conferences and journals, covering diverse topics such as agile software development, machine learning, and quality assurance in software engineering. She brings a wealth of expertise in areas such as software engineering, artificial intelligence, machine learning, and data science, fostering an environment conducive to learning, growth, and innovation.

Puneet Kumar Aggarwal, PhD is an Associate Professor at ABES Engineering College with more than a decade of experience. His research interests and scholarly contributions, showcased through numerous publications in prestigious conferences and journals, demonstrate his commitment to advancing the field of IT. His career is marked by his dedication to quality education, with extensive research contributions in cybersecurity, machine learning, and mobile applications.

Mandeep Singh is a dedicated professional with more than eight years of experience in academia. With more than 25 publications to his credit, including 15 academic papers and ten book chapters, he has established himself as a prolific researcher. His contributions span various domains, including AI, machine learning, blockchain, and Internet of Things.

Sushil Kumar Singh, PhD is an Associate Professor in the Department of Computer Engineering at Marwadi University with more than 12 years of experience teaching in the field of computer science. He has published four books and many high-quality papers in international journals and conferences. His research interests include blockchain, artificial intelligence, big data, Internet of Things, smart city security, and cyber-physical systems.

Amit Singhal is a professor and head of the Department of Computer Science and Engineering at Raj Kumar Goel Institute of Technology, Ghaziabad. With over 22 years of academic experience, his research focuses on computer networks, cybersecurity, AI, blockchain, big data, and IoT. He has published multiple books and has authored numerous research papers in high-impact journals and international conferences. His contributions extend to patents on IoT-driven intelligent monitoring systems and cloud-based public transport monitoring. He also serves as an editor and reviewer for leading journals.

Index

Also of Interest

Check out these other related titles from Scrivener Publishing

Development of 6G Networks and Technology, Edited by Suman Lata Tripathi, Mufti Mahmood, C. Narmadha, and S. Albert Alexander, ISBN: 9781394230655. *Development of 6G Networks and Technology* provides an in-depth exploration of the potential impact of 6G networks on various industries, including healthcare, agriculture, transport, and national security, making it an essential resource for researchers, scholars, and students working in the field of wireless networks and high-speed data processing systems.

Quantum Machine Learning for 6G Networks, Edited by Pallavi Sapkale, Shilpa Mehta and S. Balamurugan, ISBN: 9781394238088.

Virtual Reality and Augmented Reality with 6G Communication, Edited by B. Sundaravadivazhagan, N. Gnanasankaran, C. Pethuru Raj, and A. Saleem Raja, ISBN: 9781394336050. Stay ahead of the technological curve with this essential book, which provides a comprehensive guide to the transformative convergence of Virtual Reality (VR), Augmented Reality (AR), and 6G communication.

INTEGRATED DEVICES FOR ARTIFICIAL INTELLIGENCE AND VLSI: VLSI Design, Simulation and Applications, Edited by Balwinder Raj, Suman Lata Tripathi, Tarun Chaudhary, K. Srinivasa Rao, and Mandeep Singh, ISBN: 9781394204359. With its in-depth exploration of the close connection between microelectronics, AI, and VLSI technology, this book offers valuable insights into the cutting-edge techniques and tools used in VLSI design automation, making it an essential resource for anyone seeking to stay ahead in the rapidly evolving field of VLSI design.

DECENTRALIZED SYSTEMS AND DISTRIBUTED COMPUTING, Edited by Sandhya Avasthi, Suman Lata Tripathi, Namrata Dhanda, and Satya Bhushan Verma, ISBN: 978139420436. This book provides a comprehensive exploration of next-generation internet, distributed systems, and distributed computing, offering valuable insights into their impact on society and the future of technology.

ELECTRIC VEHICLE DESIGN: Design, Simulation and Applications, Edited by Krishan Arora, Suman Lata Tripathi, and Himashu Sharma, ISBN: 9781394204373. This book will serve as a definitive guide to conceptual and practical knowledge about the design of hybrid electrical vehicles (HEV), battery electrical vehicles (BEV), fuel cell electrical vehicles (FCEV), plug-in hybrid electrical vehicles (PHEV), and efficient EV charging techniques with advanced tools and methodologies for students, engineers, and academics alike.

INDUSTRIAL CONTROL SYSTEMS, Edited by Vipin Chandra Pal, Suman Lata Tripathi, and Souvik Ganguli, ISBN: 9781119829256. This volume serves as a comprehensive guide in the journey of industrial control systems with a multidisciplinary approach to the key engineering problems in the 21st century.

MODERN AUTOMOTIVE ELECTRICAL SYSTEMS: Theory and Applications, Edited by Pedram Asef, Sanjeevikumar Padmanaban, and Andrew Lapthorn, ISBN: 1119801047. Presenting the concepts and advances of modern automotive electrical systems, this volume, written and edited by a global team of experts, also goes into the practical applications for the engineer, student, and other industry professionals.

NANODEVICES FOR INTEGRATED CIRCUIT DESIGN, Edited by Suman Lata Tripathi, Abhishek Kumar, K. Srinivasa Rao, and Prasantha R. Mudimela, ISBN: 9781394185788. Written and edited by a team of experts in the field, this important new volume broadly covers the design of nano-devices and their integrated applications in digital and analog integrated circuits (IC) design.

EXPLAINABLE MACHINE LEARNING MODELS AND ARCHITECTURES: Real-Time System Implementation, Edited by Suman Lata Tripathi and Mufti Mahmud, ISBN: 9781394185849.

This cutting-edge new volume covers the hardware architecture implementation, the software implementation approach, and the efficient hardware of machine learning applications.

MACHINE LEARNING TECHNIQUES FOR VLSI CHIP DESIGN, Edited by Abhishek Kumar, Suman Lata Tripathi, and K. Srinivasa Rao, ISBN: 9781119910398. This cutting-edge new volume covers the hardware architecture implementation, the software implementation approach, and the efficient hardware of machine learning applications with FPGA or CMOS circuits, and many other aspects and applications of machine learning techniques for VLSI chip design.

INTELLIGENT GREEN TECHNOLOGIES FOR SMART CITIES, Edited by Suman Lata Tripathi, Souvik Ganguli, Abhishek Kumar, and Tengiz Magradze, ISBN: 9781119816065. Presenting the concepts and fundamentals of smart cities and developing "green" technologies, this volume, written and edited by a global team of experts, also goes into the practical applications that can be utilized across multiple disciplines and industries, for both the engineer and the student.

DESIGN AND DEVELOPMENT OF EFFICIENT ENERGY SYSTEMS, Edited by Suman Lata Tripathi, Dushyant Kumar Singh, Sanjeevikumar Padmanaban, and P. Raja, ISBN: 9781119761631. Covering the concepts and fundamentals of efficient energy systems, this volume, written and edited by a global team of experts, also goes into the practical applications that can be utilized across multiple industries, for both the engineer and the student.

Electrical and Electronic Devices, Circuits, and Materials: Technical Challenges and Solutions, Edited by Suman Lata Tripathi, Parvej Ahmad Alvi, and Umashankar Subramaniam, ISBN: 9781119750369. Covering every aspect of the design and improvement needed for solid-state electronic devices and circuit and their reliability issues, this new volume also includes overall system design for all kinds of analog and digital applications and developments in power systems.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.