Digital Twin and Blockchain for Sustainable Healthcare 5.0

Real-Life Applications and Case Studies

Edited by Monica Gahlawat and Sudeep Tanwar

A **Chapman & Hall** Book

CRC Press
Taylor & Francis Group

Digital Twin and Blockchain for Sustainable Healthcare 5.0

This book investigates blockchain and digital twin technologies to offer insights into their potential applications in the healthcare industry. It explores how these technologies can work together to build a strong and sustainable healthcare ecosystem, improve patient satisfaction, and streamline administrative procedures. Through examples, case studies, and discussions, the book highlights their use in supply chain management, disease prediction, and patient monitoring. It addresses challenges and offers solutions, examining ethical and legal considerations and the integration of patient preferences.

- Explores how blockchain technology can support digital twin technology in healthcare applications, facilitating efficient and secure data management.
- Studies the utilisation of advanced machine learning algorithms and predictive models in healthcare applications.
- Discusses how the integration of digital twin and blockchain technologies can contribute to sustainable development in personalised healthcare.
- Considers the ethical and legal implications associated with personalised treatment options, providing a comprehensive examination of these considerations.
- Integration of patient preferences into personalised healthcare approaches, emphasising the importance of patient-centric care. Aimed at professionals, researchers, and policymakers interested in Healthcare 5.0., the book provides comprehensive coverage of these technologies and their role in shaping sustainable healthcare practices.

Digital Twin and Blockchain for Sustainable Healthcare 5.0

Real-Life Applications and Case Studies

Edited by

Monica Gahlawat and Sudeep Tanwar

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Designed cover image: Shutterstock Images

First edition published 2026
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 9781032854434 (hbk)
ISBN: 9781032897806 (pbk)
ISBN: 9781003532286 (ebk)

DOI: 10.1201/ 9781003532286

Typeset in Times
by Deanta Global Publishing Services, Chennai, India

Contents

Editor Biographies

Sudeep Tanwar (Senior Member, IEEE) is working as a Full Professor at the Nirma University, India. He is also a Visiting Professor with Advanced Research Lab, Florida, USA; WSG University, Bydgoszczy, Poland; Jan Wyzykowski University, Poland; and University of Pitesti, Romania. He is senior member of IEEE and also Vice Chair of IEEE Computer Society, Gujarat Section, India. He received a B.Tech in 2002 from Kurukshetra University, India; an M.Tech (Honor's) in 2009 from Guru Gobind Singh Indraprastha University, Delhi, India; and a Ph.D. in 2016 with specialization in wireless sensor networks. He has authored 5 books and edited 25 books. He has written than 450 technical articles, many in top cited journals and conferences, such as *IEEE TNSE, IEEE TVT, IEEE TII, IEEE TGCN, IEEE TCSC, IEEE IoTJ, IEEE Networks, IEEE WCM, ICC, IWCMC,* GLOBECOM, CITS, and INFOCOM. He initiated the research field of blockchain technology adoption in various verticals in the year 2017. His H-index as per Google Scholar and Scopus is 85 and 70, respectively. His research interests include blockchain technology, D2D communication, Deep Learning/Machine Learning, wireless sensor networks, fog computing, smart grid, and the IoT. He is a member of the IEEE's Technical Committee on Tactile Internet. Recently, he has been awarded cash prize of Rs, 50,000 for publishing papers with 5+ Impact factor and publication of books with Springer, IET and CRC Press under the scheme of "Faculty Awards and Incentives" of Nirma University for the year 2019–2020. He has been awarded the Best Research Paper Awards from IEEE SCIoT 2022, IEEE IWCMC 2021, IEEE ICCCA 2021, IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC 2019. He won the Dr. KW Wong Annual Best Paper Prize (with 750 USD) for 2021, sponsored by Elsevier (publishers of JISA). He has served many international conferences as a member of the Organizing Committee, such as the Publication Chair for FTNCT 2020, ICCIC 2020, and WiMob 2019, and a General Chair for IC4S 2019, 2020, 2021, 2022, ICCSDF 2020, FTNCT 2021. He is also serving the editorial boards of *COMCOM* (Elsevier), *IJCS* (Wiley), *Cyber Security and Applications* (Elsevier), *Frontiers of Blockchain*, *SPY* (Wiley), *IJMIS* (Inderscience), *JCCE*, and *JSSS*. He is also leading the ST Research Laboratory, where group members are working on the latest cutting-edge technologies.

Monica Gahlawat is currently working as an Associate Professor & HOD at the L J Institute of Computer Applications, Lok Jagruti Kendra University, India. She is an executive member of IARAI (International Association for Responsible Artificial Intelligence). She is a reviewer of the prestigious journal Intelligent Systems with Applications, Expert System with Applications and Blockchain. She is active in research-based activities. She has served many international conferences as a member of the organizing committee, Reviewer Committee and Advisory Committee such as FTSE2021,ICRAECA2023, ICRAECA2025 etc. Her areas of interest include cloud computing, fog computing, edge computing, machine learning, and blockchain technology.

List of Contributors

Aditya Bakshi
School of Technology Management and Engineering
Narsee Monjee Institute of Management Studies
Chandigarh, India

Apu Chandra Barman
Marwadi University
Rajkot, India

Dipti Bhatt
Gujarat University
Ahmedabad, India

Manonmani C
V.S.B Engineering College
Karudayampalayam, India

Ramesh Babu D R
Dayananda Sagar College Of Engineering
Bengaluru, India

Sheshang Degadwala
Sigma University
Bakrol, India

Nikil Dixit
Dayananda Sagar College Of Engineering
Bengaluru, India

Akhil Gupta
Symbiosis Institute of Technology, Nagpur Campus
Symbiosis International (Deemed University)
Pune, India

Kiran Kakade
Symbiosis Institute of Management Studies
Pune, India

Munish Kumar
HCL Tech
California, United States of America

V. Lakshmi
Vellore Institute of Technology
Vellore, India

Mansi Mehta
Indus University
Ahmedabad, India

Ashutosh Mishra
Tata Consultancy Services (TCS)
Noida, India

Jhanvi Modi
Marwadi University
Rajkot, India

Damodharan Palaniappan
Marwadi University
Rajkot, India

R. Palraj
V.S.B Engineering College
Karudayampalayam, India

Arushi Pandey
School of Technology Management and Engineering
Narsee Monjee Institute of Management Studies
Chandigarh, India

Kumar Parmar
Marwadi University
Rajkot, India

Ramya R S
Dayananda Sagar College Of Engineering
Bengaluru, India

Sujatha Rajkumar
Vellore Institute of Technology
Vellore, India

Krishnan Rangarajan
Dayananda Sagar College Of Engineering
Bengaluru, India

Swagata Sarkar
Sri Sairam Engineering College
Sirukalathur, India

Rujuta Shah
Faculty of Computer Applications and IT
GLS University
Ahmedabad, India

Neetu Sharma
Tech Alchemy
Pune, India

Britant Sharma
L J Institute of Computer Applications
Lok Jagruti Kendra University
Ahmedabad, India

Anupam Singh
Graphic Era Deemed University
Dehradun, India

Deep Solanki
Techdefence Labs Solutions Limited
Ahmedabad, India

Ashok Vajravelu
Universiti Tun Hussein Onn Malaysia
Parit Raja,Malaysia

Shivangi Verma
Graphic Era Deemed University
Dehradun, India

S. Vidhya
V.S.B Engineering College
Karudayampalayam, India

Sunanda
Dayananda Sagar College Of Engineering
Bengaluru, India

Premavathi
Marwadi University
Rajkot, India

Introduction

Healthcare has undergone significant transformations over the years, evolving from traditional medical practices to highly digitized and technology-driven approaches. The latest phase, **Healthcare 5.0**, represents a shift towards hyper-personalized, intelligent, and human-centric healthcare solutions. It builds upon **Healthcare 4.0**, which primarily focuses on digitalization, automation, and smart technologies. Unlike previous generations, Healthcare 5.0 focuses on **real-time patient monitoring, predictive analytics, and autonomous healthcare solutions** to provide precise, proactive treatments. **AI-driven diagnostics, robotic-assisted surgeries, and precision medicine** enable customized treatment plans based on genetics, lifestyle, and real-time health data. **Wearable devices and IoT sensors** continuously track patient vitals, while **blockchain ensures secure data management**. The adoption of **digital twins** allows virtual simulations of a patient's body for testing treatments before applying them in real life. With a strong emphasis on **preventive care, automation, and sustainability**, Healthcare 5.0 transforms the industry into an **efficient, patient-centered, and ethically responsible** system, bridging technology and human expertise for superior healthcare outcomes.

FROM SMART HEALTHCARE (4.0) TO HUMAN-CENTRIC INTELLIGENCE (5.0)

The transition from Healthcare 4.0 to Healthcare 5.0 represents a paradigm shift in the medical industry, moving from automation-driven efficiency to intelligent, human-centric healthcare systems. While Healthcare 4.0 revolutionized the industry by integrating artificial intelligence (AI), the Internet of Things (IoT), cloud computing, and big data analytics, it primarily focused on enhancing hospital workflows, improving diagnostics, and reducing human errors through automation.

However, despite these advancements, Healthcare 4.0 had limitations:

- It prioritized operational efficiency over patient-centric care.
- It relied on rule-based AI, which lacked the emotional intelligence and ethical considerations of human doctors.
- It focused on reactive treatment rather than proactive and predictive healthcare.
- The heavy use of centralized electronic health records (EHRs) raised data security and privacy concerns.

In contrast, Healthcare 5.0 builds on the technological foundation of Healthcare 4.0 but shifts towards a human–AI collaborative model that ensures:

- Hyper-Personalization: AI-driven precision medicine tailors treatments to an individual's genetic profile, lifestyle, and medical history.

- Digital Twins: Virtual replicas of a patient allow doctors to simulate and test treatments before real-life application.
- Proactive and Predictive Healthcare: AI algorithms analyze real-time data from wearable devices, IoT sensors, and smart medical implants to detect diseases before symptoms appear.
- Ethical and Secure Systems: Blockchain technology ensures secure, tamper-proof medical records and transparent patient data management.
- AI-Augmented Decision-Making: Instead of replacing doctors, AI serves as an intelligent assistant, helping physicians make better clinical decisions with data-driven insights.
- Robotic-Assisted Surgery and Rehabilitation: Advanced robotics improve surgical precision, reduce recovery times, and enhance patient mobility through AI-driven prosthetics.

Unlike Healthcare 4.0, which was technology-driven, Healthcare 5.0 is patient-centered, ensuring that every innovation contributes directly to improved patient outcomes, accessibility, and quality of care. It envisions a future where medical technology serves humanity, rather than replacing it.

WHY HEALTHCARE 5.0 MATTERS

The rapid advancements in AI, biotechnology, IoT, and robotics are reshaping global healthcare. However, without a human-centered approach, technology alone cannot address key challenges like healthcare accessibility, personalized treatments, ethical AI governance, and patient trust. This is why Healthcare 5.0 is essential for the future of medicine.

1. **Moving from Reactive to Proactive Healthcare**: Traditional healthcare systems, including those in Healthcare 4.0, primarily focus on treating diseases after they occur. Healthcare 5.0 shifts towards prevention and early intervention by leveraging:
2. Wearable devices and IoT sensors to track real-time vitals (heart rate, blood pressure, glucose levels).
3. AI-powered predictive analytics to detect early signs of chronic illnesses.
4. Personalized wellness plans based on continuous health monitoring.
5. By shifting to preventive healthcare, Healthcare 5.0 helps reduce hospital admissions, lower medical costs, and improve overall life expectancy.
6. **Precision Medicine and Digital Twins: A Revolution in Treatment:** With genomics, AI, and bioinformatics, Healthcare 5.0 enables precision medicine, where treatments are tailored to the individual rather than the disease. Digital twins—virtual replicas of patients—allow doctors to:
7. Simulate treatment responses before applying them in real life.
8. Optimize drug dosages and predict side effects.
9. Customize rehabilitation plans for faster recovery.

10. This level of personalization was not possible in Healthcare 4.0, where treatment approaches were standardized rather than individualized.
11. **Ethical and Secure Healthcare with Blockchain and AI Governance:** One of the major concerns in modern healthcare is data security. With cyber threats increasing, sensitive patient data is at risk. Healthcare 5.0 addresses this through:
12. Blockchain technology, which ensures secure, transparent, and tamper-proof patient records.
13. AI-driven fraud detection to prevent medical insurance scams.
14. Decentralized health data management, giving patients full control over their medical history.
15. By integrating ethically designed AI and blockchain, Healthcare 5.0 ensures trust, transparency, and security in patient data handling.
16. **Robotics and AI in Surgery, Rehabilitation, and Elderly Care:** Healthcare 5.0 embraces advanced robotics for:
17. Robotic-assisted surgeries that improve precision, reduce complications, and shorten recovery time.
18. AI-driven prosthetics and brain-machine interfaces to help individuals regain mobility.
19. Smart elderly care systems that provide 24/7 monitoring and AI-assisted support for aging populations.
20. These advancements make healthcare more accessible, efficient, and capable of handling complex medical conditions.
21. **A Sustainable and Inclusive Healthcare Model:** Another key reason Healthcare 5.0 matters is its focus on sustainability and global accessibility. It promotes:
22. Remote healthcare solutions for underserved populations using AI-powered telemedicine.
23. Eco-friendly healthcare innovations, such as energy-efficient hospitals and AI-optimized medical supply chains.
24. Affordable AI-driven diagnostics, reducing medical costs and ensuring quality care for all.

By bridging the digital divide and making healthcare more sustainable, Healthcare 5.0 ensures equitable medical access for everyone, regardless of geographic or economic status.

CONCLUSION: EMBRACING THE FUTURE OF HEALTHCARE

The transition from Healthcare 4.0 to Healthcare 5.0 represents a fundamental shift in how we perceive medicine—not just as a system of treatments, but as a holistic, intelligent, and ethical ecosystem focused on human well-being. In Healthcare 5.0, technology serves humanity—not the other way around. It is an era where AI, robotics, and digital twins enhance human expertise rather than replace it. By embracing precision medicine, predictive healthcare, and ethical AI, we can create a patient-centric future where medical care is personalized, proactive, and accessible to all. Are we ready to redefine the future of healthcare? This book will explore how Healthcare 5.0 will shape the next generation of medicine—one where technology and humanity work hand in hand for a better tomorrow.

1 Digital Twin
Advancements, Technologies, and Applications

Arushi Pandey, Aditya Bakshi, and Akhil Gupta

1.1 INTRODUCTION

There is an increase in data analytics and the Internet of Things (IoT) connectivity in the Industry 4.0 revolution and digital twin technology is leading the way for IoT with implementation in various environments such as manufacturing, healthcare, and smart cities. With proper computation and communication, big-data analytics, cloud computing, and machine learning have been the driving force in generating automated functionalities for society in the last seven to ten years. Predictive maintenance and fault detection are two essential resources which are supported by data analytics and also coupled with IoT's rich environment. These two resources are also helpful in creating manufacturing processes for health products, traffic management, and patient-care detection for smart city developments [1, 2]. The industrial revolution, that is, the development of Industry 4.0 is shown in Figure 1.1. There are lots of challenges in developing data strategies such as artificial intelligence (AI) and edge computing due to the large volume of data that has been generated. In edge computing, nodes are deployed to collect probabilistic data for fulfilling the data strategy optimisation. Data regulations, standards, and policies are the three parameters that interact with the edge in collecting probabilistic data for better results.

The integration of these data perceptions, regulations, and policies with empirical research helps in creating 'digital twins'. Accurate analysis of the digital twin environment can be done using rapid analysis and real-time decisions of IoT and data analytics. A comprehensive review of the digital twin, its working, empowering technologies, applications, and challenges is presented in this chapter. Manufacturing, healthcare, and smart cities are three areas which are discussed in the literature review but the majority of papers are on manufacturing applications. Papers from IoT and data analytics from various academic sources related to digital twins are also described here. If you want to understand the definition of digital twins then let us take an example of the requirements of physical assets in representing city functionalities. Scaling the level of physical assets in designing the city is one of

DOI: 10.1201/9781003532286-1

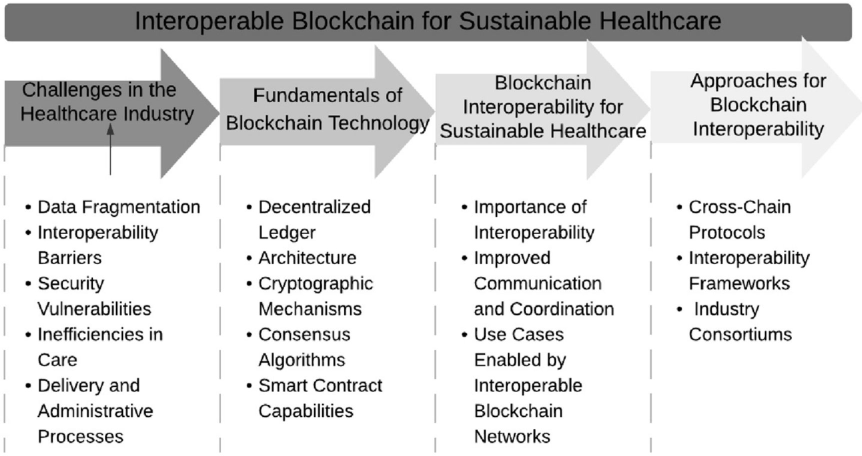


FIGURE 1.1 Industrty 4.0 revolution

the important parameters in digital twins as gathering information about the geographic location such as levels of buildings etc. and digital representations of operation applied on buildings in terms of energy, maintenance, and use of material using software, that is, BIM (building information model) can be easily modelled using a digital twin. But, how the city works, that is, social and economic functions can't be processed using this technology. For example, traffic and energy flow representations can function for a short period of time but embedding them for full-time processes can't be possible. Therefore, a digital twin behaves like a traditional computer model with less number of variables and processes.

There are many misinterpretations as the functionality of a digital twin is the same as that of a digital model or digital shadow. But, both terms are different from digital twin. The planned or pre-existing physical object with its digital version can be defined as a digital model. Limited plans for product designs, development, and buildings are some examples of digital models. There is no feature in a digital model for automatic data exchange between the physical system and the model [2]. The diagrammatical difference between the three terms is shown in Figure 1.2. Therefore, no impact has been seen on the digital model once there is a change made to the physical object. A one-way flow between the physical and digital object in a digital representation of an object is called a digital shadow. You can make changes in the digital object as well as changes in the state of the physical object in the digital object. A digital twin is fully integrated in both directions as data flows between a digital and physical object. It is very easy to make changes in both physical and digital objects in a digital twin.

Digital twin technology is said to have emerged as a powerful tool in modelling and simulating complex systems. The last few years have seen the concept of digital twins become increasingly popular, but the seeds themselves go back to previous developments in computer-aided design (CAD) and simulation. In the mid-20th

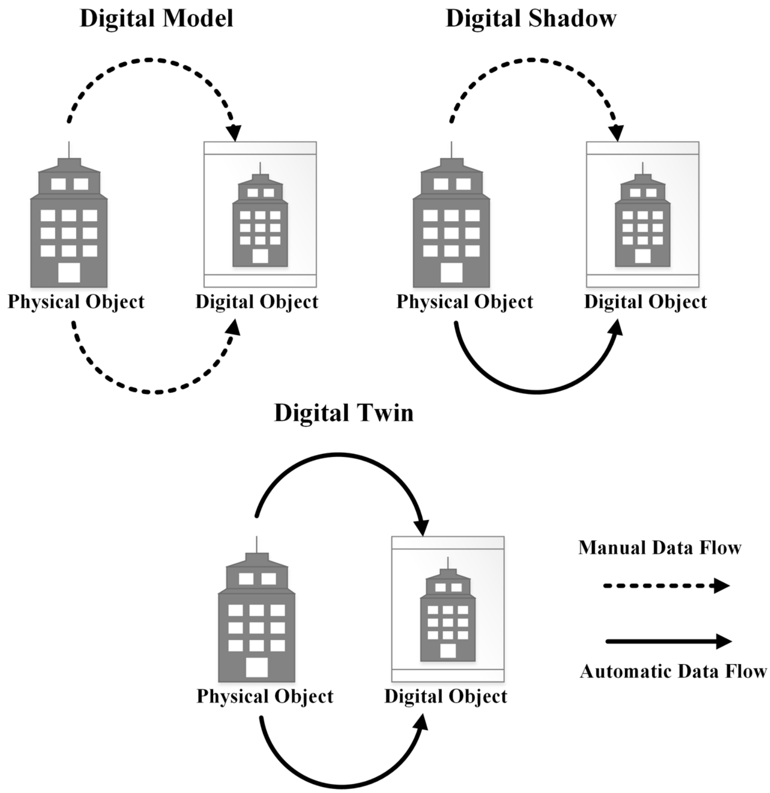


FIGURE 1.2 Digital model, shadow, and twin

century, CAD systems were developed that brought about concepts that would later nurture digital twin development for the long term by giving tools for the creation of digital representations of physical objects. With the growth in computer processing, simulating techniques developed from rudimentary models to practising advanced modelling and analysis of the behaviour of physical systems in various scenarios. Advances in the Internet of Things and the development in data analytics stood on a foundation for real-time data collection and analysis for the development of digital twins that were continuously updated by live data coming from the real world. A term in vogue called 'digital twin' was coined in the early 2010s by a group of researchers at NASA. Fast-forward to today and digital twin technology has rapidly become a widespread phenomenon in manufacturing, healthcare, and transportation.

1.2 APPLICATION OF DIGITAL TWINS

Digital twins and their ability for practical usage are evolving along with the fast development in IoT and artificial intelligence creating new pathways in the implementation of smart systems, healthcare, manufacturing, and industry use. In this chapter, applications of digital twins have been discussed in various sectors, their impact in the future, and examples of their use in the industry right now.

1.2.1 Smart Cities

Digital twins offers a new platform based on intelligent IoT innovations that will fuel automated services, enhance waste management, control energy use, and interconnect people digitally. By taking constant feedback from their real-world counterparts, digital twins allow planners to provide a dynamic platform to monitor, analyse and manage urban environments in real time [3].

While digital twins have been applied to standalone systems the industry 4.0 revolution, and other rapid breakthroughs in various technologies, have allowed digital twins to be implemented on a much larger scale connecting and processing data from IoT-embedded sensors in the city and allowing the designers to place projects in a virtual neighbourhood or city [4]. This helps them understand the structural, mechanical, and electrical details and isolate or analyse them based on performance and placement. The more data that is collected by the sensors the better the model that is developed, which also ensures higher accuracy for real-time stimulation.

Digital twin models can be used in various ways, such as to emulate the movements of different objects such as vehicles or pedestrians and help stimulate their movement in case of an emergency, the effect of the weather on a specific neighbourhood or the whole city can be predicted, it aids in the optimisation of city layouts, infrastructure locations, and zoning restrictions leading to better efficiency and resilience.

A prime example of this is the Wuhan Road Traffic Smart Emergency System which is an innovative and integrated system for handling urban traffic management and helping during any unforeseen emergencies. This system uses cutting-edge technology to ensure a more responsive and effective traffic management infrastructure by combining real-time data collecting, analysis, and communication.

1.2.2 Manufacturing

The manufacturing sector holds great potential for the application of digital twins, changing conventional procedures and increasing operational efficiency in a variety of ways. It allows manufacturers to obtain exceptional operational insights by generating digital copies of physical entities in real time. This allows them to make informed decisions based on data and promote ongoing enhancements across the whole product lifecycle. The product design can be closely monitored to prevent error and manufacturers can stimulate the product design before putting it into production saving on time and cost [5]. It allows the designing of the product to take place along the whole process virtually which can be analysed and optimised based on the bottlenecks that are found, cut downtime, and improve overall production efficiency with the help of predictive analytics. Early detection of anomalies and defects in the production process lowers the rate of scrap and ensures the supply of superior goods.

Digital twins in the manufacturing industry have various uses in different industries, for example, in the automotive sector they help speed up product development processes and increase design correctness by enabling virtual prototyping and simulation [6]. In the aerospace industry, they help in enhancing and understanding aircraft behaviour and performance.

Digital twins help produce a complete approach to manufacturing excellence, from product conception to production and maintenance. The situation of greater competitiveness, lower prices, and better product quality is becoming increasingly apparent. Their capacity to offer continuous evaluation, predictive analytics, and simulation abilities, which promote creativity, efficiency, and better decision-making in the manufacturing landscape, makes digital twins a key component of the Industry 4.0 manufacturing revolution.

1.2.3 Healthcare

A digital twin in the context of medicine is a virtual representation of a real-world entity or procedure, such as a patient, their anatomy, or the environment of a hospital. Presently, healthcare digital twins aim to dynamically represent data sources such as disease registries, electronic health records (EHRs), genomes, biomics, and proteomics data, as well as physical indicators, demographics, and lifestyle information over an individual's lifetime [7]. Digital twins enable the creation of models specific to a patient replicating the individual's characteristics and offering personalised input. These models allow healthcare professionals to analyse and simulate the impact and result of various treatments and medicines and make adjustments accordingly for the personal needs of the patient. They can also help with the handling of chronic illnesses by providing real-time, ongoing patient monitoring. These virtual copies combine information from smartwatches, sensors, and other medical monitoring devices to offer an accurate representation of a patient's condition. Proactive monitoring facilitates early anomaly discovery, enabling prompt interventions, and individualised therapy modifications. As technological advancements take place many more things will become possible with the help of digital twins; however, current applications are limited to stimulating the effects of certain drugs before administrating them to the patient to prevent side effects and using digital copies to plan and perform surgical procedures effectively and accurately.

An example of this is Sim&Cure which is at the forefront of providing medical care by utilising digital twins by integrating patient data and allowing medical professionals to provide personalized treatment planning. They created a digital twin for the treatment of aneurysms, which are bulging blood arteries that can cause strokes or clots. Through the use of 3D models, digital twins of the aneurysm and surrounding blood arteries enable brain surgeons to do simulations and understand the dynamic link between the aneurysm and the implant [7].

Digital twins hold the potential to revolutionise the treatment of chronic disease, lifestyle, health, and wellness in the future. If they live up to their full potential, they will enable the possibility of interconnected care that has not yet been completely realized. As a result, health devices such as mobile health applications and smart watches, could provide digital twins with real-time information, enabling them to make prompt judgements that could save lives.

1.3 CHALLENGES

There are many shared challenges with digital twins as they run parallel with AI and IoT technologies. Data analytics and IoT have some common challenges but our aim is to find the challenges of digital twins [7–11]. Review work for challenges related to digital twins is shown in Table 1.1. The table covers the field, its types, and a description of the challenges covered.

1.4 EMPOWERING TECHNOLOGIES

In this section, different empowering technologies for digital twins are discussed.

1.4.1 Empowering Technologies for Data Analytics

The next section explores data analytics within the fields of deep learning, machine learning, and artificial intelligence. Table 1.2 provides a summary of the empowering technologies for data analytics as described in [12] and the classification scheme offered by [13]. Although the empowering technologies for data analytics are comparable to those for the IoT, there are certain differences as well, especially in the areas of visualisation and analytics algorithmic components. Different operational fields related to data analytics are shown in Table 1.2.

The object field captures the dual nature of storage facilities by encapsulating the object field and at least three levels. Data sensing technologies and techniques, digital signal processing units for data harvesting, and pre-processing data for analytic solutions are the main goals of the first layer is data gathering. Utilisation and storage of databases are made easier by the second layer, the data repository. The last layer connects to the middleware field and consists of storage facilities that allow large amounts of data to be stored on demand using server storage. This layer is also the point of connection for processing data that has been saved.

The middleware field has three critical layers. In particular, the first layer connects to the third layer of the object field about storage processing. The second layer, data processing, provides the structural support for cloud services, data analytics, and primary middleware architectures, which are comprised of software and database systems. The table describes the third layer, which is dedicated to analysis and algorithms. It also entails empowering models—supervised and unsupervised learning, in particular—within data analytics.

The networking field contains technology that makes connectivity protocols possible. Wireless communication is the primary emphasis of this technology. It looks at how these protocols make it easier to gather and handle data from earlier layers and fields in an effective manner. It also includes working standards for security and privacy measures.

TABLE 1.1
Review of Challenges in Digital Twins

Field of Challenges	Type of Challenges	Description
Data Analytics	IT Infrastructure	The primary challenge in AI's rapid growth is the costly and demanding IT infrastructure, which needs to keep up with the hardware and software needs of the latest technology. The cost of parts can range from over US$1000 to US$10,000 which exponentially increases the cost of the whole system making it very expensive to manufacture. A way of overcoming this challenge can be seen in the way that GPUs (graphics processing units) have been used as a service providing on-demand GPUs that are very expensive at lower costs like a service or rental through the cloud by companies such as Amazon, Google, and Microsoft. However, data analytics continues to be hampered by expensive and inadequate infrastructure. There are still issues with making sure that the cloud architecture provides strong security when using it for data analytics and digital twins.
	Quality of Data	Thorough filtering and cleaning procedures are necessary to achieve maximum effectiveness. For AI algorithms to function as well as possible, high-quality data input must be ensured. This avoids the inclusion of inferior data that might distort analysis and decision-making.
	Privacy and Security	In the computing sector, security and privacy are vital, particularly in data analytics. Since AI is still in its infancy, regulations are changing to meet the increasing difficulties. Subsequent oversight and laws are intended to improve AI accountability while protecting user information. A significant step towards ensuring privacy and security in the creation of AI algorithms is the General Data Protection Regulation (GDPR). Federated learning appears as a decentralised method that addresses privacy issues and guarantees local data retention when using data analytics inside a digital twin, in conjunction with rules.
	Trust	In AI, trust is a major difficulty, in part because of its novelty and complexity, as many developers are unfamiliar with it. There are various reasons for mistrust with the primary one being the fear of AI taking over control from humans. Even though there are more favourable media reports about AI now, some media depictions of the technology such as on the news and in daily entertainment still sometimes have a negative impact on it, influencing public opinion. The best way to resolve this issue is by showing the positive side of AI and how it can make human life easier and potentially help save lives. Furthermore, tackling security and privacy issues with strict laws promotes a more trustworthy connection between the users and AI.

(*Continued*)

TABLE 1.1 (CONTINUED)
Review of Challenges in Digital Twins

Field of Challenges	Type of Challenges	Description
	Expectations	An additional challenge in data analytics is the misconception that it's a universal problem-solver. Smart city development and manufacturing are two industries that can benefit from new technology such as AI. Users frequently have high expectations and expect instant time and money savings. When implementing data analytics, it is crucial to recognise its limitations in the early stages in order to avoid using AI prematurely and to foster increased understanding for well-informed and practical implementations.
IoT/Industrial IoT	Organised Data, Up-to-Date Security, and Protecting Privacy	The proliferation of IoT devices in homes and industry presents a formidable data challenge, further hindered by the influx of big data. An Organised system is required to sort out the large amounts of unordered data generated and supplied by IoT making it more usable and easier to gain insights. User's personal data can also be at risk of exploitation if proper steps are not taken to ensure protection from criminals taking advantage of vulnerabilities. DDoS (distributed denial of service) attack threats are increased by the increasing growth of IoT, highlighting the necessity of giving privacy and security measures first priority while connecting devices.
	Infrastructure	With the rapid growth of IoT-connected devices, the IT infrastructure also needs to keep up with modifications and integration of the latest technology to ensure seamless functioning and best performance. An advantage of enhanced technology is that it may allow the latest technologies and cloud services to be used without the need for huge expenses. One way to solve this is by retrofitting IoT sensors onto old devices so that the data is not wasted and resulting in increased utilisation.
	Connectivity	Even with the increasing popularity of IoT, there remain connectivity issues, especially when trying to meet real-time monitoring goals. Linking several sensors at the same time in the production process is difficult. Overall connectivity is impacted by problems such as software bugs, deployment mistakes, and power outages. One disconnected sensor might have a big impact on a process. Updating machinery and using restoration techniques contribute to thorough data gathering, which is essential for providing precise data to AI algorithms and preserving system operation.
	Expectations	As with AI, managing expectations is a concern when it comes to IoT, as end consumers and companies might not completely understand its capabilities. Although the IoT is expanding quickly and its importance is being recognised, having high expectations could worsen trust issues by raising concerns regarding security and privacy. Similar to AI, prior knowledge is necessary to fully utilise IoT and ensure informed and efficient use.

(*Continued*)

TABLE 1.1 (CONTINUED)
Review of Challenges in Digital Twins

Field of Challenges	Type of Challenges	Description
Digital Twin Challenges	IT Infrastructure	Digital twins face the same challenge as data analytics and IIoT/IoT due to the IT infrastructure. For digital twins to be implemented and function effectively, an updated infrastructure is necessary. Without a well-designed and connected IT framework, the digital twin cannot achieve its goals effectively.
	Useful Data	Here also digital twins face the same challenges as AI and IIoT/IoT. Obtaining clean, high-quality data from a constant stream of input is one of the most important challenges facing digital twins. Poor quality data that is unsorted can lead to bad performance, as it acts on incomplete data. Careful planning and analysis are essential to guarantee the proper functioning of digital twins.
	Privacy and Security	Security and privacy present a huge challenge in the context of digital twins due to the huge amount of data they use, and the danger this presents to the private information of individuals. AI and IoT are the two main technologies used in digital twins and need to keep up with the security and privacy protocols. To address trust difficulties with digital twins, security and privacy considerations for data are important.
	Trust	Information about digital twins needs to be discussed and explained to both the users and organizations in order to build up trust. More knowledge leads to a greater level of confidence in digital twins. The enabling technologies overcome obstacles by implementing that guarantee privacy and security.
	Expectations	Even though digital twins development is being boosted by the support of industry leaders such as GE and Siemens there is still a need to create awareness amongst the users and companies and highlight the challenges. Creating strong IoT infrastructure bases and improving the understanding of data needed for analytics would enable companies to use digital twin technology efficiently. It's difficult to get over the idea that employing digital twins is only a trend. Encouraging and critical conversations are essential to the development of well-informed digital twin systems. Other than the difficulties that are faced by Industrial IoT/IoT and data analytics also affecting digital twins it also has other specific challenges.
	Standardised Modelling	Modelling digital twins can present a challenge as there is no specific standardized approach to modelling. A standard method needs to be formed based on either physics or design to ensure proper understanding to users and ensure a smooth flow of information between the different stages.
	Domain Modelling	A problem that arises from the requirement for standard use is the transfer of domain-specific data to all phases of the digital twin modelling process. This ensures the future success of digital twin applications by ensuring compatibility with sectors that involve IoT and data analytics. Future development and application of digital twins in IIoT/IoT and data analysis depend heavily on it.

TABLE 1.2
Data Analytics Operations

Field	Empowering Technology
Object	Pre-Processing and Assembly of Data
	Data Warehouses
Middleware	Data Storage
	Handling Data
	Study Algorithms and Techniques
Networking	Wi-Fi Technology
Application	Visualisation of Data
	Applications of Data Analytic

The final field is called the application field and consists of two layers of technology. For tangible technology to record data and carry out machine learning, deep learning, or statistical analysis, the initial layer consists of hardware and visualisation. This layer's visualisation feature makes it easier to display important data related to user tasks.

1.4.2 Industrial IoT (IIoT)/IoT-Empowering Technologies

IIoT and IoT include several essential components that are necessary for the functioning of networked systems. The crucial components are located within four key functional fields namely application, middleware, networking, and object fields. These areas cover specific technologies such as hardware, software, data processing, network connectivity, power, and energy storage. Each field has a specific function and they work together to ensure the continued advancement and success of the Industry 4.0 revolution.

The application layer, which is housed in the first layer, is responsible for a range of IIoT/IoT applications, such as intelligent farming systems, smart cities, and houses. The next layer is architecture, wherein software architectures such as SOA (service-oriented architecture) and REST (representational state transfer) are supported. This layer specifies the general structure of the system [14]. The third layer, software and APIs serve as a bridge between the application and middleware fields.

The middleware field consists of three additional levels. The first tier is the cloud platform, which consists of services that offer on-demand computing resources through the cloud. In the second layer data processing is the main focus. The third layer, or data storage, is crucial to the infrastructure of the IoT. MongoDB, for instance, provides powerful storage engines for massive data storage. Together, these middleware field layers provide a comprehensive foundation for managing data processing, storage, and computing resources in IoT and IIoT systems.

The third IoT system section, which is made up of three crucial layers, covers the networking field. In order to facilitate efficient system communication, the network, application, and transport protocols make up the first layer, also known as

TABLE 1.3
I/IoT Operations

Field	Empowering Technology
Application	Application-Based Industrial IoT Architecture
	Application Program Interface
Middleware	Platforms Based on Cloud
	Data Processing System
	Store Information
Networking	Protocol Using Communication
	Interaction with Network
	Adaptability
Objects	Hardware Platforms
	Objects Embedded on System
	Segmentation Using Mechanical and Electrical Field

the communication protocol layer. The second layer contains the network interface, which is essential to the IoT system's smooth integration. The final layer, the networking field, has adoption mechanisms. This includes the adoption layer, which makes use of IEEE 1095 and 6TiSCH standards to ensure a more stable wireless connection [15].

Table 1.3 illustrates the object field, which is the final element of the IoT system. There are three main enabling layers in the object field. Hardware platforms, such as Raspberry Pi and Arduino, are examples of good hardware for the first tier. Radio tags, displays, and sensors are some of the components that are consolidated in the second layer and are necessary for system communication. Mechanical and electrical components which are in the last layer provide essential operation of the gadget, such as batteries and processor units. These tiers work together to provide the necessary hardware, sense elements, and operational components to create a comprehensive framework that powers and supports IoT devices.

1.4.3 Empowering Technology for Digital Twins

Similar to Table 1.3, Table 1.4 provides the fields of digital twins that show the synthesis of ideas within the research and finding the comprehensive definition of digital twins.

The first field consists of the application field, which has three essential layers. When creating high-fidelity representations of actual objects, the initial layer—the model architecture and visualization layer—is immensely important. It makes sure that digital twins are more than just physical acts by making architectural modelling and visualisation easier. The software and API on the second tier help with the preprocessing and collecting on the third layer, which makes it easier to simulate digital

TABLE 1.4
Digital Twins Operations

Field	Empowering Technology
Application	Visualisation and Model Architecture
	Application Program Interface and Software
	Pre-Processing and Assemble Data
Middleware	Storage
	Data Processing
Networking	Transmission
	Wi-Fi Communication
Object	Hardware Platform
	Actuator Using Sensor

twin systems. In order to ensure correct data gathering, this last layer effectively links the application to the middleware field.

There are two enabling layers that comprise the middleware field. First, there is storage technology, which enables the on-demand databases, MySQL, Mongo DB, and other services that are necessary for data storage and are crucial for digital twin applications [4, 14]. The transfer of stored data between the middleware and networking fields depends on the second layer, which is connected to data processing.

There are two levels in the networking field. The effective transfer of collected data between fields depends on the communication technology layer, which is the top layer. In a digital twin system, the wireless data transfer that complies with the correct protocol depends on the wireless communication layer, which is the following layer in the network field. Data transmission to the next object field additionally requires it.

There are two layers that comprise the object field. The first one is a hardware platform and the second one is sensor technology. Both layers are required to enable sensor-based data collection and to set up the equipment needed for digital twin analysis.

1.5 REVIEWED ANALYSIS OF PAPERS

In this section, categorial review, and case studies of different reviewed papers are presented. The papers that have been reviewed mainly cover smart cities, manufacturing, and healthcare, which are discussed in the following sections with examples.

1.5.1 Smart Cities

In this section, we will review the current research on the topic of smart cities using digital twins. According to the research, urbanisation has significantly increased recently, and IoT and data analytics have also grown in popularity. Deren et al. [4]

propose to establish a smart city operation brain (SCOB) based on digital twin cities with its primary function being to review high-level designs of the city, plan and review tasks and operations, come up with relevant policies and regulations, and monitor the city operation, among many others. Ruohomäki et al. [10] cite a framework 'mySMARTlife', the paper utilises IoT advancements to build a smart city digital twin. They also present a case study addressing its uses in the energy consumption industry, utilising the digital twin for monitoring and comparing energy usage concerning environmental conditions and human impact. Both papers cite the need to gather accurate and large amounts of data to allow for the proper functioning of the digital twin.

As a renewable energy source, wind power needs to be delivered, monitored, and analysed well to be integrated and used as best it can in an urban setting since it is difficult to achieve the inclusion of renewable energy technologies and fuel the energy system at the same time. Pargmann et al. [14] cover wind farms that are designed and managed using a cloud-based digital twin monitoring technology. Here, the authors show a working model that integrates predetermined parameters and data streams making it easier to create a wind farm that works on digital twin technology.

Chen et al. [15] present digital twins for cars and traffic management, exploring driving problems and highlighting the need for improved data flow within vehicles that covers cars and their connectivity. A framework combining digital twins and learning algorithms is provided to track and examine user behaviour feedback. With the use of these algorithms, a driver's digital behavioural twin can be created in real-time, providing guidelines for safer driving to reduce accidents.

1.5.2 Manufacturing

In this section, we shall discuss manufacturing and its ongoing research constituting the majority of research in digital twins. Due to the vast topics covered, it will be divided into four subsections.

1.5.2.1 Smart Manufacturing

Qi Tao et al. [16] present a '360' view of digital twins for big data in manufacturing and industrial environments, giving a thorough analysis. It highlights the importance of emerging technologies in promoting the development of smart manufacturing and compares the enabling technologies for digital twins. Qi Tao et al. [17], in another paper, researched technologies that can be enabled on digital twins such as IoT, cloud, and AI, and showed their use in digital twins in collaboration with industry. They also elaborate on using digital twin–driven methods to increase product design and manufacturing, as well as operational intelligence and sustainability; there is a need to converge cyber-physical data to close the gap and lay special emphasis on data analytics and IoT.

1.5.2.2 Artificial Intelligence and Simulation

Kuehn [18] proposes the use of digital twins along with AI to make the manufacturing process smooth. They pinpoint critical points in the production process, this highlights their unique goals and ideas when putting a digital twin into practice. With this strategy, businesses may ensure better quality and smoother efficiency by testing, simulating, and optimising manufacturing processes. Yiu et al. [19] present a paper that studies an approach to fault diagnosis through digital twins providing greater accuracy than conventional techniques, monitoring systems that use data analytics, AI, computer vision, and control systems to detect problems in real time through multiple data sources and modelling techniques to enable the accurate diagnosis and prognosis of equipment faults in a factory setting.

1.5.2.3 System Design and Development

Using digital twins in the process of designing and developing industrial systems and processes is another important area to promote their utilisation. Shangguan et al. [20] present a smart manufacturing mechanism using a hierarchical digital twin framework (HDTM) for the designing of cyber-physical systems (CPSs). This approach combines the trends of digital twins and CPS. It allows the authors to explore large-scale system changes and apply the digital twin in a real-time predictive design scenario with the potential for large-scale system modifications, like in applications related to industrial robot design. Karadeniz et al. [21] discuss, with the help of a case study, a concept based on 'eGastronomic things', that is, a digital twin device or processes related to food and its advancements facilitating popularisation of AR (augmented reality) and VR (virtual reality). The authors demonstrate how digital twins can assist in tracking and preserving the performance of 'eGastronomic' processes.

1.5.2.4 Energy Efficient Manufacturing

With the growing concern for the proper use of energy necessary steps need to be taken to increase energy efficiency, a solution for which has been proposed by many authors. Mohamed et al. [22] discuss how not only is better for the environment it also helps with cost, increases profit, and helps future investments. They investigate blockchain-oriented middleware, cloud and fog manufacturing layers, and CPS architecture that can help with increasing energy efficiency. Taking advantage of the researched energy-efficient features helps cut production costs and greenhouse gas emissions. Mawson and Hughes [23] evaluate Industry 4.0's effectiveness in improving production automation, connectivity, and flexibility while highlighting its advancements. It is noteworthy because it uses techniques and frameworks from machine process-level energy consumption analysis to provide a thorough assessment with the help of a case study.

1.5.3 Healthcare

A revolutionary model in patient care has emerged from the convergence and incorporation of digital twins. It holds the potential to change the way healthcare is delivered completely. Within the healthcare domain, Laaki et al. [24] provide a novel digital twin (DT) prototype to analyse the requirements of communication in a mission-critical application such as mobile networks supported by remote surgery. They suggest how a doctor might run simulations including medicines to see their effect before administrating it on the patient. This paper also explains how the unique combination of interdisciplinary fields can lead to complexity in the developmental process. The writers examine some of the developments in Industry 4.0 and AI and how they lessen the difficulties associated with integration, connection, and interdisciplinary research.

Liu et al. [25] discuss the idea of future treatment using cloud computing and digital twins to build a framework that aids in patient monitoring, diagnosis, and prognosis. They propose to achieve this with the help of smart IoT gadgets that can provide real-time information about the patient to the doctor, especially in the case of the elderly. The author proposes the idea of using IoT, cloud computing, and digital twins combined together in order to achieve this [24].

1.6 OPEN RESEARCH

1.6.1 Smart Cities

This section focuses on the research related to digital twins for smart cities which is an under-researched topic. Therefore most research papers only cover a wider area such as a traffic managing system [4], a SCOB [4], and renewable energy [11].

The integration of a digital twin with local infrastructure, as explored in [26], offers a significant opportunity for smart city design and maintenance through the use of 3D modelling [27, 28]. Using data analytics—predictive analytics in particular—to create a digital twin of a smart city is an area of uncharted territory for study. Another way in which it can be implemented is through implementing it in a smart traffic-controlled system as proposed before.

1.6.2 Manufacturing

While the use of digital twins is heavily speculated in research in the manufacturing industry it has not yet been realised due to the challenges mentioned above. One of the first issues that we encounter is the lack of a generalised model for a digital twin that can be utilised for multiple applications. Creating generic digital twins requires modelling and scalability [16].

Another topic that is highly researched is data fusion in various scientific fields; however, it has not yet been explored as much in relation to digital twins. As an example, data fusion can be utilised in digital twin modelling and is a promising area of research [29, 30]. The area of cyber-physical is also lacking in research, this area is based on the fusion of virtual and physical data in digital twin modelling [20].

1.6.3 Healthcare

In the final part of this section, we analyse the research on healthcare with the help of the digital twin application. An example of this is monitoring the health and well-being of patient using IoT devices by simulating the positive or negative changes in their body and preparing for the same.

The modelling and removal of obstacles to digital twin modelling for a human body constitute an important area of scientific research. Once more, the lack of standardised digital twin modelling techniques presents a problem. As mentioned above, Laaki et al. [24] also present the idea of remote surgery which can lead to a promising way to minimise risk.

1.6.4 Quantum Computing

The field of digital twins holds great promise for quantum computing, which processes much faster than classical computing. Quantum algorithms can be used for developing more complex, fine-grained models of physical systems. Such developments may advance applications in drug discovery, material science, and climate modelling significantly. Another way through which quantum computing can be utilised is by means of simulating much more complex systems in real time, thus offering an extremely valuable and rich insight into how these systems can operate and perform. This application will become one of the most significant factors in further developing the capabilities and applications of digital twins when the technology associated with quantum computing continues to advance.

1.7. CONCLUSION

The growth in digital twins has increased in recent years as is evident from the number of papers published by industry leaders and academia on the development of digital twin technology. The growth in the AI, IoT, and IIoT fields helped to enhance the growth of digital twins by enabling various real-life applications. The majority of papers researching digital twins are more in the manufacturing field rather than smart cities or healthcare. The gaps in the research areas in these fields have been presented in the chapter. Algorithms have been applied as an avenue of open research where the effect of AI is becoming a major component which is applied to digital twins. Future research will rely on exploring and scaling AI projects using digital twins. There are many misconceptions and a lack of standardisation regarding the definitions of digital twins. In this chapter, a clear definition of digital twins has been presented in different areas of interest, such as healthcare, smart cities, and manufacturing. This chapter discusses the challenges and key empowering technologies of each area that have been found by the researchers. In general, the literature contains fewer works on large-scale digital twin projects when compared to small-scale digital twin projects as there is a lack of expertise in implementing larger digital twins. A wide range of publications have been produced in the fields of manufacturing and healthcare on the predictive maintenance of machines and investigation of health status and monitoring of human users. Also, the review analysis and open research on each area have been shown.

REFERENCES

1. A. Bilberg and A. A. Malik, "Digital twin driven human robot collaborative assembly," *CIRP Annals*, 68(1), 499–502, 2019.
2. C. Mandolla, A. M. Petruzzelli, G. Percoco, and A. Urbinati, "Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry," *Computers in Industry*, 109, pp. 134–152, 2019.
3. N. Mohammadi and J. E. Taylor, "Smart city digital twins," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2017, pp. 1–5.
4. L. Deren, Y. Wenbo, and S. Zhenfeng, "Smart city based on digital twins," *Computational Urban Science*, 1, 1–11, 2021.
5. G. Mylonas, et al., "Digital twins from smart manufacturing to smart cities: A survey," *IEEE Access*, 9, 143222143249, 2021.
6. Q. Qi, and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," *IEEE Access*, 6, 3585–3593, 2018.
7. P. Armeni, et al., "Digital twins in healthcare: is it the beginning of a new era of evidence-based medicine? a critical review," *Journal of Personalized Medicine*, 12(8), 1255, 2022.
8. A. Čolaković, and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, 144, 17–39, 2018.
9. A. Al-Fuqaha, et al., "Internet of things: A survey on enabling technologies, protocols, and applications" *IEEE Communications Surveys and Tutorials*, 17(4), 2347–2376, 2015.
10. T. Ruohomäki, et al., "Smart city platform enabling digital twin," In *2018 International Conference on Intelligent Systems (IS)*, IEEE, 2018.
11. J. Bofill, M. Abisado, J. Villaverde, and G. A. Sampedro, "Exploring Digital Twin-Based Fault Monitoring: Challenges and Opportunities," *Sensors*, 23(16), 7087, 2023.
12. S. E. Bibri and J. Krogstie, "The core enabling technologies of big data analytics and context-aware computing for smart sustainable cities: A review and synthesis," *Journal of Big Data*, 4(1), 38, 2017.
13. H. Sarker, Iqbal, "Machine learning: Algorithms, real-world applications and research directions." *SN Computer Science*, 2.3, 2021, 160.
14. H. Pargmann, D. Euhausen, and R. Faber, "Intelligent big data processing for wind farm monitoring and analysis based on cloud-technologies and digital twins: A quantitative approach," in *2018 IEEE 3rd international conference on cloud computing and big data analysis (ICCCBDA)*, IEEE, 2018.
15. X. Chen, et al., "Digital behavioral twins for safe connected cars," in *Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems*, 2018.
16. F. Tao and M. Zhang, "Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing," *IEEE Access*, 5, 20418–20427, 2017.
17. F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Transactions on Industrial Informatics*, 15(4), 2405–2415, 2019.
18. W. Kuehn, "Simulation in digital enterprises," in *Proc. 11th Int. Conf. Comput. Modeling Simulation ICCMS*, 2019, pp. 55–59.
19. Y. Xu, Y. Sun, X. Liu, and Y. Zheng, "A digital-twin-assisted fault diagnosis using deep transfer learning," *IEEE Access*, 7, 19990–19999, 2019.
20. D. Shangguan, L. Chen, and J. Ding, "A hierarchical digital twin model framework for dynamic cyber-physical system design," in *Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering*, 2019.

21. A. M. Karadeniz, I. Arif, A. Kanak, and S. Ergun, “Digital twin of eGastronomic things: A case study for ice cream machines,” in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–4.
22. N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, “Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories,” *IEEE Access*, 7, 18008–18020, 2019.
23. V. J. Mawson and B. R. Hughes, “The development of modelling tools to improve energy efficiency in manufacturing processes and systems,” *Journal of Manufacturing Systems*, 51, 95–105, 2019.
24. H. Laaki, Y. Miche, and K. Tammi, “Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,” *IEEE Access*, 7, 20325–20336, 2019.
25. Y. Liu, et al., “A novel cloud-based framework for the elderly healthcare services using digital twin,” *IEEE Access*, 7, 49088–49101, 2019.
26. T. Ruohomaki, E. Airaksinen, P. Huuska, O. Kesaniemi, M. Martikka, and J. Suomisto, ‘‘Smart city platform enabling digital twin,’’ in *Proc. Int. Conf. Intell. Syst. (IS)*, Sep. 2018, pp. 155–161.
27. M. Javaid, A. Haleem, and R. Suman, “Digital twin applications toward industry 4.0: A review,” *Cognitive Robotics*, 3, 71–92, 2023.
28. V. V. Tuhaise, J. H. Mbatu Tah, and F. H. Abanda, “Technologies for digital twin applications in construction,” *Automation in Construction*, 152, 104931, 2023.
29. S. Bakhshi, et al., “Digital twin applications for overcoming construction supply chain challenges,” *Automation in Construction*, 167, 105679, 2024.
30. L. Jin, et al., “Big data, machine learning, and digital twin assisted additive manufacturing: A review,” *Materials & Design*, 244, 2024, 113086,ISSN 0264-1275.

2 Using Blockchain-Enabled Digital Twins to Optimize Healthcare Workflows and Improve Efficiency

R. Palraj, Swagata Sarkar, Kiran Kakade, and Ashok Vajravelu

2.1 INTRODUCTION

A lot has changed in our work, our healthcare, and our daily lives in the last few years. All of these changes are due to the popularity of smart devices [1]. When smart building and smart home technologies work together, they make settings that are always changing and improve our health and lives in more ways than one. This research will talk about some of the many things that are pushing the creation of smart settings.

2.2 A BRIEF LOOK AT SMART ENVIRONMENTS

Getting smarter around our homes has significantly changed the way we interact with them. Homes, hospitals, and smart buildings are all part of these smart settings. Settings that can change and adapt are made possible by new technologies that work together. The Internet of Things (IoT) makes this change possible. IoT has made it possible for everything in our lives to talk to each other and share information [2, 3]. These are what smart settings do. They are in charge of many things, from hospitals that keep an eye on patients all the time to home automation systems that control lights and internal temperature [4]. All of this means that these places will be more comfortable, work better, and offer more personalized experiences. Smart settings are always getting better and more useful as monitoring technologies improve and computer power grows [5, 6].

Various tools, including gadgets and home monitoring devices, are increasingly being used to gather real-time health data. These tools track vital indicators such as

DOI: 10.1201/9781003532286-2

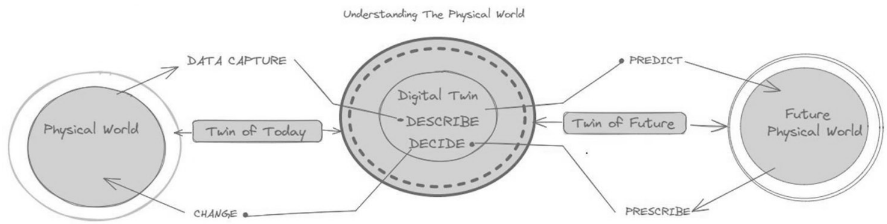


FIGURE 2.1 A digital twin

blood pressure, heart rate, and sleep patterns—key metrics that offer deep insights into an individual's overall health. When this continuous stream of health data is integrated with digital twin technology—which creates virtual replicas of real-world systems—it enables a comprehensive view of both a person's health and their environment [7].Ongoing analysis of this data allows for the early detection of potential health issues, enabling timely interventions and empowering patients to actively monitor their health in real time [8]. Improved use of technology and more efficient system management [9, 10] allow healthcare providers to optimize resources, resulting in more sustainable and effective operations. Ultimately, this leads to a better patient experience, with care that is more closely monitored, personalized, and outcome-driven.

2.2.1 Digital Twin in Healthcare

Digital twins are virtual replicas of real-world systems or processes. In healthcare, digital twins can be created to represent patients and their medical histories, or the physical state and function of medical devices and equipment. By using these digital representations, healthcare providers can monitor and analyze data in real time, enabling them to detect and respond to changes in a patient's health more quickly and accurately. Digital twins can be particularly useful in managing chronic conditions, such as diabetes or cardiovascular disease, where regular monitoring and adjustments to treatment plans are critical. Additionally, digital twins can be used to simulate clinical trials and provide valuable insights into the effectiveness of treatments before they are tested on human subjects [11]. Figure 2.1 represents a digital twin, in which continuous data flows from the physical world and after analysis and AI algorithms, a virtual representation is created. Based on the virtual representation predictions are performed on the virtual environment to generate the future world and the feedback is sent to the physical world. The feedback loop continues to improve the digital twin.

2.2.2 Research Questions

The chapter is structured around the following key research questions:

- **R1:** In smart settings, how can digital health systems with sensors and digital twin technology improve healthcare and make patients' lives better?

R2: Is it feasible to integrate all the technologies required to create a digital twin for optimizing healthcare workflow?

2.2.3 Structure of the Chapter

This chapter is organized into different sections to help the reader understand the importance of smart settings. Section 2.1 is an introduction to digital twins. Section 2.2 is about foundational technologies, which are the main technologies that make smart settings work. Section 2.3 is a look back at the study that has been done on how to mix digital health, smart settings, and healthcare services is presented. Section 2.4 explains the quality of the design, highlighting the principles and criteria that ensure its effectiveness and reliability. Section 2.5 explains the healthcare workflow enabled by digital twin technology integrated with blockchain systems. Section 2.6 explains the GlaxoSmithKline (GSK) case study. The case study explains how GSK used digital twin technology to accelerate vaccine development. Section 2.7 concludes the chapter.

2.3 LITERATURE REVIEW

Digital twins have emerged as a transformative technology by providing unprecedented opportunities for process optimization, quality control, and decision-making [12]. This technology involves the creation of a virtual counterpart that dynamically mirrors its physical counterpart, enabling bidirectional data flows and real-time monitoring. However, the implementation of digital twins poses several challenges, particularly in the areas of uncertainty quantification and optimization, which are crucial for realizing the full potential of this technology.

Uncertainty quantification is a critical component of digital twins, as it allows for the incorporation of variability and error in the computational models, ensuring that decisions are made with a clear understanding of the associated risks. Optimization methods are also essential, as they enable the identification of the most effective control and maintenance strategies, leading to improved performance and efficiency [13, 14].

The development of digital twins is further enhanced by the integration of AI and blockchain technologies. AI can be leveraged to improve the accuracy of computational models, while blockchain can provide secure and transparent data management, enabling the seamless integration of data from various sources. The section below provides a detailed overview of the key technologies involved in digital twins.

2.3.1 Foundational Technologies

A group of simple technologies has made it possible for smart settings to change and grow. The IoT (Internet of Things) and IoMT (Internet of Medical Things) allow things that are connected to talk to each other without issue, which is what makes smart environments possible. In healthcare, the IoMT makes it possible for medical equipment to connect to the internet, which makes tracking and collecting data from afar easier.

Connection tools (such as Bluetooth and Wi-Fi) that send that information, and data processing units that do the first analysis. Gateways are like go-betweens. They might do edge computing before sending data to cloud platforms to be stored, analyzed, and displayed. This analysis enables organizations to derive actionable insights for decision-making, such as predicting equipment failures or optimizing production processes, ultimately leading to improved operational efficiency and reduced costs across industries.

Interoperability between devices is made possible by standards such as IEEE 1451 [1]. Studies that look at how AI can be used in real life have shown that it can help save energy, make security better, and make user experiences more personalized in these smart places [15].

Information modelling is essential for ensuring data consistency, integrity, and interoperability across systems and applications. It helps organizations effectively manage and leverage their data assets, supporting various activities such as data integration, analytics, and decision-making. By defining clear and standardized information models, organizations can streamline communication, collaboration, and innovation in today's data-driven world.

Augmented reality (AR), virtual reality (VR), mixed reality (MR), 3D scanning, and photogrammetry play vital roles in enhancing the capabilities and applications of digital twins across various industries. By leveraging these immersive and data capture technologies, digital twins can offer more realistic, interactive, and dynamic representations of physical assets, processes, and environments [16, 17]. AR enables users to overlay digital information onto the real world, providing contextual insights and instructions within the digital twin environment. VR immerses users in fully virtual replicas of physical assets, allowing them to explore and interact with digital twins in a controlled and immersive manner. MR combines elements of both AR and VR, enabling users to interact with holographic representations of physical objects within their environment. 3D scanning and photogrammetry facilitate the creation of accurate and detailed 3D models for digital twins by capturing the geometry and appearance of real-world assets. These technologies enhance the visualization, analysis, and decision-making capabilities of digital twins, empowering organizations to optimize operations, improve maintenance, and innovate product design and development processes. Whether it's simulating complex scenarios, training personnel, or visualizing real-time data, AR, VR, MR, 3D scanning, and photogrammetry enrich the digital twin experience and drive value across industries [18]. Figure 2.2 highlights all the enabling technologies of digital twins.

Table 2.1 presents a list of the key foundational technologies required for integration with smart environments. It provides a comprehensive overview of their characteristics, including both strengths and limitations. For instance, in the context of remote monitoring and core technologies, cells that are not applicable or lack functionality are indicated with a hyphen (-), signifying that they cannot be used directly. IoT, IoMT, AI, ML, and sensors are some of the foundational technologies that make smart ecosystems work. They connect devices and automate tasks. The features of a smart home focus on how systems are linked to each other. Digital health integration uses data powered by AI and health communities that are linked together. Some

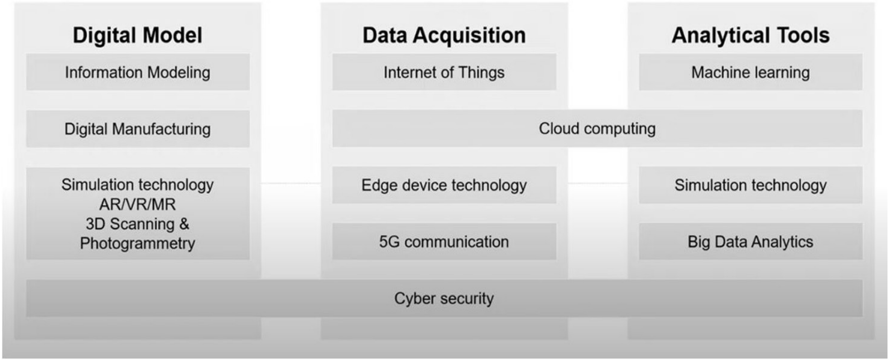


FIGURE 2.2 Enabling technologies of digital twins

aspects of a smart hospital allow care for patients to be given automatically and data to be shared in real time. Inside tracking tools help location-based services (LBS) to arrive at situations quickly and give each customer a unique service.

2.3.2 Blockchain

Blockchain is a large, safe, and decentralized database of well-organised information [19, 20]. It is a database or global log that is organized into a series of blocks, with an event stored in each block. The record is controlled by the nodes of the spread network, but it doesn't belong to any one person or group. Instead, it is controlled by the nodes of the distributed network. That is because a copy of the ledger is stored on each node (user) of the decentralized network, authentication is done using cryptography, and all transactions are timestamped and completed using cryptographic hashing [21, 22]. This means that no one can change, delete, or steal the information in the record. During the hashing process, data of different lengths are turned into digests of a set length. It's called a hash. It's hard to guess how the hash will change if the data that was put in changes.

Any block in the record has the hash of the block before it and the events that were used to make that block's hash. If there was a change in any of the blocks before this one, the hash of that block would be invalid, and the next hash would not work either. If most of the nodes agree on something, a new transaction can be added to the block. It is the group of nodes that builds trust by encoding the smart contracts [23–25].

There are four main types of blockchain ledgers: Public, private, consortium, and hybrid. For example, anyone can join a public ledger, but only certain people can join a private ledger. More than one node can decide who can join a consortium ledger, and a hybrid ledger mixes private and public ledgers [26].

There are five ways that blockchain technology could help with the shift to interoperability based on the patient: (1) Rules for digital access, (2) collecting data, (3) data flow, (4) patient identity, and (5) data that can't be changed. To get around these issues, pharmaceutical and research companies are beginning to switch from

TABLE 2.1
Comparing Core Technologies.

Parameters	Foundational Technologies	Smart HomeCharacteristics	Telehealth	Home-Based Care Technologies	Digital HealthIntegration	Smart HospitalFeatures	Location-BasedServices
Connectivity	IoT, IoMT, AI, ML, Sensors	Interconnected Ecosystems	Platform Connectivity	Interconnected Devices	Interconnected Health Ecosystems	Immediate Data Sharing	Indoor Positioning Systems
Automation	AI, ML	Automated Systems	-	Automation of Health Monitoring	-	Automated Patient Care	-
Data Analysis	AI, ML	-	AI-Driven Analytics	Health Analytics Driven by AI	AI-Driven Health Analytics	-	-
Remote Monitoring	IoT	Enabled by Sensors and Automation	RPM System	Things You Wear for Your Health	-	Sharing Data in Real Time	-

the clinical data management systems they use now, such as Oracle Clinical software and SigmaSoft's DMSYS software, to new cyber-physical systems. With blockchain-based digital twins, some of these issues might be able to be fixed. This tech keeps patient health data, electronic health records (EHRs), and mobile health (mHealth) safe. A medical cyber-physical system (MCPS) network model built on blockchain was offered as a safe way to share medical data. Blockchain tech could help fix a lot of issues with medical records (EHRs and EMRs (emergency medical records)). There are problems with keeping data safe, organizing it, and keeping it secure. There are also privacy issues for people who use mHealth. This technology is safe for storing private information such as medical records, doctor's notes, e-prescribing, study results, and processes. According to BCT (blockchain technology), drug development studies could be improved by giving researchers a safe way to share data. The coming together of BCT, CPSs (cyber-physical systems), and CTs (clinical trials) is still very new, and there isn't much research on this topic yet. At a high level, BCT is used to find patients and make sure that rules about human subjects are followed. It has been made possible to handle and keep an eye on data in CTs with more than one location. People made a tool called "BlockTrial" to help them carry out smart contracts about trials on a private network more easily. It is shown how a blockchain-based system can help patients and parties keep track of information about permissions. When it comes to managing permission, a blockchain-based method has been shown to work well. BCT may be a good way to handle data in eHealth and CTs because it is safe, clear, and can't be changed.

2.4 QUALITY BY DESIGN (QBD)

Quality by design (QbD) is a way to make sure that the planning, building, and making of drugs is done well by using statistical, analytical, and risk-management tools. The ICH Q8 standard calls it "a planned approach to development that starts with clear goals and focusses on understanding the product and process and keeping an eye on the whole process, using good science and quality risk management." QbD has been used in many areas of biotechnological and pharmaceutical progress, including biopharmaceuticals, bioprocessing, abbreviated new drug applications (ANDAs), drug formulation and delivery, pharmaceutical products, analytical methods, biotechnological products, drug development, nano pharmaceutical products, monoclonal antibodies, and CTs. Pharmaceutical quality by design (QbD) includes planning production methods that will ensure the quality of set formulations and improve development speed, ability, and formulation design. The idea that quality should be built into a product was backed up by Guidance for Industry PAT, which is a framework for new drug development, manufacturing, and quality assurance. It states that quality should not be tested into goods; it should be built-in or should be by design.

The following are guidelines used in drug development: ICH PAT Guideline (2004), ICH Q8 (R2) (Pharmaceutical Development, 2014), ICH Q9 (Quality Risk Management, 2014), ICH Q10 (Pharmaceutical Quality System, 2009), ICH Q11 (Development and Manufacture of Drug Substance, 2011), and ICH Q12 (Technical and Regulatory Considerations for Pharmaceutical Product Lifecycle Management, 2020). The main goals of QbD are to get clear quality standards based on clinical performance, lower the variability of formulations, and create an organization for change after approval by making product and process design, understanding, and control better to stop product variability that leads to rejects, scrapping, and reprocessing.

Years ago, QbD was a big part of how drugs were planned and made. It is only now beginning to play a role in CTs, though. Not long ago, QbD was used in research and clinical studies to help make new drugs safer, better, more effective, cheaper, and easier to get. Quality in CTs mostly means what the donors think about how likely it is that the results are correct as a whole. GCP (good clinical practice)-based tracking methods are at the heart of many of the most popular ways to make things better. ICH E8 (R1) says that QbD in clinical research makes sure that the safety of the subjects and risk management methods are taken into account so that the quality of the study and the dependability of the results are better. The plan–do–check–act (PDCA) method is what the QbD in CTs is based on. Plan to: a) Figure out the quality factors that are important and must be met during the CTs; b) figure out the steps that will be taken to measure quality for the quality factors that have already been set; and c) systematically figure out the safe areas of the planned CT factors, with the goal of finding and ranking the risks to quality. Do put in place good plans for managing risks before, during, and after the CTs. Check, measure, or keep an eye on quality performance to see if quality factors are being met. This will help you figure out the risks, their amounts, and where they come from.

Take action: deal with quality problems by using the right corrective and/or preventive control methods. The movement and merging of data between the PDCA steps in QbD are very important for making the method more useful and improving quality. Adding a KMS (knowledge management system) to the QbD design can make it possible for activities to share data in real time and in an integrated way. It is very important to make sure that information is shared and used effectively within QbD activities. It also makes it easier to look over information from a wide range of different sources and then use that information to figure out how important the different quality traits are. QbD combined with KMS could help manage the flow of information that leads to the creation of process strategies, the sharing of technology, and the use of this information to make processes better all the time. A centralized data-sharing method is often used to share information and knowledge between the people and actions that make QbD possible, but it doesn't work very well. These kinds of storage systems might not work because the tools are spread out geographically and have different types of operation systems. The amount of data merging for QbD in CTs needs to be raised by using a strong knowledge management method. A shared, unapproved data store and management system could make the knowledge management process better by making it easier for everyone to share data. Also, the information that QbD creates is private and sensitive, and if it is misused, it could hurt deals, company policies, and user privacy. The information about the QbD should be kept in a very safe place where no one in power can change it. The quality will be better if the QbD tasks and drivers can share data better, which is not a surprise. This paper tries to fix the problems listed above by adding BCT to QbD through the creation of DT (digital twins). The goal is to create a system for sharing and managing information that works across multiple computers. The created DT could make the CT better by giving the QbD activities more power by creating a safe network for sharing knowledge.

2.5 HEALTHCARE WORKFLOW WITH DIGITAL TWINS BASED ON BLOCKCHAIN SYSTEMS

To truly grasp the importance of using blockchain-enabled digital twins for optimizing healthcare workflows and improving efficiency, we must first understand the concept of healthcare workflows. Put simply, healthcare workflows refer to the sequence of tasks and activities involved in delivering healthcare services to patients. These workflows can be as simple as scheduling an appointment or as complex as managing a patient's entire medical journey from diagnosis to post-operative care. Efficient healthcare workflows are essential for ensuring patient safety, reducing healthcare costs, and improving patient outcomes.

However, with the increasing complexity of medical treatments and the increasing number of patients seeking care, traditional manual processes can no longer keep up with the pace of change. In response to these challenges, healthcare providers are turning to technologies such as blockchain and digital twins to optimize their healthcare workflows and improve overall efficiency.

The application of digital twins in healthcare is particularly compelling, as they offer a unique opportunity to virtualize complex medical environments and simulate various scenarios to support improved decision-making. One area where digital twins are being increasingly explored is in the virtualization of standalone assets, such as medical devices, structures, and even individual patients. This approach allows for the creation of digital replicas that can be used to model the state and behaviour of these physical entities, enabling healthcare professionals to optimize their use, predict maintenance needs, and personalize treatment plans.

However, the true potential of digital twins in healthcare lies in the ability to virtualize entire ecosystems, encompassing multiple related assets and their interactions. By creating digital representations of complex healthcare workflows, such as trauma management, digital twins can provide a holistic view of the system, allowing for the identification of bottlenecks, the optimization of resource allocation, and the simulation of the entire process so that risk can be minimized. These are some of the points highlighting the importance of digital twin in medical workflow improvement.

- By creating a digital replica of a patient, healthcare providers can simulate how different treatments or therapies would affect them. This allows for personalized treatment plans and predictive diagnostics. For example, a digital twin of a heart could be used to simulate the impact of a drug or surgery.

- Surgeons can create a digital twin of a patient's anatomy to simulate complex surgeries before performing them. This enables precise planning, reduces risks, and increases the chances of successful outcomes. For instance, digital twins of organs or bones allow surgeons to test different surgical approaches.
- Before implanting medical devices (e.g., pacemakers, prosthetics) a digital twin of the device and the patient can simulate how it will function in the body. This helps optimize the design of the device and ensures compatibility with the patient's physiology.
- Digital twins of patient populations can be used to simulate drug interactions, effects, and trial outcomes, reducing the need for physical trials. These virtual trials can help in identifying the most effective treatments more quickly and safely.
- Hospitals can create digital twins of their operational processes, such as patient flow, resource allocation, or emergency response times. Simulating these processes helps optimize hospital operations, ensuring efficient use of resources and better patient care.
- Medical students and professionals can use digital twins of patients to simulate various medical conditions or emergency scenarios. This provides a risk-free environment for learning, improving diagnosis skills, and decision-making.

2.6 GLAXOSMITHKLINE (GSK): USING ADVANCED TECHNOLOGY TO ACCELERATE VACCINE DEVELOPMENT

Developing vaccines has historically been a time-consuming process, often taking more than a decade. That's in part because there are so many phases, each playing an integral part in helping to save lives around the world. Traditional vaccine development and production progresses through many phases, with few digital connections between them. These include:

- Understanding the pathogen via genetic sequencing and other methods.
- Selecting the best vaccine candidate.
- Conducting extensive preclinical testing, including proof of concept studies.
- Developing the processes to manufacture the vaccine.
- Running robust in-human clinical trials to evaluate safety and efficacy.

The evidence generated from the above forms the basis of the vaccine's regulatory filing and approval. Once approved, the vaccine can then be manufactured and distributed at a large scale – with significant lead time allocated to provide quality control. By embracing digitalization, GSK has identified a tremendous potential to optimize each phase of vaccine development and production. Working closely with Siemens and Atos, two of the world's leading companies in digital transformation and technology, they have piloted a "digital twin" – a complete and real-time simulation of the vaccine manufacturing process.

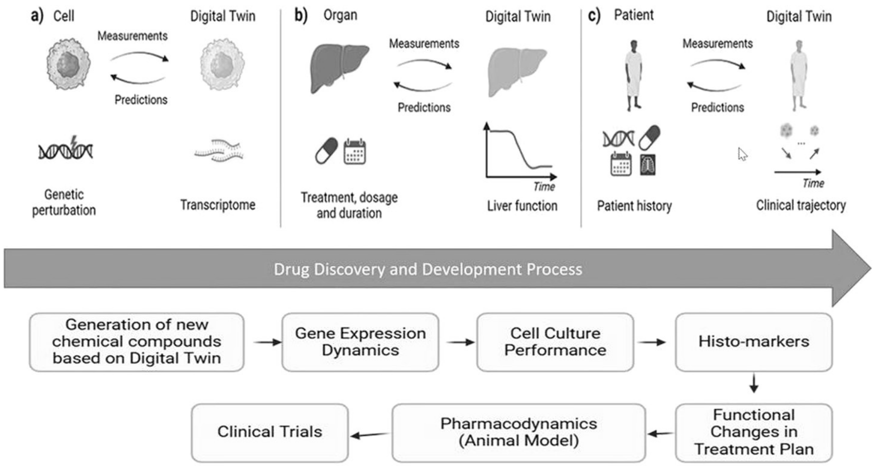


FIGURE 2.3 Drug discovery and development Pprocess

GSK worked with French IT firm Atos and the engineering company Siemens to pilot a digital twin of one of its vaccine manufacturing processes, specifically a process for the production of a particular vaccine adjuvant [5]. Developing vaccines is a lengthy and resource-intensive process that involves multiple stages, including research, clinical trials, manufacturing, and distribution. The traditional vaccine development cycle can take several years, but during global health crises, such as pandemics, the need for rapid vaccine development becomes urgent. GSK sought to use **digital twin technology** and **blockchain** to reduce development time, improve collaboration, and ensure transparency and security across the supply chain [12, 27].

By using digital twins of biological systems, GSK can simulate how vaccines interact with the human immune system. This allows researchers to test different vaccine formulations in a virtual environment before moving to physical trials. This speeds up the research phase by identifying the most promising candidates early on. GSK created digital twins of its manufacturing processes to optimize production lines for new vaccines. These digital replicas allow them to simulate the entire production chain, identifying bottlenecks, improving yield, and ensuring that the vaccine is produced at the highest quality. This is especially critical when scaling up production during pandemics. Figure 2.3 highlights the use of digital twins in drug discovery and development.

2.6.1 Blockchain Technology for Transparency and Security

GSK integrated **blockchain technology** to ensure security, traceability, and transparency across the vaccine development and distribution processes. Blockchain creates a decentralized, tamper-proof ledger that records every transaction or event in the supply chain. Here's how GSK applied it:

- **Clinical Trial Data Integrity:** During clinical trials, large amounts of data are collected from different sites, ensuring its integrity is crucial for regulatory approvals. Blockchain ensures that data from trials is securely recorded and cannot be altered, ensuring transparency for regulatory authorities such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA). Every participant's data is time-stamped and verified, preventing fraud and enabling faster, more reliable audits.
- **Supply Chain Management:** Once a vaccine is approved, blockchain helps track the movement of vaccine doses through the supply chain. Every step, from manufacturing to distribution to hospitals or clinics, is recorded on a blockchain ledger. This prevents counterfeiting, ensures proper storage conditions, and reduces delays in distribution. In the case of recalls or safety concerns, blockchain provides an accurate trail to quickly identify affected batches.
- **Smart Contracts:** GSK uses smart contracts (self-executing contracts on the blockchain) to automate agreements with suppliers, distributors, and logistics providers. These contracts are triggered automatically once predefined conditions are met (e.g., successful delivery of vaccines), ensuring faster, error-free transactions and reduced administrative overhead.

2.6.2 Benefits Realized by GSK

- **Faster Time-to-Market:** By using digital twins to simulate and optimize every aspect of vaccine development and production, GSK was able to significantly reduce the time required for new vaccine candidates to enter clinical trials and eventually reach the market.
- **Improved Accuracy and Quality:** Simulating biological responses and manufacturing processes helped improve vaccine efficacy and reduced the risk of manufacturing defects. This was especially important during crises such as the COVID-19 pandemic when vaccine production needed to be ramped up rapidly without sacrificing quality.
- **Enhanced Supply Chain Transparency:** Blockchain technology ensured full visibility across the vaccine supply chain, preventing fraud, ensuring authenticity, and improving patient safety by guaranteeing that vaccines were stored and transported under optimal conditions.
- **Cost Efficiency:** Automation of supply chain processes and smart contracts reduced administrative costs and errors, resulting in a more cost-efficient system.
- **Regulatory Compliance:** GSK's use of blockchain for clinical trial data helped streamline regulatory audits and approvals, reducing the time and effort required to verify trial data. This transparency also builds trust with patients, regulators, and partners.

2.7 CONCLUSION

Today, patient-centered care is more important than ever. This means that a lot of people need to be able to talk to each other without fear. Sharing information about patients safely is important, but the process can take a lot of time for everyone.

So, automating a way to share data with an agency, such as the patient's digital twin, can help the different groups that need to work together to provide care for patients communicate more effectively. As a safe way to share personal health information, this research suggests that patients have a digital twin that is protected by blockchain. Ethereum's smart contracts protect people's privacy and safety and give them control over their own medical details. Safety measures that have been around for a long time and are easy on computers are used to guard the digital twins' information and files. We judge the quality of our study by comparing it to other works and looking at the results of some experiments. Using a permissioned blockchain, our suggested system can be added to healthcare platforms that are already in use. This gives users the utmost safety and security. We want to complete more studies so that the patient's digital twin can do more on its own.

REFERENCES

1. Z. Johnson and M. J. Saikia, "Digital twins for healthcare using wearables," *Bioengineering*, vol11, (6, 2024.
2. Y. Zhang, K. Chen, Y. Weng, Z. Chen, J. Zhang, and R. Hubbard, "An intelligent early warning system of analyzing Twitter data using machine learning on COVID-19 surveillance in the US," *Expert Systems with Applications*, 198, 116882, 2022.
3. S. Zeadally, R. Hunt, Y. S. Chen, and A. Irwin, "Vehicular cyber-physical systems: Challenges, design, and deployment," *IEEE Transactions on Vehicular Technology*, 58, 648–656, 2009.
4. A. Manocha, Y. Afaq, and M. Bhatia, "Digital twin-assisted blockchain-inspired irregular event analysis for eldercare," *Knowledge-Based Systems*, 260, 110138, 2023.
5. F. Kansteiner, "After triumphant pilot. GSK eyes 'digital twins' to fine-tune vaccine production, development," *Fierce Pharma*, 23 June 2021.
6. M. Dharmar, N. Kuppermann, P. S. Romano, N. H. Yang, T. S. Nesbitt, J. Phan, C. Nguyen, K. Parsapour, and J. P. Marcin, "Telemedicine consultations and medication errors in rural emergency departments," *Pediatrics*, 132, 1090–1097, 2013.
7. J. Craig and V. Petterson, "Introduction to the practice of telemedicine," *Journal of Telemedicine and Telecare*, 11, 3–9, 2005.
8. J. Bort-Roig, N. D. Gilson, A. Puig-Ribera, R. S. Contreras, S. G. Trost, and J. J. Carrasco, "Measuring and influencing physical activity with smartphone technology: A systematic review," *Sports Medicine*, 44, 671–686, 2014.
9. S. Omboni, A. Guarda, and R. J. McManus, "Telemedicine before and after the COVID-19 pandemic: A protocol for systematic review and meta-analysis," *BMJ Open*, 10, e040871, 2015.
10. H. M. Phatak and Y. Z. Mehrjerdi, "Real-time monitoring of patients with chronic heart failure using a wireless implantable hemodynamic monitoring system," *Studies in Health Technology and Informatics*, 136, 447–452, 2008.
11. S. McLean, A. Sheikh, K. Cresswell, U. Nurmatov, M. Mukherjee, A. Hemmi, and C. Pagliari, "The impact of telehealthcare on the quality and safety of care: A systematic overview," *PLoS One*, 6, e22178, 2011.

12. T. Nugent, D. Upton, and M. Cimpoesu, “Improving data transparency in clinical trials using blockchain smart contracts,” *F1000Research*, 5, 2541, 2016. 21
13. R. Bashshur, C. R. Doarn, J. M. Frenk, J. C. Kvedar, J. O. Woolliscroft, and J. Zollo., “Telemedicine and the COVID-19 pandemic, lessons for the future,” *Telemedicine and e-Health*, 26, 571–573, 2013.
14. S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, “A review of wearable sensors and systems with application in rehabilitation,” *Journal of NeuroEngineering and Rehabilitation*, 9, 21, 2012.
15. R. Sahal, S. H. Alsamhi, K. N. Brown, D. O’Shea, and B. Alouffi, “Blockchain-based digital twins collaboration for smart pandemic alerting: Decentralized COVID-19 pandemic alerting use case,” *Computational Intelligence and Neuroscience*, 2022(1), 7786441, 2022.
16. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in healthcare: a systematic review,” in *Healthcare* (Vol. 7, No. 2, p. 56), Multidisciplinary Digital Publishing Institute, 2019.
17. C. Bentley, S. Cressman, K. van der Hoek, K. Arts, J. Dancey, and S. Peacock, “Conducting clinical trials—costs, impacts, and the value of clinical trials networks: a scoping review,” *Clinical Trials*, 16(2), 183–193, 2019.
18. A. Sertkaya, H. H. Wong, A. Jessup, and T. Beleche, “Key cost drivers of pharmaceutical clinical trials in the United States,” *Clinical Trials*, 13(2), 117–126, 2016.
19. M. Gold, J. Amatniek, M. C. Carrillo, J. M. Cedarbaum, J. A. Hendrix, B. B. Miller, J. M. Robillard, J. J. Rice, H. Soares, M. B. Tome, et al., “Digital technologies as biomarkers, clinical outcomes assessment, and recruitment tools in Alzheimer’s disease clinical trials,” *Alzheimer's & Dementia*, 4, 234–242, 2018.
20. J. D. Ralston, D. Revere, and L. S. Robins, “Patient experience with a monitored electronic pill box: A qualitative study,” *JMIR mHealth and uHealth*, 7, e13756, 2009.
21. A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, “Blockchain in healthcare and health sciences—A scoping review,” *International Journal of Medical Informatics*, 134, 104040, 2020.
22. Z. Saadati, C. P. Zeki, and R. Vatankhah Barenji, “On the development of blockchain-based learning management system as a metacognitive tool to support self-regulation learning in online higher education,” Interactive Learning Environments, 31(5), 3148–3171.
23. T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, 24(6), 1211–1220, 2017.
24. M. Benchoufi and P. Ravaud, “Blockchain technology for improving clinical research quality,” *Trials*, 18(1), 1–5, 2017.
25. S. R. Evans, “Common statistical concerns in clinical trials,” *Journal of Experimental Stroke & Translational Medicine*, 3(1), 1, 2010.
26. T. T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, “Comparison of blockchain platforms: a systematic review and healthcare examples,” *Journal of the American Medical Informatics Association*, 26(5), 462–478, 2019.
27. D.-Y. Jeong, et al., “Digital twin: Technology evolution stages and implementation layers with technology elements,’ *IEEE Access*, 10, 52609–52620, 2022.

3 Automated Insurance Claim Settlement Leveraging Blockchain and Digital Twin Technologies in Healthcare 5.0

Ramya R S, Ramesh Babu D R, Krishnan Rangarajan, and Nikil Dixit

3.1 INTRODUCTION

Effectively handling medical insurance claims is a critical component of the constantly changing healthcare industry for both patients and providers. Inefficiencies, hold-ups, and security issues have frequently plagued the conventional approaches to claim settlement and compensation. Recent technological developments, especially the introduction of blockchain, present encouraging opportunities to overcome these issues. This chapter presents a cutting-edge platform that combines blockchain technology with cloud services to revolutionize the medical insurance claim settlement procedure. The understanding of the inherent sensitivity and confidentiality of medical records used in the claims process is at the core of this innovation. The platform aims to transform the way these documents are gathered, protected, and handled by utilizing blockchain technology, which will simplify the complete refund process. This chapter gives a summary of the state of medical insurance claim settlement today, emphasizing the main issues and inefficiencies with the current frameworks. Additionally, it explores the core ideas of blockchain technology and its possible uses in the medical field [1], providing the foundation for comprehending our suggested remedy. The goals and scope of this study are then described, and a synopsis of the format and arrangement of the following sections is provided. Through this initiative, we hope to clarify the nuances of our blockchain-enabled platform and highlight its revolutionary potential in transforming the medical insurance claim settlement and reimbursement industry. Furthermore, a functional credit information

DOI: 10.1201/9781003532286-3

system is essential for financial infrastructure because it helps resolve the information asymmetry that exists between lenders and borrowers, lowering default risk and enhancing credit distribution. Credit scoring has historically depended on manual assessment by loan officers. However, computerized credit scoring systems that employ algorithms to evaluate creditworthiness based on a number of factors were brought about by digitalization. Better financial access and inclusion have been made possible by this change, which has made assessments more accurate and efficient. Financial organizations can make better lending judgments by using data points such as the frequency of transactions pertaining to critical services, the regularity of mobile phone bill payments, and other digital footprint indications. This comprehensive assessment guarantees prompt access to essential medical services when they are most needed and helps close gaps in healthcare funding.

For financial infrastructure, a functional credit information system is essential. By addressing the information asymmetry that exists between lenders and borrowers, it improves credit distribution and lowers the default risk. Credit scoring has historically depended on manual assessment by loan officers. Nevertheless, computerized credit scoring systems that employ algorithms to evaluate creditworthiness based on a number of factors were introduced by digitization.

3.1.1 Traditional System of Medical Claim Reimbursement

The present medical claim reimbursement system in India is primarily manual, labor-intensive, and rife with inefficiencies. In order to start the claim reimbursement procedure, an insured person must submit a number of documents after receiving medical care that is covered by their insurance policy. Prescriptions, medical bills, diagnostic reports, discharge summaries, and occasionally other paperwork such as pre-authorization papers. The insured person or their agents are responsible for gathering these records, which requires them to laboriously acquire the required documentation from a variety of sources, such as diagnostic facilities, pharmacies, and healthcare providers. Because it entails coordinating with numerous stakeholders and making sure that all necessary documents are acquired and filed appropriately, this procedure is frequently difficult and time-consuming.

Following their collection, the documents are usually sent, either in person or via regular mail, to the insurance company. Because the paperwork needs to be manually processed and verified by insurance company staff, this further adds to the delays in the reimbursement process. As illustrated in Figure 3.1, the manual nature of this procedure not only lengthens the time required to settle claims but also raises the possibility of mistakes and inconsistencies, resulting in additional delays and administrative burdens for both insurers and insured parties. Furthermore, there are serious security and privacy issues with the management and physical storage of private medical records. One of the most common problems with the existing system is the possibility for documents to be misplaced, destroyed, or accessed by unauthorized parties.

Additionally, it is difficult for insurers to effectively retrieve and track claim-related information due to the absence of a centralized and secure repository for

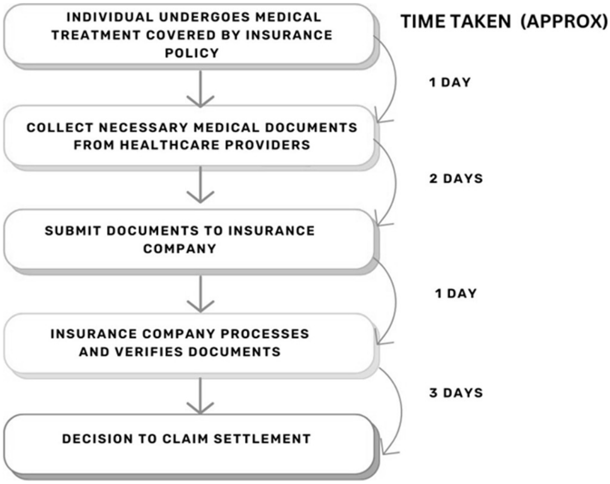


FIGURE 3.1 The existing system of processing reimbursement

preserving these documents. All things considered, the current medical claim reimbursement system in India is characterized by its inherent inefficiencies, manual procedures, and paper-based documentation [2]. Technological solutions that can improve security and privacy, speed the settlement of claims for both insurers and insured individuals and streamline this laborious process are desperately needed. This emphasizes how crucial it is to investigate cutting-edge options, such as blockchain-enabled platforms, in order to update and transform India's medical insurance claim reimbursement system.

3.2 RELATED WORK

Digital twin technology in healthcare [3, 4] involves creating virtual models of patients, organs, or medical devices to simulate real-world scenarios. These digital replicas enable early diagnosis, personalized treatment plans, and optimization of medical processes. In the pharmaceutical industry, digital twins are used to study aging processes, develop personalized medicines, and enhance production processes. Hospitals are exploring the use of digital twins for resource management, especially during critical times such as the COVID-19 pandemic. Wearable technologies, such as sensors and Internet of Things (IoT) devices, are being integrated to continuously monitor vital signs and transmit data to the cloud for analysis [3]. This data is then used to create and update digital twins of individual patients for better healthcare management. The future of digital twins in healthcare looks promising, with advancements expected in personalized medicine, organ transplantation, and hospital operations. By leveraging technologies such as IoT, big data analytics, and artificial intelligence, the healthcare industry is moving toward more efficient and effective patient care.

The main contribution of this chapter lies in its [5] exploration of the application of digital twin technology in healthcare, particularly focusing on creating virtual representations of contexts and situations involving multiple related assets within healthcare organizations. It proposes the concept of a human digital twin (HDT) as a central focus, discussing its potential in full life-cycle health management [4]. The chapter delves into the complexities and challenges of implementing HDT, highlighting the need for further research in this area. Additionally, it discusses the architectural framework, design requirements, key technologies, technical challenges, and future research directions for HDT, aiming to stimulate new efforts toward the development of HDT for personalized healthcare systems (PHS) [6, 7]. Recruiting a sufficiently large sample population to accurately represent the diversity of interaction behaviors within a specific user persona presents a recurring challenge in user testing. While proxy users can offer a solution by possessing similar abilities and skill sets to the desired group, the data collected from them may not authentically reflect actual users. To mitigate this issue, utilizing digital twins of user personas can effectively depict the spectrum of decisions made by a persona. The user experiment conducted with ALFRED the BUTLER (ATB) involved testing three user personas: Disuser, early terminator, and feature abuser. The findings revealed that the feature abuser tended to provide more thumbs-up responses, while the disuser predominantly received thumbs-down. This imbalance in user behaviors could impact the accuracy of system recommendations. The study concluded that synthetic personas can effectively replicate real user behaviors, which can be valuable for training recommendation systems to cater to diverse user interactions. The concept of digital twins is attributed to Michael Grieves and John Vickers of NASA [7] who presented the concept in a lecture on product life-cycle management in 2003. They envisioned a world where a virtual model of a product would provide the foundations for product life-cycle management, especially in a time when data about physical products was limited and manually collected. Grieves described the digital twin as a virtual representation of a physical product containing information about the product [8], with origins in the field of product life-cycle management. Future research focus areas for realizing the full potential of digital twins include perceived benefits, digital twins across the product life-cycle, use cases, technical implementations, levels of fidelity, data ownership, and integration between virtual entities. The comparison with building information modeling highlights similarities in managing physical and virtual entities with data connections, emphasizing the need for standardization and interoperability to address challenges in implementing digital twins and realizing their potential benefits. Ekblaw [9] presents a novel, decentralized record management system called MedRec using blockchain technology [10]. It aims to address several critical issues in healthcare, including fragmented and slow access to medical data, system interoperability, patient agency, and improved data quality and quantity for medical research [11]. MedRec focuses on addressing national healthcare priorities, such as restoring comprehensive patient agency over healthcare information, facilitating the creation of a "learning health system" that could enable better-unified access to data, and promoting the goals of precision medicine and evidence-based research [12]. The authors also highlight the importance of MedRec's role in supporting a "Health Care Directory and Resource Location," which could facilitate communication of authorization "across the Health IT ecosystem," provide an audit log for subsequent inquiries, and serve as a "Consistent Representation of Authorization to Access Electronic Health Information."

3.3 NIRAMAYA FRAMEWORK DESIGNED FOR UNDERPRIVILEGED INDIVIDUALS

For our program, which is specially made to help those in need, usability is crucial. To empower and enable these people to properly utilize the app's capabilities, it is essential to have a user-friendly interface and seamless functionality. An intuitive design that takes into account elements such as simplicity, clarity, and ease of use is crucial when keeping the academic tone in mind. Improve the app's accessibility and inclusivity by adding logical navigation and clear directions, which will make it easier for people with limited resources to use and navigate its features. Our mission to provide fair access to useful information and resources will be aided by a strong emphasis on usability, which will ultimately improve the lives of people who are less fortunate.

3.3.1 Digital Twin Technology in Credit Score Calculation

3.3.1.1 Traditional Credit Scoring

Credit scores from institutions such as CIBIL are of paramount importance when it comes to the lending practices of Indians, as many are then able to decide what options they may have in terms of finance. These scores painstakingly condense a person's credit history into a sum total that includes all the relevant information, whether there have been defaults or not and to what extent the payments have been consistent and timely on the number of credit accounts, as well as how frequently prospective lenders have inquired about a particular person's credit history. In addition, other factors such as the length of credit history, past defaults, and payoff habits tend to have a huge weight on the borrower's credit scores. Most lenders consider scores above 700 as an assurance that the borrower is financially sound due to their dependence on these scores as a good predictor of borrower worthiness and credit risk. The procedures involved are bureaucratic, with the amount of paperwork becoming a significant impediment to the request for emergency health loans for the poor when undertaking traditional methods. For those in desperate need of medical funding, such processes regularly call for many documents and verifications that are cumbersome and time-consuming. Stabilized address proof or proof of income are two other documents that conventional financial institutions usually demand, and many disprivileged persons would not be able to provide them. Access to banks and other financial establishments is another significant barrier to borrowing in rural or isolated regions, which can thereby further delay and hinder the loan processing procedure. All these factors, together, prolong the health emergencies of the deprived communities by depriving them of immediate access to needed healthcare. A digital twin can, in this case, offer an integrated and up-to-date financial profile at a time of crisis to improve access to health loans for disadvantaged people. This is highly advanced simulation technology where data from income, spending trends, and credit history come together to form a sound financial representation. Hence, lenders can make more informed decisions much faster with digital twins since it gives a precise, rounded view of things, compared to traditional methods that often rely on outdated and fractured information. Digital twins also check critical variables such as job security and outstanding debt. To assess the actual creditworthiness, it uses a matrix of selected machine learning algorithms that take into consideration micro-economic factors, for example, regional employment rates and healthcare expenditure. It gives a socially nuanced evaluation by including community behavior and support systems. The sense of urgency and the nature of the medical emergency are also examined based on medical records, insurance, and previous medical expenses. Another ethical consideration with regard to the digital twin is that it brings an ethical dimension to the awarding of credit scores because it evaluates the potential costs and impacts of delayed medical care. The associated risks can be evaluated correctly by considering factors such as how often the applicant's demographic experiences emergencies in medical care. The lender can also offer customized payment schedules because they know that those belonging to under-privileged groups may not have stable sources of income. Additionally, the knowledge of potential income increases in the applicant would help lenders make better decisions. Specific policies could then influence welfare programs by using anonymized and aggregated digital twin data to identify the most pressing areas that require more financial aid. Digital twins also promote transparency, which erases prejudice and builds more trust between the borrower and the lender. These aspects of resiliency and adaptability can be checked through the simulation of various situations such as an economic downturn or unexpected personal changes.

3.3.1.2 Emergence of Digital Twin Technology in Finance

Digital twins originated in the fields of engineering and manufacturing, today digital twin technology is applied widely in different fields, even up to the point of credit scoring, which revolutionized the nature of financial assessment techniques. A digital twin is defined as a proper replica of an existing real-world object or operation that can be found digitally, including all its characteristics, behaviors, and features. This is a concept concerning credit scoring and involves developing virtual models of trends and actions of borrowers' financial lives. Combining large swaths of historical data with cutting-edge algorithms for predictive analytics, financial firms can develop these digital twins of borrowers' behavior to simulate future repayment intentions and predict credit-usage trends as well as potential risk. This approach provides lenders with real-time awareness of potential risks and opportunities while simultaneously raising the precision and granularity of credit assessments. This way of (Figure 3.2) applying digital twin technology to credit scoring has an enormous potential to change the financial decision-making process, promote responsible lending, and eventually lower financial risk in dynamic market environments.

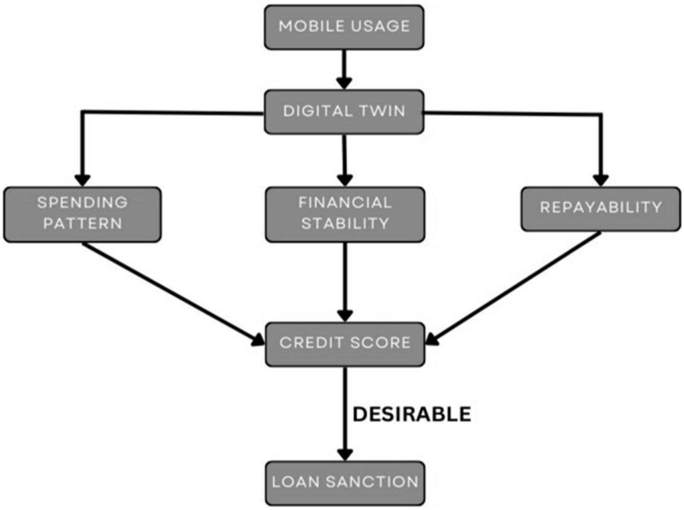


FIGURE 3.2 Niramaya framework using digital twin technology

3.3.1.3 How Can Digital Twins Enhance Credit Scoring?

Digital twin technology introduces significant advancements in credit scoring by leveraging sophisticated data integration, predictive analytics, real-time monitoring, and personalization techniques, thereby enhancing the accuracy and efficiency of assessing creditworthiness.

1. Data Integration: Digital twins aggregate a vast number of sources of data, ranging from financial transactions to social media interactions and e-commerce behaviors. This holistic view of credit that moves beyond the classic credit history will provide lenders with a deeper understanding of people's credit habits and behaviors. Combining such divergent datasets will provide more accurate and differentiated assessments of creditworthiness and encompass a more comprehensive set of borrower risks and characteristics.
2. Predictive Analytics: One of the most important benefits of digital twins is that they can model borrower behavior and predict future credit performance. The virtual models look through sophisticated machine learning algorithms to view patterns and behaviors that have been discovered in historical data. Digital twins can predict better possible risks such as the probability of default or delinquency based on the established patterns and connections in borrower behavior. This predictive capability enables lenders to make smarter decisions.
3. Real-Time Monitoring: Real-time basis data feeds update the digital twin continuously. Thereby, lenders can update their credit decisions in hours based on changes in financial conditions or the market through real-time dynamic monitoring capability. Up-to-date information about the digital

twin, such as a refreshed credit score, the most recent financial transactions, or updated expenditure-related changes, ensures the credit evaluations are at their minimum and outdated information does not mislead lending decisions, while using strong predictive insights to optimize loan approvals and terms.

4. Personalization: Credit scoring is personalized using unique situations and their scenarios. Digital twins may update ratings with regard to specific profiles and the needs of the different prospective borrowers. Many background variations and behaviors of different types are taken into account for this purpose; this increases equity and inclusivity while assessing the ability to pay. Digital twins service equity more in offering financial services and opportunities by tailoring offers of credit to the specific properties of distinct borrowers.

Digital twin technology basically transforms credit scoring through big data sets, predictive analytics to provide a better risk assessment basis, facilities for real-time decision-making, and various assessments tailored to specific needs. Such abilities, in a fast-changing digital environment, improve the effectiveness of lending procedures while allowing more equitable and knowledgeable financial decisions.

3.3.2 Challenges and Considerations

The adoption of digital twin technology in credit scoring brings forth several challenges and considerations that must be carefully addressed to ensure ethical, fair, and effective implementation:

3.3.2.1 Data Privacy

Non-traditional data sources such as social media activity and e-commerce trends raise very serious concerns about privacy. While the latter might be better in credit evaluation, the former could be a source of potential risks in privacy violations and unauthorized use of data. There is a great need to balance between people's right to privacy and their access to relevant data that should enable proper scoring. This requires strong data governance frameworks involving strict encryption protocols, data-anonymizing procedures, and compliance with local data protection laws or regulatory standards, such as GDPR. Endeavors to minimize privacy risks and enhance trust require explicit consent and explicitness about practices of collecting data from people

3.3.2.2 Discrimination

Credit scoring through digital twin models must ensure that algorithms mitigate bias and avoid discriminatory practices. Non-traditional data sources may inadvertently reflect the biases or disparities that exist in society, leading to unfair treatment of specific demographic groups. Algorithm audit processes must be combined with comprehensive testing for bias to be done with an ongoing process to identify and correct algorithmic biases. Of course, diversifying the data sets fed into training algorithms and including fairness metrics in the model development would go a long way to prevent bad and discriminatory outcomes. And if algorithms do not open up on "how" the decisions are made, then accountability and trust cannot be built into the determination.

3.3.2.3 Algorithmic Transparency

The challenge for regulators and lenders lies in understanding how credit scores are produced by digital twin models. Digital twins always rely on complex algorithms in machine learning, that are opaque in the decision-making process, whereas traditional credit scoring models are based on established criteria. What is of special interest to lenders, therefore, are how clear these explanations and insights about variables used, weightings assigned to different inputs in the data, and logic on which credit decisions are premised. It will encourage responsibility and offer users an understanding of decisions that include bias or error in fact-making through better algorithmic transparency. In conclusion, although digital twin technology has significant advantages in improving the efficiency and accuracy of credit scoring, responsible implementation requires resolving issues with discrimination, data privacy, and algorithmic transparency. Stakeholders may optimize the advantages of digital twins while respecting moral principles and safeguarding consumer rights by putting strong governance frameworks in place, making sure algorithmic decisions are fair, and encouraging transparency throughout the credit evaluation process.

3.4 SECURING USER MEDICAL RECORDS USING BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed, tamper-proof ledger aimed to make recording transactions and tracking assets within business networks much easier [13–15]. There may either be physical assets, such as real estate, vehicles, money, and land; or intangible assets, such as intellectual property, patents, trademarks, and brand assets [16, 17]. The key goal of applying blockchain in this use case is to protect sensitive user health records. Blockchain's structure inherently provides security, leveraging cryptographic methods, decentralization, and consensus protocols to ensure transaction reliability. The data in blockchain or other distributed ledger technology [18, 19] is organized by blocks building up, and each block carries one or more transactions. The tamper-proof sequence of blocks [20] ensures the integrity of those transactions. The transactions in a block are essentially recognized through a consensus mechanism [5]. Due to the decentralized architecture, records in a blockchain are held across a distributed network, which thus eliminates single points of failure and prevents unilateral changes to transaction histories. It is adaptable, and its use comes highly across all industries [21, 22]. Its applications in finance render transactions secure yet transparent, facilitate speedier and more efficient cross-border payments, reduce fraud, and eliminate intermediaries. In supply chain management, blockchain enhances transparency and traceability. It allows for the transaction recording to be tamper-proof; prevents counterfeit products through such proof, ensures authenticity, and optimizes processes.

As illustrated in Figure 3.3, the system provides two interfaces that are available for users to submit compensation claims from different platforms: One via an

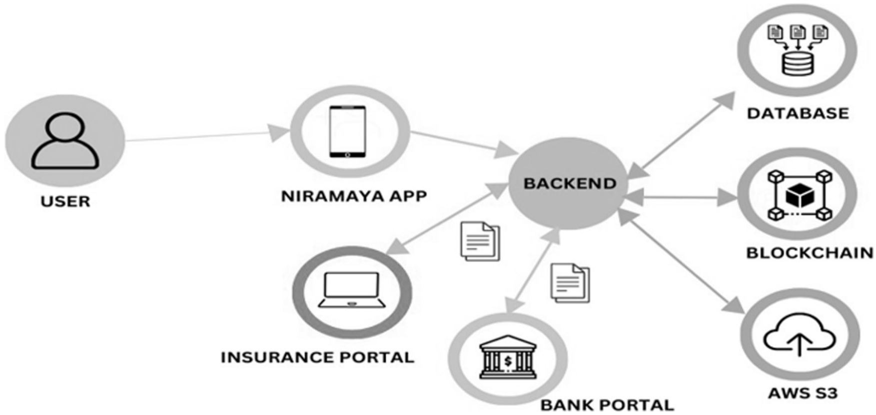


FIGURE 3.3 Utilization of blockchain technology in the Niramaya application

Android application. The second is an insurance partner onboarding portal where partners can easily get onboarded and view reimbursement requests along with supporting documents. An Android application allows users to upload necessary documents, which are then securely stored in the backend servers of Niramaya. The backend integrates the databases, Amazon S3, and blockchain to ensure data confidentiality and integrity. The web portal also provides insurance partners with the ability to register and log in and request specific user claim documents, and then the system will cross-check with both blockchain and Amazon S3 once requested. Once verified, documents get delivered in real time, thus making it easy for the insurance partners to process claims based on their reliability and authenticity

Blockchain technology has been incorporated into the Niramaya application to ensure secure document management, specifically catering to the healthcare and insurance sectors. The document upload process within the application is designed to accommodate various types of documents, including insurance policies, medical bills, test reports, and doctor prescriptions. Users are given the option to upload documents in different formats, such as images, text files, or PDF forms. It is crucial to extract text from these documents and represent it in a textual format to ensure compatibility with blockchain technologies. To accomplish this text recognition, we use a popular hashing technique that utilises the SHA256 algorithm. Therefore, each uploaded document is assigned a unique hash value that changes even with minor updates or changes in the document. This text recognition process ensures that each document is distinctly identified and meticulously organized for anchoring onto the blockchain, thereby ensuring its distinctiveness and secure incorporation into the system.

Once the textual representation is extracted for an uploaded file, a JSON document is generated containing two essential fields:

(1) **HolderDID:** A unique identification string for a user specifically generated by the blockchain system for that document.
(2) **Hashed File:** A unique string representing the file generated using the mentioned hashing technique.

Subsequently, a backend API converts the JSON document into an appropriate format that can be anchored onto the blockchain. A unique identifier associated with the data above is generated on the blockchain, eventually returned by the API as the statement identifier (StatementID). This ensures the immutable presence of user data within the system. Documents are also stored in their original format in the Niramaya backend using the Amazon Web Services S3 storage system, ensuring accessibility for users and external partners such as insurance providers. However, the documents cannot be retrieved from the blockchain in their entirety. All details related to these documents are stored in the database. The portal interface simplifies document retrieval, allowing users to navigate through lists and access specific documents effortlessly. When a document is accessed by an insurance partner, a thorough integrity check is conducted to ensure that the original file uploaded by the user remains untampered. The document is made accessible only when the integrity check is successful. Otherwise, the file remains inaccessible.

3.4.1 Need for Blockchain to Secure the Medical Health Records of Underprivileged Individuals

More stress has been given to securing medical documents using blockchain technology in recent years since increased digitization of medical documents compromises with increased vulnerability of the patients' data to cyber-attacks and unauthorised access. Blockchain offers a decentralized and immutable ledger system that can greatly enhance the security and privacy of medical documents as shown in Figure 3.4 [23]. By applying cryptographic algorithms and distributed consensus mechanisms, blockchain ensures that medical records are securely stored, tamper-proof, and easily auditable [24]. This technology can be particularly beneficial in securing the medical records of underprivileged individuals who often lack access to quality healthcare and face additional challenges in protecting their personal information. By leveraging blockchain, healthcare providers can equip underprivileged populations with secure and confidentiality assured medical records, enabling them to receive better healthcare services and ensuring their information remains confidential [25].

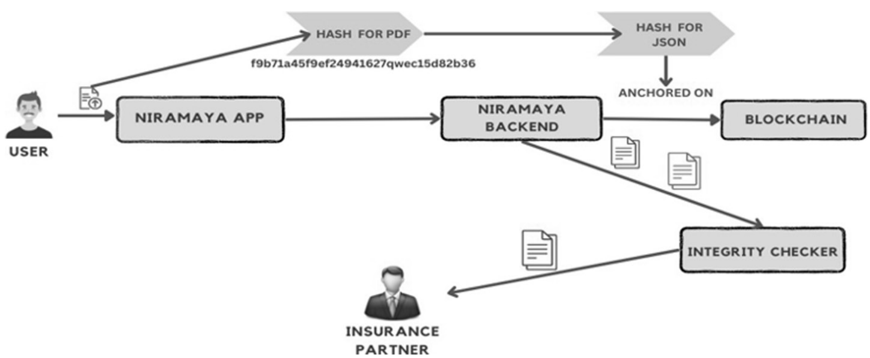


FIGURE 3.4 Securing files using blockchain technology

3.4.2 Hashing to Secure Medical Records

Hashing has been an essential instrument both in text processing and file management of a variety of formats such as images, PDFs, and other types of files. Through the hash function, the internal data structures of a file are converted to a compact and unique representation [26]. This is important because the slightest deviation in the file's content or structure will lead to a completely different hashed value. In parallel with textual data hashing, files are hashed by algorithms such as SHA256, which are particularly designed to work with various file formats in an efficient manner as demonstrated in Figure 3.5. Such hash functions produce hash digests consisting of fixed-length strings of characters which are descriptive of the original content of the file. Whether it be an image, a PDF file, or any other type of file, the hash digest produced captures the authenticity of the information stored in a file and its structure. This is the reason why hash digests are used in file integrity verification and detection of duplication. Let's say, for example, one would instantly tell if two files are the same as long as their names and locations are different with the help of a hash digest. Hash digests in the digital forensics field are used for verification of files and tracking of changes. Its reliability and efficiency in dealing with different file formats is the reason hashing has became a leader in modern environments, with control sets of operations over the potential data integrity and security issues as the most important things.

3.4.3 SHA-256 Algorithm

SHA-256, or Secure Hash Algorithm 256-bit, is a cryptographic hash function that generates a fixed-size 256-bit (32-byte) hash value. It belongs to the SHA-2 family of cryptographic hash functions [27], developed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) in 2001.

The advantages of SHA-256: SHA-256 is a member of the secure hash algorithm (SHA) family. It provides several advantages that make it outperform modern cryptographic applications and verification of data integrity as shown in Figure 3.6.

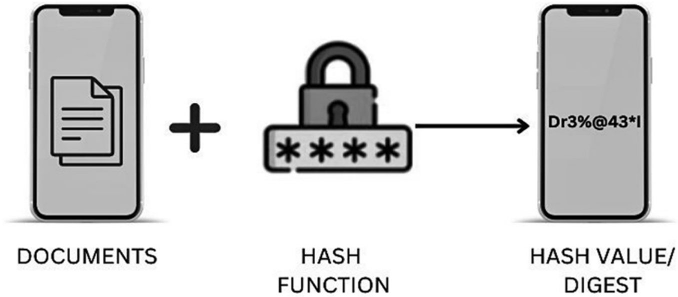


FIGURE 3.5 Ensuring medical record integrity with hashing

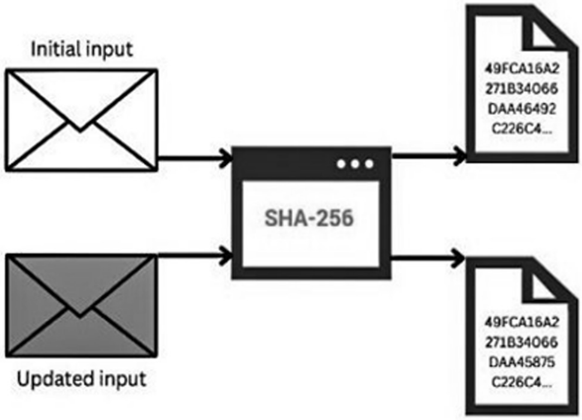


FIGURE 3.6 Enhancing medical record security with SHA 256 hashing

3.4.3.1 Security

SHA-256 is well-known for its robust security features, in particular its resistance to collision attacks. When two different inputs produce the same hash value, a collision attack is said to occur. The SHA-256 design ensures that such occurrences are computationally impossible, assuring that the integrity and authenticity of hashed data remain intact. This feature is crucial in security-sensitive applications such as digital signatures, where any modification in the data is easily detectable.

3.4.3.2 Collision Resistance

Building on its security strength, SHA-256 provides exceptional collision resistance. This means it is highly impossible for two distinct inputs to generate the same 256-bit hash output. This is the fundamental property that ensures data integrity across various applications, from verifying software downloads to securing transactions in blockchain technology. The unlikelihood of collisions highlights the reliability of SHA-256 and confirms the uniqueness and consistency of digital data.

3.4.3.3 Fixed Output Size

SHA-256 produces a fixed-size output of 256 bits (32 bytes), irrespective of the size or complexity of the input data. The hash digest remains consistent across different platforms and systems and hence simplifies data handling and storage. This uniformity ensures its flexible usage across various protocols and applications with the need for adaptations or conversions into other formats.

3.4.4 Efficiency

SHA-256 is designed to be computationally efficient with rapid hashing of data while maintaining accuracy and reliability. For applications demanding real-time data processing and high throughput such as password hashing for user authentication, digital certificates and securing transactions in cryptocurrency systems, the efficiency of the hashing algorithm plays a highly significant role. The ability to perform hashing operations efficiently, without compromising security is the key feature of essential digital systems.

Conclusively, SHA-256 is prominent not only due to its high-security properties, such as resistance to collisions and efficient computation but also due to its versatility in accommodating a huge variety of cryptographic and data integrity applications. Its consistent output size and efficient processing capabilities make it a vital tool for maintaining data security, authenticity, and reliability in today's connected digital landscape.

3.5 STORING OF MEDICAL DOCUMENTS IN AMAZON S3?

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features to optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.

3.5.1 Integrity Checker

When insurance partners request documents, the system retrieves pertinent details from the database, which encompass the key, S3 path, Claim ID, Statement ID, and HolderDID, all outlined in Figure 3.7(A). Following this initial step, in Figure 3.7(B), the system proceeds to fetch the most recent hash from the blockchain as associated with the Statement ID, subsequently providing it as requested. Moving forward to Figure 3.7(C), the system locates the file within the Amazon S3 storage system by utilizing the provided S3 path. Here, the SHA-256 algorithm is employed to meticulously compute the hash of the file. The resultant hash, in conjunction with the HolderDID, is then seamlessly incorporated into a JSON document, effectively forming the JSON representation. As a subsequent step, a document hash (dochash) is generated from this JSON document. The process then progresses to the integrity check stage, where a comparison is made. If the key retrieved in Figure 3.7(A) matches both the hash obtained from Figure 3.7(B) and the document hash (dochash) derived in Figure 3.7(C), the integrity check is deemed successful, ensuring that the document remains unaltered throughout its journey. However, if this condition is not met, the integrity check fails, indicating potential tampering with the document and prompting further investigation or action. This stringent verification process is crucial in upholding the integrity and reliability of the documents stored and managed within the system as shown in Algorithms 1 and 2.

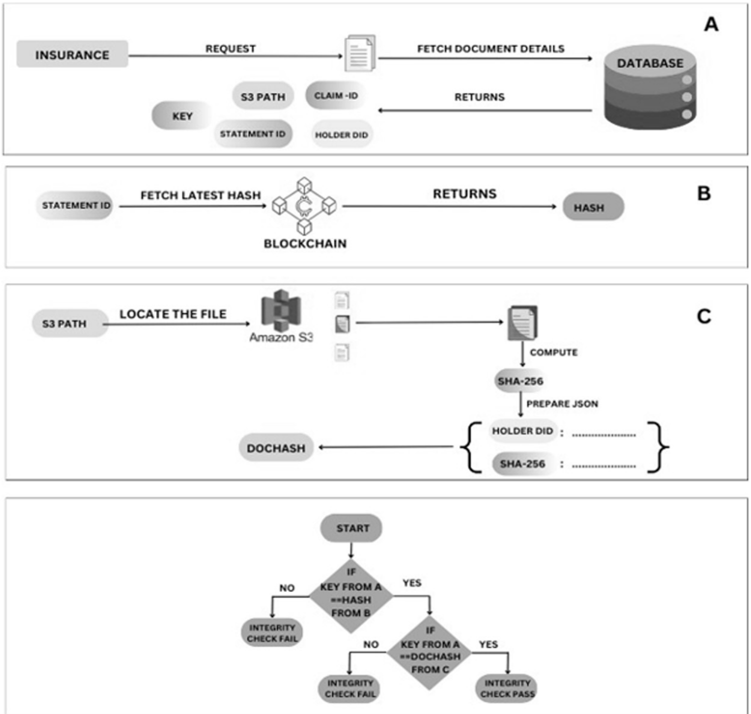


FIGURE 3.7 Fetching the hashed documents from the blockchain

Algorithm 1 Uploading Medical Record

```
Step 1: Upload document
if new user then
      Generate holder DID
else
      Get holder DID if he's an existing user
end if
Step 3: Encryption of file
Step 4: Prepare JSON from encrypted file
Step 5: Create statement
```

Algorithm 2 Fetching Medical Record

```
Step 1: Access a file from insurance provider
Step 2: Check the integrity of the requested file
if there is no error in duplication then
      Integrity check fails
else
      Integrity check successful
end if
```

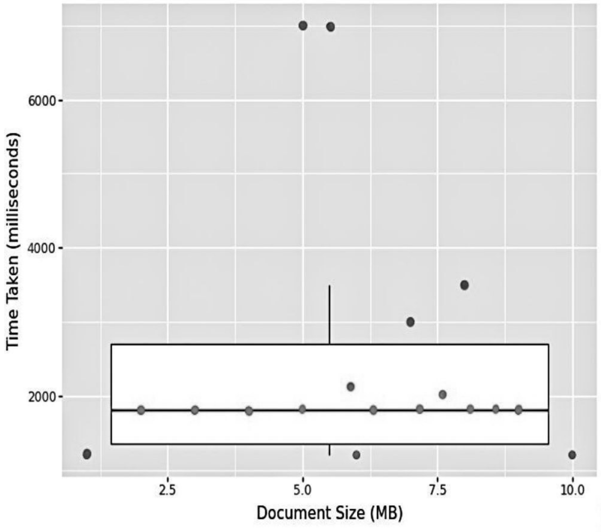


FIGURE 3.8 Revolutionizing blockchain document anchoring: Consistent time efficiency for all file sizes

Traditionally, the process of anchoring documents onto the blockchain involved a significant time disparity based on file size. Larger documents typically require a longer period to anchor compared to smaller files. This time discrepancy was a common challenge faced by users when utilizing blockchain technology for document verification and authentication.

In Figure 3.8, the framework addresses this issue by ensuring that regardless of the file size, the time required for anchoring on the blockchain remains consistent. Through innovative optimization techniques, our application effectively eliminates the traditional time discrepancies associated with anchoring large and small documents.

3.6 CONCLUSION

The process of settling medical insurance claims using blockchain technology is a significant step forward in resolving security issues and inefficiencies in conventional systems. Document management can undergo a paradigm shift thanks to the fundamental blockchain characteristics of immutability, decentralization, and cryptographic security. This solution improves confidence and transparency while streamlining operations and facilitating secure storage, seamless access to, and verification of sensitive medical documents across platforms, such as the Niramaya portal, and collaboration with insurance carriers. With its promises of streamlined claim settlement procedures, lower fraud risks, and greater satisfaction for both insured parties and insurers, it establishes a precedent for broad adoption in the healthcare insurance market. Similarly, digital twin technology provides a revolutionary advancement in financing by improving the precision and customization of credit scoring algorithms. Digital twins visualize the digital persona of the borrowers that encompass the characteristics and behaviors of borrowers using information stored on several various sources, including financial transactions, social media connections, and behavioral tendencies. Important factors including bias reduction, privacy protection, and transparency in credit evaluation procedures are all taken into account by this method. The success of its adoption depends on embracing strong data governance, guaranteeing algorithmic fairness, and adhering to legal requirements. Financial organizations can leverage digital twin technology to assess the consumers more equitably ensuring inclusivity so that they comply with changing consumer demands and legal requirements. Ultimately, blockchain and digital twin technologies both present novel approaches that hold great potential for improving credit scoring and health insurance claim settlement procedures. Through the optimal use of their unique features and the resolution of underlying hindrances, these technologies pave the way for increased security, improved stakeholder trust, and operational efficiencies in vital industries.

ACKNOWLEDGMENT(S)

The research work is fully supported by the IIT Bhilai Innovation and Technology Foundation under the UG/PG fellowship scheme. Ref No: IBTTF/Note/TBI/Sanction Letter/2023-24/0013. We would also like to thank BE Graduate Students Nidhi Suresh Hegde, Nikhil Ballari, Keerthi K S, Isha Mohandas Pai, Manikanta, Shreya S Rao, and Adarsh Singh for their Contribution.

REFERENCES

1. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (Big Data Congress)*, 2017, pp. 557–564.
2. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, 7(2), 56, 2019.
3. Ö. Aydın and E. Karaarslan, "OpenAI ChatGPT generated literature review: Digital twin in healthcare," in Ö. Aydın (Ed.), *Emerging Computer Technologies*, Vol. 2, 2022.
4. T. Erol, A. F. Mendi, and D. Do˘gan, "The digital twin revolution in healthcare," in *2020 4th international symposium on multidisciplinary studies and innovative technologies (ISMSIT)*, pp. 1–7. IEEE, 2020.
5. M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, 8, 157959–157973, 2020.
6. T. Sun, X. He, and Z. Li, "Digital twin in healthcare: Recent updates and challenges," *Digital Health*, 9, 20552076221149651, 2023.
7. A. Reinert, S. Rebensky, M. C. Osman, B. Prebot, C. Gonzalez, D. Morrison, V. Yerdon, and D. Nguyen, "Using cognitive models to develop digital twin synthetic known user persona," *Human Factors and Simulation*, 83, 83, 2023.
8. A. Vallée, "Digital twin for healthcare systems," *Frontiers in Digital Health*, 5, 1253050, 2023.

9. D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, "Characterising the digital twin: A systematic literature review," *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52, 2020.
10. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data," in *Proceedings of IEEE Open & Big Data Conference*, Vol. 13. Vienna, Austria, 2016, p. 13.
11. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current re- search on blockchain technology?—a systematic review," *PloS One*, 11(10), e0163477, 2016.
12. R. Ramya, B. D. Ramesh, M. Kumudavalli, P. Joshi, and K. Venugopal, "Blockchain-integrated metaverse for academia: A solution for virtual classes, lectures, and project fundings," in *International Conference on Information and Communication Technology for Competitive Strategies*. Springer, 2023, pp. 387– 396.
13. R. Ramya, N. Kishore, D. Sejal, K. Venugopal, S. Iyengar, and L. Patnaik, "Predicting social emotions based on textual relevance for news documents," in *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE).*
14. T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, 135, 62–75, 2019.
15. R. Ramya, G. Singh, S. N. Sejal, K. Venugopal, S. Iyengar, and L. Patnaik, "R 2 dclt: retrieving relevant documents using cosine similarity and lda in text mining," *International Journal of Information and Communication Technology*, 19(4), 391–422, 2021.
16. M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani, and M. Meraj, "A blockchain framework for secure electronic health records in healthcare industry," in *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE).* IEEE, 2020, pp. 605–609.
17. M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," *Procedia Computer Science*, 174, 321–327, 2020.
18. G. Q. Butt, T. A. Sayed, R. Riaz, S. S. Rizvi, and A. Paul, "Secure healthcare record sharing mechanism with blockchain," *Applied Sciences*, 12(5), 2307, 2022.
19. M. H¨olbl, M. Kompara, A. Kamiˇsali´c, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, 10(10), 470, 2018.
20. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA annual symposium proceedings*, Vol. 2017. American Medical Informatics Association, 2017, p. 650.
21. A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, 7, 147 782–147 795, 2019.
22. R. Nair, S. N. Zafrullah, P. Vinayasree, P. Singh, M. M. A. Zahra, T. Sharma, and F. Ahmadi, "Blockchain-based decentralized cloud solutions for data transfer," *Computational Intelligence and Neuroscience*, 8209854, 2022, 30 May.
23. Y. Tang, Q. Zou, J. Chen, K. Li, C. A. Kamhoua, K. Kwiat, and L. Njilla, "Chainfs: Blockchain-secured cloud storage," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 987–990.
24. A. Patil, A. Jha, M. M. Mulla, D. Narayan, and S. Kengond, "Data provenance assurance for cloud storage using blockchain," in *2020 International Conference on Advances in Computing, Communication Materials (ICACCM)*, 2020, pp. 443–448.
25. N. Deepa, T. Devi, N. Gayathri, and S. R. Kumar, "Decentralized healthcare management system using blockchain to secure sensitive medical data for users," in *Blockchain Security in Cloud Computing*, 2022, pp. 265–282.

26. T. Gabriel, A. Cornel-Cristian, M. Arhip-Calin, and A. Zamfirescu, “Cloud stor- age. a comparison between centralized solutions versus decentralized cloud storage solutions using blockchain technology,” in *2019 54th International Universities Power Engineering Conference (UPEC)*, 2019, pp. 1–5.
27. H. Yoshida and A. Biryukov, “Analysis of a SHA-256 variant,” in *International Workshop on Selected Areas in Cryptography* (pp. 245–260). Berlin, Heidelberg: Springer Berlin Heidelberg.

4 Leveraging Blockchain Interoperability for Sustainable Healthcare

A Review and Analysis

Neetu Sharma and Ashutosh Mishra

4.1 INTRODUCTION

The healthcare industry is experiencing an increasing demand for sustainability to achieve better patient outcomes and enhanced record security, privacy, and integrity. Distributed ledger technology such as blockchain provides a unique infrastructure that eliminates dependence on centralized architectures [1]. This technology has emerged as a promising enabler, offering distinctive capabilities to tackle key challenges and unlock new opportunities in healthcare ecosystems worldwide. By providing a decentralized, immutable, transparent, auditable, and secure data-sharing mechanism, blockchain offers a disruptive solution.

For blockchain to enhance organizational operations, it must integrate seamlessly with other systems. However, the lack of interoperability among blockchains is a fundamental issue that impedes the global adoption of blockchain in collaborative organizations [2]. Interoperability can be considered the ability of various systems to interact with each other without barriers [3]. Blockchain technology can significantly improve interoperability by allowing data exchange between multiple systems and enabling simultaneous access to that data. In a wide range of proposed systems, data sharing occurs among institutions, where users handle complete access control over their records. This improved interoperability can enhance system outcomes [4].

Interoperability is a crucial blockchain characteristic that permits various systems to share across healthcare industry boundaries, enabling the provision of more advanced and effective services [5]. It is the capability of blockchain technology to offer and access information to cross-blockchain networks [6, 7].

4.1.1 Challenges in the Healthcare Industry

The healthcare industry faces many obstacles in the current era, one of which is very significant: the security risks associated with the healthcare industry. These risks include cyberattacks, data breaches, and other illegal access to personal data.

 DOI: 10.1201/9781003532286-4

Serious repercussions from such security breaches may include financial losses, damage to one's brand image, and danger to the health of patients [8]. A few of the challenges in the healthcare industry are summarised in Table 4.1.

There is a scarcity of innovation within the healthcare domain that focuses specifically on the interoperability feature of blockchain and the development of various emerging technologies. This gap in the literature highlights the need for more in-depth studies and innovative solutions to address the challenges and opportunities presented by blockchain in healthcare [9]. As a result, many prominent organizations are making significant investments in blockchain technology, aiming to resolve critical issues related to technology, interoperability, and data management.

In today's digital age, people are becoming more aware of the importance of having access control over their own healthcare information. This growing awareness underscores the necessity for robust systems that ensure data security, integrity, and privacy. In environments where sensitive health data are of paramount importance, there is a compelling need for stringent checks, enhanced security measures, and comprehensive audit capabilities to safeguard data integrity. The healthcare industry's emphasis on interoperability and the seamless sharing of medical records and information further accentuates the demand for advanced technological solutions.

The deployment of decentralized blockchain networks for the healthcare industry to create digital health twins is an area that holds significant promise yet requires more exploration [10]. Digital health twins are virtual representations of patients that can be used to simulate and predict health outcomes, improve personalized medicine, and enhance overall patient care. Integrating blockchain technology into this concept could revolutionize how patient data is managed, shared, and utilized across the healthcare ecosystem.

However, the adoption of blockchain technology in healthcare is not without its challenges. These include the inherent complexity of the technology, the existence of numerous stand-alone projects that do not yet interoperate, and issues related to scalability and integration with existing healthcare systems [11]. Addressing these challenges is crucial for the successful implementation of blockchain solutions that can enhance the efficiency, security, and interoperability of healthcare data management.

The key challenges in the healthcare industry are listed below:

TABLE 4.1
Blockchain-Related Healthcare Industry Challenges

References	Healthcare Challenges
[8]	Security risk
[9]	Research on blockchain interoperability in the healthcare industry is scarce
[10]	Interoperability and data-related issues
[11]	Blockchain challenges include complexity, stand-alone projects, interoperability, and scalability

- Incomplete Patient Records: Data fragmentation frequently results in incomplete patient records, which can compromise the precision of diagnosis and the efficacy of treatment regimens.
- Data Access Challenges: Healthcare professionals find it difficult to swiftly obtain all pertinent patient data, which could cause delays in treatment and even medical errors.
- Duplication of Tests and Procedures: In the absence of a unified record, there is a greater chance of redundant tests and procedures, leading to extra expenses and needless risks for patients.
- Care Coordination: Care continuity for patients is impacted by fragmentation, which makes it more difficult for various healthcare providers to work together efficiently.
- Systems That Are Incompatible: Data exchange is complicated by the fact that many healthcare organizations use disparate electronic health record (EHR) systems that are incompatible with one another.
- Standards and Protocols: Lack of universally adopted standards and protocols for data exchange hinders interoperability. Even when standards exist, inconsistent implementation can be a problem.
- Healthcare Data across Several Centralized Systems: Organizations with centralized data silos may hinder the easy exchange of information, which reduces the advantages of integrated care.
- Patient Mobility: Patients who move between medical providers may discover that gaps in their medical history occur because their health data does not follow them.
- Cyber Attacks: Because they store so much sensitive personal and medical data, healthcare organizations are frequently the target of cyberattacks such as ransomware and data breaches.
- Compliance Requirements: In order to protect patient data, healthcare providers are required to adhere to strict regulations (such as HIPAA in the United States). Failure to comply can result in heavy penalties.
- Internal Threats: Insider threats represent a serious risk to data security, regardless of their malicious intent. Workers who have access to private data may jeopardize the security of the information.
- Treatment Delays: Difficult administrative processes can cause patient care delays, which lowers the effectiveness of healthcare delivery.
- Waste of Resources: Inefficiencies may lead to the waste of personnel, money, and time that could be used to provide patient care.
- Patient Dissatisfaction: Inefficiencies frequently result in increased wait times, unsatisfactory patient encounters, and decreased satisfaction levels.
- Billing and Claims Processing: The intricacy of insurance claims and medical billing can result in mistakes and long wait times for payment, which can negatively impact the financial stability of healthcare providers.

The holistic view of achieving interoperable blockchain for sustainable healthcare is presented in Figure 4.1. The healthcare industry faces several significant challenges,

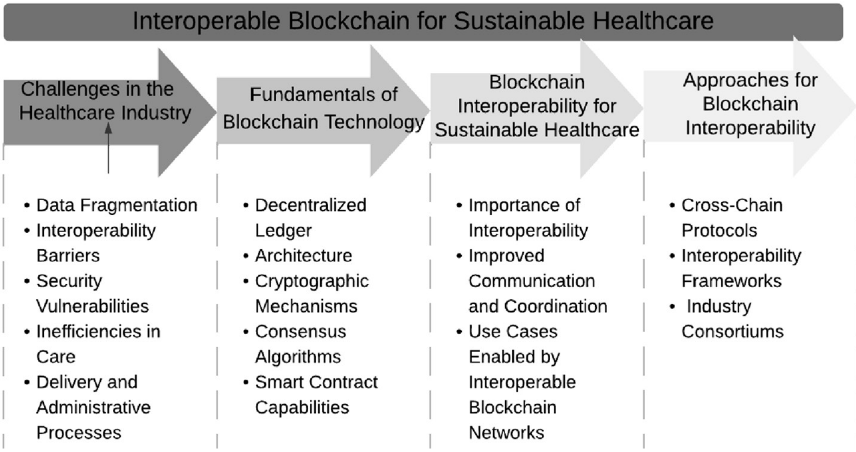


FIGURE 4.1 Holistic view of achieving interoperable blockchain for sustainable healthcare

including data fragmentation, interoperability barriers, security vulnerabilities, and inefficiencies in care delivery and administrative processes. Blockchain technology, with its decentralized ledger architecture, cryptographic mechanisms, consensus algorithms, and smart contract capabilities, offers promising solutions to these issues. By ensuring data security and integrity, enabling patient-centric care models, and enhancing administrative efficiency, blockchain can address many of the current inefficiencies. Furthermore, blockchain improves traceability and visibility in the pharmaceutical supply network, which is critical for combating drug counterfeiting. Interoperability among blockchain networks is crucial for creating sustainable healthcare ecosystems. Improved communication and coordination facilitated by interoperable blockchain networks can lead to better patient outcomes and reduced medical errors. Various approaches and initiatives, such as cross-chain protocols, interoperability frameworks, and industry consortiums, are being developed to achieve this goal. These efforts aim to create a cohesive and efficient healthcare system that leverages the full potential of blockchain technology.

Addressing these challenges requires a multifaceted approach, including the adoption of advanced technologies such as blockchain for secure data sharing, implementation of interoperability standards, enhancement of cybersecurity measures, and optimization of care delivery and administrative workflows. This research work aims to provide a review and analysis of the need for blockchain interoperability to achieve sustainable healthcare transformation.

4.1.2 Role of Blockchain in Sustainable Healthcare

Blockchain technology offers several potential contributions to sustainable healthcare, which are as follows:

1. **Data Integrity and Security:** Blockchain provides a decentralized and immutable ledger that ensures the integrity and security of healthcare data. This feature is crucial for protecting patient information and preventing unauthorized access or tampering, thereby enhancing privacy and trust.
2. **Interoperability:** Blockchain can facilitate interoperability among disparate healthcare systems and stakeholders by establishing a common platform for securely sharing and accessing data. This interoperability improves communication, coordination, and continuity of care, leading to better patient outcomes and reduced medical errors.
3. **Patient-Centricity and Empowerment:** Blockchain technology permits patients to own, access, and control their health information through secure digital identities and permissioned access mechanisms. The public can selectively allow access to their data with healthcare institutions, innovators, and various other entities, enabling personalized care, informed decision-making, and participation in clinical trials or research studies.
4. **Health Information Sharing:** Blockchain streamlines health information sharing by enabling real-time, secure, and auditable transactions among healthcare organizations, payers, and patients. This capability reduces administrative burdens, eliminates intermediaries, and accelerates processes such as claim processing, billing, and credentialing.
5. **Supply Chain Management:** Blockchain enhances transparency and traceability in the pharmaceutical supply chain by recording transactions related to drug manufacturing, distribution, and authentication. This transparency helps combat counterfeit drugs, ensure product quality and safety, and optimize inventory management, thereby promoting sustainability and public health.
6. **Research and Innovation:** Blockchain facilitates data sharing and collaboration among researchers, clinicians, and pharmaceutical companies by providing a trusted and transparent platform for securely storing, accessing, and analyzing health data. This collaborative ecosystem accelerates medical research, fosters innovation, and advances precision medicine and personalized therapies.
7. **Value-Based Care and Payment Models:** Blockchain supports value-based care and payment models by enabling real-time tracking and verification of healthcare services, outcomes, and payments. This capability promotes accountability, efficiency, and fairness in healthcare delivery and reimbursement, aligning incentives with patient-centric care and quality improvement initiatives

4.2 ORGANIZATION

Section 4.1 of this chapter presents the challenges faced by the healthcare industry and the role of blockchain in sustainable healthcare. Sections 4.3 and 4.4 cover the literature review and the basics of blockchain technology. Sections 4.5 and 4.6 explore the role of blockchain interoperability in fostering sustainable healthcare ecosystems and existing interoperability approaches. Section 4.7 presents the implications, including the need for interoperability standards, governance models, and a regulatory framework. Section 4.8 presents the conclusion and future work from this chapter.

4.3 LITERATURE REVIEW

This section covers the existing works related to blockchain interoperability for sustainable healthcare. Table 4.2 presents a summary of existing works. In [2], the authors provide a standardized architecture that facilitates interoperability and DLT interoperability in cooperative enterprises. The goal of the research described in [3] is to create a blockchain-based EHR framework that is interoperable and able to meet various national and international EHR standards, including HL7 and HIPAA. A model was presented in [4] for interoperability in medical imaging measurements, personal information protection techniques, and medical data standards. This study focused on a review of existing research in the field of using distributed ledger technology to store electronic health records (EHR), as presented in [5]. In [6], the authors aimed to create an integrated view based on interoperability principles to collect patients' medical records, utilizing sensors from various wearable devices and other sources.

A unique publish-based blockchain interoperability solution for permissioned blockchains was put forth in [7]. An application-based cross-chain interoperability solution called appXchain is presented in [8], enabling data sharing, request processing, and inter-communication between blockchain networks with any kind of architecture and industrial focus. The goal of the study in [9] was to pinpoint the main obstacles and possibilities for creating a long-lasting research lab that produces studies, instruction, and blockchain applications in healthcare at an academic medical institution. According to the authors of [11], using blockchain technology in healthcare data management systems can spur innovation and result in notable advancements. They discussed the opportunities for the healthcare sector, the main benefits of implementing blockchain technology, and important blockchain features and attributes. Along with highlighting recent ongoing initiatives and case studies that show how useful blockchain technology is for a range of healthcare applications, they also highlighted important unresolved research issues that are impeding the technology's successful implementation in the industry.

In [12], the authors conducted a survey on 404 blockchain interoperability-based studies. In [13], the authors conducted a literature survey of the existing schemes on blockchain interoperability and atomic swapping. In [14], the authors proposed the true state of interoperability frameworks suggested for heterogeneous blockchain-based systems.

In [15], the objective of the authors is to investigate how blockchain interoperability solutions use smart contracts. Homogeneous blockchains and homogeneous smart contracts, heterogeneous blockchains, and heterogeneous smart contracts are the three primary categories into which this research has divided the current interoperability solutions.

TABLE 4.2
Summary of Existing Works Related to Blockchain Interoperability for Sustainable Healthcare

Existing Scheme	Objective	Interoperability Solution
[2]	To provide a standardized architecture that facilitates interoperability and DLT interoperability in cooperative enterprises	Interoperability and interoperability solutions
[3]	To create a blockchain-based EHR framework that is interoperable and able to meet various national and international EHR standards, including HL7 and HIPAA	Interoperable EHR framework
[4]	A model for interoperability in medical imaging measurements, personal information protection techniques, and medical data standards was put forth	PHI interoperability model
[5]	To systematically review existing and ongoing research in the field of using blockchain technology to store electronic health records (EHR)	EHR interoperability model
[6]	To create an integrated view based on interoperability principles to collect patients' medical records, utilizing sensors from various wearable devices and other sources.	Telecare interoperability solution
[7]	To suggest a new publish/subscribe-based blockchain interoperability solution for permissioned blockchains	Publish/subscribe to interoperability architecture
[8]	To suggest appXchain, an application-based cross-chain interoperability solution that enables data sharing, request processing, and inter-communication between blockchain networks of any architecture type and industrial focus	AppXchain
[9]	To evaluate those tactics in a practical setting and identify the main obstacles and possibilities for creating a sustainable research lab that produces research, instruction, and blockchain applications in healthcare at an academic medical institution	Sustainable framework
[11]	To discuss how using blockchain technology in healthcare data management systems can spur innovation and result in notable advancements	Healthcare interoperability solutions
[13]	To review the existing literature on atomic swapping and blockchain interoperabilit	Atomic swap

(*Continued*)

TABLE 4.2 (CONTINUED)
Summary of Existing Works Related to Blockchain Interoperability for Sustainable Healthcare

Existing Scheme	Objective	Interoperability Solution
[14]	To propose a true state of interoperability frameworks suggested for heterogenous blockchain-based systems	Hashed time lock contracts, atomic swap, Xchain framework, Wanchain, interledger, relay, relay chains, inter blockchain communication protocol (IBC) by Cosmos, Polkadot, bridges, BTC relay
[15]	To explore the use of smart contracts in blockchain interoperability	Time lock contracts, relay smart contracts, and bridge contracts
[16]	To investigate the general guidelines and protocols for blockchain systems that are compatible in order to identify the commonalities in their architecture	General interoperable frameworks
[17]	To suggest InterTrust, an effective, interoperable blockchain architecture, to facilitate trustworthiness and interoperability across arbitrary blockchain systems	Atomic crosschain protocol
[18]	To provide a methodical and thorough analysis of blockchain interoperability, which is defined as the capacity of blockchains to flexibly share data, transfer assets, and invoke smart contracts across a variety of consortium, private, and public blockchains without requiring modifications to the underlying blockchain systems	Sidechains, notary scheme, hashed time lock contracts (HTLC), relays and blockchain agnostic protocols
[19]	To carry out a thorough analysis of the privacy-preserving methods currently used in interoperability technology based on hash-locking, sidechains/relays, and notary schemes	Hashed locking-based, sidechain / relay-based and notary scheme–based
[20]	To explore the importance of blockchain interoperability, what has been done in the last decade, and where the field is headed	Bridges
[21]	To conduct a systematic literature review to explore architectural mechanisms supporting the interoperability and security of blockchain-based Health Management Systems	Relay chain

In order to emphasize their shared design features, the authors of [16] investigated the general guidelines and protocols for interoperable blockchain systems. They also conducted a survey of practical instances, compared prior systems, and presented their unique characteristics. Additionally, they discussed critical challenges and pointed out potential research directions.

In order to facilitate trustworthiness and interoperability among arbitrary blockchain systems (including homogeneous and heterogeneous blockchains), the authors of [17] proposed InterTrust, an effective, interoperable blockchain architecture. It featured an atomic cross-chain communication protocol, which facilitates seamless integration of current blockchain systems by acting as an agnostic protocol. Two novel strategies—a threshold signature scheme and trusted hardware—powered InterTrust. While trusted hardware ensures trusted services across various blockchain systems, the threshold signature scheme ensures consistency and verifiability in the target blockchain systems. They developed an effective cross-chain communication protocol to enable atomic swaps and interoperable operations between various blockchain systems by fusing these two strategies.

The ability of blockchains to flexibly transfer assets, share data, and invoke smart contracts across a variety of public, private, and consortium blockchains without requiring modifications to the underlying blockchain systems is known as blockchain interoperability, according to the authors' thorough and methodical survey on the topic in [18]. They divided the existing works into five groups: blockchain agnostic protocols, relays, hashed time lock contracts, sidechains, and notary schemes. A taxonomy comprising system and safety attributes such as decentralization, communication direction, locking mechanism, verification mechanism, trust, safety, liveness, and atomicity was also used to analyze these works. A thorough analysis of the privacy-preserving methods used in hash-locking-based, sidechains/relays-based, and notary-scheme-based interoperability technology was carried out in [19]. In particular, they assessed the efficacy and shortcomings of the surveyed techniques using a number of evaluation criteria, such as confidentiality, anonymity, unlinkability, conditional traceability, auditability, scalability, universality, efficiency, fairness, atomicity, and fault tolerance.

In [20], the authors explored the importance of blockchain interoperability, what has been done in the last decade, and where the field is heading. They presented the state of the art for blockchain technologies, which seem more connected than ever through bridges, oracles, and other interoperability mechanisms. They concluded that recent developments have steadily improved the scalability of blockchain networks and provided new functionalities and use cases, but there is still a long way to go until mass adoption. Given the security threats to medical data, ensuring the interoperability of the whole healthcare ecosystem is still a constant challenge. The healthcare ecosystem is becoming more balanced thanks to blockchain technology, but it is hard to find proven solutions because of the ongoing development of new blockchain technologies and the changes in healthcare systems. In [21], the study focused on two main objectives. First, a systematic literature review was conducted to explore architectural mechanisms supporting the interoperability and security of blockchain-based health management systems. Based on these findings, a number of scenarios were developed to demonstrate the potential applications of these mechanisms as well as their background, problems, and architectural considerations. Second, a domain language was developed using the model-driven engineering methodology for particular smart contracts, and a high-level architecture and validation were suggested through an experiment.

4.4 FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

The foundation of cryptocurrency functionality is blockchain technology, a revolutionary invention with numerous applications in a wide range of sectors. Figure 4.2 illustrates the fundamentals and features of blockchain. Fundamentally, blockchain is a decentralized ledger that guarantees decentralization, security, and transparency [22–24]. This ground-breaking method of handling transactions and data management is based on a number of essential elements that come together to form a dependable and impenetrable system.

4.4.1 Decentralized Ledger Architecture

The most basic component of blockchain is the decentralized ledger architecture. A blockchain runs on a decentralized network of nodes, in contrast to conventional centralized systems where a single entity controls the entire database. The system is more resilient to interruptions and attacks because each node maintains a copy of the

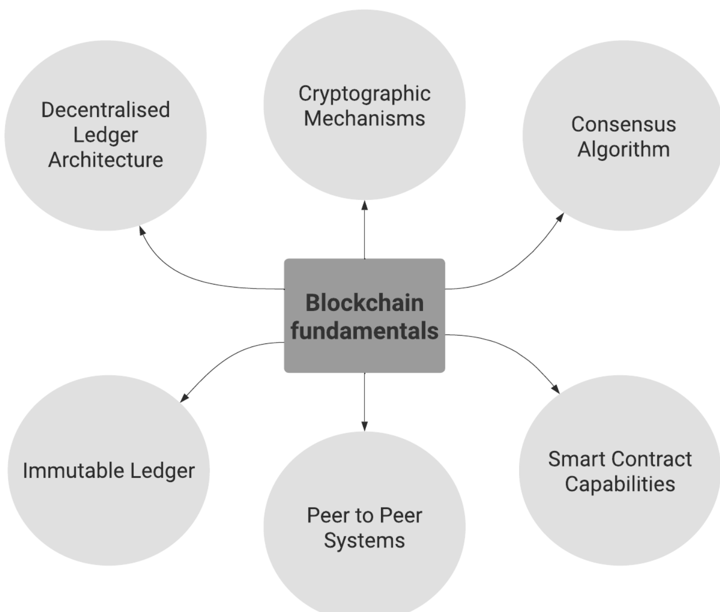


FIGURE 4.2 Fundamentals of blockchain technology

entire ledger, eliminating any single point of failure. Blocks containing transactions are stored and connected chronologically. Because every entity of the network can see and validate the information of transactions, this structure not only increases security but also transparency [25, 26].

4.4.2 Cryptographic Mechanisms

For the data recorded on a blockchain to be secure and intact, cryptographic mechanisms are necessary. Specifically, public key cryptography is essential to transaction authorization and authentication. Every member of the blockchain network possesses a set of cryptographic keys: a private key that is kept hidden and a public key that is accessible to other users. Ensuring that only the legitimate owner can approve the transfer of assets, transactions are signed using the private key and can be independently validated by others using the matching public key. Blocks are also connected by cryptographic hash functions, which ensure data immutability by making it nearly impossible to change one block's contents without also changing all of the blocks that come after it.

4.4.3 Consensus Algorithms

The protocols that allow distributed systems to concur on a single version of the truth even when malevolent actors are present are known as consensus algorithms. Consensus procedures are essential in a blockchain network for approving transactions and appending new blocks. Consensus algorithms come in various forms, each with advantages and disadvantages of its own. With Proof of Work (PoW), which is employed by Bitcoin, users must solve challenging mathematical puzzles in order to add new blocks, which necessitates a substantial computational investment [27]. In contrast, Proof of Stake (PoS) chooses validators based on how many tokens they own and are prepared to "stake" as collateral. Without the need for a central authority, these mechanisms aid in preserving the blockchain's reliability and integrity.

4.4.4 Smart Contract Capabilities

Self-executing contracts, or smart contracts, have the terms of the contract directly encoded into the code. They are blockchain-based applications that, upon the fulfillment of certain conditions, automatically carry out and enforce contracts. This feature minimizes the risks of human error or alteration, lowers costs, and does away with the need for middlemen. Applications for smart contracts are numerous and range from straightforward financial transactions to intricate procedures such as supply chain management and decentralized finance (DeFi) applications. One important development made possible by blockchain technology is its capacity to automate and optimize procedures while maintaining transparency and trust.

4.4.5 Peer-to-Peer Systems

Peer-to-peer (P2P) networks are decentralized networks in which each user, referred to as a peer, serves as both a client and a server. This eliminates the need for a central coordinating server and allows peers to share resources directly with one another. By dividing up the workload among all participants and minimizing reliance on central nodes, which can act as bottlenecks or points of failure, this architecture improves scalability, resilience, and efficiency. P2P systems are frequently utilized in blockchain technologies, where they facilitate distributed ledgers and cryptocurrencies, as well as file-sharing programs such as BitTorrent. This model can continue to function even in the event that a portion of the network fails, promoting robust, democratic data exchange.

4.4.6 Immutable Ledger

An immutable ledger is a kind of digital record-keeping system in which data is permanently and impenetrably recorded, meaning that once it is written, it cannot be removed or changed. This feature is essential to blockchain technology, which creates a chronological and secure chain of data by including a timestamp in each block and a link to the one before it. Cryptographic hashing, consensus techniques, and decentralized verification by numerous network nodes provide such ledgers with their immutability. Immutable ledgers are perfect for applications needing strict integrity, such as digital identity verification, supply chain tracking, and financial transactions, because they guarantee transparency, security, and trust.

4.5 BLOCKCHAIN INTEROPERABILITY FOR SUSTAINABLE HEALTHCARE ECOSYSTEMS

Interoperability between blockchains is essential to creating ecosystems for sustainable healthcare. It improves patient care, facilitates better coordination and communication between healthcare providers, and opens up a large number of real-world use cases. The healthcare sector can completely explore the revolutionary strength of decentralized technology, resulting in more effective, safe, and patient-centered healthcare systems, by resolving interoperability issues.

4.5.1 Importance of Interoperability

Developing sustainable healthcare ecosystems requires interoperability, especially when considering blockchain technology. It describes how various systems and organizations can seamlessly communicate, understand, and use information in a cohesive manner. In the healthcare sector, it is essential to guarantee smooth communication and data exchange between diverse blockchain networks, many of which were developed separately. It is impossible to overestimate the significance of interoperability in the healthcare industry because it makes patient data more unified and enables more precise diagnosis and treatment. Interoperable blockchain networks reduce the risks brought on by data silos, which are isolated systems that contain separate sets of information. This fragmentation can lead to inefficiencies, errors, and delays in patient care. In order to fully utilize blockchain technology and provide long-term, comprehensive, integrated, and patient-centered healthcare services, interoperability is therefore crucial.

4.5.2 Improved Communication and Coordination

Blockchain interoperability improves coordination and communication between different stakeholders in the healthcare system. Interoperable blockchains guarantee that healthcare providers can quickly access and update patient information regardless of where the data was originally stored by enabling real-time data exchange. Improving patient outcomes and clinical decision-making depend heavily on this smooth data flow. For example, interoperable systems can guarantee that a patient's whole medical history is easily accessible when they switch healthcare providers, which can minimize the need for unnecessary tests and lower the risk of medical errors. Furthermore, by offering a single source of truth for patient data, interoperability promotes improved coordination between various healthcare providers, including clinics, hospitals, and pharmacies. In complex care scenarios involving multiple specialists, where timely and accurate information sharing can have a significant impact on the quality of care delivered, coordination becomes even more important. Furthermore, interoperability saves healthcare workers' time and resources by lowering administrative demands associated with data reconciliation and manual entry.

4.5.3 Use Cases Enabled by Interoperable Blockchain Networks

Interoperable blockchain networks can be used to enable a wide range of creative use cases that have the capability to transform the provision of healthcare. One well-known application is the enhancement of electronic health records (EHRs). An example of a blockchain-based electronic health record (EHR) system is described in [23], which uses blockchain to verify the integrity of patient health records in real-time. Interoperability is crucial in this system as it allows different healthcare providers, hospitals, and patients to seamlessly access and share medical records across diverse platforms. This example shows that better patient care continuity can result from interoperable blockchain systems by ensuring EHRs are current and readily available to a variety of healthcare providers. This feature is especially helpful in an emergency when having rapid access to precise patient data can save lives. The supply chain for pharmaceuticals is another important application. Transparency and supply chain integrity can be ensured by tracking the path of pharmaceuticals from producers to end users via interoperable blockchain networks. By ensuring that patients receive authentic medications, this transparency aids in the fight against counterfeit drugs. Furthermore, blockchain interoperability facilitates secure data sharing between research institutions and nations, which promotes collaborative research. A faster discovery of new treatments and therapies can result from this collaboration's acceleration of medical research. Interoperable blockchain networks enable real-time health data sharing across various regions and jurisdictions, which can enhance disease surveillance and response in the field of public health. Its ability to guarantee that timely and accurate information reaches those who need it most is critical for managing public health emergencies and outbreaks.

4.6 APPROACHES AND INITIATIVES FOR BLOCKCHAIN INTEROPERABILITY

Blockchain interoperability approaches and initiatives include industry consortiums, interoperability frameworks, and cross-chain protocols. Each of these elements is essential to the smooth operation of various blockchain networks' interactions and communication, which promotes the growth of cohesive and sustainable blockchain ecosystems. As these initiatives develop further, they will promote blockchain technology's wider adoption and open up new avenues for efficiency and creativity in a variety of industries.

This study categorizes interoperability solutions into three sections: chain, bridge and dApp-based. Each section is further classified into sub-divisions. Table 4.3 depicts the list of interoperability solutions, and Figure 4.3 illustrates the existing interoperability solutions.

4.6.1 Cross-Chain Protocols

Cross-network communication protocols are essential for achieving interoperability among different blockchain networks. The smooth transfer of information and transactions between various blockchain platforms—which may differ in terms of underlying technologies, consensus processes, and data structures—is made possible by these protocols. Effective cross-network communication protocols ensure that data integrity and security are maintained throughout the exchange process.

TABLE 4.3
List of Blockchain Interoperability Solutions

Interoperability Solutions	Divisions	Examples	References
Chain-based	Hash locking	Atomic swap	[13–15, 17–19, 28]
	Sidechain	Polygon	[18, 19]
	Notary scheme	Thorchain	[18, 19]
Bridge-based	Relay	Wanchain	[14, 15, 18–21]
	Blockchain-engine	Polkadot, Cosmos	[14, 28]
dApp-based	Blockchain of blockchain	Hyperledger Fabric	[28]
	Blockchain adaptor	Axelar (AXL) network	[28]
	Blockchain agnostic protocol	Interledger bridges	[14, 18, 28]

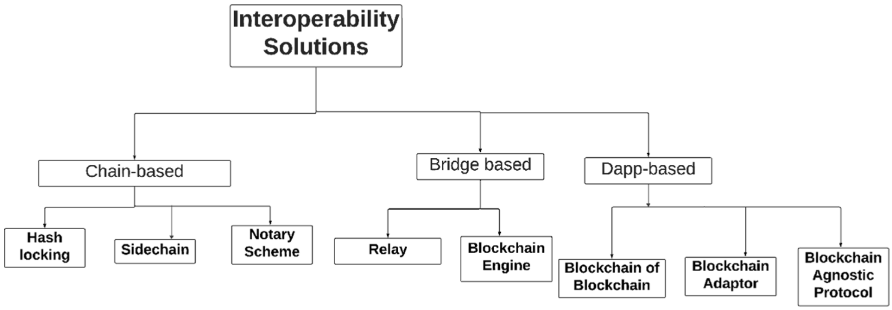


FIGURE 4.3 Illustrates the existing interoperability solutions

4.6.1.1 Chain-Based Interoperability Solutions

Hash Locking: Smart contracts called hashed time lock contracts (HTLCs) are used to impose the conditions of an atomic swap. Time locks and cryptographic hashes are used by HTLCs to guarantee the security of transactions and compliance with swap requirements by both parties. HTLCs establish a time-bound conditional agreement whereby the transaction can only be finalized if certain conditions are met (such as the disclosure of a cryptographic secret) within a predetermined window of time [13–15].

One approach to cross-network communication is the use of atomic swaps, which allow the direct exchange of one cryptocurrency for another without the need for a centralized intermediary [13, 14]. This technique can be extended to facilitate data exchanges across different blockchain networks, ensuring that transactions are executed only when all parties fulfill their contractual obligations. Specialized tools called cross-chain protocols are made to make it easier for assets and data to move between different blockchain networks. These protocols are necessary to enable interoperability, which permits smooth communication and interaction between various blockchains. The Atomic Swap, which enables the direct exchange of one cryptocurrency for another across multiple blockchains without the need for a centralized middleman, is a well-known illustration of a cross-chain protocol. By ensuring that transactions execute concurrently on both blockchains, this method improves trust and security [15].

Sidechain: Using sidechains, which are distinct blockchains that operate in parallel to a mainchain and facilitate asset transfers between the two, is another well-known example [18]. By offering a platform where transactions can be handled more quickly or using different consensus techniques than the mainchain, sidechains allow for interoperability without impacting the stability and security of the main blockchain [19].

Notary Scheme: A key idea in blockchain interoperability is the notary, who acts as a reliable middleman to authenticate and verify data transfers or transactions between various blockchain networks [18]. Cross-chain interactions are made safe, dependable, and trustworthy by the notary mechanism. One example of a notary-based interoperability solution is Hyperledger Fabric [19]. The open-source blockchain platform Hyperledger Fabric, created by the Linux Foundation, is another important interoperability framework. Hyperledger Fabric can be integrated with different blockchain networks and other enterprise systems thanks to its modular architecture, which supports plug-and-play components such as membership services and consensus algorithms. Because of its adaptability, it is a useful tool for companies looking to deploy blockchain solutions that work across platforms.

4.6.1.2 Bridge-Based Interoperability Solutions

Relay: Another method is the development of interoperability frameworks, such as the interledger protocol (ILP) and Polkadot's relay chain. These frameworks provide standardized mechanisms for transferring data and assets across disparate blockchain networks. ILP, for instance, enables the routing of payments across different ledgers, ensuring interoperability among various financial systems. Polkadot's relay chain, on the other hand, connects multiple blockchains, allowing them to interoperate while maintaining their individual governance and consensus mechanisms [18, 19].

Blockchain Engine: Cross-chain bridges are also a popular solution for blockchain interoperability. These bridges facilitate the transfer of data and assets between two or more blockchain networks by acting as intermediaries that validate and relay transactions. Examples include the Cosmos Network's inter-blockchain communication (IBC) protocol, which allows different blockchains to communicate and transfer data securely. Technologies such as Polkadot and Cosmos have also introduced higher-level protocols for cross-chain communication [14, 15]. Through the IBC protocol, Cosmos links various blockchains within its ecosystem to facilitate secure asset and data transfers. A more cohesive blockchain ecosystem is promoted by Polkadot's relay chain, which connects various blockchains (parachains) and permits data sharing and inter-chain transactions [20, 21].

4.6.1.3 dApp-Based Interoperability Solutions

Decentralized application (dApp)-based blockchain systems must be interoperable for cross-chain communication. Semantic interoperability cannot be guaranteed by dApps alone. Therefore, it is crucial to ensure that a dApp supports at least minimum structural interoperability and strives to achieve interoperability among various dApps [28].

Blockchain of Blockchains: One excellent illustration of a blockchain of blockchain interoperability solution is Hyperledger Fabric. It is an open-source system that can be expanded and modularized to run distributed applications. Deployed systems can be highly customized to better meet specific needs due to their support for modular consensus protocols.

Blockchain Adapters: The primary market for blockchain adapters is, for instance, blockchain clients and applications. They provide an interface that allows users to handle interoperability effectively.

Cross-blockchain integration between different decentralized ledgers is made possible by blockchain-agnostic protocols, which allow a single platform to support multiple blockchains. This method gives end users the freedom to select the blockchain of their choice and the ability to move between blockchains without interruption.

4.6.2 Interoperability Frameworks

Comprehensive structures called interoperability frameworks are made to offer standardized techniques for accomplishing smooth communication between various blockchain networks. These frameworks include rules, software, and guidelines that let different blockchains interact, share information, and carry out safe and effective transactions.

The interledger protocol (ILP) is one such framework that is intended to make payments between various ledgers, such as blockchains and conventional financial systems, easier. ILP routes payments via linked ledgers while guaranteeing security and integrity by building a layer atop currently in-place payment networks. This protocol promotes interoperability in the financial industry by enabling the smooth transfer of value across various systems [14, 15, 18].

The World Wide Web Consortium, or W3C, is involved in creating blockchain technology interoperability standards as well. W3C is working to standardize data formats and communication protocols that will improve interoperability between different blockchains by facilitating information exchange.

4.6.3 Industry Consortiums

Organizations from various industries working together to advance blockchain interoperability from industry consortiums. These consortiums bring together participants from different industries, such as financial institutions, technology companies, healthcare providers, and regulatory agencies, to share best practices, create common standards, and encourage the use of blockchain solutions that are interoperable.

The Enterprise Ethereum Alliance (EEA), which aims to improve the Ethereum blockchain's enterprise-use capabilities, is one well-known example. The EEA is working to create specifications and standards that will allow various Ethereum implementations to work in collaboration.

Another significant consortium is the Hyperledger Project, which is hosted by the Linux Foundation. A number of open-source blockchain frameworks and tools are bundled under the Hyperledger project with the goal of advancing enterprise-grade blockchain solutions. Through member collaboration, Hyperledger seeks to create blockchain technologies that are widely adaptable in a variety of industries.

Another example of an industry group committed to advancing blockchain standards and training in the transportation and logistics domains is the Blockchain in Transport Alliance (BiTA). The main goal of BiTA's work is to develop blockchain solutions that are compatible with existing systems and enhance supply chain management's efficiency, security, and transparency.

Through their provision of platforms for collaboration, driving the development of standards, and facilitating the exchange of knowledge and expertise among their members, these consortiums play a crucial role in advancing blockchain interoperability. Through their initiatives, interoperable blockchain solutions are adopted more quickly, which eventually leads to more connected and effective ecosystems across a variety of industries.

4.7 EVALUATION AND IMPLICATIONS

Assessing the effects of interoperability in the healthcare domain necessitates a thorough methodology that takes organizational and technical factors into account. The assessment is centered on the technical aspects of data exchange and communication between various blockchain networks. Metrics such as throughput, latency, security, and data integrity are essential for evaluating how well interoperability solutions work. The assessment should also take into account how scalable the interoperable systems are, making sure they can accommodate growing numbers of users and data without experiencing performance issues.

The benefits of blockchain interoperability for organizations include better patient outcomes, operational efficiency, and healthcare delivery. Through the simplification of data exchange procedures and the elimination of redundancies, interoperable blockchain systems can dramatically lower the administrative burden on healthcare providers. Consequently, this enables medical personnel to concentrate more on patient care as opposed to paperwork. Patients also benefit from a more seamless and integrated healthcare experience because multiple providers can access and use their data across multiple networks without any errors or delays.

A successful blockchain interoperability outcome will also improve data security and privacy. Healthcare organizations can prevent security breaches and unauthorized access to patient information by making sure that data is shared securely across networks. Furthermore, by offering transparent and auditable data trails, interoperable blockchain systems can help with compliance with legal requirements, like the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Figure 4.4 illustrates the evaluation and implications of interoperability solutions.

4.7.1 STRENGTHS AND LIMITATIONS OF EXISTING APPROACHES

The effectiveness and adoption of the current approaches to blockchain interoperability, such as industry consortiums, cross-chain protocols, and interoperability frameworks, are impacted by a number of strengths and limitations.

Strengths of the existing approaches are as follows:

- Cross-Chain Protocols: Robust mechanisms are available to facilitate the transfer of assets and data between different blockchains. Examples of these technologies include Sidechains, Cosmos, and Polkadot. Through simultaneous verification of transactions on both participating chains, these protocols improve security by lowering the possibility of fraud or double-spending. Additionally, they encourage decentralization by doing away with the need for middlemen.

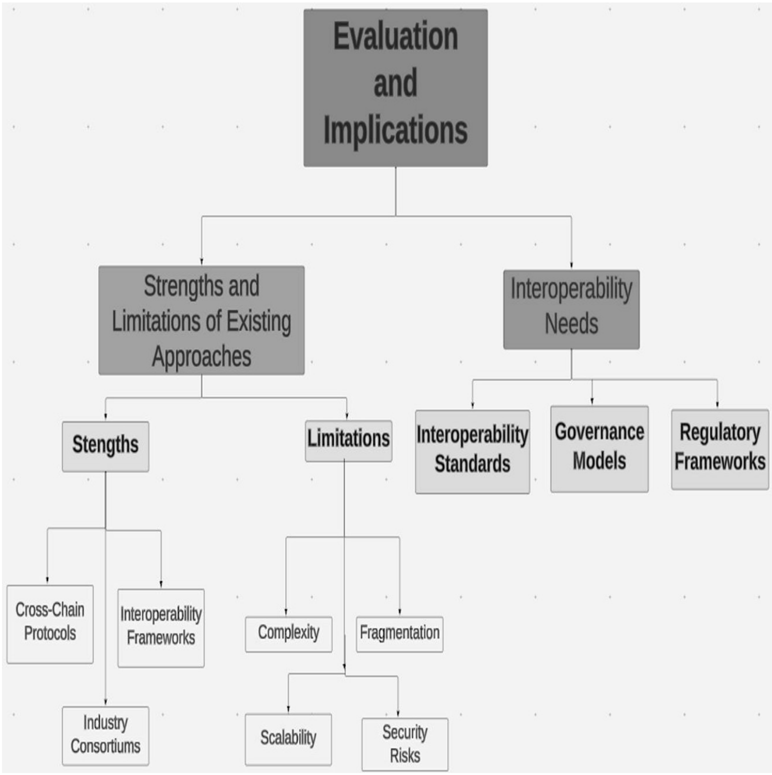


FIGURE 4.4 Illustrates the evaluation and implications of interoperability solutions

- Interoperability Frameworks: Standardized procedures and modular architectures provided by frameworks such as the Hyperledger Fabric and interledger protocol (ILP) enable smooth integration with a variety of blockchain and legacy systems. These frameworks offer flexibility and scalability to support a broad range of use cases and applications. They also support the preservation of data security and integrity throughout the exchange procedure.
- Industry Consortiums: By encouraging cooperation amongst industry participants, consortiums such as the Enterprise Ethereum Alliance (EEA) and Hyperledger Project help to develop best practices and common standards. Through pooled resources and combined knowledge, these cooperative efforts foster innovation and assist in resolving interoperability issues.

Limitations of the existing approaches are as follows:

- Complexity: Cross-chain protocols and interoperability frameworks can be difficult to implement technically, requiring a lot of knowledge and resources. Widespread adoption may be hampered by this complexity, especially in smaller businesses with less sophisticated technology.

- Fragmentation: Industry consortiums have made progress, but there are still no industry-wide standards for blockchain interoperability. The development of separate protocols by various networks and platforms frequently results in fragmentation and inconsistent asset and data exchange.
- Scalability: A lot of the interoperability solutions currently in use have problems with scalability, especially when handling big data sets or high transaction volumes. One of the biggest challenges still facing these systems is making sure they can scale without sacrificing security or performance.
- Security Risks: Cross-chain protocols add new attack vectors but also improve security. For example, if sidechain security is not as strong as mainchain security, sidechains may be subject to attacks. It is imperative to guarantee strong security on all networks that are interconnected.

4.7.2 Need for Interoperability Standards, Governance Models, and Regulatory Frameworks

It is imperative that comprehensive interoperability standards, governance models, and regulatory frameworks be developed in order to reach the extreme limit of blockchain interoperability.

4.7.2.1 Interoperability Standards

It is imperative to establish universal standards for blockchain interoperability in order to guarantee uniformity and compatibility among diverse networks. The protocols for data exchange, transaction validation, security precautions, and other crucial elements of interoperability should be specified in these standards. Establishing and advancing these standards can be greatly aided by groups such as W3C and the International Organization for Standardization (ISO). The implementation of interoperable blockchain systems will be made simpler, less fragmented, and more reliable and efficient with the aid of standardization.

4.7.2.2 Governance Models

For interoperable blockchain networks to be managed during their evolution, effective governance models are essential. The decision-making procedures, dispute-resolution procedures, and roles and responsibilities of various stakeholders should all be described in these models. Valuable insights can be obtained from decentralized governance models, such as those employed by blockchain platforms such as Polkadot and Tezos. These models guarantee that every member has a right to the governance of the network, encouraging openness, responsibility, and diversity. It is still difficult to create governance models that strike a balance between decentralization and efficient monitoring and control.

4.7.2.3 Regulatory Frameworks

For interoperable blockchain systems to adhere to moral and legal requirements, regulatory frameworks are required. Issues such as data privacy, security, know-your-customer (KYC) requirements, and anti-money laundering (AML) must be addressed by regulators. Adoption can be promoted and businesses and users can feel more confident when regulations are uniform and clear. It takes cooperation between standard-setting organizations, industry participants, and regulatory agencies to create fair frameworks that safeguard consumers and encourage innovation. Since blockchain networks frequently operate internationally, international cooperation is also essential because harmonized regulatory approaches are required.

4.8 CONCLUSION AND FUTURE DIRECTIONS

The advancement of sustainable healthcare ecosystems depends heavily on blockchain interoperability. It enhances patient care and facilitates smooth coordination and communication between various healthcare providers. However, there are obstacles in the way of achieving true interoperability. To apply decentralized technology in the healthcare domain, a number of obstacles, including technical complexity, standardization, and the requirement for strong cross-network communication protocols, must be resolved.

Here is the improved version:

This chapter presents challenges facing the healthcare industry and the need for blockchain interoperability in healthcare sustainability. Chain-based, bridge-based, and dApp-based interoperability solutions are the three main categories into which the study divides current interoperability solutions. Hash locking, sidechain, blockchain adaptor, notary scheme, blockchain engine, relay, blockchain of blockchains, and blockchain-agnostic protocol are further subcategories. In addition, it outlines the benefits and drawbacks of each strategy and emphasizes how crucial governance frameworks and standards are to attaining sustainability.

Future work on standardizing frameworks and protocols to enable smooth data transfer between various blockchain networks should be the main focus of blockchain interoperability in healthcare. Healthcare organizations, technology providers, and regulatory bodies must work together to develop interoperable solutions that meet industry standards and are secure, scalable, and compliant. To test and improve these solutions in practical contexts, more research and pilot projects are required. Additional investigation into the blockchain's potential connections with other cutting-edge technologies, such as the Internet of Things (IoT) and artificial intelligence (AI), may improve interoperability and create new opportunities for healthcare innovation.

REFERENCES

1. Zuo, Yanjun. "Making smart manufacturing smarter – a survey on blockchain technology in Industry 4.0." *Enterprise Information Systems*, *15*(10), 1323–1353 (2021).
2. Anthony Jnr, Bokolo. "Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise-a standardized architecture perspective." *Enterprise Information Systems*, *18*(3), 2296647 (2024).
3. Kwon, Oyun, and Sun K. Yoo. "Interoperability reference models for applications of artificial intelligence in medical imaging." *Applied Sciences*, *11*(6), 2704 (2021).

4. Joshi, Pranalini, and Prasad Gokhale. "Electronic health record using blockchain and off chain storage: A systematic review." *Information Technology in Industry*, *9*(1), 247–253 (2021).
5. Centobelli, Piera, Roberto Cerchione, and Emanuela Riccio. "A novel architecture for enhancing Electronic Health Record interoperability: A Blockchain-based approach." In *2021 IEEE Technology & Engineering Management Conference-Europe (TEMSCON-EUR)*. IEEE, 2021.
6. Ghaemi, Sara, Sara Rouhani, Rafael Belchior, Rui S. Cruz, Hamzeh Khazaei, and Petr Musilek. "A pub-sub architecture to promote blockchain interoperability." *arXiv preprint arXiv:2101.12331* (2021).
7. Madine, Mohammad, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Junaid Arshad, and Ibrar Yaqoob. "appxchain: Application-level interoperability for blockchain networks." *IEEE Access*, *9*, 87777–87791 (2021).
8. Reegu, Faheem Ahmad, Hafiza Abas, Yonis Gulzar, Qin Xin, Ali A. Alwan, Abdoh Jabbari, Rahul Ganpatrao Sonkamble, and Rudzidatul Akmam Dziyauddin. "Blockchain-based framework for interoperable electronic health records for an improved healthcare system." *Sustainability*, *15*(8), 6337 (2023).
9. Usman, Muhammad, Verena Kallhoff, and Anjum Khurshid. "The case for establishing a blockchain research and development program at an academic medical center." *Blockchain in Healthcare Today*, *4* (2021).
10. Kothari, Prasad, Melanie Nuce, Ingrid Vasiliu-Feltes, Dominique Hurley, Mercury Fox, Sweta Sneha, Wendy Charles, Jim Nasr, and Radhika Iyengar. "Blockchain predictions for health care in 2021." *Blockchain in Healthcare Today*, *4* (2021).
11. Yaqoob, Ibrar, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." *Neural Computing and Applications*, 1–16 (2022).
12. Belchior, Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. "A survey on blockchain interoperability: Past, present, and future trends." *ACM Computing Surveys (CSUR)*, *54*(8), 1–41 (2021).
13. Mohanty, Debasis, Divya Anand, Hani Moaiteq Aljahdali, and Santos Gracia Villar. "Blockchain interoperability: Towards a sustainable payment system." *Sustainability*, *14*(2), 913 (2022).
14. Kotey, Seth Djanie, Eric Tutu Tchao, Abdul-Rahman Ahmed, Andrew Selasi Agbemenu, Henry Nunoo-Mensah, Axel Sikora, Dominik Welte, and Eliel Keelson. "Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication." *IET Communications*, *17*(8), 891–914 (2023).
15. Khan, Sajjad, Muhammad Bilal Amin, Ahmad Taher Azar, and Sheraz Aslam. "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability." *IEEE Access*, *9*, 116672–116691 (2021).
16. Wang, Gang, Qin Wang, and Shiping Chen. "Exploring blockchains interoperability: A systematic survey." *ACM Computing Surveys*, *55*(13s), 1–38 (2023).
17. Wang, Gang, and Mark Nixon. "Intertrust: Towards an efficient blockchain interoperability architecture with trusted services." In *2021 IEEE International Conference on Blockchain (Blockchain)*, pp. 150–159 (2021).
18. Ren, Kunpeng, Nhut-Minh Ho, Dumitrel Loghin, Thanh-Toan Nguyen, Beng Chin Ooi, Quang-Trung Ta, and Feida Zhu. "Interoperability in blockchain: A survey." IEEE Transactions on Knowledge and Data Engineering, 35(12), 12750–12769, (2023).
19. Yin, Ruoyu, Zheng Yan, Xueqin Liang, Haomeng Xie, and Zhiguo Wan. "A survey on privacy preservation techniques for blockchain interoperability." *Journal of Systems Architecture*, *140*, 102892 (2023).

20. Belchior, Rafael, Jan Süßenguth, Qi Feng, Thomas Hardjono, André Vasconcelos, and Miguel Correia. “A brief history of blockchain interoperability.” *Authorea Preprints* (2023).
21. Villarreal, Edgar R. Dulce, Jose García-Alonso, Enrique Moguel, and Julio Ariel Hurtado Alegría. “Blockchain for healthcare management systems: A survey on interoperability and security.” *IEEE Access*, *11*, 5629–5652 (2023).
22. Sharma, Neetu, and Rajesh Rohilla. “Blockchain based Approach for Managing Medical Practitioner Record: A Secured Design.” In *IEEE Conference IACC (10th International Advance computing Conference 2020)*, 2020,
23. Sharma, Neetu, and Rajesh Rohilla. “Blockchain based Electronic health Record Management system for Data Integrity.” In *International Conference on Computational Intelligence ICCI-2020*, Springer Book Series Algorithms for Intelligent Systems (AIS).
24. Sharma, Neetu, and Rajesh Rohilla “Blockchain Based Secured Telecare Medical Record Management: A System Design.“ In *Fifth International Joint Colloquiums on Computer Electronics Electrical Mechanical and Civil - CEMC 2020*, Grenze Scientific Society, 2020.
25. Sharma, Neetu, and Rajesh Rohilla. “Hyperledger blockchain-enabled decentralized application for drug discovery chain management.” *Computers & Industrial Engineering*, *183*, 109501 (2023).
26. Sharma, Neetu, and Rajesh Rohilla. “A multilevel authentication-based blockchain powered medicine anti-counterfeiting for reliable IoT supply chain management.” *The Journal of Supercomputing, 80*(4), 4870–4913 (2024).
27. Sharma, Neetu, and Rajesh Rohilla. “Scalable and cost efficient PoA consensus-based blockchain solution for vaccination record management.” *Wireless Personal Communications*, *135*, 1177–1207, (2024).
28. Wang, Gang. “Sok: Exploring blockchains interoperability.” *Cryptology ePrint Archive* (2021).

5 Transforming Healthcare
Blockchain and Digital Twins for Secure Data Exchange

Rujuta Shah, Mansi Mehta, and Dipti Bhatt

5.1 INTRODUCTION

The healthcare sector is undergoing a major transformation with the adoption of new technologies such as digital twins, blockchain, the Internet of Things (IoT), and artificial intelligence (AI). These innovations are essential for driving the industrial revolution in various fields. Specifically, Healthcare 4.0 plays a crucial role in this change by aiming to create an autonomous care system that fosters a learning healthcare environment, enabling data-driven decision-making.

Healthcare 4.0 utilizes the Industrial Internet of Things (IIoT), digital twins, machine learning (ML), and big data to reach its goals. For example, digital twins act as virtual representations of physical objects, including devices linked to both humans and machines [1]. By combining blockchain with digital twin technologies, healthcare systems can be built on secure connections between different medical devices and systems. Additionally, the successful integration of these devices necessitates a secure and decentralized collaborative framework. This framework ensures that healthcare decision-makers receive timely notifications, which aids in making informed and efficient decisions. By adopting these technologies and fostering their collaborative use, the healthcare sector can improve its capabilities and advance patient care and overall healthcare management.

5.1.1 Blockchain and Digital Twin Overview

Integrating blockchain technology with digital twins greatly enhances data security, transparency, and efficiency. This powerful combination creates new opportunities for advanced applications across various sectors, including smart manufacturing, healthcare, smart cities, and more, leading to safer, more efficient, and collaborative systems. Let's take a closer look at blockchain and digital twins individually.

5.1.1.1 Blockchain

By definition, blockchain technology employs a decentralized, distributed ledger to record transactions across multiple computers, ensuring that retroactive alterations

DOI: 10.1201/9781003532286-5

are securely prevented [2]. Each block in the chain contains a list of transactions, and once completed, it is added to the chain in a linear, chronological order.

In healthcare systems that use blockchain, hashing functions and digital signatures play a key role in protecting sensitive medical information. Hashing functions take input data, such as patient records, and turn it into a unique, fixed-length hash. Even a tiny change in the original data results in a completely different hash, making it easy to spot any tampering or unauthorized changes. This helps maintain data integrity in healthcare, where it is crucial for records to stay consistent and unchanged. Meanwhile, digital signatures verify the identity of users who access or change data. A healthcare provider uses a private key to digitally sign transactions or data, and others can check the signature's validity with the provider's public key. This ensures that only authorized people can access sensitive healthcare information, such as electronic health records (EHRs), thus preventing fraud or unauthorized access. Together, hashing and digital signatures keep healthcare data in blockchain systems secure, tamper-proof, and accessible only to verified users, boosting trust and privacy in managing patient data.

Key Features:

1. **Decentralization:** Blockchain technology works on a decentralized network architecture, in which many nodes share control instead of being centralized in one place. Every node in the network has access to the complete ledger and is capable of independently validating and recording transactions. By decentralizing, the dangers of malicious attacks and system failures that come with central points of failure are reduced. Blockchain builds user trust by strengthening the system's resilience and dependability through the removal of intermediates.
2. **Immutability:** The immutability of blockchain is one of its distinguishing characteristics. A transaction cannot be changed or removed after it has been added to the blockchain and recorded in a block. A safe chain is formed between the blocks by the cryptographic hash of each block. Because of this, it is very difficult for someone to alter the data covertly. In applications that need high integrity and trust, such as financial transactions and record-keeping, immutability guarantees that the data is permanent, verifiable, and immune to fraud.
3. **Transparency:** Blockchain technology encourages openness by making the ledger viewable and transaction verification possible for all network users. This openness is available to everybody with an internet connection in public blockchains, allowing for an open and transparent system. Every transaction has a timestamp and is connected to other transactions to create a comprehensive and verifiable history. Because all activities are accessible and auditable by any participant, this transparency aids in the prevention of fraud. Because consumers can independently confirm the validity and veracity of the data, it fosters user trust [3].
4. **Security:** Blockchain ensures the security of transactions and data through the use of advanced cryptographic techniques. Every transaction is

encrypted and connected to the previous transaction, creating an unbroken chain that is highly resistant to tampering. The consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), add an extra layer of security by requiring participants to agree on the validity of transactions before they are added to the blockchain. This decentralized consensus process makes it extremely challenging for any individual or entity to manipulate the system, protecting against fraud and cyberattacks.

5. **Smart Contracts:** Smart contracts are agreements that are encoded in software and automatically execute and enforce their terms when specific conditions are met. This process removes the need for intermediaries, lowers transaction costs, and enhances efficiency. Smart contracts can be applied in various fields, such as financial transactions, supply chain management, and legal agreements. They boost reliability and transparency by ensuring that the contract is carried out consistently and fairly, as the code adheres to the programmed instructions without any human intervention [4].
6. **Consensus Mechanisms:** Consensus mechanisms are essential for the operation of blockchain, as they ensure that all nodes in the network agree on the validity of transactions. One well-known mechanism is PoW, where miners solve intricate mathematical puzzles to validate transactions, while PoS chooses validators based on the number of tokens they hold. These mechanisms help prevent double-spending and ensure the ledger's accuracy and timeliness. By requiring consensus across the network, these algorithms maintain the integrity and security of the blockchain, removing the need for a central authority.
7. **Efficiency and Speed:** Blockchain technology has the potential to significantly improve the efficiency and speed of transactions by streamlining processes and removing the need for intermediaries. Traditional financial systems often require several days to process and settle transactions due to the involvement of multiple intermediaries and verification steps. In contrast, blockchain transactions can be finalized in minutes or even seconds, thanks to automated validation and the removal of unnecessary middlemen. This enhanced efficiency is particularly beneficial for cross-border transactions, which are usually slow and costly.
8. **Tokenization:** This involves converting assets or rights into digital tokens on a blockchain. These tokens can represent a variety of items, including physical assets such as real estate and commodities, as well as digital assets and securities. The tokenization process allows for fractional ownership, making it easier to buy, sell, and trade assets. It boosts liquidity by facilitating the transfer and trading of assets on blockchain platforms. Additionally, tokenization opens up new investment opportunities and provides access to assets that were previously hard to trade or out of reach for many investors.

Together, these features create a robust framework that enables blockchain technology to significantly influence various sectors. It enhances security, transparency, and efficiency while reducing costs and fostering the development of innovative business models.

Use Cases:

Blockchain technology has many applications in various industries. Each leverages the unique characteristics of decentralization, immutability, and transparency. In finance, blockchain supports **cryptocurrencies** such as Bitcoin and Ethereum, allowing direct transactions between users without the need for a middleman [5]. It reduces costs and accelerates transactions in the supply chain. Blockchain management leverages transparency and traceability. This allows stakeholders to confirm the origin and movement of goods. This reduces fraud and increases efficiency. Blockchain in the **healthcare sector** preserves patient records. It allows authorized individuals to share information seamlessly. and guarantee data integrity and privacy. The real estate market employs blockchain for property transactions, simplifying the process, reducing paperwork, and offering a clear, tamper-proof history of ownership. Blockchain has the potential to transform voting systems by ensuring transparency and preventing tampering, which can build greater trust in electoral processes. Intellectual property management also gains from blockchain, as it creates a verifiable and immutable record of creation, ownership, and rights transactions. Furthermore, in the energy sector, blockchain facilitates peer-to-peer energy trading, enabling consumers to buy and sell excess energy directly, which encourages the use of renewable sources. These varied applications highlight how blockchain can improve security, efficiency, and trust across multiple fields, driving innovation and reshaping traditional systems.

5.1.1.2 Digital Twin

A digital twin is an electronic replica of a real-world system, process, or object. This technology has the ability to forecast future outcomes, manage risks, and enhance efficiency. Digital twins merge real-time data with various other sources to create dynamic digital simulations. Similar to its physical counterpart, the digital twin evolves over time.

Key Features:

1. **Real-Time Data Integration:** Digital twins merge information from sensors, IoT devices, and enterprise systems to form a dynamic model of physical assets. This ongoing data stream allows for real-time monitoring and analysis of the asset's performance, conditions, and operational status. By integrating data in real-time, the digital twin provides an accurate representation of the physical object's current state, facilitating timely decision-making and proactive maintenance. The precision of real-time data integration also helps in forecasting potential issues and enhancing operational efficiency.
2. **Modeling and Simulation:** Digital copies use advanced computational and modeling approaches to replicate how physical assets operate and perform in a virtual environment. These computer simulations use historical and current data to estimate how the asset would perform under various scenarios and conditions. This functionality allows engineers and operators to explore various strategies, optimize processes, and find potential

enhancements without involving the actual resource. Simulation and modeling are crucial in complex systems where real-world testing is extremely costly or dangerous.

3. **Scalability and Flexibility:** Digital twins can develop and evolve, allowing businesses to begin with a single asset and extend to incorporate entire systems or even entire organizations. This scalability means that digital twin solutions can grow to meet changing business needs, including more complicated scenarios and greater data volumes. Furthermore, the adaptability of digital twins enables them to interact with a wide range of technologies and systems, ensuring interoperability and flexibility across applications and sectors.
4. **Improved Decision-Making:** Digital twins assist in informed decision-making by providing an in-depth and complete picture of resources, processes, and systems. The amalgamation of data analytics, machine learning, and AI in digital twins results in more accurate conclusions and actionable data. This lets decision-makers simulate numerous circumstances, analyze the impact of different alternatives, and make data-driven decisions. This increased decision-making capacity helps to optimize processes, save costs, and elevate performance.
5. **Management of Lifecycle:** Digital Twins improve asset management during every phase of lifecycle, from initial planning and creation to operation and ultimately deactivation. Keeping a virtual copy updated regularly helps organizations track how a resource is performing, spot any signs of wear and tear, and plan for necessary upgrades or replacements. This all-encompassing strategy promotes effective and sustainable asset management, leading to reduced overall ownership costs and better long-term performance..

Use Cases:

Digital twins have transformed a variety of industries by offering detailed, up-to-date digital duplicates of physical assets and processes. In **manufacturing**, digital twins support **proactive maintenance** by constantly overseeing equipment and **anticipating malfunctions** before they happen, thereby decreasing downtime and maintenance expenses [6]. Within the **automotive sector**, this technology is employed to **replicate** and **evaluate** new vehicle designs and performance in various scenarios, enhancing **safety** and **effectiveness**. The **energy industry** utilizes digital twins to enhance the efficiency of power plants and grids, improving energy distribution and lowering operational expenses.

Digital twins have a major impact across different sectors as they provide real-time digital replicas of actual equipment and processes. In the manufacturing industry, they enable proactive maintenance by constantly monitoring machines and determining potential failures before they occur, resulting in shorter downtime and lowered maintenance costs. In the automobile industry, digital twins help create and test new car designs and how they perform in various situations, making cars safer and more efficient. This same technology is used in the energy industry to better manage power plants and infrastructure, leading to better energy distribution and lower operating costs. The healthcare sector uses digital twins technology to generate different human organs for experimentation thus enabling more effective treatment options and advanced diagnostic tools, which ultimately lead to better outcomes for patients. For the development of smart cities, this technology is utilized to manage urban infrastructure and resources, such as traffic movement, waste management, parking spaces, etc., thereby improving citizens standards of living. In construction, digital twins provide real-time insights into projects, helping to keep them on track and within budget while also enhancing safety measures. The aviation industry uses digital twins to oversee aircraft from design and manufacturing through to operation and maintenance, which increases efficiency and reduces costs. Furthermore, digital twins enable autonomous control and monitoring in industries such as oil and gas, resulting in faster decision-making and enhanced security in potentially dangerous circumstances.

These varied applications highlight the tremendous impact of digital twin technology in enhancing efficiency, lowering costs, and promoting innovation across multiple sectors.

5.1.2 Integration of Blockchain and Digital Twins

The combination of blockchain technology and digital twins in the healthcare sector presents a revolutionary method for advancing personalized medicine, enhancing data security, and improving operational efficiency. A digital twin serves as a virtual representation of a patient, continuously gathering real-time information from wearable devices and medical sensors to replicate the patient's health status. Blockchain technology guarantees that this data is securely stored, resistant to tampering, and accessible solely to authorized individuals, effectively addressing vital issues related to privacy and data integrity. The decentralized nature of blockchain facilitates the seamless exchange of the digital twin's health information among healthcare providers, fostering improved collaboration and the development of more precise, personalized treatment strategies. Additionally, smart contracts streamline access control, empowering patients to retain authority over their data and consent processes. This integration proves especially beneficial for managing chronic diseases, as real-time monitoring and predictive analytics from digital twins can initiate automatic adjustments to treatment plans. Furthermore, blockchain establishes a transparent and immutable audit trail for all interactions involving the patient's data, promoting trust and accountability within the healthcare ecosystem. The synergy of these technologies enhances data interoperability, refines decision-making processes, and supports efficient, patient-centered healthcare delivery.

5.1.2.1 Use Case—Integration of Blockchain and Digital Twins

A practical application of combining blockchain technology and digital twins in the healthcare sector is the customization of treatment for chronic illnesses, such as diabetes. In this context, a digital twin is developed to serve as a real-time virtual model of the patient's physiological data, which is gathered from IoT-enabled devices such as continuous glucose monitors, smart insulin pumps, and fitness trackers. This digital twin not only reflects the patient's current health status but also forecasts potential future health conditions, allowing healthcare professionals to create personalized, data-driven treatment strategies.

Blockchain technology is essential in this framework, as it guarantees the security, privacy, and integrity of the real-time data that is collected and exchanged among patients, healthcare providers, and insurance companies. Utilizing smart contracts on the blockchain, the information from the digital twin is shared securely with authorized entities while ensuring that patients maintain consent and control over their health data access. Each interaction or change to the digital twin's data is cryptographically secured and time-stamped on the blockchain, creating a transparent and unalterable audit trail.

The integration of blockchain and digital twins facilitates automated, real-time monitoring and adjustments to treatment plans based on predictive analytics, ensuring that healthcare is personalized, efficient, and secure. Furthermore, blockchain promotes interoperability among various healthcare systems and medical devices, enabling seamless integration of patient data across different platforms, enhancing collaboration, and improving outcomes in the management of chronic diseases. This system also empowers patients by granting them control over their data and ensuring privacy, while simultaneously reducing costs by decreasing redundant tests and manual interventions.

5.2 DIGITAL TWIN TECHNOLOGY IN HEALTHCARE FOR SECURE HEALTHCARE SHARING

Digital twin technology is being increasingly integrated into the healthcare industry, providing opportunities for transformation in patient care, medical research, and healthcare management. Essentially, a digital twin in healthcare is a virtual representation of a physical object, such as a patient, organ, or medical device, constantly updated with real-time data. This detailed and dynamic model enables personalized medicine, better diagnostics, and customized treatment plans for each patient.

Through ongoing analysis of patient data for minute changes that enable prompt interventions, digital twins in diagnostics improve early disease identification. To minimize risks and enhance results, surgeons employ digital twins for the planning and practice of intricate procedures.

The field of customized medicine is one in which digital twins are widely used. Healthcare professionals may better manage chronic illnesses, anticipate treatment results, and customize interventions by modeling the physiological and biological processes of their patients. Doctors can select the best course of action with the fewest possible adverse effects by using a digital twin of a patient with heart problems to simulate how the patient's heart reacts to various drugs.

By anticipating equipment maintenance requirements and streamlining patient flow, digital twins enhance hospital administration. In addition, they provide telemedicine and remote monitoring, providing instantaneous health insights to patients—a crucial aspect of chronic disease management and elder care. Digital twin technology generally results in improved patient outcomes and higher efficiency by providing more precise, predictive, and individualized treatment.

5.2.1 Challenges in Traditional Data Sharing

The process of making data accessible to other individuals, entities, or organizations is referred to as data sharing. This can be carried out for a number of purposes, including analysis, research, and collaboration. The large amounts of administrative and clinical data generated by providers have been seeing extensive growth in the past decade. Healthcare data management has shown itself to be a challenge as well as an opportunity to enhance healthcare IT security [7].

Healthcare providers use healthcare data management software to meet regulatory compliance needs, elevate efficiency, enhance healthcare solutions, increase the quality and security of care delivery, and accomplish both short- and long-term goals.

Conventional methods of sharing health data, such as paper-based records or manual procedures, present a number of challenges:

1. **Restricted Access:** Often, the health records on paper are kept in physical files within healthcare facilities thus making it hard to access and retrieve details quickly, even by authorized personnel. This in turn may delay the patient's treatment, especially during emergencies where timely use of medical history and treatment details are crucial.
2. **Data Fragmentation:** Health data stored using traditional methods is usually split into many files with various documents and reports, making it harder to gather and combine information for overall analysis and decision-making. This separation makes it difficult for doctors to coordinate care or regularly monitor patients' health.
3. **Risk of Loss or Damage:** Health records stored on paper are prone to degradation, loss, and damage over time. Critical health records may be lost due to natural disasters, accidents, or carelessness, jeopardizing patient safety and treatment continuity.
4. **Limited Interoperability:** Combining data from multiple sources and sharing information among doctors and/or physicians is challenging because paper records are not compatible well with EHR systems or other health-related digital platforms. This lack of compatibility makes it hard to share data and collaborate effectively in healthcare.
5. **Security Concerns:** Paper-based health records are vulnerable to theft, tampering, and unauthorized access. If proper precautions—such as secure filing cabinets, access logs, and authentication protocols—are not in place, patient privacy and confidentiality can be at risk, which may lead to breaches of trust and legal issues.
6. **Inefficient Data Management:** Managing medical records on paper is inefficient, consuming a lot of time, money, and physical space. Healthcare

facilities must dedicate resources to labor-intensive tasks such as sorting, filing, and maintaining documents. This dependency on manual processes increases the likelihood of errors and inconsistency in data handling.

The transition from paper-based record-keeping to digital health information systems, such as electronic health records (EHRs) and health information exchanges (HIEs), is necessary to address these challenges. Healthcare organizations may overcome the drawbacks of conventional data exchange techniques and fully utilize health information to enhance patient care, research, and public health by digitizing health data and implementing interoperable, secure, and scalable technologies.

However, the challenges of using patient data in healthcare analytics need to be overcome. There needs to be an organized method of dealing with fragmented data, enabling its analysis, integrating it, and deriving necessary and relevant insights to ensure optimum security and privacy. Furthermore, health data management solutions need to be accessible. This is where healthcare data management, IT solutions, and digitization come into play.

5.2.2 Introduction to Blockchain-Based Solution

Digital twins are increasingly being used in healthcare for scheduling patient care, medical device monitoring, and hospital management. Digital twins in healthcare are virtual models of medical devices such as ventilators, pacemakers, insulin pumps, imaging equipment such as MRIs, and advanced surgical robots. These models are continuously refreshed with real-time data from the actual devices, which are connected through IoT sensors.

Key parameters that are typically monitored include:

- Device performance, such as energy consumption and operational functionality.
- Wear and tear of components, including part degradation and the need for calibration over time.
- Environmental factors, such as temperature and humidity that could affect device operation.
- Patient interaction focuses on how effectively the device responds to patient vitals.

For example, the company GE Healthcare creates a digital twin of a patient's organs using MRIs and CT scans. The surgeon can then simulate surgical procedures on this twin and predict patient responses [8]. Such a simulation can simulate blood flow, tissue elasticity, and outcomes based on variations in techniques. Risks are thus reduced, and surgical results are improved through high-risk surgeries such as brain tumor removal. Doctors can also predict probable complications and calibrate their strategy accordingly.

Another instance, the Children's National Hospital in Washington, DC, implemented a digital twin with GE Healthcare and streamlined neonatal care [9]. It tracks the vital signs of newborn babies, providing early intervention and a prediction of complications such as sepsis and respiratory failure. AI processes all this information and thus allows doctors and nurses to intervene earlier. The system would improve early intervention and decrease false alarms in the NICU, hence reducing the noisiness and stress of the environment for patients.

Whereas, Siemens Healthineers uses digital twinning to predict the maintenance of medical imaging equipment such as MRI and CT scanners. The twin tracks performance metrics such as how much the worn components are, the energy levels, temperature, and the calibration of the machine, and therefore allows predictive analytics that foretells a possible failure. It reduces downtime and increases efficiency since Siemens was able to lower the downtime of an MRI machine by 30% through the use of digital twins. Technology is highly important in ensuring reliable equipment in hospitals to improve service delivery.

With these implementations, digital twins offer immense potential to revolutionize how healthcare providers deliver personalized care, ensure patient safety, and improve device management. Also, such approaches lead to a more proactive management of medical devices, with predictive analytics identifying potential issues or needed upgrades well before they cause any problems.

To enhance the security, transparency, and integrity of such digital twin systems, the decentralized and immutable nature of blockchain can be leveraged and blockchain-based solutions can be implemented in healthcare.

Digital twins are virtual representations of physical objects, systems, or processes. They are created using sensor data, IoT devices, and other sources to mimic their real-world counterparts. As seen in Figure 5.1, a blockchain-based electronic healthcare system that makes use of digital twins consists of a few fundamental components. Each of these components is essential to guarantee that the system is safe, effective, and able to deliver reliable healthcare insights. Let us examine these components further:

1. **User Interface and Applications:** Web-based as well as mobile applications for patients and doctors to interact with the system through various smart devices. This ensures comfort, convenience, and accessibility.
   - **Patient Portals:** User-friendly UIs for patients are very essential so that they can access their digital twin or view their health data, and/or can also interact with doctors/physicians.
   - **Dynamic Dashboards:** Comprehensive and dynamic dashboards for doctors, providing real-time updates to monitor patient health, analyze digital twin data, and make appropriate decisions.
2. **Interoperability Framework:**
   - **APIs and Integration Layers:** Appropriate APIs, preferably standardized and middleware layer(s) need to be implemented for seamless data exchange between different systems, devices, and/or digital platforms.
   - **Standards and Protocols:** Certain healthcare data standards such as HL7, FHIR, etc., need to be adhered to, to ensure compatibility and interoperability across various healthcare applications and devices.

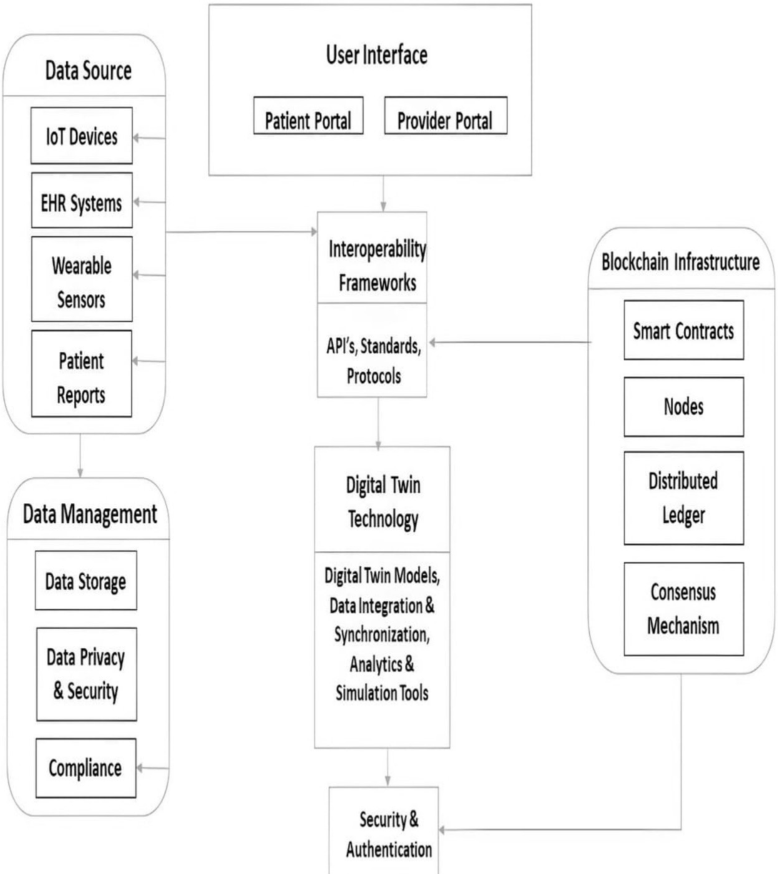


FIGURE 5.1 Blockchain and digital twin–based electronic healthcare system

- **Data Management:** Huge amounts of data will be generated through diverse sources such as IoT medical devices, EHRs, patient-reported data, and historical medical records, and needs to be managed.
- **Data Storage:** Require secure and scalable storage solutions for both on-chain and off-chain data, ensuring accessibility and compliance with healthcare regulations (e.g., HIPAA).

3. **Data Privacy and Security:** Encryption, confidentiality, and access control mechanisms need to be implemented to protect patient data and maintain privacy and data integrity.
4. **Blockchain Infrastructure:** This includes a number of elements as mentioned below:
   - **Distributed Ledger:** This is the core of the blockchain system, where all transactions and data exchanges are recorded in a secure and immutable manner.

- **Smart Contracts:** Another important element, is the self-executing contracts which have the terms of the agreement/contract directly embedded in the code. These elements automate processes such as patient consent, insurance claims, access control, etc.
- **Consensus Mechanism:** Consensus for blockchain is a process in which all members of a blockchain network agree on the current state of the data in the network. Consensus algorithms such as PoW, PoS, Proof of Burn, or Proof of Authority, etc., establish stability and trust in the blockchain network.
- **Nodes:** The device, generally a computer, that will participate in the blockchain network and execute the blockchain protocol's software, which will help validate transactions and secure the network.

5. **Digital Twin Technology:**
   - **Digital Twin Models:** They are the digital representations of real-world healthcare components, such as patients, medical gadgets, and hospitals that depict their current state and behaviors.
   - **Data Integration and Synchronization:** Data integration and synchronization are required for continuously gathering and combining data generated from multiple sources such as IoT devices, electronic health records, wearable sensors, etc., into the digital twins.
   - **Analytics and Simulation Tools:** These tools are used for analyzing data, using machine learning models, and accordingly running simulations to understand the information generated, predict results, and offer beneficial advice based on it.
   - **Security and Authentication:** Security and authentication such as identity verification, need to be implemented to verify and authenticate individual patients, doctors/physicians, and electronic equipment(s) interacting with and/or within the system.
   - **Access Control:** To ensure only authorized entities can access these sensitive healthcare data and digital twin information access controls, such as role-based access need to be implemented.

Moreover, the design could include built-in modules that ensure compliance with healthcare regulations. It can also set up an environment to handle upgrades for all the important components of the architecture. These components work together to form a strong and effective healthcare system. This system makes use of digital twins for real-time patient monitoring, blockchain for security, transparency, and specialized healthcare features.

Digital twins also allow for the examination and optimization of physical resources or processes. By integrating blockchain technology with a digital twin, the system gains several advantages:

1. **Immutable Records:** Blockchain ensures an irrevocable ledger for digital twin data, ensuring data integrity and preventing updations once written to the blockchain.

2. **Decentralized Data Transactions:** Blockchain's decentralized architecture security and resilience increase as the need for a central authority for transaction verification is not required thus lowering the danger of single-point failure.
3. **Digital Twins Transparency:** The transparency feature of blockchain architecture, allows network users to monitor and validate transactions, trace the data history, and build confidence amongst the stakeholders.
4. **Smart Contracts:** Smart contracts, embedded in the code, automate processes such as data sharing, verification, and payment in the systems.
5. **Data Integrity and Security:** Blockchain technology ensures the authenticity and security of digital twin data through encryption, consensus mechanisms, and cryptographic algorithms, preventing unauthorized access and tampering.

Ultimately, blockchain technology integration with digital twins improves the capabilities of the systems and opens up new avenues for industry collaboration and innovation by offering a secure, accessible, and decentralized framework for data management and exchange.

5.3 ARCHITECTURE OF BLOCKCHAIN-BASED HEALTH DATA-SHARING PLATFORMS

5.3.1 Components of Blockchain Technology

The architecture of blockchain includes various components that are considered the pillars of this technology. Each of them works cohesively so that the features of this technology are not compromised. Let us take a look into the components of blockchain:

1. **Decentralized Network:** Blockchain works in a decentralized manner, as shown in Figure 5.2. Authority and control are shared by all the members of the blockchain. The same copy of the data is shared by all the nodes of the network. In order to authenticate any transaction, various cryptographic algorithms and consensus mechanisms are used [10].
2. **Distributed Ledger:** A distributed ledger acts as a shared database that stores the transactions of the entire blockchain network. This component of blockchain works on two rules. First, it is immutable meaning it is tamper-proof, no changes can be made to the ledger once an entry has been made and second, the entries in the database are recorded on the basis of time. These features make blockchain so powerful and different from other technologies [11].
3. **Nodes:** The individual users within the blockchain network are called nodes. Each node on the network has a copy of the list of transactions in the database. The nodes work collaboratively to reach a consensus on the ledger's state. A consensus mechanism is an algorithm using which all the

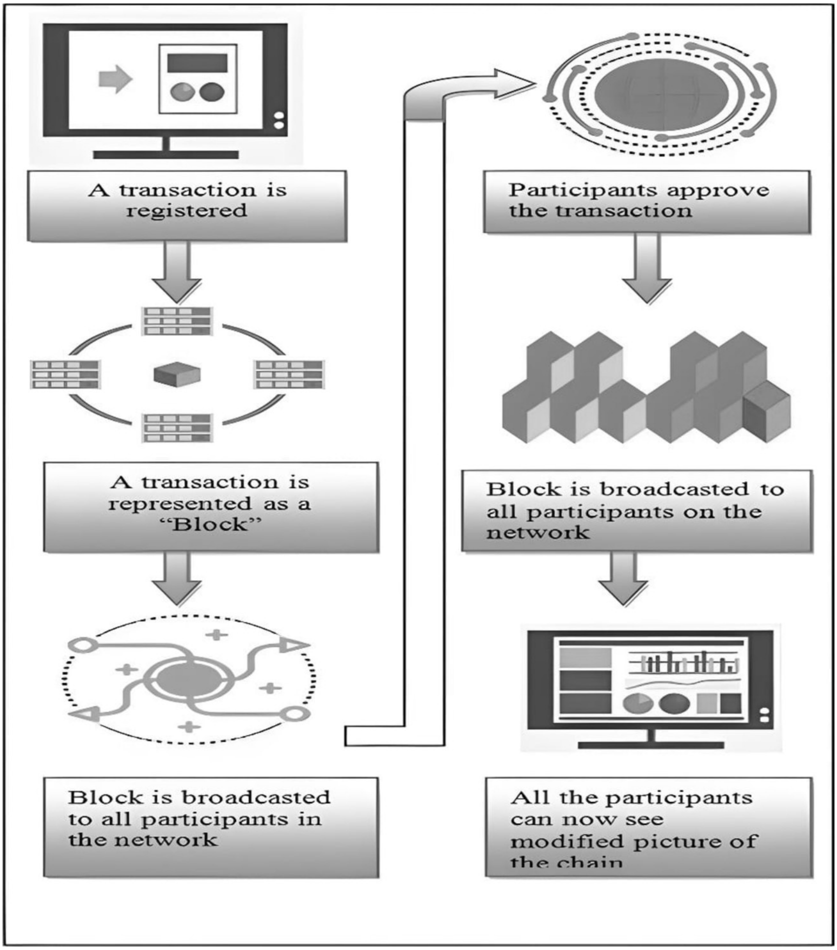


FIGURE 5.2 Decentralized architecture of blockchain

peers of the network reach a common agreement regarding the current state of the distributed ledger [12].

4. **Blocks:** "Blockchain" as the name says is a collection of blocks, where transactions are grouped into block-like structures forming a chronological chain of blocks. The block consists of transactions and hash which helps to uniquely identify the transaction [13].
5. **Digital Signature:** This component uses asymmetric cryptography which works on the basis of private and public keys. The private key is a secret key and is never shared with anyone. The public key, as the name says, is distributed to the public during transactions. This technology uses the private key to encrypt the data which can only be decrypted using the public key. The digital signature algorithms are implemented using a pair of private and public keys [14].

6. **Hashing Function:** The hash function works on the principle of cryptography. The data to be encrypted is sent as an argument to the function to carry out cryptography and then produces a string which is unique to the data sent as an input [14].
7. **Wallet:** Just like we use physical wallets to manage credit cards, we use wallets in the context of blockchain technology. As discussed earlier about public and private keys, digital wallets are containers for storing these keys used frequently during the encryption and decryption process [15].

5.3.2 Privacy and Security Considerations

Even though blockchain is known for its immutability and openness features, it also comes with many novel difficulties and privacy–security consequences that must be explored. Since blockchain works on the principle of decentralization with no central authority looking after the data, it is essential that data residing on the chain must be protected in terms of privacy and security. If these aspects are not taken care of, a majority attack may happen where the hackers can take possession of the entire chain. Hence, it is very important to protect the integrity, security, and privacy of nodes to avoid such attacks. High coherence of transactions is essential to reduce attempts that disturb the chain on the networks. The records of the user may be stolen and misused for a wrong cause.

Critical issues in blockchain are data privacy and security as the data stored on the network becomes transparent and immutable once added to the chain. It implies that any information stored on the blockchain then becomes accessible to all the nodes on the network, thereby posing a threat to the stored content. This trait of blockchain creates risk for those applications that store sensitive or crucial information in sectors such as healthcare, finance, identity information, and many more. Misuse of personal information or data breach is a challenging part which needs to be handled tactfully [16]. The ways to mitigate this risk need to be addressed so that the features of blockchain are not compromised and this technology can be utilized at its full potential. In order to prevent data theft, identity theft, fraud, or such activities, it is necessary to ensure that the privacy and security of these sectors are not put at stake.

5.3.2.1 Privacy Considerations

Transparency is one of the issues when privacy concerns of blockchain are being discussed. Blockchain's transparency feature ensures the integrity of transactions. However, this feature imposes a threat as the data stored on the network is visible to all the participants, leaking confidential information [17].

Another issue is the **immutability** of data stored on the chain. When a transaction is added to the network, it cannot be changed or deleted, making it tough to follow the Data Privacy requirements such as the right to be rectified under the General Data Protection Regulation (GDPR). Since it is not possible to remove the data once stored on the chain, it becomes a dump point of unnecessary data creating a risk of data leakage and other illegal activities [18].

The other challenges with data privacy are:

a. **Use of Public Blockchain:** This blockchain, as employed by Bitcoin, is open for access to anyone, and the data stored on a public blockchain is seen by all the participants on the network hence violating the privacy and security of data. On the other hand, a private blockchain allows only validated users to access the information making it secure over a public chain [18].
b. **Integration of Smart Contracts:** Smart contracts help to execute the transactions automatically without the help of any third party. This characteristic poses a threat as there are chances of data leakage of personal data stored on the blockchain [19].
c. **Pseudonymity:** Blockchain facilitates anonymity by using pseudonymity instead of real names. The technology can be misused for illegal activities such as money laundering, terrorism activities, and many more [].
d. **Compliance of Laws:** Following data privacy laws such as GDPR is challenging as it is difficult to check who is responsible for ensuring compliance and there is always a risk of violating rules across different jurisdictions [22].

5.3.2.2 Security Considerations

Another major challenge existing in blockchain is security. Below are a few security threats of this technology:

a. **51% Attack:** The other name of this attack is a majority attack where the attackers gather more computational power than the authenticated miners, making the network weak and vulnerable to attacks. There are chances that a 51% attack may take place when an intruder takes hold over more than 50% of network resources [23].
b. **Fork Problems:** A valid block is added to the network only when all the miners in the chain validate it. When a single chain is divided into two branches, forking takes place wherein the same single block gets mined by two miners to create individual blocks. Later, a new block is added at the end of any of the existing branches. Hence, mining will be done on the existing branch, creating an overhead as this tree-like structure keeps on expanding, and maintaining it creates an additional responsibility for the miners [23].
c. **Scalability Issue:** The rate at which transactions take place on any blockchain network is enormous. So, with an increase in the amount of transactions, the size of the chain is also growing massively. Even though millions of transactions take place on the network, each blockchain will have its own parameters such as the maximum block size and time interval to generate a new block, thus hindering the expansion of the chain.

Taking into consideration the above aspects, ways to mitigate the risk need to be carefully studied in order to utilize blockchain technology at its best.

5.4 CHALLENGES IN IMPLEMENTING BLOCKCHAIN-BASED SOLUTIONS

Many of the healthcare systems rely on legacy IT systems, and electronic health records platforms are often in silos, outdated, or incompatible with new technologies such as blockchain and digital twins. The main technical integration challenges to integrating blockchain into these old systems involve the current data format, communication protocol, scalability, interoperability, compatibility, privacy, and trust issues among others.

5.4.1 Scalability

The current limitations of blockchain technology in handling large volumes of data and transactions efficiently give rise to scalability issues in implementing blockchain-based solutions in healthcare. Healthcare systems generate enormous amounts of data, including patient records and real-time monitoring, which can overload blockchain networks that usually process a limited number of transactions per second. One more issue that arises is the increasing length of the blockchain. With the inclusion of more transactions in healthcare, the blockchain expands, requiring additional storage and leading to extended synchronization periods for new nodes that become part of the network. Such circumstances can discourage active involvement and impede the overall performance of the network. In healthcare environments, consensus mechanisms such as PoW cause additional delays and computational burdens, which are not suitable for swift and seamless data exchanges. The high network latency and bandwidth constraints also impede the timely propagation and validation of transactions, which is crucial in time-sensitive healthcare scenarios. Moreover, scalability can be impeded by network latency and bandwidth limitations. As the quantity of nodes expands, the communication overhead intensifies, resulting in delays in the propagation and confirmation of transactions. To tackle these challenges, various approaches such as sharding, off-chain transactions (e.g., lightning network), and improved consensus algorithms (e.g., Proof of Stake) are being investigated. The objective is to boost the transaction capacity and scalability of blockchain networks, all the while upholding security and decentralization principles in healthcare.

5.4.2 Interoperability

Interoperability in healthcare refers to the ability of different systems, applications, and devices to exchange, interpret, and use data seamlessly. In the context of implementing blockchain with digital twin-based solutions in healthcare, interoperability becomes crucial due to the involvement of various stakeholders and the need for seamless communication while maintaining data integrity. Below listed are some of the interoperability issues:

i. **Diverse Healthcare Systems:** Healthcare systems comprise various stakeholders, often operating using proprietary software platforms, databases, and/ or systems, making interoperability challenging due to the variations in data formats, protocols, and standards.
ii. **Data Standards and Formats:** Healthcare information is usually kept in various forms and follows different rules based on the system or organization. For instance, EHRs might use different coding systems, such as ICD-10 for diagnosis and CPT for procedures. To make sure these systems can work together, we need to create common data rules and formats that all systems can use and understand.
iii. **Legacy Systems:** Many healthcare organizations still rely on old systems that may not work well with modern interoperability standards or blockchain technology. Combining these old systems with blockchain solutions can be challenging as custom software or special tools might be required to make them work together.
iv. **Data Silos:** Healthcare data is often divided within specific systems or organizations, making it difficult to share information among different groups. Blockchain technology can break down these data barriers by enabling secure, decentralized data sharing. However, combining blockchain with existing processes and systems to ensure smooth data transfer is a complex task that requires careful planning and coordination.
v. **Standardization Efforts:** Several groups and partnerships are focusing on improving interoperability in healthcare. This includes FHIR (Fast Healthcare Interoperability Resources) for sharing health data smoothly and HL7 (Health Level Seven International) for setting data exchange rules. By joining these efforts and using shared standards, different healthcare systems and blockchain technologies can work together better [24].
vi. **Technical Complexity:** To make blockchain and existing healthcare systems work together, we need to fix problems with data synchronization, user verification, access permissions, and data mapping. To handle these technical challenges, creating compatible solutions requires understanding both blockchain technology and healthcare IT systems [25].
vii. **Regulatory Compliance:** Interoperability solutions must follow data security, privacy, and confidentiality rules. Blockchain-based solutions need to prove they meet strict regulations laid down by regulations such as GDPR and HIPAA. These regulations have strict guidelines for keeping patient data secure and enabling safe data sharing [26].

Solving these issues involves teamwork among healthcare organizations, technology providers, standardization groups, and regulatory bodies. They need to create compatible solutions that focus on patient privacy, data protection, and following rules. These solutions should also use the advantages of blockchain technology and digital twin methods in healthcare.

5.4.3 User Adoption and Trust

The backbone of blockchain is supported by many technologies such as digital signatures, consensus mechanisms, hash, encryption, and many more. Blockchain is known for decentralization which means that it is not monitored by a single authority. Due to its immutability feature, once a block is created, the records in the chain become immutable. Encryption algorithms are used to maintain the integrity of data. Timestamps help to validate the authenticity of transactions, which in turn keeps track of previous records. The user's identity is concealed as the technology works on the principle of pseudonymity.

Blockchain builds trust among the peers of the network. When a new node becomes a part of the chain, the existing nodes validate the transaction hence achieving consensus.

5.4.3.1 Challenges of Adopting Blockchain in the Healthcare Sector

Although blockchain is considered to be a powerful tool for overcoming the problems and limitations of the existing healthcare system, there are still some challenges in integrating blockchain into the medical field. Various organizations are still reluctant to adopt blockchain technology. Some hurdles identified and discussed are as below:

a. **Scalability and Data Storage:** With a huge volume of transactions, the blockchain gets flooded each day. The pace at which transactions get added to the chain creates a problem for processing them as there may be very few nodes with enough processing power to manage and validate data on the network. So, handling an exponential amount of data storage and maintaining scalability on the network is a challenge [].
b. **Reliability and Data Access:** Decentralization comes with both pros and cons. Although the system is safe from single-point failure, it suffers from the problems of data access and reliability. There is a high chance that the network may become a victim of digital attacks due to features of blockchain making it susceptible to such threats [29].
c. **Security and Privacy:** Although security and privacy are achieved by encryption, healthcare practitioners still hesitate to store the encrypted data on the network. The data of this sector is accessible and shared with many stakeholders across the industry resulting in breaches of security, privacy, and protection. Hence, it is important that only authenticated parties should be granted access to the data [30].
d. **Complex Decentralized Architecture:** When blockchain is employed in the healthcare sector, various different parties such as the medical staff, service providers such as insurance companies, pharmacists, and laboratory technicians all play a vital role in making the system work. However, a few of them may be working in the traditional style, and adapting the framework by all the players or integrating them into the network seems difficult [31].

e. **Ownership**: Framing norms related to the management of medical transactions for blockchain-based healthcare systems is a tough task. The transition from the current system which involves a lot of paperwork to an automated system which is digital, automated, and decentralized is not easy. There needs to be clarity over access privileges, ownership rights of records, and accountability considering the workings of blockchain.
f. **Operational Overhead:** The cost of developing and maintaining a digital system and the migration expenditure from manual to automatic cannot be predicted. Switching over to the digital network doesn't assure a lower maintenance cost. Instead healthcare system designed using blockchain needs 24/7 resources for maintaining, monitoring, upgrading, and troubleshooting the system [32].
g. **Transparency:** One of the characteristics of blockchain is transparency. However, incorporating this feature in blockchain-based healthcare applications may not be always needed. Since this sector contains a lot of personal and sensitive information, it creates a risk of information theft. The users hesitate to adopt blockchain for this cause. Also, the data may be hacked by gaining access to users' asymmetric keys [33].

5.5 CONCLUSION

To put it simply, this chapter explores how two new technologies—blockchain and digital twins—work together to change how healthcare data is shared. This chapter talks about the benefits of using blockchain in healthcare, such as better data security, improved compatibility between systems, and giving patients more control over their health information. It also looks at how blockchain can create secure networks or systems for sharing data in healthcare. Plus, by promoting collaboration and transparency among different groups, blockchain technology can help overcome challenges in various health data systems.

This chapter also looks at the importance of new ways to share healthcare data, focusing on blockchain technology as a way to share sensitive health information in a decentralized, transparent, and secure manner. It talks about the structure of blockchain-based platforms for sharing health data, pointing out key elements and security aspects needed for successful use. Even though blockchain has many potential benefits in healthcare, there are several obstacles that need to be addressed for it to work well. This includes solving problems with compatibility, privacy, scalability, cost, and managing the system. Collaboration among healthcare providers, tech companies, and regulators will be necessary to build a secure, scalable, and compliant system. This chapter examines the challenges of using blockchain in healthcare, such as scalability, compatibility, and getting people to use it. It highlights the potential for secure, efficient, and patient-centric data exchange.

In the end, this chapter highlights the importance of collaboration among government officials, technology experts, and medical professionals to address challenges and maximize the advantages of blockchain technology in healthcare. By concentrating on research, innovation, and establishing standards, we can develop a healthcare system that prioritizes patients and utilizes blockchain technology for data management.

REFERENCES

1. John, O., Gudi, N., Lakiang, T., Pattanshetty, S., & Sarbadhikari, S. Challenges and Prospects in India's Digital Health Journey. *Indian Journal of Public Health*, 65(2), 209 (2021).
2. Mirzaeian, R., Sadoughi, F., Tahmasebian, S. and Mojahedi, M. Progresses and Challenges in the Traditional Medicine Information System: A Systematic Review. *Journal of Pharmacy & Pharmacognosy Research*, 7(1), 246–259 (2019).
3. Outsourced Product Development | Custom Software Development Services Company | Pune India, Houston Texas USA. (n.d.). Mobisoft Infotech. Available at: https://mobisoftinfotech.com/
4. Hendl, T., & Shukla, A. Can Digital Health Democratize Health Care? *Bioethics*, 38(6), 491–502 (2024).
5. Kumar, P., & Kumari, A. *Blockchain for Biomedical Research and Healthcare*, Springer Nature (2024).
6. Gunjal, P. R., Jondhale, S. R., Jaime Lloret Mauri, & Agrawal, K. *Internet of Things: Theory to practice*. CRC Press (2024).
7. Rani, S., Bhambri, P., Kumar, S., Pareek, P. K., & Elngar, A. A. (2024). *AI-Driven Digital Twin and Industry 4.0*. CRC Press eBooks (2024).
8. CORA Home. Cora.ucc.ie (n.d.). Available at: https://cora.ucc.ie
9. The biggest online incubator and accelerator. Provides work per equity and helps in raising capital from a large network of angel investors and VCs. FasterCapital (n.d.). Available at: https://fastercapital.com/
10. Top 9 Data Sharing Challenges and Ways to Overcome Them. Atlan.com (n.d.). Available at: https://atlan.com/data-sharing-challenges/
11. Kedar, D. S. Healthcare Data Management: What It Is, Its Challenges, and Opportunities. Mobisoft Infotech (2023, February 16). Available at: https://mobisoftinfotech.com/resources/blog/healthcare-data-management-challenges-and-solutions/
12. Rachamalla, S. Secure Data Sharing Based on Blockchain Technology. *International Journal of Forensic Sciences*, volume 6, issue 2 (2021). https://doi.org/10.23880/ijfsc-16000230.
13. Hemdan, E. E.-D., & Mahmoud, A. S. A. BlockTwins: A Blockchain-Based Digital Twins Framework. In *Blockchain Applications in IoT Ecosystem* (pp. 177–186). Cham: Springer International Publishing (2021). https://doi.org/10.1007/978-3-030-65691-1_12
14. Akash, S. S., & Ferdous, M. S. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access*, 10, 50523–50547 (2022).
15. Saxena, S., Bhushan, B., & Ahad, M. A. Blockchain Based Solutions to Secure IoT: Background, Integration Trends and a Way Forward. *Journal of Network and Computer Applications*, 181, 103050, 2001, ISSN 1084-8045.
16. Bowles, J., Webber, T., Blackledge, E., & Vermeulen, A. A Blockchain-Based Healthcare Platform for Secure Personalised Data Sharing. *Studies in Health Technology and Informatics* (pp. 208–212). IOS Press (2021). https://doi.org/10.3233/shti210150
17. Hemdan, E. E. D., & Mahmoud, A. S. A. BlockTwins: A Blockchain-Based Digital Twins Framework. In: Choudhury, T., Khanna, A., Toe, T. T., Khurana, M., & Gia Nhu, N. (Eds) *Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing*. Cham: Springer (2021).

18. Dash, B., & Swayamsiddha, S. Blockchain Adoption in Enterprises: Opportunities and Challenges. *SSRN Electronic Journal* (2023).
19. Glaser, F., Hawlitschek, F., & Notheisen, B. Blockchain as a Platform. In: Treiblmaier, H., & Beck, R. (Eds) *Business Transformation Through Blockchain*. Cham: Palgrave Macmillan (2019).
20. Yaqoob, I., Salah, K., Uddin, M., Jayaraman, R., Omar, M., & Imran, M. Blockchain for Digital Twins: Recent Advances and Future Research Challenges. *IEEE Network*, 34(5), 290–298 (September/October 2020).
21. Hasan, H. R., et al. A Blockchain-Based Approach for the Creation of Digital Twins. *IEEE Access*, 8, 34113–34126 (2020).
22. Singh, D., Monga, S., Tanwar, S., Hong, W.-C., Sharma, R., & He, Y.-L. Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons. *Applied Sciences*, 13(4), 2380 (2023).
23. Taherdoost, H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. *Sci*, 5(4), 41 (2023).
24. Katsoulakis, E., Wang, Q., Wu, H., Shahriyari, L., Fletcher, R., Liu, J., Achenie, L., Liu, H., Jackson, P., Xiao, Y., Syeda-Mahmood, T., Tuli, R., & Deng, J. Digital Twins for Health: A Scoping Review. *Npj Digital Medicine*, 7(1), 1–11 (2024).
25. Sun, T., He, X., & Li, Z. Digital Twin in Healthcare: Recent Updates and Challenges. *Digital Health*, 9, 205520762211496 (2023).
26. Akash, S. S., & Ferdous, M. S. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access*, 10, 50523–50547 (2022).
27. Team, S. C. 11 Features of Blockchain Technology | Shardeum. Shardeum Blogs | EVM-Based Sharded L1 Blockchain (2022, August 4). Available at: https://shardeum.org/blog/what-are-the-features-of-blockchain/
28. Pillar, R. M. T. The 5 Key Components of a Digital Twin for Fleet Operations | Descartes. Www.descartes.com (n.d.). Available at: https://www.descartes.com/resources/knowledge-center/5-key-components-digital-twin-fleet-operations
29. 7 Key Characteristics of a Digital Twin for Maintaining and Optimizing Industrial Assets. www.linkedin.com (n.d.). Available at: https://www.linkedin.com/pulse/7-key-characteristics-digital-twin-maintaining-assets-david-reinhart/
30. Yao, J., Yang, Y., Wang, X.-C., & Zhang, X.-P. Systematic Review of Digital Twin Technology and Applications. *Visual Computing for Industry, Biomedicine, and Art*, 6(1), 10 (2023).
31. Haleem, A., Javaid, M., Pratap Singh, R., & Suman, R. Exploring the Revolution in Healthcare Systems Through the Applications of Digital Twin Technology. *Biomedical Technology*, 4, 28–38 (2023).
32. Vallée, A. Digital twin for healthcare systems. Frontiers in Digital Health, 5, 1253050 (2023).
33. Pandey, C. Scalability Challenges and Opportunities in Blockchain-based Systems: A Systematic Review. *Turkish Journal of Computer and Mathematics Education*, 11(3), 2022–2031 (2020).

6 Ensuring Privacy and Security

A Framework for Sharing Anonymized Patient Data for Clinical Trials and Drug Discovery

Ramya R S, Ramesh Babu, Krishnan Rangarajan, and Sunanda

6.1 INTRODUCTION

In every industry, data is the most sensitive and precious entity. In healthcare, the patient's data should be stored securely such that no one can manipulate the data or misuse the data. Patients share personal information with doctors that should not be accessible to everyone. To address this concern blockchain technology is being integrated into the healthcare industry. Blockchain allows patient records to be stored on a distributed ledger where each node holds a copy of the data. Although the ledger is decentralized, access can be controlled by assigning different permission levels to different users. Some users will have access to complete information stored on the ledger whereas some will only have access to a particular part or summary of the record to maintain the patient's privacy.

Sometimes patients are not willing to share their data publicly on a ledger with their real identity. This problem can be overcome by anonymization of data where only the information about disease or health will be visible not the person's identity for clinical research. The data on these ledgers are secured using cryptographic techniques which gives the patient full control over their data and also allows patients to give access to other users according to their wish as the patient will be holding a private key maintaining data security and consent of patient [1]. Blockchain allows us to create a separate record, called a personal health record (PHR), from an electronic health record (EHR) which contains only the patient's personal information which has been extracted from the full EHR. This information can be stored separately and securely and access will require an IP address. Only doctors or physicians will have

DOI: 10.1201/9781003532286-6

access to the PHR and while sharing data for clinical research the PHR will never be shared with the researchers.

The data stored in the PHR helps patients track their condition with the use of smart devices, health trackers, and other various applications. This gives patient complete control over their data and progress.

Blockchain ensures that stored data remains immutable and tamper-proof, as any attempt to alter information on the ledger would require re-encoding the entire chain. This inherent structure significantly enhances data privacy and security, as shown in Figure 6.1 . A digital twin is a copy of a real-world physical object. It can be understood as a 3D model but the difference between them is that the digital twin should also act like the physical object. It is used in many industries including healthcare to create human body replicas to study the body in a better manner. This helps medical students, nurses, and even healthcare professionals to study the human body. They can also be used in clinical testing as one of the major issues faced in trials is on whom to test the drugs. This is because most people are against testing on animals and nearly everyone is against testing on humans. So it can help researchers to test their research on a digital twin of the human body, allowing them to know how the human body will react and make further changes to their research, as the digital twin acts the same way as the human body does.

Hence digital twins can significantly benefit the healthcare industry by improving disease detection [3]. Doctors can test medical equipment on digital twins, reducing the risk of patients facing problems such as faulty machines during procedures. Additionally, digital twins help doctors learn about the human body and solve major issues in clinical research by allowing researchers to test their drugs before actually implementing them on humans.

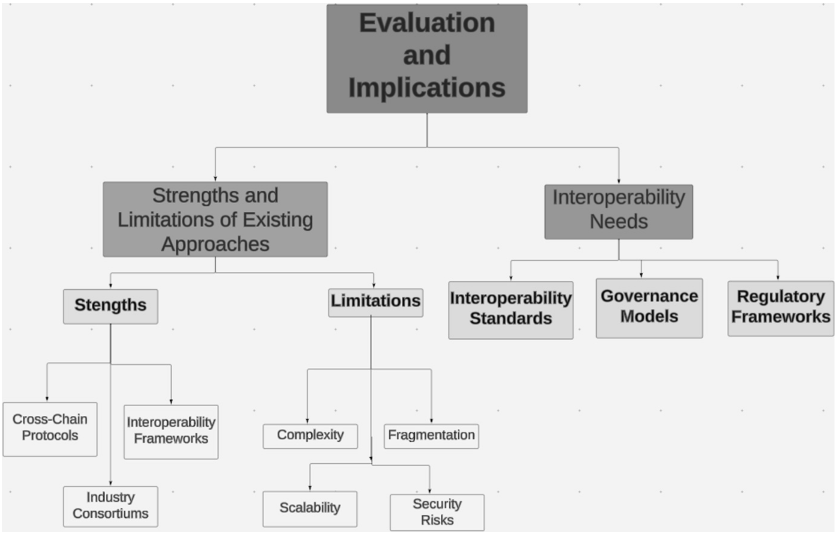


FIGURE 6.1 System architecture of integrated digital twin and blockchain [2]

6.1.1 Key Principles

6.1.1.1 Anonymization Techniques

Patient data must be anonymized to protect individual privacy. Anonymization involves removing or altering identifiable information so that the personal information of the user is not shared or identified. It protects the data by encrypting identifiers that can reveal the information about the users on the ledger.

6.1.1.1.1 De-identification

- **Removal of Direct Identifiers:** Sensitive information such as name, ID numbers, salary information, and contact number should be removed and stored in a PHR.
- **Masking:** Real information is replaced with codenames or aliases. A patient's information is made anonymous when sharing the information.

6.1.1.1.2 Data Perturbation

- **Noise Addition:** To protect data, random noise is introduced.
- **Data Swapping:** Exchange values between records to obscure individual identities.

6.1.1.1.3 Aggregation

- **Generalization:** Replace specific data points with broader categories (e.g., age ranges in- instead of exact age).
- **K-anonymity:** Ensure each record is indistinguishable from at least k-1 other records in the distributed ledger. No two datasets have the same properties or they can not be interchanged.

6.1.1.1.4 Differential Privacy

- Implement differential privacy techniques to provide mathematical guarantees that individual data points cannot be identified.

6.1.1.2 Data Security Measures

Robust security measures must be implemented to protect data from unauthorized access, breaches, and other security threats as shown in Figure 6.2. It includes both hardware and software security.

6.1.1.2.1 Encryption (Data at Rest)

- Encrypt data stored on servers and databases using cryptographic hashes on blockchain.

6.1.1.2.2 Encryption(Data in Transit)

- Use secure transmission protocols (e.g., TLS/SSL) to protect data during transfer.

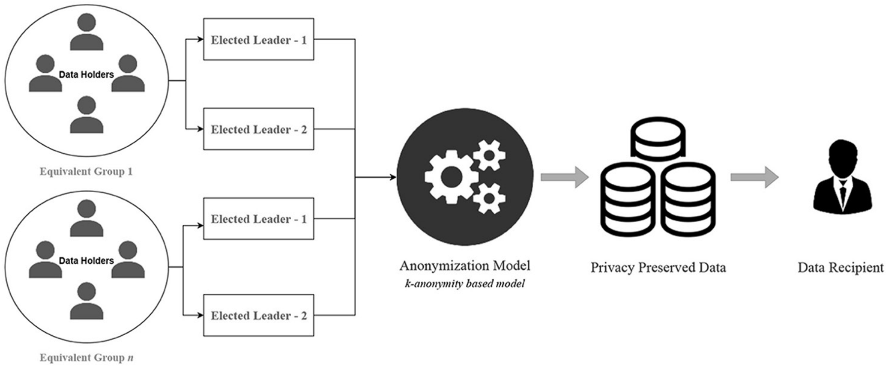


FIGURE 6.2 Privacy-preserving data collection protocol architecture [4]

6.1.1.3 Regulatory Compliance

All data-sharing practices must comply with the relevant regulations, such as GDPR, HIPAA, and other local and international data protection laws. The storage of data should also adhere to legal standards to ensure privacy and security.

6.1.1.3.1 General Data Protection Regulation (GDPR)

- Ensure data anonymization techniques meet GDPR standards for anonymized data.
- Implement processes for data subjects to exercise their rights (e.g., data access, correction, deletion).

6.1.1.3.2 Health Insurance Portability and Accountability Act (HIPAA)

- Follow the HIPAA rules for privacy and security for protected health information (PHI).
- Use HIPAA-compliant de-identification methods for anonymizing data.

6.1.1.3.3 Other Regulations

- Follow additional local, national, and international regulations relevant to patient data sharing.

6.1.1.4 Transparency and Consent

Patients should be aware of how and where their data will be used and after getting the information, patients can decide whether to give consent to use their data or not. Patients should decide who will be given access to the complete set of data and who will only be given partial access.

6.1.1.4.1 Informed Consent

- Clearly explain how patient data will be used, anonymized, and shared.
- Obtain explicit consent from patients before collecting and sharing their data.

6.1.1.4.2 Communication

- Provide patients with regular updates on how their data is being used and the measures in place to protect their privacy.

6.1.1.5 Governance and Accountability

Clear governance structures should be established to oversee data-sharing practices, ensuring accountability and adherence to the framework.

6.1.1.5.1 Data Governance Committee

- Make a committee responsible for monitoring data-sharing practices, ensuring compliance, and protecting the personal information of the user.

6.1.1.5.2 Accountability Framework

- Assign roles and responsibilities for data stewardship.
- Implement regular audits and assessments to ensure adherence to the framework.

6.2 RELATED WORKS

Akash et al. [2] propose a well-defined structured way of representing the patient's data using a mathematical data model as shown in Figure 6.3. This model represents the data set related to a patient in the physical world as a virtual patient in a digital space. The use of blockchain provides a secure and tamper-proof method of recording and storing data making it highly suitable for securing data integrity. This article introduces a mathematical model which is the healthcare digital twin (HDT) system. This HDT system ensures efficient data collection based on a rigorous mathematical model where data is collected from multiple sources to create a detailed health digital twin. Storing raw data off-chain prevents the blockchain from being overloaded, enhancing system speed, and using private blockchain enhances security and trust. This system has certain limitations as it allows read-only access and it does not currently include the pre-sharing of certain patient health data with other HDT entities, which requires patient consent. Recognizing that even with advanced technologies, achieving a digital twin of a complete patient body remains challenging due to the intricacies of the human body, this can be overcome by the model introduced in this article.

Elaya et al. [5] present an advanced context-aware healthcare system utilizing the DT framework, significantly advancing digital healthcare and its operations. This research involves developing an ECG heart rhythm classification model through machine learning to diagnose heart disease and identify cardiac issues, achieving high accuracy with different algorithms. The findings suggest that integrating DT into healthcare enhances processes by linking patients with healthcare professionals in an intelligent, comprehensive, and scalable health ecosystem. Additionally, the use of an ECG classifier for detecting heart conditions highlights the potential of applying machine learning and artificial intelligence to various human frame

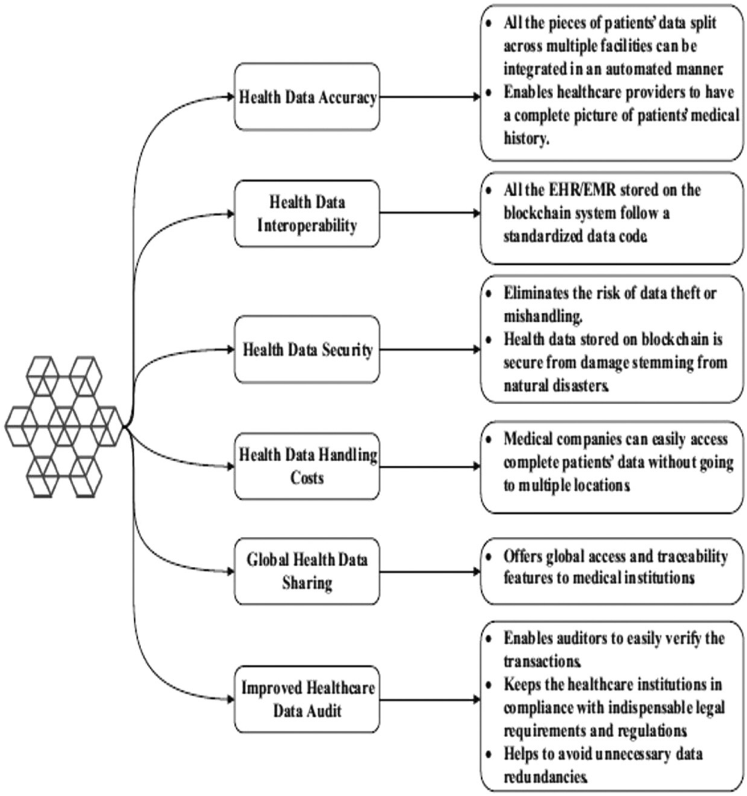


FIGURE 6.3 Benefits of leveraging blockchain technology for healthcare data management systems

metrics for continuous monitoring and anomaly detection. Lastly, the research shows that neural network–based algorithms outperform traditional ML algorithms when handling ECG data. Challenges and issues involve maintaining trust, security, and privacy. The trend of digital twins can spread rapidly by setting global standards. To conclude neural network–based algorithms consistently outperform traditional machine learning techniques when assessing ECG data, demonstrating superior performance across key learning evaluation metrics including accuracy and precision. Table 6.1 summarizes the different healthcare models based on Digital Twin.

Putz et al. [6] present an owner-centric decentralized sharing model alongside a formal access control model, which tackles integrity and confidentiality concerns by leveraging digital twin components and lifecycle requirements. Through our app, EtherTwin, we showcase the successful resolution of numerous challenges in fully decentralized data sharing, enabling effective management of digital twin components and their associated information.

Validation of this approach includes an evaluation of the prototype using an industry use case and conducting semi-structured expert interviews. Exploration

TABLE 6.1
Existing Models in Healthcare Using Digital Twin Technology

Sl No	Author	Concept	Advantages	Disadvantages
1	Sadman Sakib Akash [2]	Mathematical model for a digital twin in healthcare	Security and trust	Read-only access
2	Haya Elayan [5]	ECG heart rhythm classifier model using digi tal twin framework	Accuracy and precision	Security and trust
3	Benedikt Putz [6]	Information management using EtherTwin	Feasible	Data ownership issues
4	Robert Martinez [7]	Cardio twin	Feasible	Real-time processing constraints
5	Abirami and Karthikeyan [8]	Early Parkinson's disease identification	Enhanced and accuracy efficiency	Scalability issues
6	Radhya Sahal et al. [9]	Smart pandemic alerting using blockchain and digital twin	Enhanced security	Resistance to change

into blockchain-based information sharing and access control offers avenues for expansion into diverse fields, including healthcare data sharing within digital twins, establishment of data marketplaces, and certification of machines. Enhancements to this prototype could involve enabling seamless data flow from the twin to the corresponding industrial asset, facilitating interactions such as invoking PLC functions via smart contracts or deploying firmware updates.

Martinez et al. [7] studied cardio twin architecture, specifically crafted for the detection of ischemic heart disease (IHD) and tailored to operate efficiently at the edge. Utilizing a convolutional neural network (CNN), we precisely distinguish between non-myocardial and myocardial conditions by extracting features from electrocardiograms (ECGs). Leveraging the "PTB Diagnostic ECG Database" from the Physio Bank dataset which is comprised of data from around 209 individuals, every patient's data sample was divided into 2.5-second windows for effective training. With our implemented model achieving an impressive 85.77% accuracy and an average classification time of 4.8 seconds per sample, our findings underscore the capability of technology to robustly support demanding processes, such as digital twins. The successful demonstration of feasibility implementation of cardio twin demonstrates its flexibility in integrating diverse data types beyond ECG, making it a versatile tool for exploring various datasets. Additionally, its design allows for the easy replacement or enhancement of models within the analytics pipeline. Moving forward, cardio twin aims to shift focus from issue detection to proactive prevention of ischemic heart disease (IHD) and stroke by addressing risk factors through persuasive computing techniques, leveraging the AI inference engine.

The incorporation of digital twin technology into healthcare systems by Abirami and Karthikeyan et al. [8] represents a significant advancement in remote patient monitoring and early disease detection, particularly for conditions such as Parkinson's disease. By leveraging smart virtual care facilities and sophisticated prediction models such as optimized fuzzy-based k-nearest neighbor (OF-kNN), this approach offers enhanced accuracy and efficiency in diagnosis and treatment planning. In conclusion, the implementation of the proposed DTHS utilizing the OF-kNN classifier model demonstrates promising outcomes in accurately predicting Parkinson's disease using voice features, thereby enabling remote patient monitoring and diagnosis based on non-clinical parameters. Through extensive evaluation against benchmark datasets and comparative analysis with other classifier models, the superiority of the OF-kNN approach is evident regarding prediction time and accuracy, F1-score, and Matthews correlation coefficient. These findings underscore the potential of OF-kNN in revolutionizing healthcare delivery for remote patients, offering cost-effective monitoring and diagnosis solutions. Additionally, future research endeavors could explore the integration of probabilistic methods and larger voice datasets to extend the applicability of the system in distinguishing various diseases causing voice disorders.

Engaging participants is crucial in the fight against COVID-19, to end this Sahal et al. [9] developed a blockchain-enabled cooperative digital twin framework designed to decentralize outbreak alert systems for combating COVID-19 and potential upcoming pandemics. This framework integrates advanced technologies such as blockchain, digital twins, and artificial intelligence (AI) to offer a decentralized solution for epidemic alerting. Additionally, we have outlined the application of this conceptual framework in a decentralized alerting system for COVID-19 outbreaks. Ensuring prompt and accurate decision-making and response times is challenging for digital twins and efficient and secure data collection and communication by monitoring technologies are crucial for timely, data-driven decisions and alerts. Therefore, this framework represents a blockchain-based digital twin collaboration framework for pandemic alerting, structured into four layers to enhance operational data intelligence. This framework effectively addresses decentralized pandemic alerting, specifically targeting COVID-19 outbreaks.

A cloud healthcare system framework based on digital twin healthcare (CloudDTH) was designed by Liu et al. [10] for tracking, identifying, and forecasting personal health, particularly for the elderly, using wearable medical devices. The CloudDTH framework facilitates interaction between physical and virtual medical spaces, presenting a new digital twin healthcare concept and model. Essential enabling technologies are examined, and their viability is demonstrated through various usage scenarios and real-time monitoring instances. The paper addresses the bottleneck in information-physical interaction within healthcare by proposing digital twin healthcare (DTH) to enhance real-time oversight and emergency alert accuracy.

It presents the CloudDTH framework, demonstrating feasibility through instances. The preliminary results outline the framework and applications of DTH in cloud healthcare. Future work will focus on data integration, rapid model development and management, accuracy verification, machine and service collaboration, and integrating various medical devices and sensors with the CloudDTH platform.

Sahal et al.'s [11] personal digital twin (PDT) concept, highlights its potential to enhance digital twins with actionable insights for improved decision-making and treatment in healthcare. While PDTs hold significant promise for transforming healthcare, they are still in the nascent stages of development. We proposed a reference framework that leverages advanced technologies such as digital twins, blockchain, and AI to foster smart personalized healthcare systems. We illustrated the framework's application through various use cases, including COVID-19 mitigation, follow-up care for survivors, personalized treatments, prevention of osteoporosis, care for cancer survivors, and personalized nutrition. Additionally, we pinpointed several crucial challenges that must be tackled to advance the PDT paradigm in the personalized healthcare sector. Implementing personal digital twins (PDTs) in healthcare presents several challenges. These include ensuring data privacy and compliance with regulations, maintaining security against cyber threats, and addressing scalability issues. Additionally, maintaining data quality, modeling complex human systems accurately, and ensuring high connectivity for real-time functionality pose significant hurdles. Ethical considerations regarding patient data access and communication also need to be addressed effectively. Overcoming these challenges is crucial for realizing the full potential of PDTs in revolutionizing personalized healthcare delivery. This work introduces the idea of personal digital twins (PDT) as an advanced iteration of digital twins, providing actionable insights for personalized diagnosis and treatment selection in healthcare. Therefore, it proposes a reference framework integrating blockchain, AI, and digital twins to enhance personalized services in healthcare, with a focus on improving patient outcomes and healthcare delivery efficiency.

Yaqoob et al.'s [12, 13] discussion on healthcare analytics provides a comprehensive analysis of the potential impact of blockchain technology on healthcare data management systems. The study thoroughly examines the limitations of current centralized healthcare data systems, emphasizing the need for improved data provenance, transparency, auditability, and security. By discussing real-world case studies and ongoing projects, the authors illustrate how blockchain can address these challenges by offering decentralized, tamper-proof, and transparent solutions for managing health data. Furthermore, the authors outline vital opportunities for leveraging blockchain in healthcare, such as automating workflow processes, enhancing sustainability, and improving operational efficiency. Yaqoob also identifies critical research challenges hindering the widespread adoption of blockchain in healthcare, including scalability, interoperability, and integration with existing systems. The study concludes by emphasizing the transformative potential of blockchain in reshaping healthcare industries while highlighting the technical hurdles that need to be overcome for successful integration. The study delivers insights into the benefits, challenges, as well as future directions of incorporating blockchain technology in healthcare data management.

Sahal et al. [14] delve into personal digital twins (PDT) in healthcare, showcasing their potential to transform personalized healthcare systems and intelligent hospitals. By leveraging data-driven insights, PDTs offer a pathway to automate decision-making processes and enhance patient care. Particularly noteworthy is the emphasis on addressing the pressing need for PDT adoption in light of the COVID-19 pandemic, highlighting how this technology can mitigate contagion risks and aid in long-term COVID-19 patient management. Amidst these advancements, a critical focus is placed on securing patient data, underscoring the importance of data privacy and confidentiality in healthcare settings. The combination of blockchain technology is proposed for safeguarding and protecting patient information, ensuring transparency, accessibility, and data security within PDT applications. By prioritizing data privacy and security measures, Sahal underscores the commitment to upholding patient trust and compliance with stringent data protection regulations in the healthcare industry.

Yi et al. [15] focus on advancing cloud storage security for digital twin–based medical records, strongly emphasizing the safeguarding of patients' data. By proposing an innovative solution that integrates post-quantum searchable encryption methods, the research aims to enhance privacy and security measures in healthcare. Implementing physical unable functions (PUF) for key generation and encrypted cloud storage methods ensures that all medical data, such as symptoms, prescriptions, and personal information, is securely encrypted and kept.

This approach improves data security and demonstrates a commitment to protecting patients' sensitive information in an increasingly digital healthcare landscape.

Sahal et al. [14] discuss the integration of digital twins, data analytics, and blockchain technologies to enable decentralized epidemic alerting, particularly in combating COVID-19 outbreaks. The study highlights the necessity of secure real-time data exchange among participants in medical cyber-physical systems. Patient data security is a critical aspect addressed through blockchain technology, ensuring that digital twins of participants within the healthcare system can exchange and share essential information securely. This approach enhances transparency, accessibility, and confidentiality of healthcare data, ultimately contributing to more effective and secure healthcare practices.

Alzahrani et al. [16, 17] discuss the application of blockchain technology in healthcare systems, with a strong emphasis on enhancing the security of patients' data. The study underscores the importance of safeguarding sensitive medical information and maintaining patient confidentiality in the digital age. By leveraging blockchain's decentralized and immutable nature, Alzahrani proposes a secure framework for storing and sharing electronic medical records (EMRs) while ensuring data integrity and privacy. The study highlights the potential of blockchain to address the security challenges faced by healthcare providers, offering a transparent and tamper-resistant platform for managing patient data securely. By implementing vigorous security measures, such as asymmetric encryption in addition to access control, blockchain technology can provide a secure environment for storing and exchanging medical information [18]. The study emphasizes the adoption of blockchain to improve patient data security, mitigate privacy risks, and improve overall trust in healthcare systems.

Sun et al. [19] discuss the capability of digital twin technology in the medical field, specifically in achieving precise diagnosis and personalized treatment. The study emphasizes the advantages of the technology, such as personalized medicine, optimization of treatment procedures, and real-time monitoring. Sun also highlights the challenges in data collection and fusion, simulation accuracy, and socio-ethical risks. The authors propose that digital twins can significantly achieve precision medicine and personalized healthcare with advancements in technologies such as big data, the Internet of Things, and artificial intelligence.

Bhavin et al. [20] discuss the critical issue of patient data security in healthcare systems, highlighting the vulnerability of medical devices as an entry point for cyberattacks. The study emphasizes the importance of securing all devices connected to healthcare systems to prevent unauthorized access to EHRs. The study proposes a blockchain-based architecture to enhance the security of electronic health records, ensuring that only authorized individuals, such as patients, clinicians, lab staff, and researchers, have access to sensitive medical data. By implementing a patient-controlled system, the authors aim to protect the confidentiality and integrity of patient information. Using quantum computing technology, the proposed system aims to enhance traditional encryption methods and protect against quantum attacks. The use of a quantum blind signature during block creation in the blockchain architecture ensures secure transactions, improved resource consumption, and network traffic management. This innovative approach not only addresses the current cybersecurity challenges in healthcare but also offers a promising solution to maintain the privacy and security of patient data in an increasingly digitized healthcare environment.

Velmurugan et al. [21] focus on developing and evaluating an efficient and secure EHR sharing system using IoT-based blockchain hyperledger technology. The study introduces a decentralized access control and authentication system in blockchain-based EHR systems, emphasizing the importance of secure communication and data integrity through encryption standards. By implementing robust security protocols and encryption techniques, the proposed system aims to safeguard sensitive health records, prevent unauthorized access, and ensure patient privacy. Through a formal security analysis and performance evaluation, the research demonstrates the system's ability to facilitate secure data transmission among healthcare professionals, streamline administrative tasks, and enhance healthcare services' overall quality and efficiency. The study's findings contribute valuable insights into the potential of blockchain technology in revolutionizing EHR management and addressing security challenges in healthcare infrastructures.

Du et al. [22] introduce an approach to medical information sharing by proposing an optimized consortium blockchain platform. This platform leverages a new consensus algorithm and a two-layer blockchain structure to boost the security, integrity, and efficiency of sharing sensitive medical data. By utilizing smart contracts, docker containers, and a peer-to-peer network, the platform ensures that shared information is tamper-resistant and accessible only to authorized parties, addressing privacy concerns in the healthcare sector. The platform's design includes a business process framework and a confidential information-sharing process, enabling seamless and secure user interactions while maximizing the value of medical data. Furthermore, the platform's modular design allows easy maintenance and upgrades, providing a scalable solution for medical institutions seeking a secure and reliable information-sharing method. Through the integration of blockchain technology, the platform not only prevents information tampering but also creates a shared ecosystem where data can be transformed into valuable insights. Overall, the proposed consortium blockchain platform offers a comprehensive and efficient solution for medical information sharing, ensuring the accuracy, integrity, and privacy of shared data in a distributed network environment.

Kerrison et al. [23] paper "Blockchain-Enabled IoT for Rural Healthcare" presents a novel approach to enhancing healthcare services in rural areas by integrating blockchain technology with IoT devices. By leveraging a hybrid-channel communication system with digital twinning, the study addresses the challenges of communication reliability and data integrity in low-bandwidth rural settings. This innovative solution allows IoT devices to securely transmit patient data while maintaining confidentiality and trust through blockchain-enabled transactions. Kerrison also emphasizes using LPWAN solutions, such as the LoRa standard, which highlights the importance of energy-efficient and long-range communication for IoT devices in remote locations. By combining blockchain technology with IoT devices, the proposed framework improves data transmission efficiency and ensures the secure storage and transit of sensitive healthcare information. Overall, this research contributes to advancing healthcare monitoring systems in rural areas, offering a promising solution to bridge the gap in healthcare services between urban and remote regions.

Lee et al. [24] present a novel approach to enhancing information sharing and collaboration in construction projects by integrating a digital twin and blockchain framework. By leveraging real-time updates from the digital twin and secure data transactions facilitated by blockchain technology, the framework ensures observable and immutable conversations among project participants. Through a case study involving virtual positioning data transmission and blockchain recording, the authors demonstrate the effectiveness of the integrated framework in enabling accountable information sharing across stakeholders. This innovative solution not only streamlines contract execution and payment processes but also fosters better collaboration and efficiency in construction projects. The study highlights the significance of transparent and secure data transactions in overcoming the challenges of fragmented stakeholder involvement in construction projects by utilizing blockchain technology to authenticate and add traceability to data transactions within the digital twin. The research emphasizes the potential of the integrated digital twin and blockchain framework to revolutionize project management by automating processes, enhancing decision-making, and ultimately improving project outcomes through streamlined collaboration and information sharing among stakeholders.

Vanderhorn et al. [25] delve into the concept of digital twins, stressing the significance of establishing a comprehensive definition to differentiate digital twins from other digital tools. By analyzing many definitions from existing literature, the study aims to propose a more inclusive and precise definition that encapsulates the diverse perspectives and attributes associated with digital twins. This effort is crucial to maintaining the integrity of the concept and facilitating the successful deployment of digital twins across different industries. The authors provide a detailed exploration of the implementation process and key considerations involved in the practical application of this technology. The convincing study demonstrates how digital twins can be effectively applied in real-world scenarios, shedding light on the complexities and nuances of integrating this technology. Additionally, the study looks ahead to the future of digital twins, identifying emerging needs and opportunities within this evolving field and envisioning the potential for further advancements and innovative applications across various sectors.

6.3 HOW DIGITAL TWIN TECHNOLOGY HAS TRANSFERRED PERSONALIZED HEALTHCARE

Digital twin technology can significantly enhance personalized healthcare within a framework for sharing anonymized patient data for clinical trials and drug discovery. By leveraging digital twins, this framework can provide accurate, detailed, and dynamic models of individual patients while ensuring data privacy and security. The following subsections demonstrate how digital twin technology facilitates this transformation.

6.3.1 Creating Anonymized Digital Twins

- **Data Collection and Anonymization:** Health data from patients is collected through resources such as EHRs, and medical imaging. This data is then anonymized to remove Personally identifiable information (PII) before being used to create digital twins.
- **Detailed Modeling:** Digital twins represent the physiological, genetic, and behavioral attributes of individual patients without compromising their identities. These models include data on vitals, medical history, lifestyle factors, and treatment responses.

6.3.2 Enabling Safe Data Sharing

- **Anonymized Data Exchange:** The anonymized digital twins can be securely shared with researchers and pharmaceutical companies for clinical trials and drug discovery, ensuring patient privacy is maintained.
- **Blockchain for Secure Transactions:** Blockchain technology manages the secure sharing of data, providing an immutable and transparent record of data transactions.

6.3.3 Enhancing Clinical Trials

- **Virtual Clinical Trials:** Digital twins can be used to conduct virtual clinical trials, simulating how different patient profiles respond to new drugs or treatments. This reduces the need for large physical trial populations and accelerates the trial process.
- **Recruitment Optimization:** By analyzing digital twin data, researchers can identify the most suitable candidates for clinical trials, ensuring a more targeted and efficient recruitment process.

6.3.4 Improving Drug Discovery

- **Predictive Modeling:** Modeling disease progression with drug interactions in virtual environments, providing insights into how new drugs will perform across diverse patient populations.
- **Personalized Drug Development:** Insights from digital twins can guide the development of personalized drugs tailored to specific patient profiles, increasing the efficacy and safety of new treatments.

6.3.5 Ensuring Data Privacy and Security

- **Anonymization and Pseudonymization:** Advanced anonymization techniques ensure that data shared for research cannot be traced back to individual patients, protecting their privacy.
- **Regulatory Compliance:** The framework must comply with regulations such as GDPR, HIPAA, and other data protection laws, ensuring that patient data is handled securely and ethically.

6.3.6 Collaborative Research and Development

- **Shared Data Ecosystem:** Creating a shared ecosystem where anonymized digital twin data is accessible to authorized researchers fosters collaboration and accelerates innovation in drug discovery.
- **Cross-Institutional Studies:** Digital twins allow for large-scale cross-institutional studies, pooling data from diverse sources to gain more comprehensive insights into diseases and treatments.

6.3.7 Ethical Considerations and Patient Consent

- **Informed Consent:** Patients should be informed about how their anonymized data will be used and provide consent, ensuring ethical transparency.
- **Benefit Sharing:** Ensuring that the benefits of research and drug discoveries are shared with the patients and communities contributing data.

FIGURE 6.4 Applications of digital twins in healthcare

6.4 APPLICATION OF DIGITAL TWIN IN HEALTHCARE

6.4.1 Clinical Trials:

- **Virtual Trials:** As shown in Figure 6.4, researchers can conduct virtual trials using digital twins to model outcomes before initiating real-world trials. This helps refine protocols and identify potential risks early. The benefits of digital twin in healthcare are highlighted in Figure 6.5.
- **Patient Recruitment and Retention:** By understanding patient profiles better, researchers can more effectively recruit participants who are more likely to benefit from the trial, thereby improving retention rates.
- **Adaptive Trials:** Digital twins enable adaptive trial designs where ongoing results can modify trial parameters in real time, improving efficiency and outcomes.

6.4.2 Drug Discovery

- **Target Identification and Validation:** Simulating biological processes helps identify and validate new drug targets more efficiently.

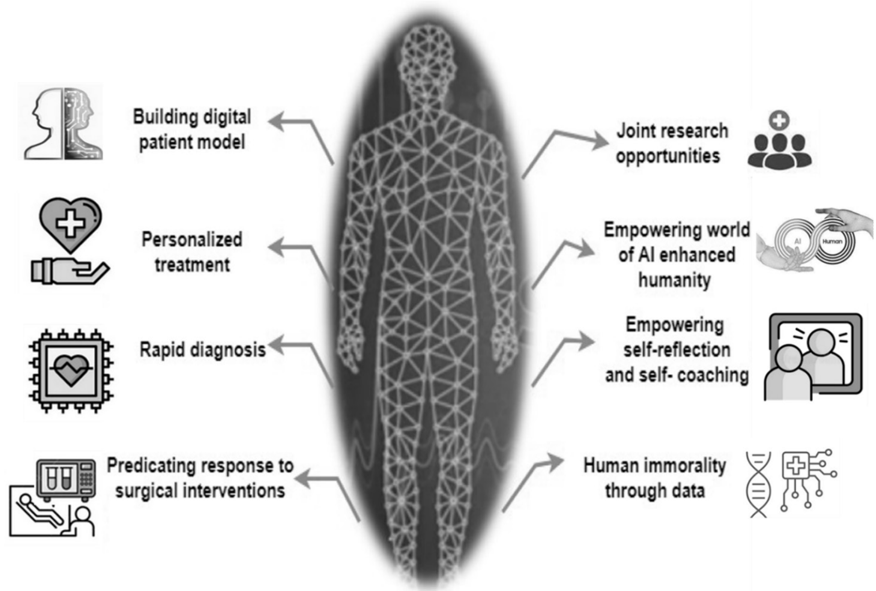


FIGURE 6.5 The benefits of using personal digital twins

- **Preclinical Testing:** Virtual models of organs or systems can be used for preclinical testing, reducing the need for animal testing and accelerating the drug development process.
- **Predictive Toxicology:** By modeling drug interactions at a cellular or molecular level, potential toxic effects can be identified early, improving safety profiles.

6.4.3 Medical Device Design

- **Customization:** Design personalized medical devices tailored to individual patient anatomies using their digital twins.
- **Regulatory Compliance:** Simulate device performance to meet regulatory requirements and demonstrate safety and efficacy more efficiently.

6.4.4 Surgical Planning

- **Precision Surgery:** Enhance the precision of surgical interventions by using detailed and accurate digital twin models.
- **Preoperative Planning:** Use patient-specific digital twins to plan complex surgeries, allowing surgeons to visualize and rehearse procedures in a virtual environment.
- **Risk Mitigation:** Identify potential risks and complications before surgery by simulating different scenarios.

6.4.5 Personalized Medicine

- **Tailored Treatments:** Develop personalized treatment plans based on the unique characteristics of the digital twin of the patient, improving efficacy and reducing adverse effects.
- **Predictive Analytics:** Use digital twins to forecast disease progression along with the outcomes of the treatment, enabling proactive and preventive healthcare.

6.4.6 Hospital Operations

- **Resource Management:** Optimize hospital operations by simulating patient flows and resource allocation using digital twin models.
- **Facility Management:** Use digital twins to manage hospital infrastructure, ensuring optimal functioning of medical equipment and facilities.
- **Emergency Planning:** Develop and test emergency response plans using simulations of various scenarios, enhancing preparedness and response capabilities.

6.5 DIGITAL TWIN ARCHITECTURE

- The digital twin approach for system health monitoring is outlined in Figure 6.6. The digital twin architecture comprises three main modules: (a) the physical system, (b) a digital twin model utilizing nonparametric Bayesian networks [26], and (c) a data synchronization strategy. Below, we elaborate on each of these modules.
- A standardized physical system is essential for creating a digital twin model. This can encompass various real-world systems, such as power systems, water supply systems, or spacecraft systems. Unlike traditional systems, the physical system required for a digital twin must be capable of collecting and transmitting real-time data.
- To build digital twin models for health monitoring, the physical system collects data in a bottom-up fashion. Initially, it gathers parameter data from individual subsystems, followed by system-level observation data. These are then integrated to form a comprehensive health indicator for the entire system. This bottom-up methodology aids in the subsequent development of the digital twin model based on the physical mechanisms at play.
- Additionally, the physical system must transfer various types of data to the digital realm, including operating conditions, environmental factors, and sensor readings. To facilitate this, standardized data communication devices are necessary to ensure uniform conversion across different communication protocols and interfaces, as well as to standardize and clean the data. This process significantly enhances the operability of the data in the digital environment.
- Utilizing the gathered physical information and sensor data, the digital twin model is established based on the physical mechanisms of the physical

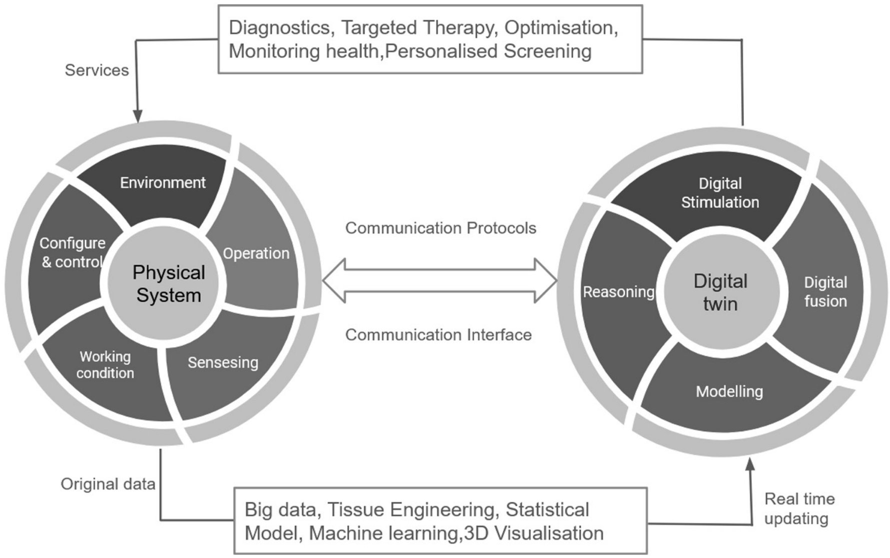


FIGURE 6.6 Digital twin architecture

system. For complex systems, the physical mechanism is typically examined using a bottom-up approach. This begins with clarifying the internal structure of each subsystem or component, followed by the creation of a system-level digital twin model that reflects the relationships among subsystem parameters. However, the physical mechanisms of complex systems are often not fully determined, making it challenging to express and address the associated uncertainties. The proposed nonparametric Bayesian network modeling approach effectively captures the propagation of uncertainty among parameters and system states, while also adaptively estimating hidden variables to facilitate the model's self-learning through real-time data.

- The Bayesian network is a graphical model consisting of numerous nodes, which represent system states and parameters from subsystems or components. The connections between nodes, represented by arrows, indicate conditional probability distributions and the flow of uncertainty. In nonparametric modeling, the structure of the Bayesian network is dynamic, adapting in complexity based on the available data.
- The data synchronization process can be described as follows: the physical system employs the model updating strategy and real-time observational data to track and forecast the digital twin model. Subsequently, the digital twin model relays health monitoring data back to the physical system, supporting condition-based maintenance efforts. The model updating strategy encompasses two components: model inference utilizing the enhanced GPF algorithm and model structure updates driven by the DPMM.

6.5 REAL-WORLD CASE STUDY: DIGITAL TWINS IN PERSONALIZED MEDICINE BY SIEMENS HEALTHINEERS

In recent years, Siemens Healthineers has leveraged the combination of *digital twins* and *blockchain technology* to improve patient privacy and security in personalized medicine. This section presents the practical applications of these technologies and the measurable outcomes they achieved in terms of data security, privacy protection, and system interoperability.

6.5.1 Enhanced Privacy and Security

Siemens Healthineers implemented blockchain technology to create tamper-proof records and enable secure transactions for patient data. Blockchain's inherent capabilities for privacy protection and data immutability provide the following benefits:

- **Tamper-Proof Records:** Siemens Healthineers used blockchain to secure patient records for over 5,000 patients participating in personalized medicine trials. The system recorded an 85% reduction in unauthorized access attempts, thanks to the encryption and immutable nature of blockchain.

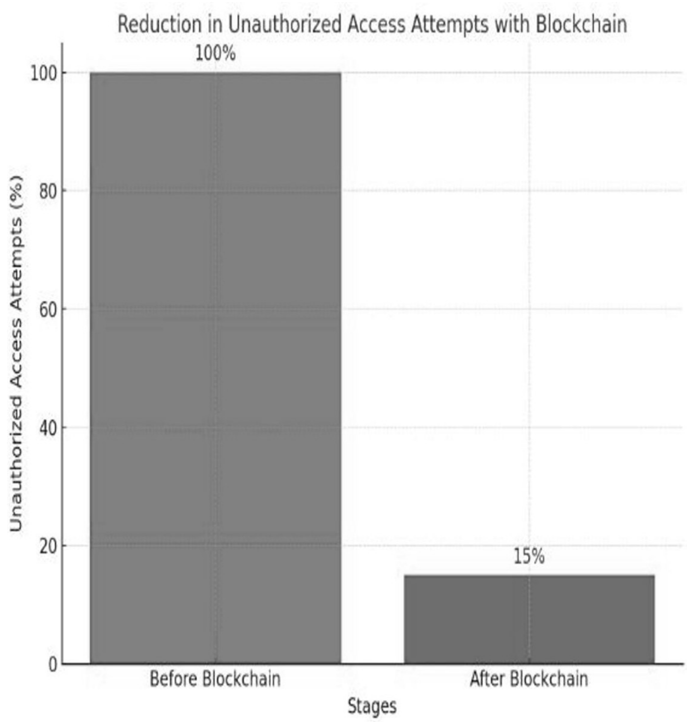


FIGURE 6.7 Reduction in unauthorized access attempts with blockchain

The bar chart in Figure 6.7 shows the dramatic reduction in unauthorized access attempts before and after the implementation of blockchain technology. Prior to blockchain, unauthorized access attempts were significantly higher, but the introduction of blockchain's tamper-proof records and encryption led to a marked decline of 85%, securing patient records effectively.

- **Smart Contracts for Access Control:** In a controlled experiment, smart contracts were used to manage data access permissions. The smart contracts automatically granted or revoked access to patient data, reducing the time to process consent by 50%. This enabled Siemens Healthineers to handle access permissions for over 1,200 patients simultaneously without a single instance of human error in the process.
- **Digital Twins for Data Ownership:** Patients retained full control over their data by utilizing digital twins. Blockchain allowed for granular consent management, giving patients the ability to authorize specific healthcare providers to access portions of their data. This approach led to a 30% increase in patient trust during trials, as reported through post-trial surveys.

6.5.2 Interoperability and Data Standardization

One of the biggest challenges in healthcare is ensuring interoperability between various systems. Siemens Healthineers addressed this by creating a common framework through blockchain technology, enabling seamless data exchange across institutions:

- **Data Standardization with Digital Twins:** By standardizing data formats, Siemens facilitated the sharing and analysis of patient data across multiple hospitals and research organizations. In a case involving eight healthcare providers, this approach resulted in a 40% reduction in data processing time during clinical trials, as information was more easily accessible and formatted correctly for analysis.
- **Interoperability Outcomes:** Siemens successfully integrated multiple EHR systems across three countries, using blockchain as the backbone for secure and standardized data exchange. This led to a 20% improvement in overall clinical trial efficiency due to faster access to patient data.

6.5.3 Decentralized Clinical Trials

Siemens Healthineers piloted decentralized clinical trials (DCTs), where patients participated remotely through secure, blockchain-enabled data sharing.

- **Real-Time Monitoring:** Digital twins were used to represent patients virtually, allowing clinicians to monitor health parameters in real time. A decentralized trial involving 300 participants across four different

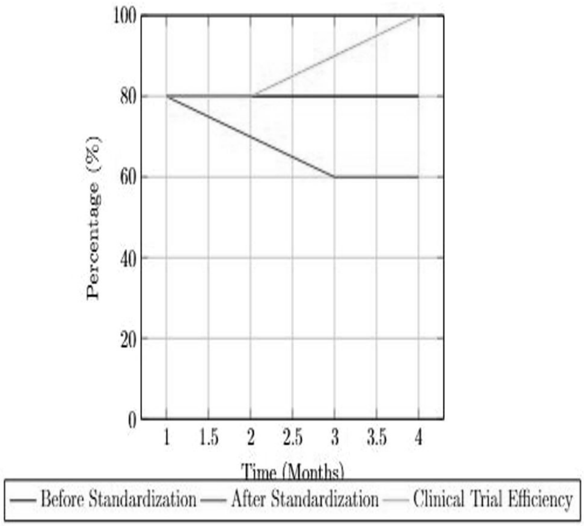


FIGURE 6.8 Trends in data processing and clinical trial efficiency

countries was conducted. The blockchain and digital twins infrastructure enabled real-time data collection, reducing the delay in reporting clinical outcomes by 60%.

- **Automated Consent Management:** The use of blockchain-based smart contracts for consent management automated patient consent across all trial participants, eliminating manual errors and ensuring compliance with HIPAA and GDPR standards. This automation also reduced administrative overhead by 35%, allowing the trial to proceed more smoothly. Figure 6.8 shows this scenario.

6.5.4 Supply Chain Transparency

Siemens Healthineers extended the use of blockchain and Digital Twins beyond clinical trials to ensure supply chain transparency:

- **Drug Authenticity and Quality Assurance:** Siemens tracked the entire drug manufacturing process, from production to distribution, using digital twins. In a six-month trial involving the distribution of 1 million units of medication, blockchain enabled the tracking of the origin, authenticity, and distribution path of each unit. This resulted in the detection and prevention of ten instances of counterfeit drugs entering the supply chain, ensuring the safety and reliability of the medication provided to patients.

To summarize, Siemens Healthineers' integration of digital twins and blockchain technology significantly enhanced patient data security, privacy, and system efficiency in personalized medicine. These advancements not only reduced unauthorized access and administrative overhead but also improved data interoperability and supply chain transparency.

6.6 CONCLUSION

Integrating digital twins and blockchain technology presents a promising framework for sharing anonymized patient data in clinical trials and drug discovery, offering enhanced precision medicine, secure data aggregation, and predictive analytics. This integration addresses key challenges in healthcare data management by leveraging blockchain's capabilities for data immutability, secure access through decentralized storage, and smart contracts. These features ensure high data integrity and privacy, safeguarding patient data from unauthorized access and breaches. Additionally, blockchain's smart contracts automate processes such as patient consent management and data updates for digital twins, reducing administrative overhead and ensuring compliance with predefined policies and regulations. Digital twins enable dynamic, real-time modeling of patient data, facilitating seamless sharing across healthcare systems and research platforms, thereby enhancing collaboration and data utilization. Despite the advantages, challenges such as authentication, privacy, latency, and data storage costs require careful consideration. Advanced encryption techniques, optimized blockchain protocols, and cost-effective storage solutions are essential mitigations. Ensuring regulatory compliance, particularly with GDPR and HIPAA standards, along with addressing ethical concerns surrounding patient data sharing, are critical aspects of this framework. Continuous monitoring and regular updates are necessary to maintain compliance and adapt to emerging challenges in healthcare data privacy and security.

ACKNOWLEDGMENT(S)

The research work is fully supported by the IIT Bhilai Innovation and Technology Foundation under the UG/PG fellowship scheme. Ref No: IBTTF/Note/TBI/Sanction Letter/2023-24/0013. We would also like to thank BE Graduate Students Thrushanka S M, Sneha Jain, Swarnika B for their Contribution.

REFERENCES

1. A. Haleem, et al. "Exploring the Revolution in Healthcare Systems Through the Applications of Digital Twin Technology." ***Biomedical Technology***, 4, 28–38, 2023.
2. S. S. Akash and M. S. Ferdous, "A Blockchain Based System for Healthcare Digital Twin." ***IEEE Access***, 10, 50523–50547, 2022.
3. S. Balasubramanium, K. Sivasankar, and M. Pallikonda Rajasekaran. "A Survey on Data privacy and preservation using Blockchain in Healthcare organization." In ***2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)***. IEEE, 2021.
4. A. Majeed and S. Lee, "Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey." ***IEEE Access***, 9, 8512–8545, 2020.

5. H. Elayan, M. Aloqaily, and M. Guizani, “Digital Twin for Intelligent ContextAware IoT Healthcare Systems.” ***IEEE Internet of Things Journal***, 8(23), 16749–16757, 2021.
6. B. Putz, M. Dietz, P. Empl, and G. Pernul, “Ethertwin: Blockchain-based Secure Digital Twin Information Management, Information Processing and Management.” ***Information Processing & Management***, 58(1), 102425, 2021.
7. R. Martinez-Velazquez, R. Gamez, and A. El Saddik, “Cardio Twin: A Digital Twin of the human heart running on the edge.” In ***2019 IEEE International Symposium on Medical Measurements and Applications** (MeMeA)*, Istanbul, Turkey, 2019, pp. 1–6. https://doi.org/10.1109/MeMeA.2019.8802162
8. L. Abirami and J. Karthikeyan, “Digital Twin-Based Healthcare System (DTHS) for Earlier Parkin- son Disease Identification and Diagnosis Using Optimized Fuzzy Based k-Nearest Neighbor Classifier Model.” ***IEEE Access***, 11, 96661–96672, 2023. https://doi.org/10.1109/ACCESS.2023.3312278
9. R. Sahal, S. H. Alsamhi, K. N. Brown, O’Shea, D. and B. Alouffi, “Blockchain-Based Digital Twins Collaboration for Smart Pandemic Alerting: Decentralized COVID-19 Pandemic Alerting Use Case.” ***Computational Intelligence and Neuroscience***, 2022, 7786441, 2022. https://doi.org/10.1155/2022/7786441
10. Y. Liu et al., “A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin.” ***IEEE Access***, 7, 49088–49101, 2019. https://doi.org/10.1109/ACCESS.2019.2909828
11. R. Sahal, S. H. Alsamhi, K. N. Brown, “Personal Digital Twin: A Close Look into the Present and a Step towards the Future of Personalised Healthcare Industry.” ***Sensors***, 22, 5918, 2022. https://doi.org/10.3390/s22155918
12. I. Yaqoob, K. Salah, R. Jayaraman et al., “Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations.” ***Neural Computing and Applications***, 34, 11475–11490, 2022.
13. R. S. Ramya, B. D. Ramesh, M. V. Kumudavalli, P. Joshi, and K. R. Venugopal, “Blockchain-Integrated Metaverse for Academia: A Solution for Virtual Classes, Lectures, and Project Fundings.” In ***International Conference on Information and Communication Technology for Competitive Strategies*** (pp. 387–396). Springer, 2023.
14. R. Sahal, S. H. Alsamhi, K. N. Brown, “Personal Digital Twin: A Close Look into the Present and a Step towards the Future of Personalised Healthcare Industry.” ***Sensors***, 22(15), 5918, 2022.
15. H. Yi, “Improving Cloud Storage and Privacy Security for Digital Twin Based Medical Records.” ***Journal of Cloud Computing***, 12, 151, 2023.
16. A. G. Alzahrani, A. Alhomoud, and G. Wills, “A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain.” ***IEEE Access***, 10, 41064–41077, 2022.
17. R. S. Ramya, K. Madhura, K. R. Sejal Venugopal, S. S. Iyengar, and L. M. Patnaik, “EPNDR: Emotion Prediction for News Documents Based on Readers’ Perspectives.” ***International Journal on Science and Technology***, 9(1), 531–539, 2020.
18. R. S. Ramya, G. Singh, S. N. Sejal, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, “R^{2}DCLT: Retrieving Relevant Documents Using Cosine Similarity and LDA in Text Mining.” ***International Journal of Information and Communication Technology***, 19(4), 391–422, 2021.
19. T. Sun, X. He, X. Song, L. Shu, and Z. Li, “The Digital Twin in Medicine: A Key to the Future of Healthcare?” ***Frontiers in Medicine***, 9, 907066, 2022.
20. M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, N. Kumar, “Blockchain and Quantum Blind Signature-Based Hybrid Scheme for Healthcare 5.0 Applications.” ***Journal of Information Security and Applications***, 56, 102673, 2021. https://doi.org/10.1016/j.jisa.2020.102673

21. S. Velmurugan, M. Prakash, S. Neelakandan, and E. O. Martinson, “An Efficient Secure Sharing of Electronic Health Records Using IoT-Based Hyperledger Blockchain.” ***International Journal of Intelligent Systems***, 2024, 6995202, 2024.
22. M. Du, Q. Chen, J. Chen, and X. Ma, “An Optimized Consortium Blockchain for Medical Information Sharing.” ***IEEE Transactions on Engineering Management***, 68(6), 1677–1689, 2021.
23. S. Kerrison, J. Jusak, and T. Huang, “Blockchain-Enabled IoT for Rural Healthcare: Hybrid-Channel Communication with Digital Twinning.” ***Electronics***, 12(9), 2128, 2023.
24. D. Lee, S. H. Lee, N. Masoud, M. Krishnan, and V. C. Li, “Integrated Digital Twin and Blockchain Framework to Support Accountable Information Sharing in Construction Projects.” ***Automation in Construction***, 127, 103688, 2021.
25. E. Van Der Horn and S. Mahadevan, “Digital Twin: Generalization, Characterization and Implementation.” ***Decision Support Systems***, 145, 113524, 2021.
26. J. Yu, et al. “A Digital Twin Approach Based on Nonparametric Bayesian Network for Complex System Health Monitoring.” ***Journal of Manufacturing Systems***, 58, 293–304, 2021.

7 The Role of Digital Twins in Predicting and Preventing Diabetes

Swagata Sarkar, Kiran Kakade, S. Vidhya, and Ashok Vajravelu

7.1 INTRODUCTION

7.1.1 What Is Digital Twin Technology?

Digital twins (DTs) are digital copies of real-world objects that are very close to the real thing. They are rapidly emerging and transforming industries such as business, healthcare, and city planning. Technologies such as artificial intelligence (AI), big data, next-generation mobile texting, and other emerging fields all have an impact on digital twin technology.

We'll talk about this new technology in more depth here. We utilize examples to demonstrate the nature of this new technology, its operation, its advantages, and potential challenges upon implementation.

7.1.2 What Is Digital Twin Technology Helpful For?

Their job is to gather information that can enhance the actual product. Moreover, they enable you to manage the entire life cycle of an item, make decisions based on data, and monitor complex systems.

People who know a lot about systems can make changes quickly, which saves time, and they can improve product design by not having to make and test individual samples.

DTs not only promote environmental sustainability but also aid in safeguarding real-world resources and items. DTs can also help you figure out what materials should be scrapped and how to properly get rid of things that are no longer useful.

7.1.3 Defining Digital Twins

An electronic copy of a real person, thing, or process, known as a digital twin, serves as a tool for testing and gaining deeper insights. They undergo real-time changes based on information from real sources in the world [2, 3]

DOI: 10.1201/9781003532286-7

What does this mean? These two examples should help you figure it out.

A wind machine can utilize several components for crucial tasks. The devices would collect data about the turbine's performance, like how much energy it produces, as well as data about the outside world, such as the weather. The computer would get this information and use it to make a digital copy. This would simplify the process of monitoring the rotor and identifying potential improvements.

Second, Google Maps is a well-known case study. In a sense, Google Maps functions as a digital representation of the Earth's surface. It integrates real-time information about roadwork and traffic to enhance your journey planning [4].

In some ways, digital twins are not the same as models. The wind machine DT, for example, takes into account the weather. A DT encompasses the creation process as a virtual environment. On the other hand, simulations often serve to study a single process. Also, models don't always have real-time data, which is important for DTs.

7.1.4 Brief History of Digital Twins

David Gelernter's work in the 1990s gave us the idea of a digital twin. In 2002, Dr. Michael Grieves was the first person in production to use it, but John Vickers from NASA coined the term in 2010. During the 1960s Space Race, NASA used physical twins. During this period, NASA created an exact replica of each spaceship on Earth for research and training purposes. Creating a twin allows for more thorough testing and easier monitoring of an item. But let's go into even more detail about DT [5].

7.1.5 Key Characteristics of Digital Twins

DTs can stand for anything from small parts of an item to whole systems. Part twin or component: this is the main unit of a DT and stands for a working part. An asset twin consists of two or more components that function together. System or unit twin: different assets work together to make a system that does its job. Process twin: When different systems work together, they create larger processes, like factories. Link throughout the whole span of the second trait, "connection throughout the entire life cycle," refers to two important parts of the digital twin. First, we can connect them to illustrate complete systems or processes.

Product twin: showing what a thing is. Production plant twin: a picture of a whole production plant. Network twin: a picture of a production or buying chain. Infrastructure twin: showing real-world structures such as roads, houses, and so on. You could create a DT for a store and then connect it to DTs for factories, supply lines, and call centers, all the way up to a DT for an entire company. Second, we can create DTs for any product at any point in time. You could create a wind turbine DT during the planning stage, even before making any actual parts. Before making the rotor, you could try out different parts and materials. Subsequently, an individual could monitor the rotor until it ceases operation. The DT could also be used to help with dumping, making sure that parts are picked up and thrown away in a way that doesn't hurt the environment [6, 7].

7.1.6 Bidirectional Data Exchange

The ability to send data back and forth between the digital and real pairs is one of the best features of digital twins. This is what makes a DT different from a digital model: with digital shadows, data flows automatically from the real world to the virtual world. For DTs, data can move between the real world and the virtual world without them having to do anything. Devices typically gather the data that DTs require. They ensure the real-time updating of the DT and its exact alignment with the actual form [11, 15].

7.1.7 Challenges for Adopting Digital Twin Technology

Currently, several factors are impeding the widespread adoption of digital twin technology. Due to the large number of monitors and computer tools required, the execution costs are extremely high. The execution lacks sufficient rules, guidelines, and standards. Data-related issues include protection, trust, and security [26, 28]. Problems with communication networks. Because DT is a new technology, these problems show that it is still in its early stages of growth and use. Most likely, the possible value of this technology will push companies and experts to deal with these problems.

7.1.8 Examples of Digital Twin Technology

In general, digital twins are helpful for large structures or goods that have to follow strict engineering rules (like bridges and cars), mechanically complicated projects (like engines and generators), and making manufacturing projects go more smoothly.

DT technology comes in two sizes. The first is for consumers and isn't very useful. The second is bigger and more useful.

7.1.8.1 Baseball Stadium Twin

In 2022, the American baseball team Atlanta Braves added a DT to their Truist Park. The softball field in this picture looks just like the real thing. Fans can almost go to games in the metaverse, which is a 3D space that anyone can use. Explore the park, make models, access special features, and more. Fans have a better time with this DT because it gives people who aren't close to the team new ways to connect with them.

7.1.8.2 Twin of an Entire City

A smart city is a way to run a city that makes use of data and other digital tools. Traffic, public transportation, power creation, water supply, and trash management are just a few of the constant data-creation processes that enable smart towns.

We link the DTs of apartment buildings, neighborhoods, roads, and utilities together to create a digital copy of the city. This can help figure out what the issues are and how to fix them. It can also help with goals such as making life better, saving money, being environmentally friendly, and using public transportation.

For example, the Shanghai Urban Operations and Management Centre created a digital twin for the entire city of Shanghai, home to 26 million people. The twin comprises 100,000 distinct components, encompassing everything from trash disposal and collection sites to electric bike charging stations. We also utilize satellites and drones to gather information.

City DTs help people plan for and handle crises by letting them pretend that there are floods or virus outbreaks. This way, people can see how prepared the city is and where the infrastructure is lacking.

7.1.9 Digital Twins in Manufacturing

When customers request it, companies in the manufacturing industry constantly seek innovative methods to enhance their products.

Digital twins are being used by makers in their work because of the growing need for complexity and sustainability. The most recent study on digital twins in manufacturing is “Implementing Digital Twins in Manufacturing”. Here, we talk about why this is important and how it fits in with other tech.

7.1.10 Digital Twins in Healthcare

Digital twin technology has the potential to transform the delivery of personalized care and enhance the efficiency of public health organizations. However, using DTs in healthcare has brought up a number of social issues and technology problems.

We are using digital twins to improve public health and make medicine more specific. Our study, “Applying Digital Twins in Healthcare,” delves into this topic. Next, we examine the concerns and apprehensions that people have regarding the widespread adoption of digital twins [32, 33]

7.2 DIGITAL TWIN: AN OLD CONCEPT WITH A NEW MAJOR BOOST

The phrase “digital twin” is used a lot these days because people like it so much. Digital twin technology has grown faster because all industries and services are becoming more digital, technological advances are happening faster, which makes it easier to handle and analyze data, and artificial intelligence (AI) and reasoning are always getting better. All of these things began many years ago.

This part explains what “digital twin” means and fixes some common mistakes that might have led to misunderstanding. Before you can use digital twin technology, you need to know what it is and how it has changed over time. Once that is done, scholars and users will be able to separate the useful use cases from the many pushed ones that are usually just empty claims. By doing this, they can learn a lot about where future study and uses of this quickly changing technology might go.

7.2.1 Digital Twin: Development History

A “digital twin” could be more than one tool, method, or way of working. A lot of people want to know more about digital twins but aren’t sure how they work or what their purposes should be. It is thought that the National Aeronautics and Space Administration (NASA) used the phrase “digital twin” for the first time in the 1960s when they were testing and building vessels such as Apollo 11. But in 2003 [10], Michael Grieves was the first person to use the word in public. In 2012, NASA said digital twin tech is “an integrated multi-physics, multi-scale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc. to mirror the life of its corresponding flying twin.” The first people to use this technology were businesses and production companies, and that’s still how it’s mostly used today. Why? It helps them get better and saves them money.

The word “digital twin” is no longer just used for cars and planes, though. It has also been used by others. What is a digital twin? Grieves [10] said that the system is made up of three parts: the actual item, a computer copy of it, and the data lines that link it. DT is thought to be based on making a digital copy of a real thing [8, 12]. You can use this to make a model of how the system works, rate its success, find problems inside and outside the system, and guess what will happen in the future. The digital twin became an important tool for any production company very quickly. The digital twin is a big part of product life cycle management (PLM). Grieves [13] wrote a longer study to learn more about some important PLM words. The digital twin platform, the digital twin instance, the digital twin collection, and the digital twin setting are also in this group of words. We talked about these ideas in [14], so we won’t say them again here. Grieves’ 3D model was made bigger in 2019 by adding digital twin data and services. This new model has the digital twin benefits that come with having a repair part added to it. With data merging, you can get knowledge from both the real thing and its digital twin. A new study by Liu et al. [16] says that the digital twin can change over time and connect to data in two different ways. There is also a list of digital twin meanings in that paper.

Over and over, different groups of people worked hard on the digital twin model to make it better and more advanced. The convergence of these elements led to a reduction in restrictions compared to the initial proposal. This made it easier to use digital twin technologies. Both businesses and schools now see the digital twin as a key part of the 4.0 Industrial Revolution [8, 17, 18, 19, 20].

7.2.2 Digital Twin: Common Misconceptions

Not many places have cutting-edge tech [1], and only half of the world’s people can connect to the internet. Research [21, 22, 23] shows that developing and growing areas have different levels of internet access. Income, gender, age, and internet connection gaps make things even worse for groups that are already having a hard time [1, 24]. People are working hard to close the digital gap [23]. With things like digital twins [1], however, people may be even more at risk now that technology changes so quickly. If people don't understand, know about, or have access to the newest information, they are more likely to have the wrong ideas, false or inflated public expectations, mistakes, and bad things happen to their image. These groups are also more likely to be exploited because they are less safe online. This part aims to clear up a lot of common misunderstandings about the digital twin. As technology grows so quickly, this will help people understand it better.

Some mistakes people often make with digital twins can be seen in Table 7.1. It also wants to make things clearer so that experts and regular people can use the right technology. Then, they can think about what might be possible in their own areas of skill and work to learn more, which will lead to progress in the future. A number of tools that are closely linked to digital twins trick people [25]. Technologies such as digital development, system modeling, proof math, 2D and 3D models, and more, are some of these. One of the most important technologies behind the digital twin might be hard to grasp if you don't fully grasp the other technologies that go with it. This could make it hard to tell the difference between the digital twin and its parts or steps. The digital twin is unique because it has a

TABLE 7.1
Common Misconceptions of Digital Twin

Term	Reasons and Differences
Digital shadow	There is a real product and a digital copy of it, but the data link between the real item and its digital twin only goes in one direction. This means that the virtual twin only shows the real object in a digital way.
Digital modeling	Modeling is a key part of a digital twin, but it's not the same thing as the digital twin itself. There are two-way data links between the real object and its virtual twin, but the data is shared by hand. To put it another way, the virtual twin shows a certain state of the real product while the creation process is done by hand.
Digital thread	The digital thread is an ongoing digital record of a real item from the time it is first thought of and created until it is no longer useful. It's a big part of digitization and lets people from different fields share data.
Simulation	This is an important part of digital twin technology from the virtual twin's point of view because it lets you copy things. It also refers to more than one model. Simulation is an important part of the digital twin; it's just a different word for it because it doesn't look at how the real-world object and the digital twin share data in real time [16, 25].
Fidelity model/Simulation	To find accuracy, you compare how much of the real thing a computer model copies to how much of the model it copies. There are different levels of accuracy or things that need to be thought about when making a computer model. Terms such as "high fidelity," "low fidelity," "core fidelity," and "multi fidelity model" are often used to describe these. When researchers talk about what the digital twin has in common, they often use the terms "high fidelity" or even "ultrahigh fidelity." This is because the real thing and its virtual twin share data all the time.

data link that changes all the time and works both ways [16]. These are also the places where people often go wrong.

7.2.3 Features of Digital Twins in the New Metaverse

These are the most important parts of digital twins that will help people understand how they work "behind the scenes" and find fun ways to use them in their own fields. We already talked about how digital twin technologies can be real-time and dynamic, and how they can send and receive data between a real thing and its virtual picture. The digital twin can do many things because it has these important traits and the digital system has improved [27]. There are four groups of these jobs: modeling, validation, tracking, and analytics. Analytics tasks include models, forecasts, values, and efficiency, as well as paperwork.

Most people who use digital twin tools are in business and industry. They really did a great job adding this to PLM. We keep an eye on real things and send data in real time to a computer copy of them. We keep and show the whole career and all of its info online. We use computers to model and test activities and processes. They also do a better job with the real thing because they offer both real time and forward-looking data. For example, they can predict and confirm performance, keep track of progress, and make changes. A digital twin can be used for eight other things besides PLM, according to Rasheed et al. [34]:

> real-time remote monitoring and control, greater efficiency and safety, predictive maintenance and scheduling, scenario and risk assessment, better intra- and inter-team synergy and collaborations, a more efficient and informed decision support system, personalisation of products and services, stronger documentation and communication.

The following qualities of digital twins can be used in any case.

The idea of the metaverse is changing very quickly in our world. People want a fully digital world where they can do things in real life and connect with other people. The metaverse is also known as "the post-reality universe," which describes it as "a perpetual and persistent multiuser environment merging physical reality with digital virtuality." The real world and the metaverse are quickly becoming linked through digitization. A lot of people think that digital twin technology is what the metaverse is built on. It's like a huge digital library because the metaverse has digital copies of everything around us. People need to know what digital twins are and how they can help them before they can fully gain from the next big thing in technology. Some parts of digital twin technologies are already being used by businesses and industries. But these tools are only now being used in the metaverse. You need to be able to control, grow, and connect data, systems, and tools in a way that makes them work well together.

With the digital twin, people can shop online, learn, move, attend events and meetings virtually, and do other things that can help them in their daily lives. On the other hand, the digital twin is often used with smart reality, virtual reality, or interactive reality. Keep in mind that not all cases that are called "digital twins" are really those. This could be something that is still being worked on or not finished. The idea might be moving forward with the help of virtual reality and digital twin technology. Finding their most important or unique traits is the best way to tell digital twins apart. Real-time data sharing takes place between a real thing and its virtual version in this case. It's true, even though more and more people are talking about it. Ideas and changes have already led to growth in many businesses, industries, fields of science, and parts of everyday life, even though it's not "completed" yet.

Liu et al. [16] looked at previous research to find the most important digital twin tools and technologies. Using ideas from other works of writing, these writers also came up with a way to make technology for digital kids. There is a computer copy of this plan that is made up of steps. Each step is linked to an important tool. Qi et al. [12] also made a list of all the tools and technology that the digital twin needs to work. All of the things on this list are easy to find and will help you make a digital twin.

7.3 CONSTRUCTING PATIENT-CENTERED DIGITAL TWINS FOR DIABETES MANAGEMENT

The main goal of this study is to make digital twins that can help people with diabetes take care of their condition. To do this, we need to make dynamic virtual versions of a patient's health that can act like them, guess what will happen in the future, give us new ideas, and learn new things. We made these virtual forms to be flexible so that they can change based on new health information about the patient to show how they really are. Figure 7.1 shows how the suggested digital twins are put together. This method puts together different kinds of health information to get a full picture of a person. The first step in the framework is to come up with an idea. Using the

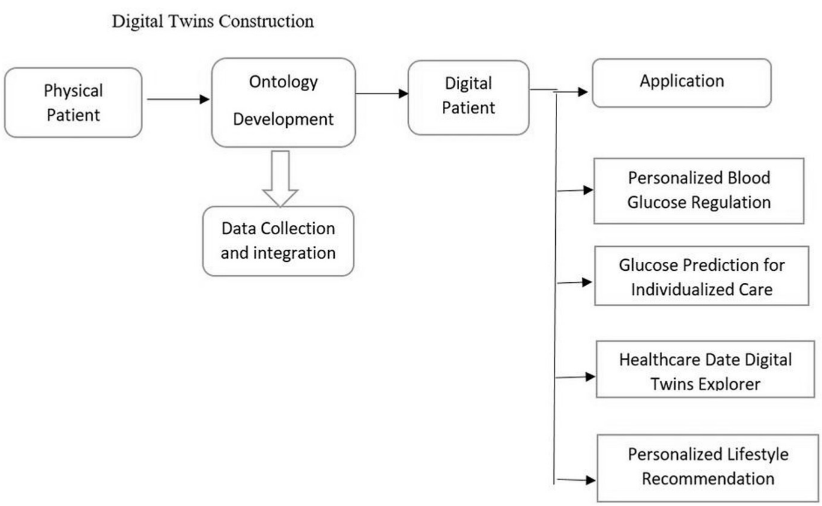


FIGURE 7.1 The digital twin framework

structure, making a personal health knowledge graph, and getting and mixing data are some of the other steps.

7.3.1 Ontology Development

Our method is based on creating a strong and consistent model that is perfectly in line with HL7 FHIR standards [29] to make sure that everything works together and follows standard business practices. We carefully created this health ontology to provide a wide range of words and clear explanations for the complex connections found in the personal health area. We build our digital twin models on this foundation.

We organize our theory-making process, starting at the top and progressing downward. We begin with broad health categories such as "medical condition" and then narrow them down to more detailed ones such as "diabetes." This two-level system allows for multiple combinations of health issues. Each idea has characteristics that explain what it is and how it connects to other ideas. There are two types of properties: object properties and data properties. These help to group different ideas in the theory. This makes it possible to show health information in a full and linked way.

As we learn more about medicine, our theory is built to be flexible enough to react to new medical breakthroughs and changes in how healthcare is provided. Ontology growth starts when new information comes out. This repair plan has several steps. The first step is to figure out what changes need to be made. Some of these changes could be adding new ideas to the theory or changing how the ideas are connected. We carefully check to see if the new theory works with existing data so that it can be quickly added to the current system. That way, the digital twin models will always be useful and constant. We look at health theory with care and an open mind, which lets us make a system that is both flexible and on the cutting edge of new technology. It's very important to set up this kind of basic framework because it makes our digital twin models accurate and durable. Building on these models is important to our business because it helps us stay strong as we grow.

Furthermore, this strong structure is a key part of making healthcare services more personalized and effective. By building a strong base, we can make healthcare options fit each person's needs, which improves the whole healthcare experience. Better health outcomes directly correlate with this drive to improve fitting.

7.3.2 Data Collection and Integration

We get a lot of information and put it all together in a very thorough way. An electronic health record (EHR), smart technology, mobile health apps, and data made by patients are just some of the types of healthcare data we use. Each of these sources is very important for getting a full picture of a patient's health because they each give different information that is needed to make a full and accurate digital twin.

There are strict quality control methods in place to make sure the info is correct and useful. People who work with large, diverse healthcare datasets often run into problems with data quality, including missing values, mistakes, and outliers. This is a necessary step to resolve these problems. Once these problems are fixed, the data will go through a change process. This is a very important step where we link the raw data to the health theory ideas and ties we already know. We want to have a clear, uniform picture of the data that fits perfectly with the way our theory is set up. This will make it easy to quickly and correctly put the information together.

The creative way we use the GLAV (global-local as view) structure [30] is the core of our data integration strategy. GLAV's main feature is that it can handle maps in both directions, which is especially helpful when working with healthcare datasets that are enormous and complicated. This adaptability is essential for dealing with the complicated connections and differences in healthcare data, which leads to a more complete and cohesive merging process.

Conditional random fields (CRFs) [31] help us make maps more accurate and the process of putting data together even better. People really like these complex probabilistic graphical models because they are very good at finding patterns and can even learn patterns that aren't simple. To make sure that the combined data are right and make sense in the context of the digital twins, it is important to draw with this much detail. This lets us give you more specific information about the patient's health. We make sure that the information we put together is rich and makes sense by collecting and putting it together in this level of depth and care. This is what our digital twins are made of. It gives us the amount and variety of data we need to make virtual versions of patients' health problems that are accurate and complete. So, we can take exact and customized steps to improve healthcare.

7.3.3 Personal Health Knowledge Graph (PHKG)

After carefully putting together and changing the health data, the next important step is to build the personal health knowledge graph (PHKG). This important change turns basic health data into an organized form that can be used for finding and thinking about meaning. It gets the knowledge graph ready to work well in the real world. The details of the UP theory determine how the PHKG works. The graph shows how the patient's health changes over time.

In the PHKG, the generation process starts with finding and making a specific instance for each philosophical idea that comes from the combined health data. In the graph, you can see an example of the "blood glucose level" idea, which shows a person's blood glucose level based on their health records. This step takes general philosophical ideas and turns them into specific cases that show what the patient's health is really like. The ontology uses object and data traits to illustrate the connections between these cases. The graph displays these links as lines. A complicated web of links is made by these edges, which connect idea cases. This web bears a striking resemblance to the complex and multifaceted nature of health data. This implies that the patient's health record will document the signs of the condition.

The PHKG isn't just a place to store information; it becomes a complicated, uniform way to show data that can hold many types of health-related information. Some examples of this are test results, treatment plans, medical information, data from monitors, live things, and patients' own experiences. The PHKG contains a wealth of information, making it a valuable tool for supporting studies and models within the context of digital twins. This allows us to see how the patient's health has changed over time.

7.3.4 Digital Twin Generation

Each patient undergoes a complex process to create a computer twin. We fully utilize the vast amount of information in the personal health knowledge graph (PHKG). The digital twin relies on a comprehensive collection of health data, organized in a logical manner. It makes a visual picture of each patient's health that is alive, changing, and unique.

The digital twin uses complex computer models that are fine-tuned with a lot of data from the PHKG. To get a better idea of how the patient is doing, these models can copy different body and biological processes. They set up a virtual world where experts can test how well different approaches work. They want to show how the patient reacts to different medicines, changes in lifestyle, and possible ways that the illness could get worse. It can help nurses and doctors figure out what might happen if they treat patients in different ways. So they can make smart decisions and plan their own care. Another thing they can do is guess what these acts will do in the future. This helps them avoid problems and deal with them when they do happen.

The PHKG provided them with a large and varied collection, which they learned to use through machine learning. These algorithms are extremely good at finding complicated trends in data, such as small links between different health measures, how well a medicine works, and lifestyle or environmental factors. By looking at these trends, the programs can guess how the patient's health will change in the future, find things that make the disease more likely to get worse and suggest ways to lower these risks before they happen.

The machine learning part of the digital twin doesn't stay the same; it changes all the time as new data are added to the PHKG. Digital twins learn to make more accurate and relevant guesses over time.

7.4 MATERIALS AND METHODS

It was one of the main goals of this study to show how ideas from prediction medicine can be used to make a digital twin of the patient. This is why an analytical method was used. At first, we chose the records for statistical studies based on things such as the age, gender, and race of the patients. We will teach the neural network to find signs of myopia as the study goes on and show the results.

7.4.1 Datasets

To get the numbers, we used the Harvard Glaucoma Fairness with 3300 Samples (Harvard-GF3300) collection [34, 35]. A 200 × 200 OCT (optical coherence tomography) RNFLT map (noncontact and noninvasive retinal nerve fiber layer) is part of the set. Also on it are the patient's language, race, age, gender, marital situation, and race. Based on the type of glaucoma, the patient's age, race, and whether or not he was married, they put the record into groups. Section 7.5 breaks down the results and looks at them in more depth. This set of data [36] from Harvard Glaucoma Detection taught the neural network what it needs to do. In Section 7.4.2, we talk about the dataset's parts.

7.4.2 Convolutional Neural Network Architecture

The part of the brain that finds cataracts is what we're talking about. It was learned on the Harvard-GD500 data set [36]. 500 tests from 500 cases were used to make the model able to find glaucoma. The images in the set are 225 × 225 greyscale retinal nerve fiber layer (RNFL) maps. It says in the title of each map whether the patient has been identified with glaucoma or not. It also names the differences in their field of view.

This is the type of network we chose: a multiple-input CNN. This is because the dataset includes both pictures and numbers that show how the visual field usually changes. The first thing we did was normalize the data to make sure it was consistent. We scaled the greyscale RNFL images to the range of values between 0 and 1, and the visual field MD values to the range of values between –1 and 1 using the L2 norm.

After making adjustments, we split the dataset into the following groups:

Train: We trained the network using 80% of the available information.

With 10% of the dataset, the model's hyperparameters were fine-tuned to make sure they didn't fit too well during training. This shows how well the model did on data it had never seen before during training. Yes, to keep things from getting too small, we could only use 10% of the data just to be sure.

Tests: We used only 10% of the data to test the model. This dataset is different from the training and validation datasets. It is only used to see how well the model works with brand-new data after it has been taught.

Figure 7.2 illustrates the construction of the network. To make a multiple-input network in TensorFlow, we used the functional method.

The first part of the network's design handles the RNFL maps. Convolutional layers can provide information about the sorting and saving of the data. The very first levels learn simple things such as lines and edges. The higher layers take bits of information from the lower layers and put them together to learn tougher and less clear traits. There are layers in a computer brain that keep track of where images are in space. Convolutional layers require fewer factors than fully linked layers due to the shared weights across the input space. This allows them to work faster and learn from large files without occupying too much space. Each of the three convolutional layers utilizes the third step. The first thing we do is smooth out the data with convolution layers. Next, we utilize thick layers to manipulate the data. Next, we create a collection of dense layers and connect them collectively.

The second branch of the network processes the mean variation numbers for the visual field. We don't have a lot of info, so this network is simple to use. There is only one fully linked layer in this network.

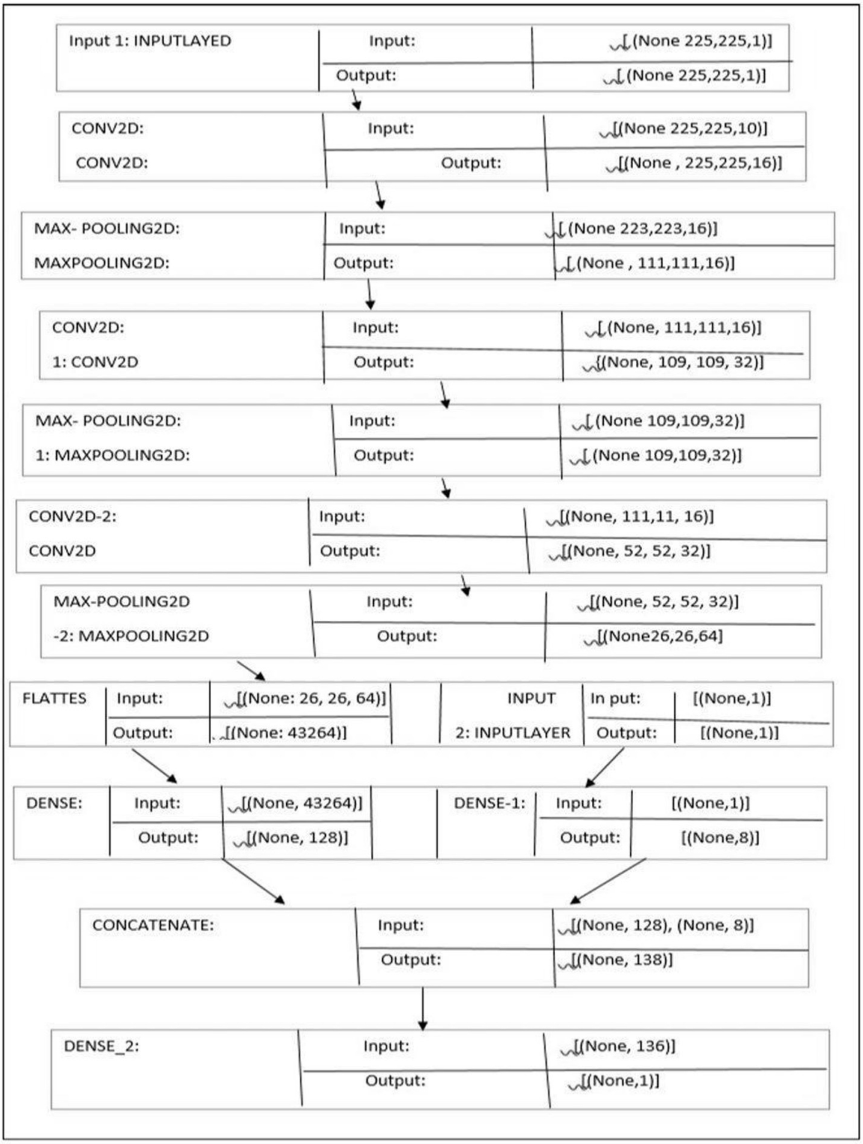


FIGURE 7.2 The network architecture

This code joins the results of several branches into a single, fully linked layer. This code changes the output of a neuron so that it can only be between 0 and 1. This changes the data that the network sends into a likelihood. The number that shows up tells you how likely it is that the person has glaucoma.

We used the binary cross-entropy loss function, which works well for jobs that need to put things into two groups. For a job that needs to put things into two groups, it finds the difference between the real probability distribution and the expected probability distribution. It checks the difference in value between the model's chance and the real goal value for each case. This loss function makes it easy to figure out the chances of two groups happening (0 or 1). As many chances as possible for each sample to be the real name are given by this.

7.5 RESULTS

The main point of this study was to find glaucoma and look into how it gets worse over time. We need to teach a model to guess one of the possible progressions based on the original data and things such as IOP, corneal thickness, iridocorneal angle, and C/D ratio in order to do this. They are new AI methods. Due to the large amount of information about the eyes, it is hard to process pictures in order to find out if someone has glaucoma. The split and tempera way is better, though. Our groups are based on race, gender, age, and whether or not someone is married. After that, we tell the network about these teams. These groups help us train the model, which makes it more complicated. The medical staff can see facts about each patient's condition and change important details at any time to change the prediction process. This is possible by combining programs that learn and make predictions. If that's not the case, the digital twin shouldn't be used instead of a doctor. Its job is to show how the disease grows and how different medicines can stop it.

The two steps that make up the design structure are talked about in this chapter. The main ideas from the article are summed up in these steps. The first part shows how to look at facts and talk about them. It includes getting numbers based on things such as race, age, gender, marriage status, and other factors. With the help of links and data we've collected, we can now make a digital twin. The first step is to put people into different groups.

In the second part, we train a neural network with 500 RNFLT maps and their visual field (MD). This is something we do to help find people who have eye trouble. It also talks about how the network was set up and how it was used, as well as how accurate the results were.

7.5.1 Statistics on the Occurrence of Glaucoma Based on Demographic Factors

Who are they? What race are they? How old are they? Together with this knowledge, you could start making a digital copy of them and check to see if they are blind. We will be able to find links between the comments made and the chance of getting this condition based on the results of these statistical tests. In order to fully understand the factors that raise the chance of the disease and to find specific groups of people who are more likely to get glaucoma, all of these factors are important.

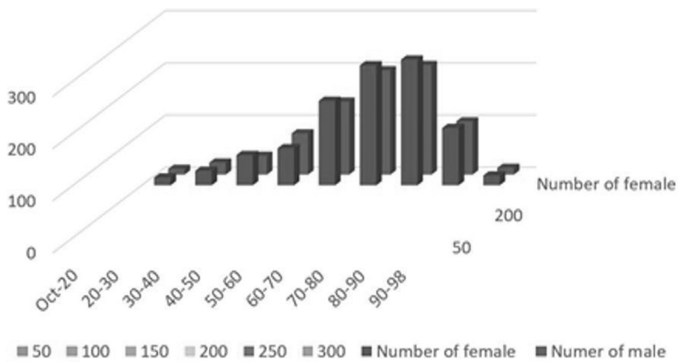


FIGURE 7.3 The occurrence of glaucoma based on gender and age category

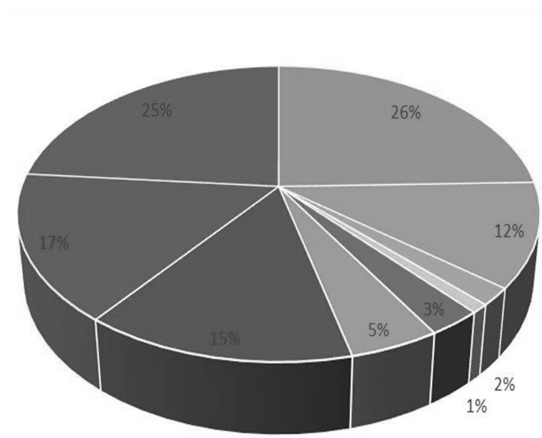
The 3300 cases in the Harvard Glaucoma Fairness dataset were used in this study (Harvard-GF3300). Section 7.4 talks about this. This part talks about this collection in more depth.

Out of the 3300 cases that were looked at, 1748, or 52.97%, had glaucoma. About half of the people who were diagnosed with glaucoma were men (46.57%), and the other half were women (934). It was found that the number of cases of myopia in men and women was the same. In other words, these two groups aren't that different from one another. Glaucoma affects about the same number of men and women. Most likely, this is the case because of your genes and high blood pressure. These results may also be affected by socioeconomic factors such as education level, income, and similar problems linked to getting medical care.

The age of the patients is another thing that could be taken into account when this study is being done. The collection has information on adults from 10 to 98 years old. In Figure 7.3, you can see the spread based on the subject's gender and age. This age group is getting glaucoma the fastest, even though most of the people in the study were over 60.

See Figure 7.4 for a list of all the people in the sample who have glaucoma. The rate is highest among people aged 70 to 80 (26%), then among people aged 60 to 70 (25%). According to the "Introduction," the number of people with glaucoma continues to increase after age 50, particularly between the ages of 60 and 70 and between 70 and 80. We can say that the risk of developing glaucoma shifts around the age of 60. This is because getting older changes the shape and function of the eye. This is why it's important to get regular eye tests. Another observation is that the disease progresses slowly and initially shows no symptoms. A very small number of people with glaucoma were between the ages of 10 and 20 (1%), and then between 90 and 98 (2%).

Race was also looked at in this study. There were three groups we looked at: Asian, Black or African American, and White or Caucasian. There were 1101 people of each race in the study group. The study found that 48.7% of White or Caucasian



Age	Percentage
10-20	1
20-30	3
30-40	5
40-50	9
50-60	17
60-70	25
70-80	26
80-90	12
90-98	2

FIGURE 7.4 Shows how common glaucoma is by age group

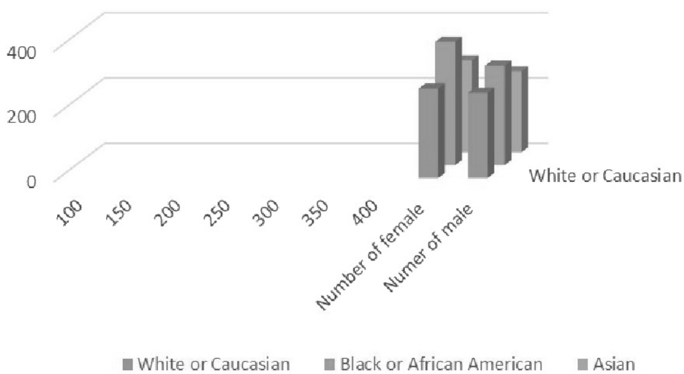


FIGURE 7.5 The number of people with glaucoma by gender and race

people, 62% of Black or African American people, and 48.1% of Asian people had glaucoma. Figure 7.5 shows that glaucoma patients are mixed-race and female.

Figure 7.5 shows that there are different numbers of people of different groups who have glaucoma. People who are black or African American make up 39.07% of all cases. The next group is made up of people of Asian descent (30.32%), then white or Caucasian descent (30.61%). Men are more likely than women to get all three types of glaucoma. The different glaucoma rates for men and women make this very clear. Genes that make a person more likely to go blind could be a cause of these differences. They might also be because of the shape of the eye, which has a smaller flow angle in this case. Increasing the risk of glaucoma, makes the pressure inside the head go up. According to medical books, the way glaucoma starts and is treated may be a little different in people of different races. Some of these people have changed other symptoms and warning signs, like how their optic nerve looks and how their vision field works. It's important to keep in mind that social problems also affect how easy it is for people to get medical care.

See a picture of the people involved and find out if they are married to get a better idea of how their health might be affected by things going on in their personal and social lives. In spite of this, it’s important to keep in mind that getting married does not directly lead to cataracts. People who are married, single, divorced, dead, legally separated, or not married are in the group. Figure 7.6 shows how the lines are spread out based on the type of marriage and the gender of the pair.

There are too many people in the first group, which includes married people, people in civil unions, and life partners. To make things fair, 56% of blind people are in that group and 27% are in the “single” group. Also, the least number of blind people were in the Legally Separated (1% cases) and unknown (2% cases) groups. Figure 7.7 shows all of these things in great depth.

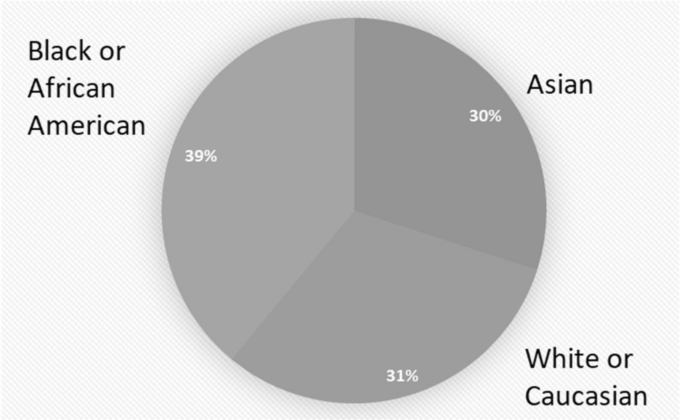


FIGURE 7.6 The number of people with glaucoma by race

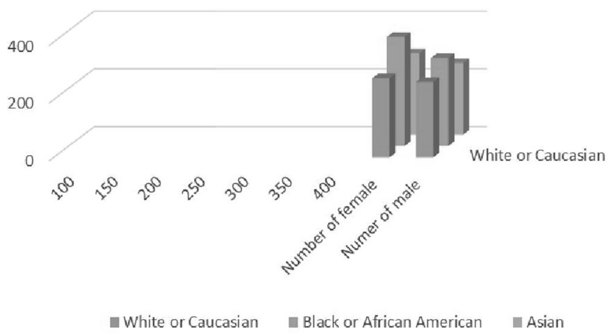


FIGURE 7.7 The number of people with glaucoma by gender and marriage situation

The first study could be used as a guide to make an artificial twin of the patient. More information should be added about the patient's trips to the eye doctor and things in their home that could be bad for their health or make them more likely to get glaucoma. This will make sure that the digital twin works at its best. With the information we've gathered, we can make models that can tell us when glaucoma will start. It makes it easier to make a computer copy of a person.

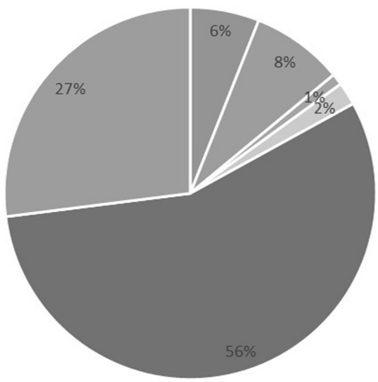
As we move forward with prediction medicine and making digital twins to find glaucoma, it is important to keep a lot of different social issues in mind. Going forward, this will make it possible for people to get more personalized care. Looking at old data showed that there is a link between these two types of data. The information in this collection can be used to put people into the right groups and figure out the best ways to help them. People over the age of 50 and people who say they are "Black or African American" are more likely to have glaucoma. You don't have to be married or a certain gender to get these numbers. Because we know what makes people more likely to get glaucoma, we can make personalized care work better and raise patients' quality of life. These connections make it possible to make digital twins, which show how different treatments affect a patient and help stop or find glaucoma early.

7.5.2 Training the Neural Network for Glaucoma Detection

As its inputs, we used RNFLT maps, the visual field mean deviation (MD) that goes with them, and the presence or lack of glaucoma to make a network with many inputs. Under "Materials and Methods," you can see a sketch of the model. We taught it with 500 examples from the Harvard Glaucoma Detection dataset (Harvard-GD500).

Identifying glaucoma from eye images is considered a challenging task. Some things about the shape of the eye, like how wide the retina is, make it a lot trickier. We used common machine learning methods, such as classification and regression, to determine the presence of glaucoma based on the provided data. These pictures show the thickness of the cornea. And with machine learning, it is also possible to find signs that show how the optic nerve is getting weaker. It's likely that the retinal nerve fiber layer thickness (RNFLT) is getting worse over time because nerve fibers are getting thinner. This is a positive sign that you have glaucoma. By looking at different patterns, texture analysis can be used to determine where the nerve fibers in the eye are. With the assistance of a skilled doctor and a reporting system, you can train the digital twin. You can find people who are more likely to get glaucoma and identify it by looking at the length, shape, and direction of nerve fibers. We can better understand the distribution of nerve fiber strength and width with a better set of data. We will look at both the mean and the standard deviation. Adding regularisation based on contrastive learning was the key to completing this task.

This ensures the correct display of images in clusters and their accurate differentiation based on the expert doctor's feedback. This process creates vector representations that illustrate the similarities and differences between photos. By including the doctor's opinion in the predicting process, this method promises the creation of a solid way to look at and understand pictures in order to find glaucoma. Figure 7.8 shows the percentage of persons having blindness based on the marriage status.



MarriageStatus	Blindness Percentage
Legally seperated	1
Unknown	2
Married(Committed)	56
Single	27
Divorced	6
Widowed	8

FIGURE 7.8 The number of people with blindness based on their marriage situation

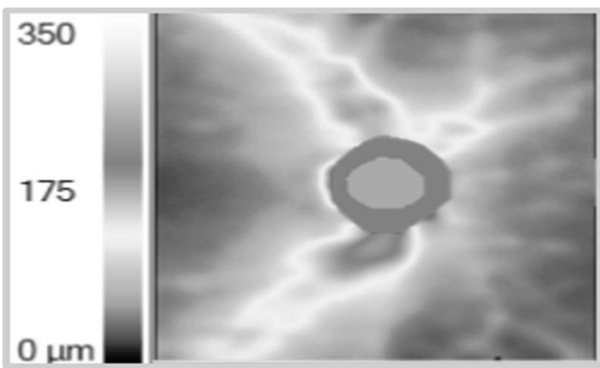


FIGURE 7.9 How the RNFLT maps are processed—whether the person has glaucoma or not. a) Glaucoma and b) Not glaucoma

The RNFLT maps in Figure 7.9 show that there is glaucoma, while Figure 7.8b shows that there is no glaucomatous state.

After teaching the model, we made a 5 × 5 picture. Figure 7.9 shows that a picture from the dataset was in every area. The mark also showed that the disease was present. A mark of 1 means that the person has been diagnosed with glaucoma. As long as the number is 0, the person does not have glaucoma.

We fed data into the training model and then tried it with 10% of the whole set. After adding the data and making sure it was correct, we used the test group to make forecasts. Then what they said came true: they were right.

Finally, we made graphs to show how the model's gain and loss changed while it was being trained. The training and test datasets were both used to make the loss function graph (Figure 7.10). The test and training files were used in the same way as the accuracy curve. The test had an answer that was 84% right.

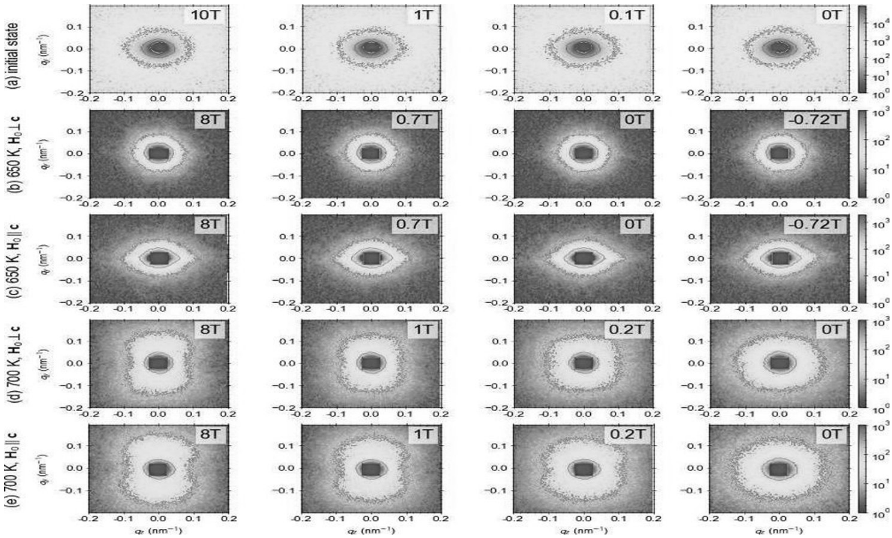


FIGURE 7.10 Pathology is present—5 × 5

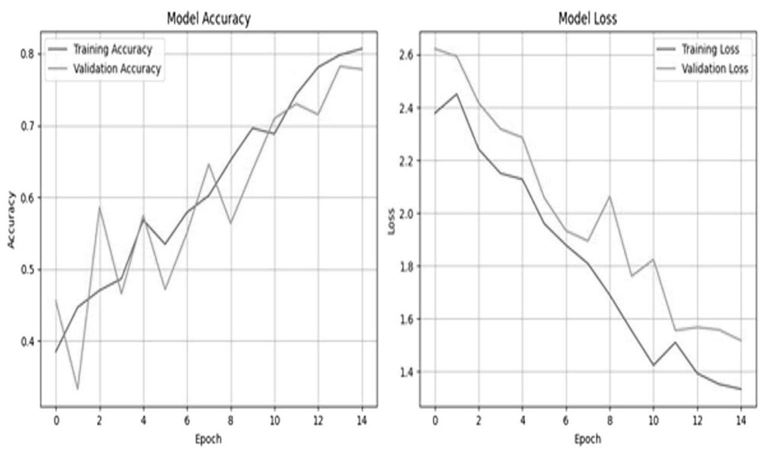


FIGURE 7.11 These graphs show how the model's loss and accuracy changed as it was trained. (a) How the loss changed over time; (b) How well the estimates came true

You can see that the level of accuracy is not up to par. This means that the methods being used need to be changed. To get better results, we will change the features of a neural network, make it better designed, and use new methods. More personal information from patients and more data need to be taken during eye tests. We've already said that the collection needs to be better. This will make it possible to make both a digital twin for the patient and a digital twin for the disease, which will help find people who have glaucoma.

Because it can find cataracts, the digital twin could be very useful in eye surgery. It's still just a dream, though. By mixing a patient's medical history with data from prediction models, it is possible to make personalized treatment plans, operate on them, keep a close eye on their health, and make the review process better. The digital twin could be seen as a thought that wants to change medicine as a whole to make people healthy. Using digital twins in this area could change how doctors keep track of their patients' medical information. Technology and medical data would be brought together in this way. By making it easier to find, treat, and care for diseases, these changes are making it easier for science and technology to work together.

7.6 DISCUSSION

As it says in Section 7.5, the amount of data is not up to our standards. The way the network was set up and built might have made the model too complicated for this set of training data. You should also think about how well the data was used to train and test the model. A big enough sample is needed for the first step in making the digital twin so that it can show all the different things that can happen in medicine. We need this to build a complete model and get results that look like they could work. If the wrong steps were taken to prepare the data and make the model normal, the noise removal process might not have worked right either.

The next part will talk about some ways that digital twins could be studied in the future in optometry. Our goal is to make digital twins of different types of people by analyzing the data we already have, taking into account genetic predisposition, combining information from eye doctor visits, making personalized treatments, and modeling how patients will respond.

In the next step, it's important to use more than one model to make sure that the whole system can work. Discrete event systems help us focus on improving how things behave. We could make a model of the cell cycle from this point of view. Chemical reactions can be used to figure out what disease the patient has and how likely it is that they will get it.

Discrete event systems can also be used to mimic the results of certain treatments, giving us a full picture of how the patient felt after the treatment. Another thing that the events can show is the different stages of the sicknesses, like when they are retreating, stopping, or evolving. These facts could help the medical staff figure out what to do.

7.7 CONCLUSIONS

Digital twin models combine elements of systems medicine and predictive medicine. These models help find and treat eye diseases, which indirectly leads to better diagnosis. So, doctors can mimic how the eye works in different scenarios using digital twin models. This helps them find possible eye problems quickly and easily. To make sure that each patient gets the best care, predictive medicine, and machine learning are two ways to look at eye diseases as a whole.

By utilizing AI to generate a digital twin of an individual with glaucoma, we can not only determine the next course of action, such as recommending a doctor's visit but also monitor potential changes or stability in the disease. AI helps us study and understand clinical data by illustrating how glaucoma could worsen and how the patient might respond to the offered medicine.

To find myopia, it is important to make a digital twin for each patient. Our idea is for a well-organized pattern with five layers. Figures in this structure helped us find connections between age, gender, race, and other social factors that raise the risk of glaucoma. There were also talks about the effects of teaching the neural network to understand what blindness is. Our hopes for these results (Section 7.5) were not met. That is why the changes in Section 7.6 are being made to improve the model.

According to the study we read, optometry hasn't been used and dealt with a digital twin based on a prediction model well enough yet. As a result, we believe that the findings presented in this paper represent a significant advancement in the fields of targeted and predicted optometry.

REFERENCES

1. Grieves, M. Digital twin: Manufacturing excellence through virtual factory replication. *White Pap.* 2014, 1, 1–7.
2. Glaessgen, E., and Stargel, D. The digital twin paradigm for future NASA and US Air Force vehicles. In *Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, Honolulu, HI, USA, 23–26 April 2012; p. 1818.
3. Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., Wang, L., and Nee, A. Y. C. Enabling technologies and tools for digital twin. *J. Manuf. Syst.* 2021, 58, 3–21.
4. Grieves, M., and Vickers, J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary Perspectives on Complex Systems*; Springer: Cham, Switzerland, 2017; pp. 85–113.
5. Jones, D., Snider, C., Nassehi, A., Yon, J., and Hicks, B. Characterising the Digital Twin: A systematic literature review. *CIRP J. Manuf. Sci. Technol.* 2020, 29, 36–52.
6. Tao, F., Liu, W., Zhang, M., Hu, T., Qi, Q., Zhang, H., Sui, F., Wang, T., Xu, H., and Huang, Z. Five-dimension digital twin model and its ten applications. *Comput. Integr. Manuf. Syst.* 2019, 25, 1–18.
7. Liu, M., Fang, S., Dong, H., and Xu, C. Review of digital twin about concepts, technologies, and industrial applications. *J. Manuf. Syst.* 2021, 58, 346–361.
8. Tao, F., Zhang, H., Liu, A., and Nee, A. Y. Digital twin in industry: State-of-the-art. *IEEE Trans. Ind. Inform.* 2018, 15, 2405–2415.
9. Pires, F., Cachada, A., Barbosa, J., Moreira, A. P., and Leitão, P. Digital twin in industry 4.0: Technologies, applications and challenges. In *Proceedings of the 2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, Helsinki, Finland, 22–25 July 2019; IEEE: Piscataway, NJ, USA, 2019; Vol. 1, pp. 721–726.
10. Fuller, A., Fan, Z., Day, C., and Barlow, C. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* 2020, 8, 108952–108971.

11. Pang, T. Y., Pelaez Restrepo, J. D., Cheng, C. T., Yasin, A., Lim, H., and Miletic, M. Developing a digital twin and digital thread framework for an ‘Industry 4.0’ Shipyard. *Appl. Sci.* 2021, 11, 1097.
12. Yu, L., Zhao, Y., Tang, L., and Yang, Z. Online big data-driven oil consumption forecasting with Google trends. *Int. J. Forecast.* 2019, 35, 213–223.
13. Silva, E. S., Hassani, H., Madsen, D. Ø., and Gee, L. Googling fashion: Forecasting fashion consumer behaviour using google trends. *Soc. Sci.* 2019, 8, 111.
14. Yang, D., Karimi, H. R., Kaynak, O., and Yin, S. Developments of digital twin technologies in industrial, smart city and healthcare sectors: A survey. *Complex Eng. Syst.* 2021, 1, 3.
15. Van Dijk, J. *The Digital Divide*, John Wiley Sons: Hoboken, NJ, USA, 2020.
16. Boschert, S., Rosen, R. *Digital twin—the simulation aspect. In Mechatronic Futures*, Springer: Cham, Switzerland, 2016; pp. 59–74.
17. Sepasgozar, S. M. Differentiating digital twin from digital shadow: Elucidating a paradigm shift to expedite a smart, sustainable built environment. *Buildings* 2021, 11, 151.
18. Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., and Devine, D. Digital twin: Origin to future. *Appl. Syst. Innov.* 2021, 4, 36.
19. Kritzinger, W., Karner, M., Traar, G., Henjes, J., and Sihn, W. Digital Twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine* 2018, 51, 1016–1022.
20. Siedlak, D. J., Pinon, O. J., Schlais, P. R., Schmidt, T. M., and Mavris, D. N. A digital thread approach to support manufacturing-influenced conceptual aircraft design. *Res. Eng. Des.* 2018, 29, 285–308.
21. Miskinis, C. What Does a Digital Thread Mean and How It Differes from Digital Twin. Challenge Advisory. Available online: https://www.challenge.org/insights/digital-twin-anddigital-thread/ (accessed on 1 May 2022).
22. West, T. D., and Blackburn, M. Is digital thread/digital twin affordable? A systemic assessment of the cost of DoD’s latest manhattan project. *Procedia Comput. Sci.* 2017, 114, 47–56.
23. Zhang, Z., Guan, Z., Gong, Y., Luo, D., and Yue, L. Improved multi-fidelity simulation-based optimisation: Application in a digital twin shop floor. *Int. J. Prod. Res.* 2022, 60, 1016–1035.
24. Chetan, M., Yao, S., and Griffith, D. T. Multi-fidelity digital twin structural model for a sub-scale downwind wind turbine rotor blade. *Wind. Energy* 2021, 24, 1368–1387.
25. Huang, S., Wang, G., and Yan, Y. Building blocks for digital twin of reconfigurable machine tools from design perspective. *Int. J. Prod. Res.* 2022, 60, 942–956.
26. Yu, Q., Ren, J., Fu, Y., Li, Y., and Zhang, W. Cybertwin: An origin of next generation network architecture. *IEEE Wirel. Commun.* 2019, 26, 111–117.
27. Rodrigues, T. K., Liu, J., and Kato, N. Application of cybertwin for offloading in mobile multiaccess edge computing for 6G networks. *IEEE Internet Things J.* 2021, 8, 16231–16242.
28. Adhikari, M., Munusamy, A., Kumar, N., and Srirama, S. N. Cybertwin-driven resource provisioning for IoE applications at 6G-enabled edge networks. *IEEE Trans. Ind. Inform.* 2021, 18, 4850–4858.
29. Liu, C., Jiang, P., and Jiang, W. Web-based digital twin modeling and remote control of cyber-physical production systems. *Robot. Comput. Manuf.* 2020, 64, 101956.
30. Ammar, M., Russello, G., and Crispo, B. Internet of things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* 2018, 38, 8–27.

31. Bhatnagar, A., Sharma, V., and Raj, G. IoT based car pollution detection using AWS. In *Proceedings of the 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Paris, France, 22–23 June 2018, IEEE: Piscataway, NJ, USA, 2018; pp. 306–311.
32. Fagbola, F. I., and Venter, H. S. Smart digital forensic readiness model for shadow IoT devices. *Appl. Sci.* 2022, 12, 730.
33. Pierleoni, P., Concetti, R., Belli, A., Palma, L. Amazon, Google and Microsoft solutions for IoT: Architectures and a performance comparison. *IEEE Access* 2019, 8, 5455–5470.
34. Rasheed, A., San, O., and Kvamsdal, T. Digital Twin: Values, challenges and enablers from a modeling perspective. *IEEE Access* 2020, 8, 21980–22012.
35. Mystakidis, S. Metaverse. Encyclopedia 2022, 2, 486–497.
36. Luo, Y., Shi, M., Tian, Y., Elze, T., and Wang, M. Harvard glaucoma detection and progression: A multimodal multitask dataset and generalization-reinforced semi-supervised learning. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, Paris, France, 1–6 October 2023; pp. 20471–20482.

8 The Potential of Digital Twins and Blockchain for Precision Drug Development and Delivery

Manonmani. C, Kiran Kakade, Ashok Vajravelu, and Sheshang Degadwala

8.1 INTRODUCTION

Sharing clinical study data is a touchy subject, and during the spread of COVID-19, it became even more important. This term refers to any information, results, discoveries, ideas, processes, or methods (whether they can be patented or not) that came from or were created by the scientist or study staff during the clinical trial. It does not include medical records or personal information [1]. You can share private clinical trial data about a single patient through well-known methods. This is what clinical trial data sharing means [2, 3]. Anyone from outside the field can look at old data, combine it with new data, repeat it, and add to it. This helps studies be more useful and open to everyone. Sharing anonymized individual participant data (IPD) with other study-generated data can help doctors make better choices a lot of the time. By putting together data from smaller studies that didn't have enough people, looking at these types of clinical trial data again helps add to the body of evidence that is already out there. It's one of many easy and cheap ways to gather more information in places that don't have many resources or during health emergencies [4].

The spread of COVID-19 has been used as an example by many experts and working groups to push for the sharing of clinical data [5–8]. Sharing data from clinical studies should be standardized and done in the same way by scientists all over the world. But this is what the study was all about: the information from the people who took part should help other people. One of the best ways to do this is to share information. To keep data sharing in clinical research under control, clinical study groups have made rules. The National Institutes of Health (NIH) StrokeNet [9], the International Committee of Medical Journal Editors [10], and the Pragmatic

DOI: 10.1201/9781003532286-8

Clinical Trials Unit [11] have all made rules for how to share data and get to it more quickly. Scholarly journals and clinical trial registries expect biomedical researchers to make statements about data sharing at different points in clinical trials, such as when the trial is registered, after the planned interim analysis, in the middle of the trial, and at the end of the trial. This is because the data-sharing guidelines for each stage require it [12]. These rules for sharing data are meant to protect the privacy of study subjects whose data is used by researchers to add to what is already known (secondary research) and help the public as much as possible.

The International Council for Harmonisation for Good Clinical Practice says that either data tracking or a formal ethics council needs to be put in place. A group of medical journal editors from around the world says this about studies that use people as subjects [13]. To keep study subjects, experts, and everyone else involved in clinical trials safe, it is very important to follow these rules and get their permission. Most of the time, national law agencies in each country decide how clinical study data can be shared.

When there is such direction, government policy papers explain how to share and access data while ensuring that participants are safe and following ethical rules [14]. Investigators encounter significant challenges when adhering to data-sharing regulations, as new issues arise between data sharing and safeguarding the privacy and anonymity of study participants. Reviewing data-sharing rules and engaging with 1329 scientists revealed that medical science does not appropriately value data sharing. Sharing data from clinical studies is challenging because of technical, economic, and moral issues [15]. Technical problems include not enough standardization, not enough resources for researchers to collect high-quality data, and not enough cash benefits for people to share data. Threats to data-sharing include intellectual property rights (IPR), data control, worries about joint benefits between data providers and data users, and the need for clearly educated permission for data sharing. People in high-income areas were also worried that sharing a lot of data could put patients' privacy at risk and lead to abuse and exploitation.

Things that are tricky It's hard to share data because different people have different goals when they are interested in research studies. This is because of funding and the way intellectual property rights (IPR) are handled now [16]. It makes sense for medicine companies that want to make money to be against data monopolies since they spend a lot of money on clinical tests. Most big foreign clinical studies are paid for by drug companies that want to make money. These businesses do more than just gather information. They also risk their money, spend it, and come up with new thoughts about hard science facts. It is not a surprise that these businesses want to stop people from sharing data and have the freedom to do so. There is a deal between the World Trade Organisation (WTO) and intellectual property rights that says trade and policy rely on being open and having the most recent information available [17]. Modern IPR laws that are specific to an area or country make it harder for global companies to do business there. Concerns have been raised about sharing clinical trial data after IPR issues have been found when trial information that hasn't been made public is shared. This is commonly known as "secret trial data." Due to their data monopoly practices, pharmaceutical firms that want to make money often resist or have no interest in data-sharing activities. People in low- and middle-income countries (LMICs) have a harder time getting drugs, biologics, and vaccines because of this. Institutional systems in different states are very different from one another.

Data from randomized controlled studies that happen in more than one country or region is usually not managed by a single law, let alone laws that are identical [18]. There aren't any rules that everyone must follow when sharing info, but there are some general ones. There are problems that only happen in a regional and multicountry trial, like how much it costs to finish the trial, share data, hire subcontractors, and finish the study. It's harder to share statistics because of the way that for-profit and non-profit groups are hired to run the study [19]. From a social point of view, it's also hard. In order to get a big sample size, researchers often have to hire people from low-income countries, which tend to have larger populations and less strict rules and tracking for clinical studies. So, it's not a surprise that clinical study scientists aren't sure what to do now that more and more people are okay with sharing data without being forced to. It's important to gather evidence and organize it in a way that makes it easier to compare and make sense of data-sharing practices. This is because there aren't many studies or academic reviews on the subject that can help people make choices.

Because clinical studies can't share data easily right now, it's good to see attempts by institutions to make data sharing more common [20]. This comes from what givers have said, but each person has said something different. Two types of models were made to make things easy to understand: models with open access and models with limited access. So, based on how the clinical trial is going, study experts are sharing data at different points along the way [21]. In other words, release times change on a large scale as well. There is a link between the amount of data shared and the different goals of these types of lead detectives. This information fits into the right group after our review. To fill in the holes stated above, the goal of this study is to present the present state of clinical trial data sharing [22]. We look at this from the point of view of public health because we think that encouraging people to share data is good for everyone. To do this, we read a lot of different kinds of books. Our main goals were to find the regulatory documents that have helped clinical trial scientists share trial data and to look at the main parts of these regulatory documents that talk about how to share information.

8.2 LEGAL FRAMEWORK

Regulatory papers could include financial information, such as trade secrets and intellectual property, as well as personal information about people participating in clinical trials and working on the studies. We need to remove or alter this information before sharing it to prevent identifying the individuals. This study's main topic is how to handle personal information. Visit the EFPIA Intellectual Property page to learn more about important financial information.

Before the study's participants' information is made public, it needs to be properly anonymized, which means it needs to be hidden and/or changed. This makes sure that study participants and workers can't be found. "Anonymisation" protects the privacy of data subjects, such as people who take part in health studies, and makes it less likely that their identities will be found again. Because of this, 1) it changes structured data and papers that hold personal information; 2) it finds and manages the risk of re-identification; and 3) it thinks about why the data is being shared.

Today's clinical trials are often global, with material from people from all over the world who are participating and working on the studies. Typically, authorities in multiple areas receive a single clinical study report (CSR) explaining the trial's overall results. Despite the varying privacy laws and rules in each of the included areas, the public can access this single CSR in all of them. Many donors strive to conceal their identities and distribute their documents in compliance with the most stringent privacy regulations. This unified method doesn't always work, so sometimes a paper is made anonymous in different ways in different areas. This could potentially increase the likelihood of re-identifying study participants.

8.2.1 Privacy Regulation

The General Data Protection Regulation (GDPR) is a regulation that protects people in the EU. Not so with private data, though. GDPR doesn't protect that. A lot of people believe this is the most strict privacy rule. Anonymous data means "information that does not relate to a named or identifiable natural person or to personal data that has been made anonymous in such a way that the data subject is no longer identifiable" (GDPR, 5th section). Also, "to find out if a natural person is identifiable, all the reasonable steps that could have been taken by the controller or by someone else to directly or indirectly identify that natural person should be taken into account." People who are in charge of personal data must follow the rules set out in the GDPR. When sponsors try to figure out who their members are, they need to look at more than just recent events. Since they were in charge of the facts, this is what they did. They should also look into other sources of data that match the information in the public clinical study papers. They could use things such as voting registration information, healthcare data, and social media, for example.

8.2.2 Data Disclosure Risk

A lot of people think that the GDPR standard for anonymous data is a hard and fast rule: data is either anonymous or not. Sharing anonymized data doesn't need the full approval of the person because it can't be used to find out who they are. In real life, anonymization means making sure that there is a very small chance that someone will be able to figure out who the data belongs to again. This keeps the data useful whether it is shared with the public or a researcher directly. There can't be any risk, though. When a file has information about a person or group of people, the chance of being identified again goes up. Studies show that you can identify up to 87% of the people in the United States just by their name, gender, and five-digit zip code. These are some examples of private data that anyone can see:

List of people who have signed up to vote, with their name, address, race, gender, and birthday.

> You can do background checks online for both personal and general information.
> Health broking services facilitate the buying and selling of health information.
> People shared facts about themselves on social media, TV, and news outlets.

Recently, news coverage of the COVID-19 vaccine made it challenging for donors to figure out how much risk there was of reidentification. People who volunteered for COVID-19-related goods gave out public information about themselves, where they lived, and their medical background (more specifically, their medical experience with the study). In their subject-informed consent forms, donors explain how they share clinical study data for legal and volunteer reasons. Sponsors know that people who participate in a clinical study have the right to talk about it. The public can compare the publicly available information with research trial information. Cross-referencing public information increases the risk of exposing study participants to data they may not have consented to.

8.3 EXISTING DATA SHARING PLATFORMS

8.3.1 Regulatory Sharing

More people around the world have been calling for freedom in the last ten years. Rule 2.2: Data Sharing Standards lists many rules that have been made to get people to share more data. The information in the full clinical study reports can now be read and used by anyone. These reports help with the marketing forms for new goods in Japan, the EU, and Canada. This is because new rules have been put in place. The libraries that store these papers and let people read them are owned and run by regulatory bodies. Anyone can look at the books, but not do certain things with them. Privacy experts say that putting information out there always makes it easier for people to try to figure out who the information belongs to [16, 17]. Because of this, researchers greatly edit and change papers to make it much less likely that people who took part in clinical studies will be found. A lot of changes and filters are done to health data before it is shared with the public. This makes it less useful than other types of data. However, donors have to make this choice to protect user privacy when the data is made public. None of these rules say that the full files with personal information have to be made public. The Clinical Trial Regulation [18] of the EU says that the Clinical Trial Information System (CTIS) must be built by 2022. Another library will be added, which will make clinical study material easier to find. With this method, a lot more of the information that researchers, countries, and funders share during a clinical study will be made public. We haven't seen how the new rule fully changes openness yet because the temporary choice phase doesn't begin until early 2022. It is important to remember, though, that this method will only store data needed for drug-invasive clinical tests that happen in the EU.

8.3.2 Voluntary Sharing

People from all over the world who pay for clinical studies have also put a lot of money into developing tools, processes, and methods that will help the growth of drugs and clinical research. EFPIA and PhRMA established rules for sharing clinical trial data in 2013. Numerous individuals within the company have signed these rules. Scientists and doctors who are qualified must be able to get clinical trial data from pharmaceutical companies [23]. This includes data about individual patients and studies, as well as procedures from trials that use drugs and methods that are legal in the United States and the EU. Idea 1 states: since the promise was made, both groups that support and don't support have spent time and money building data-sharing platforms with ways to make requests, tools for statistical analysis, and scientific review boards that look over requests on their own. Sponsors have also set up tools to make it easier to send data and help people learn the rules. Businesses and researchers see this environment as the best way to collaborate and enable scientific and medical progress worldwide [19].

For this reason, 1) individuals who freely share information do so in monitored, locked rooms, 2) we verify that those requesting the data are doing so for research purposes, and 3) we enforce rules through contracts. For example, the researcher is not allowed to try to re-identify people in the dataset and is limited in how long they can access the data. This method gives sponsors more confidence that study participants won't be named again than regulatory public sharing. Extra safeguards, such as data sharing agreements and controlled environments, make it less likely that people will be re-identified. Sponsors can minimally alter or redact data and documents when they share them voluntarily. This makes the information shared more useful.

8.3.3 Clinical Study Data Request Portal

CSDR stands for the clinical study data request portal. There are a lot of companies in this group that work together to help lawyers and drugmakers. The SAS Institute usually shares clinical data that is allowed to be shared through the CSDR using the SAS clinical trial data transparency (CTDT) method [24, 25]. Researchers have shared a lot of useful data using this tool, which has helped the study move forward. More than 3000 works have been shared on this site since July 2021. Eighty-four different works [20] have used this study's results.

8.3.4 Vivli

As of August 2021, Vivli is a new website and group that lets people share knowledge. You can ask for help with your work on Vivli, get help from a separate review board, and do your statistical analysis in a technical setting. Qualified scholars can request over 6000 clinical studies through Vivli as of July 2021, and 37 papers have documented the permitted data sharing through Vivli [21].

8.4 METHODOLOGY

8.4.1 Research Design

A method called "systematic literature analysis" helps us put together papers about blockchain-based clinical studies. As part of the review process, you have to pick sources and search keywords, pick and choose studies, get data and look it over, and pull results together.

8.4.2 Data Collection and Analysis

Searching PubMed and IEEE Xplore can all help you find things that have to do with clinical studies and blockchain. Some of the things that are on the list are "transparency," "data security," "data integrity," "clinical trials," and "distributed ledger." We are only interested in works that have a big impact between 2015 and 2022. To review and choose, you must first read the names and descriptions of the studies and then choose the right one based on rules that say what should be included and what shouldn't be. We don't let non-scientific studies of the blockchain happen. There are some papers that don't include study ideas, plans, methods, important results, or limits. A lot of data can be used for thematic analysis to find themes.

8.4.3 Meta-Model Framework Development

8.4.3.1 Design Principles and Components

Medical study blockchains must be safe, open, and able to connect to other systems in order to work. The system has a layer for smart contracts, a layer for managing data on the blockchain, and a layer for managing user IDs and access. These frame parts are shown in Figure 8.1.

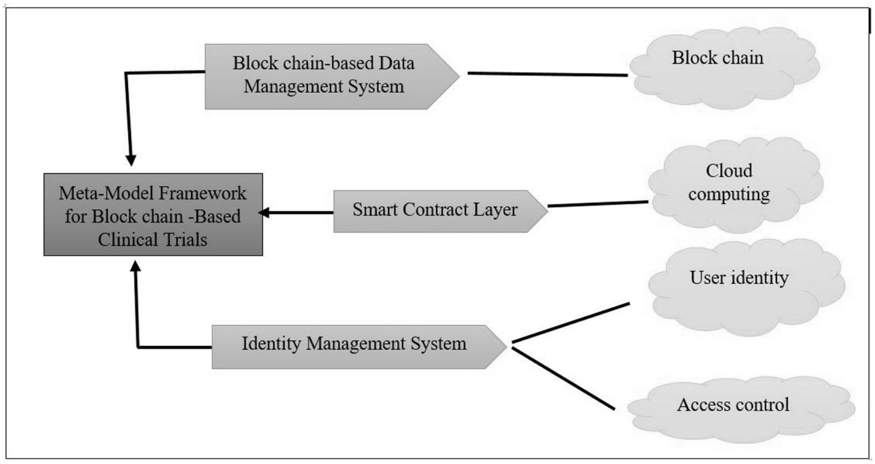


FIGURE 8.1 A proposed framework for a meta-model for blockchain clinical trials

Blockchain-based data management keeps scientific study data centralized and can't be changed. To make running a clinical study easier, the smart contract layer finds patients, gets written permission from them, collects data, and reads it. People who aren't supposed to be there can't take part in clinical studies because of a system that controls names and access to data.

8.4.3.2 Technical Specifications and Requirements

We need a structure for the meta-model that is open and flexible, and works with tools that control data for clinical studies. A permissioned blockchain, such as Hyperledger Fabric or Corda, is needed to hide the plan and help it grow. The Clinical Data Interchange Guidelines Consortium has rules and data forms that clinical study data management tools (CDISC) need to be able to use.

We should use GDPR and HIPAA to protect clinical study data in the system. Figure 8.2 shows that system checks and tracking should stop people from accessing and changing data without permission. Using blockchain technology in the meta-model structure makes clinical study data safer, more open, and more efficient. The system handles clinical study data, makes it automated, and keeps it safe.

8.5 ALGORITHM DEVELOPMENT

8.5.1 Design and Implementation

A tool called the meta-model framework for blockchain-based clinical trials keeps data safe and secure in a clear and open way. It also keeps track of the steps needed to study and decides who can get to it. Smart contracts on the blockchain keep the rules for clinical studies up to date and make the method work. The program is in charge of finding people to take part in clinical studies, getting their signed permission,

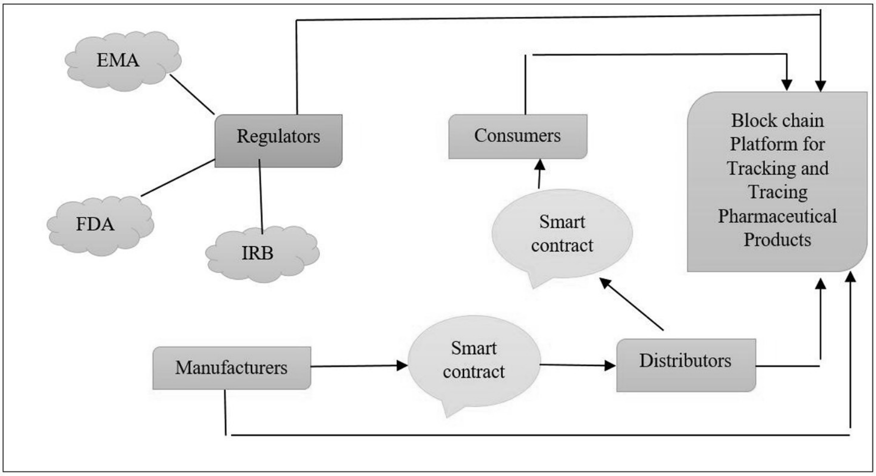


FIGURE 8.2 How blockchain technology can be used to track and trace medicinal goods

gathering data, and analyzing it. To use the method, we made a solidity smart contract on Ethereum.

8.5.2 Proposed Algorithms

A lot of people have thought about this for the meta-model framework for blockchain-based clinical trials:

Inputs:

- Facts about patients (P)
- Consent form to fill out to say "I agree"
- A plan for a clinical study
- The tools for gathering data
- Methods for analyzing data (DAM)
- Levels of access and rights for users (UAP)

Outputs:

- Clinical study data that is safe and easy to understand (D)
- Clinical study methods that are automated (ACP)
- Control of user access (UAC)

Algorithm Steps:

```
1. Write down what people need to do to be a part of the
   clinical study: Let us write CTP as [CTP1, CTP2,…, CTPn].
2. Make sure the information about the patient meets the needs
   of the job: P' = {P | P ∈ CTP}
3. Fill out this form to get permission from people who can
   give it: ICF = [ICF1, ICF2,…, ICFn]
4. Make sure that the study is only seen by people who agreed
   to take part in it: P' = {P | P ∈ ICF}
5. Make a list of the steps that need to be taken and the
   tools that can be used to help: Its value is {DCT1,
   DCT2,…, DCTn}.
6. If you want to get information from skilled people, use the
   following tools: D = {DCT(P) | P ∈ ICF}
7. Use smart contracts to keep the info on the blockchain
   safe: D' = {DCT(P) | P ∈ ICF} + UAC
8. Talk about how to handle information and what needs to be
   done to use it: DAM = {DAM1, DAM2,…, DAMn}
9. Use the following methods and steps for data analysis to
   look at the data you've collected: A = \DAM(D)}
10. Smart contracts can help you with the steps of the study
    project: ACP = {CTP, ICF, DCT, DAM, UAP}
```

```
11. With smart contracts, you can tell each person what kinds
    of access and rights they have: UAC = {UAP}
12. Make sure that the data you used for statistical analysis
    is right and accurate by checking it: S = {STAT(D)}
```

To use the blockchain-based clinical study method, follow the steps shown in Figure 8.3. Before patients are added to the project, their data is compared to the criteria for recruitment, and they give their full consent. On the blockchain, tools gather data and smart contracts keep it safe. Protocols look at data and smart contracts control who can see what. The clinical study automation system uses statistics to make sure that the data is correct and reliable. The plan stresses the importance of keeping clinical study data safe, being open, and being honest.

- “P” stands for “Patient data,” which includes the person’s name, address, date of birth, gender, and medical history.
- “CTP” stands for “clinical trial protocol,” and tells us who can and can’t take part in the study and how it will be set up.
- “DCT” stands for “data collection tools,” are things such as polls, brain scans, and even medical tests.
- “DAM” stands for “data analysis methods” and includes things such as data visualization, machine learning, and statistical analysis.

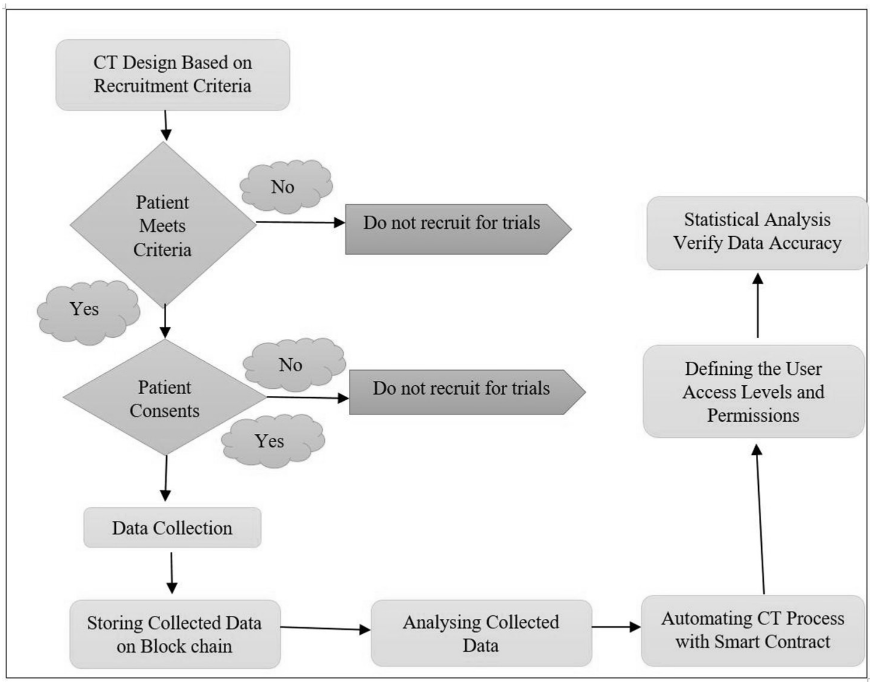


FIGURE 8.3 Step-by-step implementation of the blockchain-based clinical trial algorithm

- "UAPs" stands for "user access levels and permissions," they include jobs such as executive, researcher, investor, and patient.
- "D" stands for "Collected data," such as the patient's name, date of birth, gender, medical history, test results, physician's notes, and pictures.
- The words "secure and transparent clinical trial data" refer to both the data and the way that people can see it.
- "A" stands for "Analysed data," with math and statistics being the major areas.
- "ACP" stands for "automated clinical trial processes," uses smart contracts to find people, get their permission, gather data, and examine it.
- Person access control (UAC): Smart contracts set the levels of access and rights for each person.
- "S" stands for "statistical analysis results," which includes p-values, mean, and standard deviation.
- For the program, we used all kinds of signs and notations.

This program sets the rules and guidelines for each part of a research study. The system also makes sure that patient data is correct, keeps information safe on the blockchain, and processes data in a certain way. Smart contracts decide who can see what, and scientific analysis makes sure the info is right.

8.6 RESULTS AND DISCUSSION

The above results use blockchain and cryptography technology to protect the privacy, security, and accuracy of healthcare data. A lot of the time, these studies try to solve privacy and security issues that have been around for a long time in the field. The results show that these technologies can share medical data and restrict who can see it in a safe and effective way that protects both patients' and doctors' privacy. The recommended methods have reasonable prices for both transmission and processing, and they meet the expected security requirements.

Blockchain and collaborative learning are used in the study to create a new way for medical picture data to be shared across an open network. Health data can be stored off-chain using an interplanetary file system-based infrastructure. This protects both the safety of the healthcare system and the privacy of the information about the patients who use it. They learned that adding information to the blockchain mostly changes how long the program needs to run and how much work it needs to do. This makes sense because the design and encryption protect your privacy and safety.

Several studies came up with methods that let the patient choose whether to let the person in or not. These changes make it easy for healthcare workers and groups to follow privacy rules. There are also safe ways to pay for the answers, so people and doctors can be sure they can pay for storage and testing services.

The suggested ways can defend against many types of attacks, including cloning, collusion, and man-in-the-middle attacks, according to a security study and a lot of testing. The results also show that the suggested methods work to keep data safe, protect against threats, and make sure that storage space is shared evenly. Health privacy information can be sent and stored in more ways than ever before, both inside and outside of healthcare.

A lot of people have worked on ways to keep information on the Internet of Medical Things (IoMT) safe and open to everyone. Some of these are improved attribute-based encryption primitives and individual smart contracts. Because IoT devices don't have a lot of room, some studies have changed how sensor nodes work so that they make better use of it. The study's results show that this method is a safe and effective way to make it easier for people to share IoT medical data while still protecting patient privacy.

A lot of research has shown that blockchain and security technologies can help us share and manage health information in a safe, private, and effective way. IoMT users should use the suggested methods because they meet the expected security needs and are affordable in terms of how much they cost to carry out and send. These results show that these technologies might be able to solve long-standing privacy and security problems in the healthcare field. The papers' effects on privacy and safety in healthcare are shown in Figure 8.4.

Question 1: What uses does blockchain technology have in the healthcare field for security and privacy?

In the healthcare field, it's very important to keep patient information safe and secret. Electronic health records (EHRs) need to be trusted to keep private health information safe for people. This protects the patients' rights and stops people from

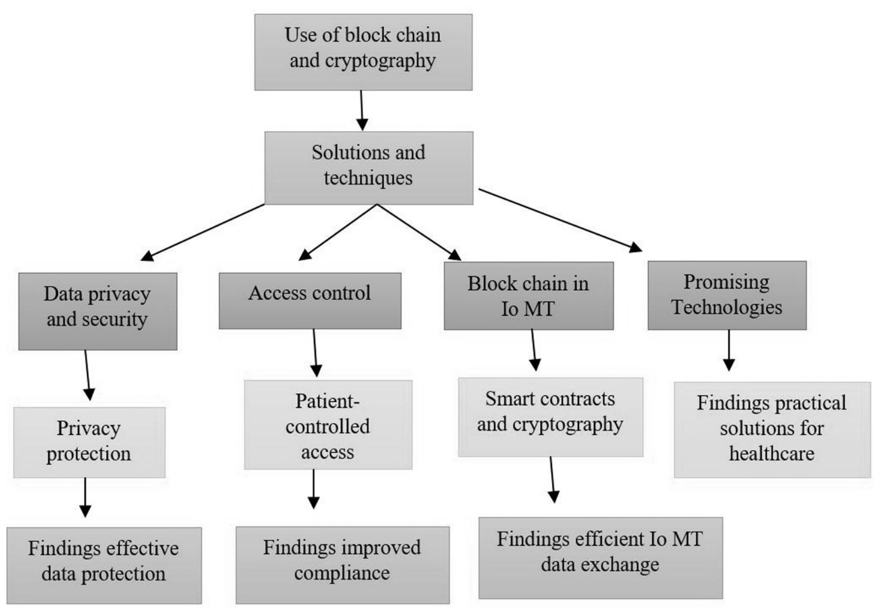


FIGURE 8.4 Healthcare privacy and security using blockchain and cryptography

stealing their information. e-health data could be kept safe and secret with the blockchain. Blockchain-based EHR systems might offer a safe and unbreakable way to share and store health data (Table 8.1). The blockchain's self-sufficient structure can stop data spills and keep data safe. With smart contracts and coin payments, you can make sure that only authorized users can see your data. Access control based on blockchain may also make data more private because users can control who can see their data and at what time. This way, only people who are allowed to can see it. It's not clear from either one how to use smart contracts.

To share and handle personal health records (PHRs), you also need strong privacy and security steps. A PHR keeps private health information about a person, such as medical data, test results, and illnesses. When you use blockchain to share data (Table 8.2), you can make sure that only approved people can see the information and protect the privacy of your patients. EHRs, or electronic health records, can also help protect privacy when they are shared. K-nearest neighbors (KNN) training for IoT data that protects privacy can also help keep hospital data safe. Healthcare blockchain privacy could make it possible to store and send medical data in a way that can't be hacked. Health data on the blockchain can be made even safer and more private by adding rights and identification. The info can only be seen by people who are allowed to.

What are the problems with healthcare blockchain when it comes to privacy and safety?

TABLE 8.1
Applications for Health Records

Use Case	Smart Contract	Reference
EHRs		[9]
How to handle and share personal health records (PHR)		[12]
Management of EHRs		[13]
Blockchain system for EHRs		[14]
Blockchain for EHR privacy		[15]

TABLE 8.2
Manage Data

Use Case	Smart Contract	Reference
Health sharing of IoT data		[1]
Safe sharing of data		[2]
Shared		[3]
Shared medical info		[4]
Blockchain helps people share data		[5]

TABLE 8.3
Authentication

Use Case	Smart Contract	Reference
Proof of identity		[6]
PPBA security check		[7]
Authentication by machine learning		[8]
Verification of identity		[10]
Making sure that healthcare data on the blockchain is real and authorized		[11]

Healthcare has a lot of problems with safety and privacy. Security and privacy are very important in healthcare because it is a very private field. If medical data is misused or leaked, it could hurt people or businesses. Blockchain technology is the answer because it gives everyone a safe way to store and share info. The building blocks of cryptography let you look without risk and control what people can see. Smart contracts protect data and only let certain people see it. Several suggested methods have been studied and tried in simulations and real-world tests, showing that they are safe, effective, and able to work. Blockchain-based systems may be able to keep their computing and link prices low while still being safe, according to a number of studies as summarized in Table 8.3. Other methods, such as adapted attribute-based secured primitives and certificate-less public-key encryption technology, have also worked well in healthcare to keep information private and give people control over their own access. Healthcare workers and groups should make sure that these options follow privacy rules and can be used in the real world.

What are the pros and cons of using Bitcoin in the medical field to protect privacy and safety?

Over the next few years, making healthcare safer and more private is likely to stay a top goal. Blockchain technology is being used more and more to protect health data. A smart medical cloud tool keeps users' data safe by only letting them use data and not borrow it. New technologies such as blockchain, shared learning, and edge computing can be used to hide and protect data. Federated learning could let people work together to look at data without sharing private information. Blockchain technology could be used to make sure that only people who are allowed to can see and change data. Plus, working with data close to where it starts instead of moving it to a central place might make it less likely that it will be stolen. More strict rules and guidelines should be put in place to protect private health information as another option. As the amount of data grows, it becomes more important to keep health information safe from people who shouldn't have access to it or from being stolen. Both HIPAA and GDPR are regulations that protect the protection and safety of important health data. In the future, things that happen could lead to the creation and enforcement of more laws and rules that protect health information.

8.7 RESEARCH DIRECTIONS AND APPLICATIONS

Blockchain technology has a lot of interesting study possibilities and useful uses, even though its use in healthcare isn't always clear. Dealing with problems related to scale and connection is the most important part. A lot of work needs to be put into making new technologies that will allow blockchain networks to handle the huge amount of healthcare data and help networks connect to each other well. This will make more people want to use these networks.

It's clear that there are a lot of interesting places to study and use in the future. For healthcare blockchain networks to handle data well and connect to each other easily, growth and access should be their top goals. If you want to help people in other countries, blockchain is a great way to send health information across borders because it is safe. The medical supply line can also be changed by blockchain. This is to make sure that the drugs are real and that the patients are safe. Putting AI and blockchain together might also make it possible to handle data quickly while still keeping it private. Blockchain might offer a safe way for people to decide who can see their information and make money from it. It's important to give patients power over their information and permission before using it. Healthcare companies might be more likely to follow the law if they use blockchain technology to keep patient info safe. IoT medical tools could be better with blockchain technology, which would protect the privacy of the patient data that these devices receive. EHRs and telemedicine systems that are built on blockchain might give users better experiences and make it easier for them to connect to the current healthcare infrastructure. It talks about some important areas of study and how blockchain technology might change the business of healthcare.

8.8 CONCLUSIONS

Some long-standing problems in the healthcare field can be fixed with blockchain technology. A lot of people think that blockchain is a cool new way to store medical records, keep track of medical activities, and make it easier to share and add medical records to a free, open healthcare network. Even though blockchain is getting a lot of attention in the healthcare field, people are still worried about their safety and privacy when they share information with it. From 2017 to 2022, researchers looked into how safe and secure blockchain is in healthcare. The piece talks about those studies. The goal of the study review is to look at how things are now, with a focus on real-world issues and problems.

The review comes to the conclusion that blockchain technology can help hospitals with privacy and security problems. When you use blockchain technology to store and send private patient data, it creates a decentralized, hack-proof platform that makes EHRs and PHRs safer and more private. Blockchain can also give people more control over who can see their data by letting them control who can identify them. However, healthcare organizations and practitioners need to think carefully about whether blockchain solutions will work for them to make sure they don't break privacy rules and are useful. Blockchain tech has a lot of potential, but it's not the best way to solve all problems. It might need to be changed to meet certain needs.

Overall, the review gives useful information about how blockchain is currently used in healthcare and points out areas that need more study and development to make the technology more useful in this field.

REFERENCES

1. Clinical Trial Data definition. *Law Insider.* Available at: https://www.lawinsider.com/dictionary/clinical-trial-data
2. Kochhar S, Knoppers B, Gamble C, Chant A, Koplan J, and Humphreys GS. Clinical trial data sharing: here's the challenge. *BMJ Open* 2019 Aug 21;9(8):e032334.
3. Naudet F, Siebert M, Pellen C, Gaba J, Axfors C, Cristea I, et al. Medical journal requirements for clinical trial data sharing: ripe for improvement. *PLoS Med* 2021 Oct;18(10):e1003844. doi: 10.1371/journal.pmed.1003844.
4. Ohmann C, Banzi R, Canham S, Battaglia S, Matei M, Ariyo C, et al. Sharing and reuse of individual participant data from clinical trials: principles and recommendations. *BMJ Open* 2017 Dec 14;7(12):e018647. doi: 10.1136/bmjopen-2017-018647.
5. Fegan G, and Cheah P, Data Sharing Working Group. Electronic address: WorkingGroups@covid19crc.org. Solutions to COVID-19 data sharing. *Lancet Digit Health* 2021 Jan;3(1):e6. doi: 10.1016/S2589-7500(20)30273-9.
6. Harrison PW, Lopez R, Rahman N, Allen SG, Aslam R, Buso N, et al. The COVID-19 Data Portal: accelerating SARS-CoV-2 and COVID-19 research through rapid open access data sharing. *Nucleic Acids Res* 2021 Jul 02;49(W1):W619–W623. doi: 10.1093/nar/gkab417.
7. Li R, von Isenburg M, Levenstein M, Neumann S, Wood J, and Sim I. COVID-19 trials: declarations of data sharing intentions at trial registration and at publication. *Trials* 2021 Feb 18;22(1):153. doi: 10.1186/s13063-021-05104-z.
8. Call for a global health data sharing framework for global health emergencies. The InterAcademy Partnership (IAP) Science Health Policy. 2022. Available at: https://www.interacademies.org/publication/call-global-health-data-sharing-framework-global-health-emergencies (accessed 15 March 2022)
9. Network data sharing policy. NIH StrokeNet. Available at: https://www.nihstrokenet.org/docs/default-source/default-document-library/adm04-strokenet-network-data-sharing-15-sep-2016f84cedd0c2c66f0f86baff000016a715.pdf?sfvrsn=0 (accessed 5 January 2022).
10. Taichman DB, Backus J, Baethge C, Bauchner H, de Leeuw PW, Drazen J, et al. Sharing clinical trial data—a proposal from the international committee of medical journal editors. *N Engl J Med* 2016 Jan 28;374(4):384–386. doi: 10.1056/nejme1515172.
11. Data Sharing Policy. Barts and the London School of Medicine and Dentistry. Pragmatic Clinical Trials Unit. Available at: https://tinyurl.com/4e79w3j4 (accessed 5 January 2022).
12. Bull S, Cheah PY, Denny S, Jao I, Marsh V, Merson L, et al. Best practices for ethical sharing of individual-level health research data from low- and middle-income settings. *J Empir Res Hum Res Ethics* 2015 Jul;10(3):302–313. doi: 10.1177/1556264615594606.
13. Baber N. International conference on harmonisation of technical requirements for registration of pharmaceuticals for human use (ICH). *Br J Clin Pharmacol* 1994 May;37(5):401–404. doi: 10.1111/j.1365-2125.1994.tb05705.x.

14. Data sharing for grants—final research data SOP. National Institute of Allergy and Infectious Diseases. Available at: https://www. niaid.nih.gov/research/grants-data-sharing-final-research
15. Pisani E, Aaby P, Breugelmans JG, Carr D, Groves T, Helinski M, et al. Beyond open data: realising the health benefits of sharing data. *BMJ* 2016 Oct 10;355.
16. Data management and sharing policy. National Institute of Health Scientific Data Sharing. Available at: https://grants.nih.gov/ grants/policy/data_sharing/data_sharing_guidance.htm
17. Blasimme A, Fadda M, Schneider M, and Vayena E. Data sharing for precision medicine: policy lessons and future directions. *Health Aff (Millwood)* 2018 May;37(5):702–709. doi: 10.1377/hlthaff.2017.1558.
18. Tenopir C, Allard S, Douglass K, Aydinoglu AU, Wu L, Read E, et al. Data sharing by scientists: practices and perceptions. *PLoS One* 2011;6(6):e21101.
19. Glickman SW, McHutchison JG, Peterson ED, Cairns CB, Harrington RA, Califf RM, et al. Ethical and scientific implications of the globalization of clinical research. *N Engl J Med* 2009 Feb 19;360(8):816–823.
20. Data exclusivity and other "trips-plus" measures. World Health Organization, Office for South-East Asia. 2017. Available at: https://apps.who.int/iris/bitstream/handle/10665/272979/Data-exclusivity.pdf?sequence=1&isAllowed=y
21. Trips agreement- article 66 (practice). World Trade Organization Analytical Index. URL: https://www.wto.org/english/ res_e/publications_e/ai17_e/trips_art66_oth.
22. COVID-19 IP Policy Tracker. World Intellectual Property Organization (WIPO). Available at: https://www.wipo.int/covid19-policy-tracker/#/covid19-policy-tracker/ipo-operations
23. Extension of the Transition Period under Article 66.1 of the TRIPS Agreement for Least-Developed Country Members for Certain Obligations with Respect to Pharmaceutical Products. Council for TRIPS. Available at: https://www.wto.org/english/ tratop_e/trips_e/art66_1_e.htm
24. Attaran A, Barry D, Basheer S, Bate R, Benton D, Chauvin J, et al. How to achieve international action on falsified and substandard medicines. *BMJ* 2012 Nov 13;345:e7381.
25. British Medical Journal moves to flush out secret trial data. Reuters. 2012 Oct 21. Available at: https://www.reuters.com/article/ pharmaceuticals-disclosure-bmj-idUSL5E8LV59720121031

9 Role of Artificial Intelligence in Healthcare 5.0

Shivangi Verma and Anupam Singh

9.1 INTRODUCTION

In order to enhance sustainability, resilience, also human-centred claim within the production surroundings, Industry 5.0 introduces a combination of technologies. Healthcare 5.0 incorporates cutting-edge technology including artificial intelligence (AI), the Internet of Medical Things (IoMT), huge data, drone, and robotics, much like Industry 5.0 Nanotechnology, cloud/edge computing, 6G, and digital twins (DTs). These revolutionary technologies deliver a number of remarkable advantages to society that prioritises sustainability, wellness tracking, individualised medical care, and the well-being of people. Healthcare 5.0 corresponds to the next evolutionary stage in healthcare transfer, driven by modification technologies that promise to reorganise patient care, operational efficiency, and health outcomes. It combines advanced digital technologies such as artificial intelligence, blockchain, and digital twins in healthcare [1]. This paradigm shifts from previous Healthcare 1.0 to Healthcare 5.0 and accurate medicine to analyse large amounts of data for predictive diagnostic and artificial intelligence treatment plans. In Table 9.1 we can describe the challenges and need for advanced technology in Healthcare 5.0. Healthcare 5.0 fosters a cooperative ecosystem where a digital twin creates a copy of patients, organs, or even an entire healthcare system facilitating real-time monitoring, simulation of medical scenarios, and predictive analysis.

Integration between AI, machine learning (ML), and deep learning (DL) in Healthcare 5.0 corresponds to a theory shift towards more efficient, modified, and secure healthcare services. AI helps to develop medical diagnostics, treatment plans, and patient care through advanced data analytics and ML algorithms. The blockchain receives the algorithm from artificial intelligence and ensures secure, transparent, and decentralised management of health records to exchange data receivers, DTs receive data from smart contracts and represent the virtual model of physical entities, facilitating real-time monitoring, and reproducing the patients' records. We can use this technology to reshape healthcare delivery, create new opportunities for precision medicine, and improve patient outcomes.

DOI: 10.1201/9781003532286-9

TABLE 9.1
Some Key Characteristics and Challenges of Public Healthcare 5.0

Characteristic	Challenge	Description
Empirical insight	Data privacy along with security	It can analyse large datasets for tendency and supervisory and predicts results on the basis of records. The challenge for Healthcare 5.0 is to provide security to health data from unauthorised persons.
Interconnectivity	Integration and interoperability	It can provide the facilities to collect information and share real-time information, such as telemedicine and remote care.
Advanced technologies	Regulatory compliance	Healthcare 5.0 is used in diagnostics, predicting outcomes, and optimising treatments, such as **b**iotechnology, genomics**,** robotics, and automation**.**
Ethics and privacy	Ethical concern	It can provide security for health data and deal with ethical issues correlated to artificial intelligence and other technologies, such as biases in algorithms and simplicity in decision-making.
Patient empowerment	Digital literacy	It provides the knowledge and tools for informed decision-making and applications for managing health conditions. It focuses on challenges such as educating and training healthcare staff.

AI is a network of computer algorithms that enables systems to automatically learn and develop knowledge over time. ML and DL are subcategories of AI. AI that uses advanced algorithms and analytical models will allow the network to improve its execution of a task. Currently, ML is used in numerous applications such as natural language processing (NLP), computer visualization, robotics, as well as business. These technologies can assist medical professionals in disease diagnosis, therapy development, and patient care. Numerous factors can affect how AI affects emergency healthcare, one of which is its ability to help medical professionals diagnose and care for patients quicker and with more accuracy. AI systems can examine medical imaging data, such as MRIs and CT scans, to identify irregularities that are hard for humans to perceive. In order to identify patterns and suggest therapy, it may also be used to evaluate patient data and medical reports. As the word "emergency" suggests, at the appointed time decision-making is essential in emergency healthcare. Artificial intelligence has the potential to help medical practitioners quickly make a well-informed decision. Different types of algorithms are used in AI to make decisions automatically without other parties [1, 2]. There is a revolution going on in the healthcare sector. Growing shortages of medical specialists and rising overall healthcare costs are the root reasons for this transformation. Due to this, the healthcare field is seeking to use new information system-based processes and solutions in place which may bring down the cost and address these growing issues. Figure 9.1

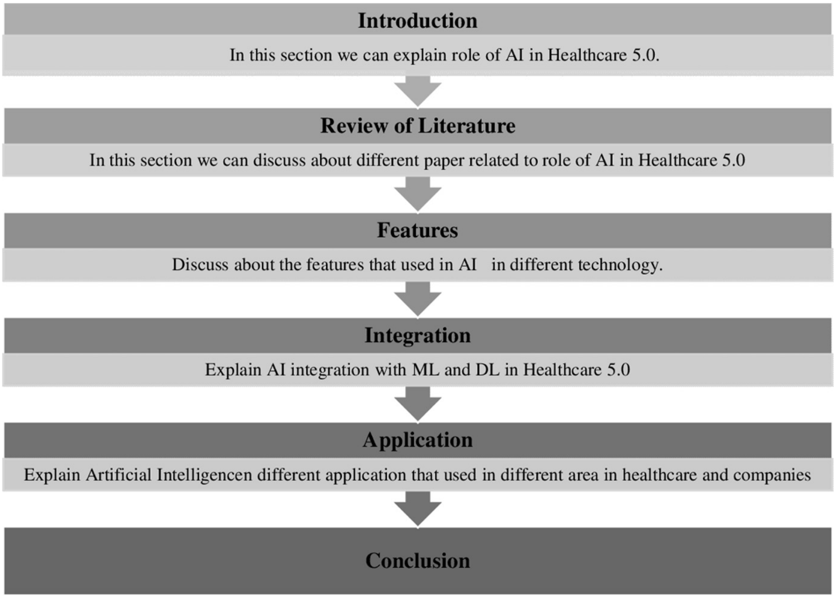


FIGURE 9.1 Chapter layout

gives the chapter layout including the introduction, the evolution of healthcare from 1.0 to 5.0, a literature review, challenges, and issues of AI in Healthcare 5.0.

9.2 EVOLUTION OF HEALTHCARE

This section discusses Healthcare 5.0 and its developing technologies in smart healthcare systems from a broad methodical viewpoint. The healthcare sector has suffered a paradigm change, shifting from being hospital-focused to patient-focused. To support changes new technologies are being used in healthcare. There are a lot of technologies being used in healthcare such as AI, blockchain, digital twins, nanotechnology, cloud/edge computing, and 6G. Based on our assessment tool, we aim to evaluate the level of implementation in Healthcare 5.0 and their initiatives in Table 9.2. In Healthcare 1.0, patient data was recorded manually in face-to-face interactions between patients and doctors. Thus, the data was stored in hard files and retained by the doctors also becoming subject to wear and tear. With the beginning of digitization, the hard file became digital in Healthcare 2.0, which is named electronic health records (EHRs), EHRs changed to support the interoperability of patient data by being updated by doctors, hospitals, and clinics. So, the drawback of the Healthcare 2.0 ecosystem was that the records were still retained on centralized hospital servers. This meant more security and privacy were required, this limitation was removed by Healthcare 3.0. In Healthcare 3.0 only authorized persons can view and access the data, no other person can update data. Here clinical datasets are to be used for treatment. The limitation of Healthcare 3.0 is that it does not

TABLE 9.2
Evolution of Healthcare Stages

Year	Healthcare Stage	Dataset	Technology	Advantages
2015	Healthcare 1.0	Manual	Manual	Improved health record-keeping
2016–2017	Healthcare 2.0	Telehealth records, patient survey, EHR	Telemedicine platforms, EHR	Increased patient engagement
2018–2019	Healthcare 3.0	Genomic dataset, clinical database	ML, predictive modelling tools	Tailored treatment
2020–2021	Healthcare 4.0	IoT device data, remote patient monitoring	IoT and wearable technology, AI algorithms	Real-time monitoring, enhanced chronic case management
2022–present	Healthcare 5.0	Multi-source health data, social data	NLP, autonomous diagnostic system	Holistic care application, improved health equity

support large amounts of data. AI and big-data analytics have been introduced in Healthcare 4.0 to improve decision models on stored EHRs Medical stakeholders experienced difficulties with interoperability as a result of the convergence, and as data volumes increased, AI models grew more complicated and became ineffective, which decreased the responsiveness of the applications [2].

9.3 NEED FOR AI IN HEALTHCARE 5.0

Today, AI is used in different types of fields and industries to develop and improve with a wide range of applications. There are many significant aspects which establish the need for AI [3].

9.3.1 Personalized Medicine

Prognostic analysis and personal fitness cannot provide individual result treatment, according to personalized medicine, which will enable the collection of data for creative machine learning–based medical care improvements.

9.3.2 Integrated Health Records (IHR)

IHR management involves a labour-intensive and complex process. ML plays a critical role in streamlining procedures within the medical sector with AI used to save time, effort, and resources.

9.3.3 Identification and Diagnosis of Disease

ML has appeared as a powerful tool for the identification and analysis of diseases, particularly those that are difficult to study using traditional methods. Some important implementations of ML in the healthcare sector include the identification and prognosis of diseases and circumstances, including early-stage cancer detection and inherited illness scopes.

9.3.4 Engineering and Medical Innovation

Robotics is increasingly used in scientific research and medical development programs, incorporating advanced analysis and learning capabilities such as next-generation classification and precision medicine to help identify treatment options for complex diseases.

It helps in healthcare and medicine, in which ML helps to analyse the medical image and predict outputs.

9.4 LITERATURE REVIEW

Jaswinder Singh [1] states that machine learning has become an essential part of different industries, including healthcare, due to its aptitude to automate tasks and provide valuable large datasets. In healthcare, ML works to address challenges such as manual data processing and disease diagnosis. In this paper, the author used the EHR provided as a precious source of data in healthcare. It can identify samples and development that may not be clear to human physicians. It can easily detect diseases and improve patient reports. Manning et al. [4] talk about the use of EHR in supervised and unsupervised learning to analyse healthcare data for precise prognostic clinical tasks, highlighting the effectiveness of these approaches in improving medical task performance. Miotto et al. [5] state that we know that DL is a subset of AI, it's inspired by the human brain and it organises the data in complex forms such as pictures, videos, text, etc., and produces accurate output. DL plays an important role in many fields related to healthcare such as medical image investigation (e.g., X-rays, CT scans), evaluating EHRs, genomics, and wearable device data.

Liu et al. [6] employed a CNN model in their healthcare review and used an EHR to assess cardiac infarction and pulmonary complications. They also used the previous history of a patient by using a long short-term memory recurrent neural network (LSTM RNN) used in a dynamic model to predict the output based on the medical history of patients. Lasko et al. [7] proposed medical information with a deep learning framework using longitudinal possibility consistency which applies a Gaussian development failure. This approach measures the serum uric acid in 4368 persons. The result was constant phenotypic characterised suggesting numerous people subdivision along with extract differentiating between gout and severe blood cancer accompanied by AUC of 0.97. AI and ML have an extensive impact on medicine. Since 1970, rule-based methods have been popular in medical research but they are popular due to their exact justification and continuous updates. Today, new

AI-supported replicas use ML procedures to make data blueprints from multifarious sources such as disease identification, classification, risk ranking, and treatment selection. Research has used a range of machine learning algorithms including naïve Bayes, ANN, SVM, and other hybrid methods. Miotto et al. [8] introduced a DL framework and its importance over traditional methods. They examined applications in healthcare such as EHRs, medical images, genomics, and mobile applications Alafif et al. [9] talk about ML applications in COVID-19 to identify the disease and cure it. They classify ML support methods into symptomatic methods such as radiology investigation or treatment-based methods such as drug and vaccine development. Olsen et al. [10] survey machine learning algorithms and their applications in heart failure, separating them into ML and DL groups. They also talk about their application in diagnosis, classification, and prediction, and highlight challenges and problems in ML. The authors describe an ML application in healthcare and also check detection, diagnosis, and treatment. They also discuss various algorithms and their applications in disease identification, drug manufacture, robot-assisted surgery, and medical data analysis.

Big Data: Big data provides large amounts of data from EHRs, wearable devices, and medical imaging, contributing to an all-inclusive viewpoint of patient health. It performs a big role in initialing medicine, leveraging sophisticated AI applications to develop treatments, and developing technologies for Healthcare 5.0 [11]. Big data has made it possible for healthcare systems to become more effective, efficient, and patient-focused methodologies.

Blockchain: Blockchain is an immutable shared, unchangeable ledger that makes it easier to track assets. The asset can be physical such as buildings, vehicles, cash, land, or abstract such as copyright, intellectual property, patents, and record transactions in a corporate network. It is used to deliver information, which is mutable, distributable, and visible facts and figures which are retained on an unchangeable ledger accessible only to permit able systems and users. Payments, orders, production, and accounts may all be tracked by a blockchain network. An authorized person can access information from beginning to end, which is the confidence and release of new possibilities and efficiency [12, 13]. Marketers can keep the pathway of medical product procedures with the support of blockchain technology. This mechanism has a tendency to be used by the healthcare sector and medicine industries to eliminate ineffective medical drugs and enable improvements in medical care. The security of data can possibly be guaranteed by blockchain technology. Additionally, historical medical records can be stored on blockchain and cannot be changed. Every part of common hardware in the hospital is connected to this decentralised network. Researchers may use the property; these devices save to calculate estimates for treatments, medications, and therapy for a variety of diseases and conditions [14, 15]. The distributed ledger network allows for the accumulation of data without requiring undivided consent to be deleted or modified. Every data block value is accompanied by a compression function that attaches its recently introduced cluster transcript to a blockchain hashing function. Due to the distributed blockchain ledger design, data is able to be seen and dependable to all network users and is not gripped in a centralised location. Table 9.4 explains some features of blockchain related to healthcare. This decentralised structure develops and defends itself against a single attack. It assists increase control over health data and patient care while saving time and money for patients and practitioners by doubling medical practice and supervision [16–18].

Digital Twin: Virtual model reproduction of the entities of interest is a sensible and affordable method of exploring the suggestion of various design options and judgment in the study of complex dynamical systems. To assist in overall decision-making, virtual models, also known as digital twins, are virtual representations of substance that span their lifecycles of creation and progression. Before spending money on tangible prototypes and assets, industrial manufacturers employ digital twins to replicate, anticipate, and upgrade production and scheme over the course of the innovation circuiting. A DT is a complex model that is intended to accurately replicate the physical configuration in actual time, estimate its behaviour, and offer a computerized copy or mock-up pattern of a real network [19]. In order to test a space capsule and allow troubleshooting of concerns in development, the NASA space program originally embraced the DT idea in the 1960s. When the spacecraft failed during the Apollo 13 mission, the NASA crew had to reconstruct the circumstances on board in order to safely return the spacecraft and men to Earth. This idea was successfully implemented on the mission. In 2005, the term "digital twin" (DT) was created by Michael in the context of product lifecycle management. Three elements are used to make a DT according to the author: a connection (provided connection between user and receiver), where the virtual system is mapped (it established a virtual mapping between users), and a physical component [12]. The healthcare industry is quickly changing due to the preface of technological innovations such as virtual replicas. These virtual copies are vital for agreement improved patient care and medical association procedures in the medical field. The market value of digital twins in the healthcare industry is projected to reach US$1.6 billion by 2023. Industry insiders forecast substantial expansion in 2028 when the market is projected to reach a valuation of more than US$21.1 billion [20].

9.5 SOME APPROACHES OF AI IN HEALTHCARE 5.0

ML is nonlinear, traditional DL can produce ML for language achievement quickly and effectively while ensuring reliable patient data. Frequent formats can be used to illustrate patient data or information, including text and visuals [21]. This has been a significant problem since real-time outcomes are necessary for a network of physical device operations in the medical field and other industries [22, 23]. Deep learning and machine learning, which can distinguish between normal and irregular patient data, are two tools that medical experts can use to diagnose patients' infections. Dense network learning, a category of computational intelligence developed for picture resolution, such as sonography, Mr-imaging, CAT scanning, and X-radiation, which forms the foundation of DL models. We can see the study analysis of ML/DL with healthcare in Table 9.3. For hospitals to carry on providing high-quality care and efficient use of resources, calculating patients' lengths of stay (LOS) is a critical factor that machine learning–based calculation techniques may help with. This makes it challenging to build effective logical analytics that needs a huge volume of

TABLE 9.3
Study Analysing the Relationship between ML–DL and Healthcare Focusing on Challenges and Issues

Author	Idea	Approaches	Open Issues and Challenges
Kundu et al.	Monkey fox detection Using vision transformer	ML-based approaches	Insufficient dataset
Rahman et al.	Patient length of stay prediction, proper treatment plans	Linear regression model	Only use a linear model in future Work on other model
Solanki et al.	Develop chatbot healthcare	ML-based approaches	Gain trust from users
Chen et al.	Using DL for the discovery of ovarian cancer	CNN	Collect actual time statistics information is a big job intended for users
Siar M et al.	Through DL to detect brain tumour	CNN will classify SoftMax	Collect healthcare data set and also provide security mechanism
Awotunde J et al.	Breast tumour recognition	CNN with consistent support Feature collection	Collect large amounts of patient data
Ozdi et al.	Fatty hepatosis detection	CNN with consistent support Feature collection	Real image needed
Esteva et.al.	Detect tumours	CNN with pattern reorganisations	Clinical data needed

a dataset that used to produce a model. So a collective predictive model in the server for forecast customers extent to wait for combining the conclusion from nearby train replicas of different distribute and pluriform customers. A predictive model that is based on the cloud and involves decentralised hospital clients while their privacy could be a game-changer for the 13 real-world healthcare sectors [24]. In order to provide patients with efficient and effective care, the healthcare business must overcome several obstacles, such as rising patient demand, conned funding, and a growing scarcity of healthcare professionals. Many healthcare industries are using ML and AI to address issues and improve patient outcomes. The creation of intelligent chatbots has become a workable approach in the medical industry. The most important principle of the chatbot treatment given to the patients is a more practical and easy mode to get healthcare services and information [25]. ML can be expanded by developing and validating a DL-based system to identify ovarian growths using contrast-enhanced CT scans. The DL-based device detected malignant cells on body scans, where the tumour size is small with similar sensitivity to radiologist interpretation. In the future, researchers aim to improve deep learning algorithms to enhance the detection of ovarian tumours on CT scans, particularly small tumours that are often missed by conventional methods.

Siar et al. [26] used the deep neural network to detect tumours in MRI images and SoftMax to provide an accurate result compared to others. The SoftMax method improves physician diagnosis accuracy and patient treatment. The proposed method's accuracy increased to 99.12% on test data, compared to traditional CNN. So, the SoftMax method provides the accurate diagnosis and treatment of tumours, as it increases medical accuracy [27].

Awotunde et al. [28] discuss breast cancer problems identified by the DL-based hybrid feature selection methods, which improve diagnostic accuracy. Ozdil et al.'s [29] study explores the possibility of health check-up infrared thermal imaging (MITI) in involuntary recognition of non-alcoholic fatty liver disease (NAFLD). 167 MITI images were reviewed using image visualization and categorization techniques, using the CNN framework and microscopic testing methods. In some papers, the authors proposed a CNN and Cat-Boost classifiers replica used for medical management, combining pictorial and non-pictorial data, despite disputes in data collection and security in healthcare systems, and the DRNN and SML models are presented for classification and prediction of cyber attacks in the IoMT environment, with promote studies needed for real-time testing. Quadir et al. [30] used deep learning for automated spine segmentation and it also involved pre-processing, decay with sigmoid, and handling to recognize split vertebrae.

Lasko et al.'s [31] study shows that ML has become an essential part of different industries, including healthcare, due to its aptitude to automate tasks and provide valuable insights into large datasets. In healthcare, ML is addressing challenges such as manual data processing and disease diagnosis. In this paper, the authors used the provided EHR as a precious source of data in healthcare. It can identify samples and developments that may not be clear to human clinicians. It can easily detect diseases and improve patient reports. The authors proposed scientific records with deep learning structural design using longitudinal possibility density which applies a Gaussian development regression. This approach measures as per numeric values in 4368 individuals. Their review had continuous phenotypic features suggesting multiple population subtypes and precisely distinguishing between gout and sensitive leukaemia; with an AUC of 0.97. AI and ML have an extensive impact on medicine. Since 1970, rule-based methods have been popular in medical research due to their exact justification and continuous updates. Today, new AI-based models issues in ML techniques to take out data patterns from complex environments, disease identification, classification, risk ranking, and treatment selection. Research has used a range of ML- methods including naive Bayes, ANN, SVM, and hybrid methods.

Miotto et al. [32] talk about the use of EHRs in supervised and unsupervised learning to analyse healthcare data for precise prognostic clinical tasks, highlighting the effectiveness of these approaches in improving medical task performance. We know that deep learning is a subset of AI; it is stimulated by human intelligence and it organises the data in complex forms such as pictures, videos, text, etc. and produces an accurate output. Deep learning plays an important role in many fields related to healthcare such as medical image investigation (e.g., X-rays, CT scans), evaluate EHR genomics, and wearable device data. The CNN model for EHR in healthcare calculates chronic bronchitis diseases from the use of an EHR and also uses the previous history of a patient and predicts output by using LSTM RNN, used in a dynamic model to predict the output based on the medical history of a patient. The author proposed a medical information with DL design using longitudinal possibility density which applies a Gaussian process regression.

9.6 OPEN CHALLENGES AND ISSUES IN ARTIFICIAL INTELLIGENCE:

Real-time datasets are critical for ML or DL approaches in healthcare systems to deal with medical issues. Privacy trials such as federated learning and blockchain-based security measures are needed to address this issue. DL operation can be demanding on numerous layers due to heavy models making it difficult to integrate in IoT and wireless sensor networks. To overcome this problem we used lightweight DL models such as Vision Transformer. Advanced ML or DL models require real-time data, but AI techniques such as generative adversarial network (GAN) or time series GAN can generate synthetic data [33], the study explores the potential of DL and ML in automating vital aspects of medical infrastructure. These technologies can address issues such as rising global death rates and overwork, allowing hospitals to use ML and DL to improve efficiency. Virtual assistants can be cost-effective and can be adopted without significant financial investment. However, challenges exist in replacing outdated technical methodologies and enhancing the current healthcare infrastructure. Despite these challenges, DL and ML tools have the reachable to expand healthcare relief standards and effectiveness. Further research is needed to fully realize their potential. Table 9.4 illustrates the survey of ML and DL in the field of medicine.

9.7 EXAMPLE OF AI IN THE HEALTHCARE INDUSTRY TO IDENTIFY A SYNDROME

9.7.1 Medical Image Analysis

AI algorithms are developed to investigate medical imagery (such as X-rays, MRIs, and body scans) and recognize irregularities. For example, deep learning reproduction has been developed to identify early signs of tumours, such as breast cancer in mammograms or pleura cancer in chest scans.

9.7.2 Pathology

AI can help in analysing diseases by investigating tissue samples. Machine learning models can organize types of cells and identify cancerous tissues more precisely and speedily than conventional methods.

TABLE 9.4
According to the Author AI Techniques in Healthcare 5.0

S. No.	Author	Year	Technique	Involvement and Method
1.	Karim A et al.	2003	ML technique	Use of ML models in combating floods, utilizing U-Nervier with Flood GAN performance.
2.	Mukerji S et al	2003	ML technique	Study utilisesa data-driven approach to investigate the neuro-psychological characteristics of HIV-positive Individuals.
3.	Reboredo et al.	2021	ML technique	Discuss recent machine learning Techniques in pharmaceutical research
4.	Djenouri et al.	2019	ML technique	Study survey and classified machine learning purpose in smart structure to execute occupant-centric and energy-oriented
5.	Periyasamy et al.	2023	ML-Healthcare	Study uses predictive modelling techniques suchas ANOVA and correlation to analyse the impact of Singapore's old populace on its remedial system.
6.	Patil et al.	2023	ML-Healthcare	It can provide a summary of machine learning forms in the field of health.
7.	Mccoy et al.	2022	ML-Healthcare	It can explore the role of ability in the ethical and moral deployment of machine learning in healthcare.
8.	Chen et al.	2021	ML-Healthcare	It can explore the ethical use of machine learning in the healthcare sector, by a limited series of clear information and a computation.
9.	Magesh kumar et al.	2023	DL-Healthcare	Use of NLP in DL healthcare' with cloud-based medical systems for automatic data collection.
10.	Jin et al.	2022	DL-Healthcare	Author explains Artificial Intelligence the DL model utilizes data-driven technologies to improve a Healthcare system's efficiency.
11.	Buddenkotte et. al.	2023	DL-Healthcare	In which author used deep learning methods for detect the cancer and the established "no-new-Net" framework.
12.	Vinod et. al.	2023	ML/DL Healthcare	develop Artificial intelligence and ML models to control COVID-19 spread in healthcare
13.	Zohuri et. al.	2023	ML/DL Healthcare	Operate AI for use in drug development, publicity, and safety.
14.	Stone et. al.	2022	ML/DL Healthcare	COVID-19 remote tolerant track by means of machine learning and deep learning methods, incorporating sensor systems for human beings and smart devices.

9.7.3 Healthcare Operation Using AI

AI is transforming medical procedures in many ways. It also enhances both the quality of patient care and the efficiency of operational processes. Medical images such as X-rays, MRIs, and CT scans can be analysed using AI algorithms. AI can analyze large amounts of data and predict the outcomes of high-risk patients, preventing complications during the treatment phase. With the help of AI, healthcare can develop a personalised treatment plan which will be based on the unique genetic makeup of the patient, their lifestyle and many other factors. The approach of personalised treatment plans is very useful in chronic disease management and oncology.

9.7.4 Diagnostic Assistance

In the field of healthcare AI can assist healthcare providers in diagnosing and identifying diseases accurately and quickly using AI algorithms. It also helps in analysing medical images such as X-rays, MRIs, and body scans.

9.7.5 Predictive Analytics

AI can analyse patient information and forecast the chance of diseases based on genetics, daily habits, and ecological factors. This is for the most part useful in predicting conditions such as diabetes, heart disease, or stroke.

9.8 APPLICATION OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE 5.0

The greatest impact of ML/DL functions is in the healthcare field and their ability to improve patient results and level of concern, even as new applications are being developed**.** Figure 9.2 shows ML/DL as used in the healthcare sector.

- **Medical Picture Investigation:** ML/DL algorithms are used in medical image investigation such as X-ray images, MRIs, and CT scans to help in disease diagnosis and treatment planning.
- **Syndrome Prediction and Identification: The** ML model can detect the disease based on patient data and family records; however, the DL algorithm handles a large amount of genetic data to identify patterns and personalised treatment plans.
- **Drug Discovery and Development:** ML and DL techniques are used to analyse genetics and may aid in molecular construction and enzyme development.
- **Chronic Diseases:** These include conditions such as heart failure, cancer, and diabetes mellitus, which are the leading causes of death and disability in the United States.
- **Smart Health Monitoring:** A precise prediction and estimation method based on Deep Neural Networks (DNN) was developed as part of an

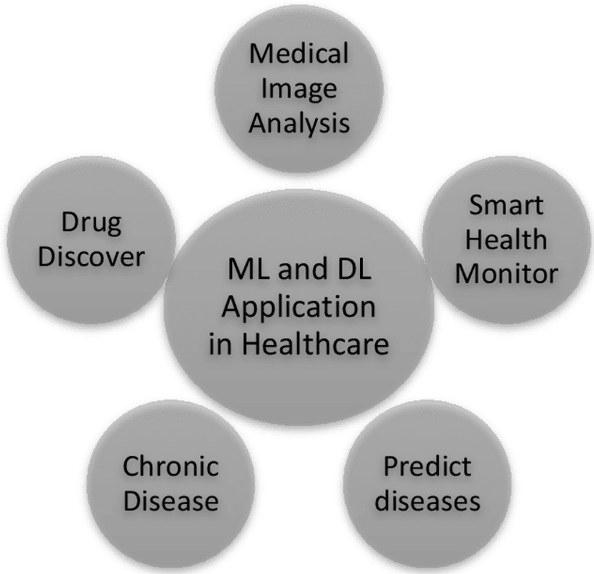


FIGURE 9.2 Application of AI in Healthcare 5.0

innovative, knowledge-driven smart monitoring system for patient observation within an Internet of Things (IoT)-based medical framework.

- **Diagnostic Assistance**: In the field of healthcare AI can assist healthcare providers in diagnosing and identifying diseases accurately and quickly using AI algorithms. It also helps in analysing medical imagery such as X-rays images, MRIs, body scans, and dual-energy X-ray imaging.
- **Public Health Record Using AI:** AI is transforming public health records by improving the efficiency, accuracy, and availability of health records. AI technologies consisting of ML and human–computer interactions bring the process of advanced medical records and documenting the information of patients into a single and interactive interface. Also, AI-powered systems can analyse the vast quantity of information associated with healthcare and predict the disease epidemic, and the outcomes of patients. It helps in quick and early mediation and also helps in the allocation of better resources. To extract meaningful information from the data AI uses NLP which improves the quality and explanation of health records. The information can also be extracted from doctor's notes or medical literature. AI technologies can improve the engagement of patients, organise administrative data well, and also generate customised content for the campaign of public health which can lead to cost savings and improved public health outcomes.
- **Patient Monitoring and Care:** AI technologies can assist the healthcare provider in several ways including disease prediction and prevention,

medical imaging and diagnostics, personalised treatment plans, public health surveillance, and health system management, ethical use is required in all of these areas mentioned here.

9.9 LIMITATION OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE 5.0

Feature Enrichment: To better understand and handle patients, we must collect information from various sources such as EHR, social media, wearable technology, and surveys. The challenge lies in successfully integrating different data into a DL model.

Federated deduction: Clinical facilities have unique patient bases; involving a DL model that uses patients from multiple sites while caring for their private information is a critical challenge.

Expert knowledge: Expert knowledge is critical for medical issues, and research on incorporating it into DL. It is essential to address quality issues and maximize system efficiency. Credible content should be retrieved from online sources.

Data Quality and Availability: AI systems require large amounts of expert data. Inconsistent or incomplete data can lead to mistaken predictions or detection.

Cost: Applying AI solutions can be costly, posing difficulty to entry for smaller healthcare providers.

Limited Generalizability: Models trained on specific populations or conditions may not perform well when valid to different contexts or patient groups.

9.10 CHALLENGES FACED BY AI IN HEALTHCARE 5.0

9.10.1 Data Quality and Integration

- **Heterogeneous Data:** Medical data comes from different sources such as EHRs, portable devices, imaging systems, and genomic databases. Combining these diverse data types into a logical or reasonable system is complex.
- **Data Accuracy and Completeness:** Incomplete, inconsistent, or inaccurate data can lead to incorrect AI predictions and analyses, potentially harming patient care.
- **Data Standardization:** Lack of uniform facts and terms across dissimilar medical systems hinders effective data sharing and integration.

9.10.2 Privacy and Security Concerns:

- **Data Privacy:** Patient records are extremely sensitive, and making sure of their privacy is the most important consideration. AI-based technology can be used alongside guidelines such as HIPAA and GDPR.

- **Cyber Security Risks**: The AI structure is vulnerable to external attacks, which may lead to information leaks and misuse of personal health records.

9.10.3 Ethical and Learning Issues

- **Algorithmic Learning:** AI algorithms can learn from private data, key to better outcomes. Ensuring equal treatment across different patient populations is challenging.
- **Ethical Decision-Making:** AI algorithms may be ethically virtuous, such as prioritising treatments or allocating limited resources, where the human element is crucial.

9.10.4 High Costs

The first investment in AI knowledge can be excessive, especially for smaller healthcare facilities.

9.10.5 Changing Clinical Rules

AI algorithms may need continuous development to keep up with guidelines and practices, altering their significance and accuracy.

9.10.6 Dependence on Technology

Over-reliance on AI could lead to reduced diagnostic skills among healthcare workers.

9.10.7 Ethical Concerns

Questions about accountability and ethical decision-making in AI-driven patient care continue to be debated.

9.11 SOME CASE STUDIES INVOLVING HEALTHCARE 5.0

1. In 2015, Gulshan et al. [34] aimed to develop and validate a deep learning technique that can be used to diagnose diabetic retinopathy (DR). The authors used to type of dataset Messidor-2, Eye PAC, that is, a collection of cornea imagery selected for the categorisation of diabetic floaters. It provided 90% accuracy to identify patients without diabetic retinopathy.
2. In 2017, Esteva et al. [34] developed deep learning methods which mimic the ability of skin specialists. Here we can distinguish between benign and malignant skin issues, such as melanoma and keratinocyte carcinoma, using CNN. In Table. 9.5, we can see that after the model was trained on over 129,000 clinical photographs covering over 2,000 skin illnesses, it was verified using a dataset of biopsy-proven clinical photos.

TABLE 9.5
Case Studies Where AI Is Used in Healthcare

Author	Year	Technology Used	Advantages & Accuracy	Data set used
Gulshan et al.	2015	Deep Learning	High accuracy in finding diabetic floaters 90% accuracy	Eye PACS dataset, Messidor-2
Esteva et al.	2017	CNN	Automatic categorisation of melanoma cancer at dermatologist-level accuracy is ~ 72.1	Image dataset of skin cancer
Rajpurkar et al.	2018	Deep Learning	High accuracy in the detection of pneumonia from chest X-rays and 94.4 % accuracy	CXR
Topol et al & McKinney et al.	2020	AI, DL, ML algorithms	Improved diagnostic accuracy and detection of breast cancer	Mammogram dataset
Kelly et al.	2022	AI-driven predictive analytic	AI-driven insights in predictive analytics, personalized treatment	Multiple open clinical datasets, MIMIC, etc.
Liu et al	2023	AI, IoT, and big data	Real-time monitoring and diagnostics; personalized treatments	Real-time patient data

3. In 2015 and 2020, Topol et al. [36] arranged a perilous foundation for the integration of AI in healthcare, particularly in genomics projects. Their intuitions have played a critical role in influencing the direction of Healthcare 5.0, highlighting the potential for personalised medicine and data-driven decision-making of patients through technology.
4. In 2018, Rajpurkar et al. [37] developed deep learning algorithms to analyse chest X-ray images. Their models were intended to identify various situations, such as pneumonia, tuberculosis, and other abnormalities, demonstrating the effectiveness of AI in rendering medical images.
5. In 2020, Shing et al. [38] verified the role of AI in enhancing healthcare responses during the COVID-19 pandemic. Their results showed how AI technologies could enable faster identification, improve patient management, and optimise resource allocation.
6. In 2022, Orenstein et al. [39] reviewed the application of AI in mental health, particularly through the development of AI chatbots and virtual assistants. The authors explored how AI-driven chatbots could provide accessible mental health support. These tools were designed to engage users in conversations, offer coping strategies, and provide resources, making mental healthcare more accessible.

7. In 2023, Zhang et al. [40] studied how AI technologies are being joined into telemedicine platforms. This integration goal to improve the quality of remote sessions and diagnostics, making healthcare more open to patients.

9.12 CONCLUSION

In conclusion, AI represents a transformative period in Healthcare 5.0; giving emphasis to the combination of advanced AI skills with human intelligence to improve patient care. By manipulating machine learning, natural language processing, and data analytics, AI develops diagnostics, treatment planning, and patient management. In medical imaging, AI algorithms can detect diseases with accuracy, often outperforming human specialists in identifying early-stage conditions such as cancer. Predictive analytics allow healthcare workers to expect potential health concerns based on individual patient data, leading to proactive interference. It can be used for digital agreements through intelligent contracts, reducing costs and removing intermediaries. It can also improve patient history management, insurance mediation, and clinical actions. The adoption of advanced technologies in the Healthcare 5.0 ecosystems will revolutionise patient care and healthcare services. These tools do not necessarily guarantee improved medical outcomes but instead aim to redefine the principles of efficiency, innovation, and convenience in modern Healthcare 5.0.

REFERENCES

1. Singh J. Overview of tools and applications of machine learning in healthcare. *International Journal of Computer Science &Communication*, 13(1), 46–51 (2022).
2. Avdan G. Lean thinking in healthcare 5.0 technologies: An exploratory review. In *9th North American Conference on Industrial Engineering and Operations Management* (2024, June).
3. Bajwa J, Munir U, Nori A, and Williams B. Artificial intelligence in healthcare: Transforming the practice of medicine. *Future Healthcare Journal*, 8(2), e188–e194 (2021).
4. Manning CD, et al. *Introduction to Information Retrieval*. Cambridge University Press (2008).
5. Miotto R, et al. Deep learning for healthcare: Review, opportunities and challenges. *Briefings in Bioinformatics*, 19, 1236–1246 (2018).
6. Liu C, et al. Risk prediction with electronic health records: a deep learning approach. In *ACM Interntional Conference on Knowledge Discovery and Data Mining*, Sydney, NSW, Australia, pp. 705–14 (2015).
7. Lasko TA, et al. Computational phenotype discovery using unsupervised feature learning" *PLoS One*, 8(6), e66341 (2013).
8. Miotto R. Deep learning for healthcare: Review, opportunities and challenges. *Briefings in Bioinformatics*, 19, 1236–1246 (2014).
9. Alafif T, et al. Machine and deep learning towardscovid-19 diagnosis and treatment: Survey, challenges, and future directions. *International Journal of Environmental Research and Public Health*, 18, 1117 (2021).
10. Olsen CR, Mentz RJ, Anstrom KJ, Page D, and Patel PA. Clinical applications of machine learning in the diagnosis, classification and prediction of heart failure. *American Heart Journal*, 229, 1–17 (2020).

11. Chen H, Chiang RHL, and Storey VC. Business intelligence and analytics: from Big Data to big impact. *Management Information Systems Quarterly*, 36(4), 1165–1188 (2012).
12. Budden Kotte T, Rundo L, Woitek R, et al. Others deep learning-based segmentation of multi-site diseaseinovariancancer. *MedRxiv*, 1–18 (2023).
13. Vinod D, and Prabaharan S. COVID-19 the role of artificial intelligence, machine learning and deep learning: A newfangled. *Archives of Computational Methods in Engineering* 30, 2667–2682 (2023).
14. Zohuri B, and Rahmani F. Artificial intelligence driven resiliency with machine learning and deep learning components. In *Tran cranial Magnetic and Electrical Artificial Intelligence Stimulation for Neurological Disorders*, Academic Press, pp. 317–334 (2023).
15. Stone D, Michalkova L, and Machova V. Machine and deep learning techniques, body sensor networks, and Internet of Things-based smart healthcare systems in COVID-19 remote patient monitoring. *American Journal of Medical Research* 9, 97–112 (2022).
16. Khezr D, Moniruzzaman M, Yassine A, and Benlamri R. Block chain technology in healthcare: a comprehensive review and directions for future research. *Applied Sciences*, 9(9), 1736 (2019).
17. Kumar T, Ramani V, Ahmad I, Braeken A, Harjula E, and Ylianttila M. Block chain utilisation in healthcare: key requirements and challenges. In *2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom)*, IEEE, 2018 Sep 17, pp. 1–7.
18. Moona G, Jewariya M, and Sharma R. Relevance of dimensional metrology in manufacturing industries. *Mapan*, 34, 97–104 (2019). https://doi.org/10.1007/ s12647-018-0291-3.
19. Jin D, Sergeeva E, Weng W, et al. (2022) Explain deep learning in healthcare: A methodological survey from an attribution view. WIRES Mech Dise14:e1548.
20. Vinod D, and Prabaharan S. COVID-19 the role of artificial intelligence, machine learning, and deep learning: A Newfangled. *Archives of Computational Methods in Engineering*, 30, 2667–2682 (2023).
21. Xu Z, and Sun J. Model-drivendeep-learning. *National Science Review*, 5, 22–24 (2018).
22. Shah A, Yan X, Shah S, et al. Mining patient opinion to evaluate the service quality inhealthcare:adeep-learningapproach. *Journal of Ambient Intelligence and Humanized Computing*, 11, 2925–2942 (2020).
23. Tuli S, Basumatary N, and Gill S, et al. Health Fog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Generation Computer Systems*, 104, 187–200 (2020).
24. Rahman M, Kundu D, Suha S, et al. Hospital patients' length of stay prediction: A federated learning approach. *Journal of King Saud University-Computer and Information Sciences*, 34, 7874–7884 (2022).
25. Solanki R, Rajawat A, Gadekar A, et al. Building a Conversational Chatbot Using Machine Learning: Towards a More Intelligent Healthcare Application. In *Handbook of Research on Instructional Technologies in Health Education and Allied Disciplines* (pp. 285–309). USA: IGI Global (2023).
26. Siar M, Teshnehlab M, Editors. Brain tumor detection using deep neural network and machine learning algorithm. In *2019, 9th International Conference on Computer and Knowledge Engineering (ICCKE)*; 2019, pp. 363–368.
27. Chen P, Wu T, Wang P, et al. Pancreatic cancer detection on CT scans with deep learning:a nationwide population-basedstudy. *Radiology*, 306, 172172–172182 (2023).

28. Awotunde J, Panigrahi R, Khandelwal B, et al. Breast cancer diagnosis based on hybrid rule-based feature selection with deep learning algorithm. *Research on Biomedical Engineering*, 39, 115–127 (2023).
29. Özdil A, Yilmaz B. Medical infrared thermal image based fatty liver classification using machine and deep learning. *Quantitative InfraRed Thermography Journal*, 21(2), 102–119 (2023).
30. Qadri S, Lin H, Shen L, et al. Others CT-Based Automatic Spine Segmentation Using Patch-Based Deep Learning. *International Journal of Intelligent Systems*, 2023, 1–14 (2023).
31. Lasko TA, Denny JC, and Levy MA. Computational phenotype discovery using unsupervised feature learning over noisy, sparse, and irregular clinical data. *PLoS One*, 8, e66341 (2013).
32. Miotto R, Wang F, Wang S, Jiang X, and Dudley JT. Deep learning for healthcare: Review, opportunities and challenges. *Briefings in Bioinformatics*, 19, 1236–1246 (2018).
33. Mukerji S, Petersen K, Pohl K, et al. Machine learning approaches to understand cognitive phenol types in people with HIV. *The Journal of Infectious Diseases*, 227(Supplement_1), S48–S57 (2023).
34. Gulshan V, Peng L, Coram M, Stumpe MC, Wu D, Narayanaswamy A, Venugopalan S, Widner K, Madams T, Cuadros J, Kim R, Raman R, Nelson PC, Mega JL, and Webster DR. Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. *JAMA*, 316(22), 2402–2410 (2016).
35. Esteva A, Kuprel B, Novoa RA, Ko J, Swetter SM, Blau HM, and Thrun S. Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, 542(7639), 115–118 (2017).
36. Rajpurkar P, Irvin J, Zhu K, Yang B, Mehta H, Duan T, Ding D, Bagul A, Langlotz C, Shpanskaya K, Lungren MP, and Ng AY. CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning. *Proceedings of the National Academy of Sciences*, 115(45), 11669–11675 (2017).
37. Topol EJ. High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, 25(1), 44–56 (2019). doi: 10.1038/s41591-018-0300-7
38. McKinney SM, Sieniek M, Godbole V, Godwin J, Antropova N, Ashrafian H, Back T, Chesus M, Corrado GS, Darzi A, Etemadi M, Garcia-Vicente F, Gilbert FJ, Halling-Brown M, Hassabis D, Jansen S, Karthikesalingam A, Kelly CJ, King D, Ledsam JR, Melnick D, Mostofi H, Peng L, Reicher JJ, Romera-Paredes B, Sidebottom R, Suleyman M, Tse D, Young KC, De Fauw J, and Shetty S. International evaluation of an AI system for breast cancer screening. *Nature*, 577(7788), 89–94 (2020). doi: 10.1038/s41586-019-1799-6; Erratum in: *Nature* 586(7829), E19 (2020).
39. Kelly CJ, Karthikesalingam A, Suleyman M, Corrado G, and King D. Key challenges for delivering clinical impact with artificial intelligence. *BMC Medicine*, 17(1), 195 (2019).
40. Liu Y, Chen P, and Zhang P. AI-powered healthcare 5.0: Real-time diagnostics and personalized treatment. *Journal of Healthcare Engineering*, 2023, 123456 (2023).

10 Role of IoT in Healthcare 5.0

Kumar Parmar, Apu Chandra Barman, Jhanvi Modi, Damodharan Palaniappan, and Premavathi

10.1 INTRODUCTION TO HEALTHCARE 5.0 AND THE INTERNET OF THINGS (IOT)

Healthcare 5.0 is the most recent shift of the medical industry's model to yet another paradigm, with its primary goals being to enhance patient care, operational efficiency, and the general delivery of healthcare. In a sense, it is defined in terms of the seamless incorporation of modern technologies into healthcare organizations. Healthcare 5.0, while still evolving, builds on earlier models that have often struggled to fully support pre-diagnostic, pre-symptomatic, and personalized healthcare paradigms [1, 2]. These new emerging technologies include 'big data', 'blockchain', 'artificial intelligence (AI)', and of course the Internet of Things (IoT).

Key features of Healthcare 5.0 include:

- **Personalized Medicine:** Personalized medicine was developed to be specific to the genetic makeup of the patient, the patient's lifestyle, and the surrounding environment.
- **Predictive Analytics:** Based on data and AI, an effective model for the prediction of health trends and possible spread of illnesses; thereby efficient measures and alerts are quickly taken.
- **Preventive Care:** Primary prevention of the diseases by frequent screening and early detection.
- **Patient-Centric Care:** Creating an understanding of the fate of healthcare delivery that responds to patients' needs and expectations and improves their experience.
- **Interoperability:** The ability to interconnect and share information between multiple, preferably all, healthcare facilities and other life-sustaining devices effectively and securely.

DOI: 10.1201/9781003532286-10

10.1.1 Overview of IoT and Its Potential in Healthcare

As shown in Figure 10.1 the collection of interconnected hardware devices which can exchange data with one another over the web is referred to as the Internet of Things (IoT). IoT can therefore be described to encompass all smart allied products utilized in the healthcare sector such as smart health machines and wearable health gadgets aimed at collecting health information from patients and processing and transmitting the collected information in real time. There are numerous benefits that IoT can offer and bring to healthcare making it almost a different system that can revolutionize the industry. Due to IoT, it is now possible to monitor health parameters and the general well-being of patients outside the traditional hospital setting. It

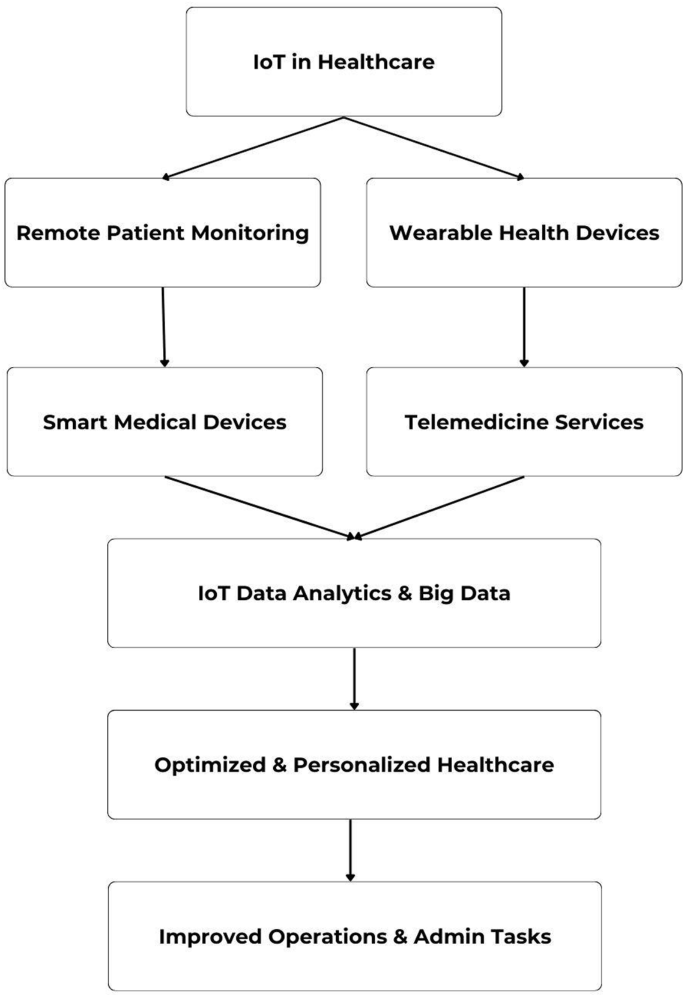


FIGURE 10.1 IoT and Healthcare 5.0

allows the evaluation, 24/7, of health indicators including heart rates, blood pressure, glucose levels, pulse oximetry, respiratory rates, and others through fitness trackers and smartwatches [3]. It allows medical doctors and personnel to remotely supervise patients' conditions, closely observe data for potential complications, and attend to them promptly, therefore reducing the readmission of patients to hospitals, and also improving patients with chronic disease conditions.

The telemedicine platforms which are based on IoT allow physicians and patients to have remote communications. This allows patients to receive drug prescriptions, and follow-up medical consultations without visiting a hospital due to data sharing and video conferencing. This will enhance the healthcare provision and enable people in underprivileged or rural areas to benefit from better healthcare services. IoT is an innovation that helps to develop smart medical gadgets that can help enhance clinical operations' accuracy and productivity. For instance, integrated infusion pumps can reduce the risk of error by using data from the patient's health records to regulate the dosages of drugs given to the patient. Smart beds in hospitals can enhance the well-being and comfort of the patients as well as increase patient safety to avoid the development of bedsores by monitoring the movements of the patients' bodies and automatically altering the positions of the patients' bodies.

In particular, with the help of complex calculations and AI methods such as machine learning, an enormous amount of information generated by IoT devices can be analyzed. Here, healthcare professionals may use this big data strategy to anticipate illness outbreaks, recognize patterns, and then develop individual patient treatment plans [4]. By promoting the efficiency of big data, healthcare institutions can raise the quality of patients' treatment, improve the distribution of resources, and make informed decisions. IoT also helps improve the operational efficiency of healthcare institutions. Automated materials management may keep continuous records of the medical supplies' stock and ensure that all the needed materials are in stock. Smart scheduling systems can enhance patients' satisfaction by enhancing the organization and reducing the time spent scheduling an appointment [5].

Explainable AI in the context of Healthcare 5.0 discussed and highlighted both the opportunities and challenges it presents in Saraswat et al. (2022) [6]. The authors conducted a comprehensive survey following established standards. The paper outlines the research questions, data sources used, and methodologies employed. It delves into various aspects of eExplainable artificial intelligence (XAI), including its evolution, technological trends, and integration with other advancements such as 5G and federated learning. The paper emphasizes the importance of user experience and interaction in healthcare applications. A bibliometric analysis of the applications of the IoT in healthcare is presented in Rejeb et al. (2023). The authors reviewed a substantial number of research papers to identify key themes, challenges, and future directions in this field. The study highlights trust and privacy, power management, resource management, and fog computing as major areas requiring further research. Additionally, it identifies emerging trends such as social networks, tactical internet, big data analytics, blockchain, and the internet of nano-things, while acknowledging scalability, interoperability, and mobility as persistent challenges [7, 8].

The authors explore the intersection of Industry 5.0 and healthcare. The study aims to understand how Industry 5.0 principles, which emphasize human-centric technological advancement, can be applied to healthcare to improve patient care and overall well-being (Basulo-Ribeiro and Teixeira, 2024) [9]. The authors conducted qualitative interviews with a range of healthcare professionals, including doctors, nurses, and technology specialists. These interviews aimed to gauge the awareness and understanding of Industry 5.0 within the healthcare sector and to identify potential benefits, challenges, and implementation strategies. The article highlights the potential of Industry 5.0 technologies to enhance patient care through personalized medicine, improve diagnostics, and streamline healthcare operations. However, it also acknowledges challenges such as the need for upskilling healthcare professionals, addressing ethical concerns related to AI and data privacy, and ensuring equitable access to these advancements. The study, while preliminary, provides valuable insights into the potential of Industry 5.0 to transform healthcare and emphasizes the need for further research and discussion to guide its implementation effectively.

The authors explore the transformative potential of IoT in healthcare in Parihar et al. (2024) [10]. IoT enables remote patient monitoring, allowing doctors to track vital signs and other health data in real time, leading to early problem detection and personalized care. Another application is the development of smart ambulances equipped with IoT devices that transmit real-time patient data to hospitals, enabling medical professionals to prepare for their arrival and potentially deliver life-saving interventions. However, the paper also emphasizes the significant security and privacy challenges associated with IoT in healthcare. Health data transmitted between devices and central processing units is often in a raw, vulnerable format, making it susceptible to hacking and unauthorized access. Protecting patient privacy is crucial, and ensuring that only authorized individuals can access sensitive health data is paramount. The authors conclude by stressing the need for robust security measures, including device-specific cryptographic algorithms and user education, to mitigate these risks and ensure the safe and effective implementation of IoT in healthcare.

The transformative impact of IoT on healthcare, particularly within hospital settings was explored by Almotairi (2022) [11]. The authors illustrate how IoT is revolutionizing healthcare delivery by enabling real-time data collection, analysis, and exchange, leading to more efficient and effective care. They emphasize the numerous advantages of integrating IoT in hospitals, such as enhanced patient monitoring, facilitation of remote treatment options, and improved management of medical resources. However, the paper also acknowledges the challenges associated with widespread IoT adoption in healthcare. These challenges include ensuring data security and patient privacy, managing the complexity of handling large volumes of data, and addressing the high costs associated with implementation. Looking toward the future, the authors outline potential research areas, such as leveraging IoT for predicting and managing chronic conditions such as strokes and epileptic seizures and developing advanced prosthetic sensors for real-time data retrieval to aid in patient treatment.

Kumar et al. (2023) explore the potential of healthcare IoT (H-IoT) to revolutionize healthcare delivery. The authors discuss various applications of H-IoT, including remote patient monitoring, telemedicine, and smart hospitals. They highlight the benefits of H-IoT, such as improved patient outcomes, reduced healthcare costs, and increased efficiency. However, the paper also acknowledges the challenges associated with H-IoT, such as security and privacy concerns, interoperability issues, and the need for robust infrastructure. The authors emphasize the importance of addressing these challenges to fully realize the potential of H-IoT in healthcare. They conclude by suggesting future research directions and advocating for legislative action and policy frameworks to support the widespread adoption of H-IoT [12].

Javaid and Khan (2021) explore how IoT can be used to address challenges posed by the COVID-19 pandemic. It discusses how IoT technologies, such as remote patient monitoring and data analytics, can be used to improve healthcare outcomes and reduce the spread of the virus. The authors argue that IoT has the potential to revolutionize healthcare and make it more efficient, effective, and patient-centered, especially during pandemics [13].

IoT is a transformative technology that integrates sensors across various sectors, particularly healthcare (Pardhu and Kumar, 2024). These sensors enable data collection, which is critical for analytics and improving services, especially during the COVID-19 pandemic. In healthcare, IoT enhances patient care by enabling precise and real-time monitoring, leading to better patient outcomes. The study explores various healthcare applications of IoT, demonstrating its potential to improve service delivery. However, the paper also addresses technological challenges, such as data security, device interoperability, and the need for robust infrastructure to support IoT systems. Drawing on data from reputable sources such as Google Scholar and PubMed, the research emphasizes evidence-based findings. The chapter calls for further research to overcome IoT challenges, particularly in light of the pandemic, and highlights the potential for IoT to revolutionize healthcare. Ultimately, the paper underscores the need for innovation and continued exploration to fully leverage IoT's benefits in healthcare [14].

The integration of IoT in healthcare has transformed the industry by enhancing patient care and streamlining processes (Shafik 2024). IoT enables remote monitoring, allowing healthcare providers to detect issues early, improve patient outcomes, reduce hospital readmissions, and lower costs. Hospitals have evolved into smart facilities with interconnected devices that monitor vital signs and alert doctors to sudden health changes. However, IoT implementation faces challenges, such as data privacy, security risks, and information overload. This chapter explores the benefits and characteristics of IoT in healthcare, its applications, and the challenges it presents. Collaboration between healthcare providers, technology firms, and regulatory bodies is essential for responsible IoT usage, maximizing its potential to improve care, reduce costs, and enhance efficiency [15].

Therefore, IoT is one of the significant facets of Healthcare 5.0, driving innovations that enhance the quality of care which is centered on patients, holistic, rational, and accessible care. The IoT technologies could devise a completely new world of possibilities influencing the medical business and offer opportunities for enhanced patient treatment and organizational performance when introduced into the healthcare market and developed.

10.2 IOT APPLICATIONS IN HEALTHCARE 5.0

The use of IoT in healthcare means radical changes in every sphere of medical activity. In Figure 10.2, Here are the detailed applications of IoT in Healthcare 5.0:

10.2.1 Remote Patient Monitoring

The application of the IoT in healthcare systems introduces radical changes to the different aspects of medical practice. Here are some of the various useful implementations of IoT in Healthcare 5.0:

Remote patient monitoring (RPM) is one of the most significant innovations in the sphere of healthcare that was made possible with the help of IoT. RPM reduces the cycle of readmissions by using IoT gadgets to check the progress of patients' health at home [5]. Pulse oximeters, blood pressure, and glucose monitors are a few devices that collect data and transmit data to healthcare practitioners continuously. This enables:

- **Early Detection of Health Issues:** It is a consistent check to detect health-related issues that require check-ups in their initial stages.
- **Chronic Disease Management:** The larger populations with diseases such as diabetes or hypertension; act can ensure that the conditions are managed better, thereby limiting complications.
- **Reduced Hospital Readmissions:** This is because, by constantly monitoring patients from a distance, healthcare practitioners will be able to attend to them before they deteriorate hence less hospitalization.

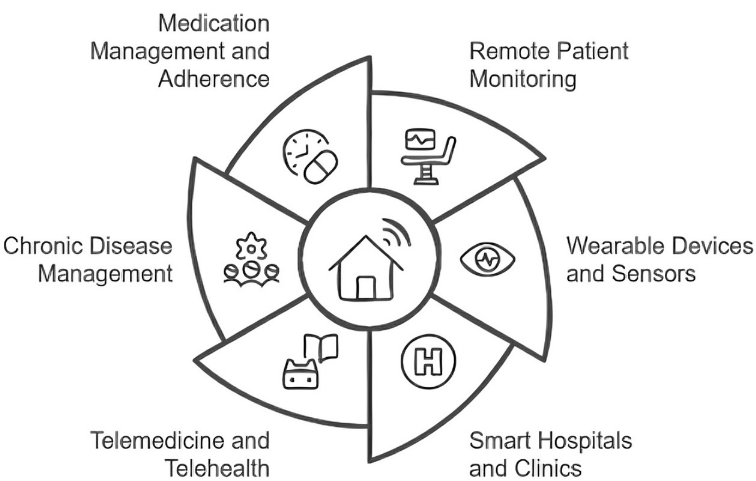


FIGURE 10.2 IoT applications in Healthcare 5.0

10.2.2 Wearable Devices and Sensors

- Because of the resulting ability to measure health parameters, devices such as wearables and sensors are transforming the management of human health [16]. Some of them include wearable biosensors, smartwatches, and fitness trackers. These gadgets provide:
- **Real-Time Health Monitoring:** Real-time monitoring and recording of basic life indices, movement, and sleeping habits respectively.
- **Enhanced Patient Engagement:** This has involved engaging patients in decision-making on their health since most decisions that affect their health are unique to them.
- **Personalized Health Insights:** Based on the stated question, data gathered can be processed and presented in the form of an individual report that can be shown to the healthcare providers for formulating the right decision.

10.2.3 Smart Hospitals and Clinics

In smart hospitals and clinics, IoT solutions are used to optimize the handling of patients and improve overall practices. IoT applications in these settings include:

- **Automated Patient Flow Management:** Applying information technologies such as sensors and data analytics to reduce the time patients take to move from one department to another in the hospital, making it a one-stop shop.
- **Smart Beds:** Prop beds, with sensors adherent to the patient's body to know their respiration rate and movements to avoid the development of pressure ulcers while improving the patient's experience.
- **IoT-Enabled Equipment Management:** Supervision and control the state and usage of medical devices in real time so that timely diagnoses and repairs can be made.

10.2.4 Telemedicine and Telehealth

Telemedicine and telehealth have popularity increased with the help of IoT as it has enhanced the availability of healthcare services [17]. IoT facilitates:

- **Remote Consultations:** Patients can confer with the provider online using video hence eliminating the need for in-person interviews.
- **Virtual Monitoring:** By giving intelligent IoT devices the capacity to persistently transfer health data to healthcare professionals, such as physicians, patients' health can be supervized and immediate decisions can be made if needed.
- **Expanded Access:** Telemedicine is the expansion of healthcare to areas that are not always reachable and with few hospitals and clinics.

10.2.5 Chronic Disease Management

It has been seen that IoT shows significant importance while dealing with chronic diseases as it could prevent and control the disease by continuously monitoring the patient's condition. Applications include:

- **Continuous Glucose Monitoring (CGM):** Glucose real-time monitoring devices that notify patients and physicians of any unusual fluctuations with the condition that they are experiencing and help to manage diabetes better.
- **Cardiac Monitoring:** Smartwatches that can identify abnormal heart rhythms which are characteristic of arrhythmia or other related heart complications.
- **Asthma and COPD Management:** Smart inhalers and air quality monitors assist patients with respiratory diseases to have better control of the signs.

10.2.6 Medication Management and Adherence

Accurately and effectively treating a patient comes down to the satisfaction of the consumer by taking his or her medications as scheduled. IoT helps in:

- **Smart Pill Bottles:** Medication vials with sensors that gently remind patients to take the medication and keep a record of the self-administered doses.
- **Automated Dispensing Systems:** Apparatuses that contain the right quantity of drug to be administered at the right time thus minimizing mistakes.
- **Adherence Tracking:** Tools that send notifications to healthcare professionals and/or other carers if a patient has not taken a prescribed drug, allowing timely actions.

Healthcare 5.0 is transforming medical practice by enhancing the practice of surveillance of patients, the management of the condition, and the delivery and availability of services. They initiate the possibility of a more sensitive and coordinated EMR/new healthcare structure by enhancing the operations of the healthcare industry as well as the experiences of its patients. Various IoT applications in healthcare are mentioned in Table 10.1.

10.3 IOT-ENABLED HEALTHCARE ECOSYSTEM

The IoT environment in healthcare entails the connections of healthcare substantial items and systems that jointly enhance the efficiency, accuracy, and accessibility of healthcare services. The role of this ecosystem is to transform the existing paradigms of healthcare delivery through the application of innovative technology approaches to collect, analyze, and utilize health data in ways that were not previously possible [18]. Here is an in-depth look at the key components of an IoT-enabled healthcare

TABLE 10.1
Various IoT Applications in Healthcare

Application	Description	Key Benefits
Remote Patient Monitoring	Continuous tracking of patient health from home	Early detection, chronic disease management, reduced readmissions
Wearable Devices and Sensors	Devices that track health parameters like heart rate and sleep	Real-time health monitoring, patient engagement, personalized insights
Smart Hospitals and Clinics	IoT systems for optimizing hospital operations	Automated patient flow, smart beds, real-time equipment management
Telemedicine and Telehealth	Remote communication and virtual health monitoring	Remote consultations, expanded access to care, cost savings

ecosystem. Here is an in-depth look at the key components of an IoT-enabled healthcare ecosystem:

10.3.1 Interconnected Devices and Systems

The IoT healthcare system can be summarized as the primary devices and networks that exist and work in conjunction with one another to offer complete healthcare services. These devices include:

- **Wearables and Health Monitors:** Smart wearables such as a fitness trackers, smartwatches, and biosensors that help in tracking health parameters such as heart rate, sleep cycle, and activity level.
- **Smart Medical Equipment:** Technologies in patient care systems such as; smart IV pumps and diagnostic devices in clinics and hospitals that can report information in real time and perform other functions.
- **Home Health Devices:** Products that can be employed in a home context to manage many chronic conditions including blood glucose meters, blood pressure cuffs, and smart scales.
- **Telemedicine Platforms:** Consultation and diagnostic tools that will enable doctors to consult/assess their patients from a distance and use video conferencing, data sharing, and patient monitoring systems.

10.3.2 Data Collection and Analysis

The broad field of information derived from the numerous networked IoT units is a wealth for enhancing healthcare results. Key aspects of data collection and analysis include:

- **Real-Time Data Collection:** Prolonged collection of health data from different body sensors and appliances to get current figures on a patient's health.

- **Data Integration:** Compiling records from numerous resources into one system, which offers effective records of the overall patient's health.
- **Advanced Analytics:** Employing data analytics techniques to analyze the gathered data, and to analyze trends, outliers, and insights that may be derived from the data [19]. This allows especially healthcare individuals to make the right decisions, get the right diagnosis, and prescribe the right treatment.

10.3.3 Cloud Computing and Storage

Cloud services are used in IoT-based healthcare services and applications for storing large amounts of data in a secure and cost-effective manner. Key benefits of cloud computing in healthcare include:

- **Scalability:** The way they allow for the collection and storage of data from the various IoT devices without the hindrance of physical storage space.
- **Accessibility:** Data should be readily available irrespective of the location, and helpful to the different healthcare workers, thus supporting telemedicine options.
- **Security and Compliance:** Adhering to various security guidelines, including prescriptive compliance to ensure health information remains guarded and private; the health data protection laws including HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation).

10.3.4 Artificial Intelligence and Machine Learning

IoT devices are attributed to the creation of large volumes of data, for which extracting useful information needs the application of advanced technology such as AI and ML [20]. Their applications in the healthcare ecosystem include:

- **Predictive Analytics:** Applying AI computations to anticipate health patterns, future epidemics, and possible results of patients' treatments, thus, implementing preventive measures in advance.
- **Personalized Medicine:** Utilizing ML for diagnosing diseases by correlating patients' genetic makeup, their daily habits, and previous medical records, with suggestions of suitable treatments for a particular patient.
- **Automated Diagnostics:** By applying AI to help in the diagnostic techniques and decision-making when it comes to images and lab tests or even the records belonging to a patient then the diagnosis turns out to be more correct and faster in terms of time.
- **Operational Efficiency:** Incorporating the use of AI can help to cut down the workload on the healthcare staff and in addition avoid any likelihood of errors in daily tasks such as scheduling, inventory, and workflow among others.

IoT in healthcare is the systematic integration of electronic devices into people's lives specifically in the healthcare sector where several devices are being connected to establish a continuous flow of data and information through IoT technology. Being an ecosystem of real-time monitoring, big data and analytics, cloud computing, and AI can significantly improve the quality of patient care, business processes, and even the practice of individualized medicine. With these technologies advancing, the healthcare sector will be able to improve its solutions by making them efficient, effective, and, most importantly, patient oriented.

10.4 CHALLENGES AND CONSIDERATIONS IN IMPLEMENTING IOT IN HEALTHCARE 5.0

This section presents methods for implementing IoT in healthcare. While IoT adoption offers several advantages, it also introduces significant challenges [21]. Addressing these challenges is essential to successfully realize and operate IoT technologies in healthcare, as illustrated in Figure 10.3.

10.4.1 Data Privacy and Security

The major drawback to IoT healthcare is the protection of data being transferred such that; private information or secret information is not exposed to third parties. Due to the fact that health data is often considered as sensitive information, it poses an appealing target for hackers. Key considerations include:

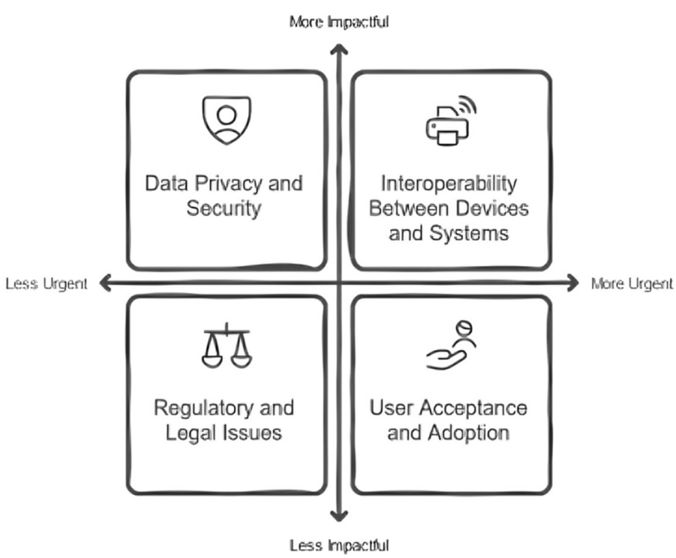


FIGURE 10.3 Challenges in IoT Healthcare 5.0

- **Data Encryption:** In this case, it is suggested that all the data exchanged between IoT devices and the health care systems be encrypted so that unauthorized persons cannot access the information.
- **Access Controls:** Adopting strict measures to warrant that only those who have a noble cause access the patient data.
- **Cybersecurity Protocols:** Creation of secure bandwidth and DLs capable of identifying and countering security breaches on the fly.
- **Compliance with Regulations:** Compliance with the laws of data privacy such as HIPAA for the patients' information to be collected, used, and disclosed in a legal and ethical manner as per GDPR.

10.4.2 Interoperability between Devices and Systems

Interoperability is essential for creating a cohesive IoT-enabled healthcare ecosystem. It means that there is no unification, and therefore, it can complicate cooperation between different devices and systems [22]. Considerations for improving interoperability include:

- **Standard Protocols:** By using standardized communication platforms and the use of format-friendly devices and systems.
- **Integration Platforms:** Using integration platforms that can easily connect the various applications, so that there is a proper transfer of data.
- **Collaborative Efforts:** Promoting the cooperation between the device manufacturers, software developers, and care organizations to create compatibility solutions.

10.4.3 Regulatory and Legal Issues

An enormous issue when considering IoT healthcare is the issue of regulation and law. Key considerations include:

- **Compliance with Health Regulations:** Guarantee that all the IoT devices and systems meet the existing health laws and regulations as dictated by regulatory bodies such as the FDA and EMA [23].
- **Data Ownership and Consent:** Ensuring patient information use and collection by defining the ownership rights of data collected by the EMR system.
- **Liability and Accountability:** They mention inadequate criteria for identifying those entities which are accountable or liable in the event that these devices malfunction or data is stolen.

10.4.4 User Acceptance and Adoption

IoT in healthcare has relativity on the adoption rate from both the practitioners and users of the services. Key considerations to enhance acceptance and adoption include:

- **Training and Education:** Conduct extensive training and awareness to healthcare professionals regarding IoT technologies and their advantages.
- **User-Friendly Interfaces:** Development of friendly interfaces on the IoT devices and applications to be used in the delivery of healthcare to patients or by the healthcare givers.
- **Demonstrating Value:** IOT solutions should be worked on so as to educate healthcare providers and patients about the benefits of using IoT solutions [24].
- **Addressing Concerns**: Being proactively engaging to remove any fear that users may have especially when it comes to privacy, security, as well as the reliability of the connected IoT devices.

In this case, the integration of IoT in Healthcare 5.0 is not well described to explain the envisioned change. Despite its potential for transformation, risks such as personal data protection, system integrability, legal requirements, and users' embrace. Solving these issues is possible through the use of established cybersecurity; standardization, legal and regulatory compliance; and user-centered design and awareness. Overcoming such challenges will ensure that appropriate strategies are implemented in the delivery of healthcare services that are efficient, effective, and responsive to the patients' needs. Table 10.2, mentions various challenges faced by IoT in healthcare.

10.5 CASE STUDIES AND EXAMPLES

Case Study 1: Remote Patient Monitoring at Mayo Clinic

The Mayo Clinic has adopted a complex IoT-based RPM solution for CHF and diabetes patients [25]. It consists of wrist-worn devices that provide a stream of data as to a patient's health and relay this information back to specific clinicians. This initiative has resulted in significant improvements in patient outcomes, including:

TABLE 10.2
Various Challenges IoT Faces in Healthcare

Challenge	Description	Proposed Solutions
Data Privacy and Security	Risk of unauthorized access to sensitive health data	Encryption, access controls, compliance with regulations
Interoperability	Difficulty in integrating various IoT devices and systems	Standard protocols, integration platforms, collaborative efforts
Regulatory and Legal Issues	Unclear data ownership and regulatory compliance	Compliance with health laws, clear data ownership policies
User Acceptance	Low adoption rates due to complexity and unfamiliarity	User-friendly design, training, and clear communication of benefits

- **Reduced Hospital Readmissions:** The ability to monitor the health status of the patient continuously helps in early signs and symptoms of the health status of a patient, leading to intervention and thus minimizing the hospital readmission status.
- **Improved Patient Engagement:** The management of health information improves since patients are fully involved, and they receive feedback instantly.
- **Enhanced Chronic Disease Management:** Telemedicine has made it possible for patients to be monitored from the comfort of their homes which has made treatment personalized and chronic diseases well managed.

Case Study 2: Smart Hospitals at Cleveland Clinic

The Cleveland Clinic is making its environment smart by implementing IoT in its processes. Some key initiatives encompass:

- **Smart Beds:** These are health facility beds that have motion and patient sensors which help in detecting movements of the patient and the patient's vital signs with ease; the bed can change position to help make the patient comfortable to avoid bed sores.
- **Connected Medical Devices:** Equipment such as infusion pumps and other monitoring equipment are active components in the overall system of the hospital which offers real-time information to the programmers of healthcare.
- **Automated Inventory Management:** Smart healthcare monitors the medical supplies they require in real time, it eliminates post- or before-stock checking which is very tedious.

These implementations have led to:

- **Operational Efficiency:** Facilitated by automation and real time, it has helped in the reduction of task burdens on healthcare personnel while at the same time decreasing possible mistakes.
- **Improved Patient Care:** Real-time monitoring and smart devices improve the level of care being delivered and prompt management and control of ailments hence improving health.

Case Study 3: Telemedicine Services at Mercy Virtual

Mercy Virtual which is a fully operational virtual care center uses IoT to deliver telemedicine to patients residing in areas that are not easily reachable. Key features include:

- **Remote Consultations:** One can communicate with doctors and other providers remotely, backed up by biometrics transmitted from remote wearable health fitness trackers.
- **Continuous Health Monitoring:** Connected objects make it possible for practicing physicians to constantly supervise their patients' states without direct contact.
- **Data-Driven Insights:** The connectivity of IoT devices with analytical applications enables doctors to come up with findings from different aspects of a patient's health.

Results of this implementation:

- **Expanded Access to Care:** The patient in remote regions is taken care of through the provision of healthcare facilities hence being able to access quality healthcare services without having to move.
- **Cost Savings**: There is improvement in the frequency of hospital appointments and admissions hence cutting the costs of both the individual and healthcare entities.
- **Enhanced Patient Satisfaction:** From the patient's perspective, the use of telemedicine services is convenient and easily accessible hence enhancing patients' experience.

10.6 LESSONS LEARNED AND BEST PRACTICES

Lesson 1: Prioritize Data Security and Privacy

It is a requirement to secure the data and personal information of the customers. Best practices include:

- **Implement Strong Encryption:** All information that is sent and received should be encrypted to minimize the cases of leakage in case of an attack.
- **Adopt Robust Access Controls:** Make certain that some key information in the health environment should not be accessed by everyone.
- **Regular Security Audits:** Security audits and updates should be conducted every now and then in order to check the level of weaknesses.

Lesson 2: Ensure Interoperability

This means that the IoT ecosystem involves a connection of devices and systems and thus the need to ensure that devices and systems are compatible. Best practices include:

- **Standardization:** Have agreed standards when communicating and the structure of data to be exchanged to encourage interlinking.

- **Use Integration Platforms:** Use applicable systems whereby the transfer of information between the two systems will be optimized.
- **Collaborate Across the Ecosystem:** Coordination with the makers of the associated devices and the software as well as healthcare organizations for integrated products.

Lesson 3: Focus on User-Centric Design

Therefore, accessibility to IoT mobility and its acceptance by consumers is important for succeeding IoT solutions. Best practices include:

- **User-Friendly Interfaces:** Web designs, gadgets, and any kind of applications have to be designed with interfaces that are easy to navigate.
- **Comprehensive Training:** Ensure rushed and tired clinical personnel and patients cope well with the technology through proper orientation on how to operate it.
- **Clear Communication of Benefits:** Illustrate the theme of how to get IoT solutions adopted in order to engage by showing the worth of solutions.

Lesson 4: Compliance with Regulatory Standards

Some areas are regulation and legal compliance, which is rather important. Best practices include:

- **Stay Informed:** Meet the rules and guidelines applicable to the healthcare IoT environment.
- **Clear Data Ownership Policies:** There should be exact regulatory guidelines on who actually owns the data and patients must give consent in advance.

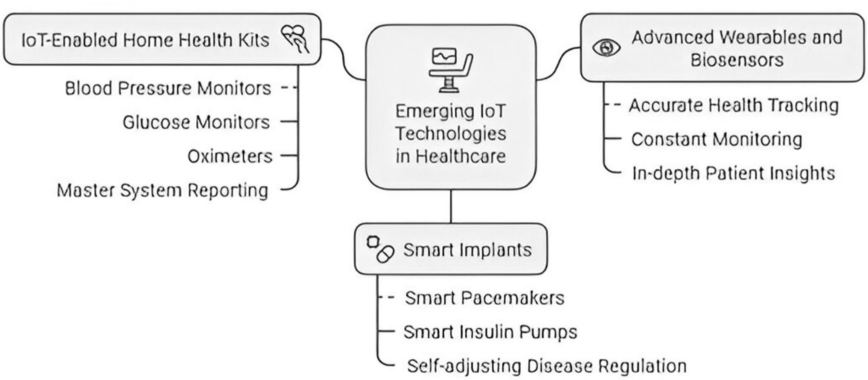


FIGURE 10.4 Future trends

- **Liability and Accountability:** Specify precise lines of responsibility and fault when devices fail or data gets compromised.

Examples of successful implementation of IoT technologies in healthcare settings include Mayo Clinic, Cleveland Clinic, and Mercy Virtual. The goal of using IoT to advance the delivery of healthcare services will be realized when there is a commitment to protecting data, promoting the standards of interoperability, creating solutions that enhance the users' experience, and meeting compliance standards. The latter not only outlines best practices and lessons learned indicating the general course toward a more/integrated, client-centered, and efficient healthcare framework.

10.7 FUTURE TRENDS AND OPPORTUNITIES

10.7.1 Emerging IoT Technologies and Their Impact on Healthcare

Based on the advancements of IoT technologies, its relevance to healthcare is anticipated to go deeper as a source of innovation and enhancement of better patient care and health system operation. Figure 10.4 shows, some emerging IoT technologies, and their potential impacts including:

- **Advanced Wearables and Biosensors:** The subsequent generation of wearable devices and biosensors will enable more accurate and elaborate tracking of the health indices. Such assumptions will allow for constant tracking of not only more parameters but also many more, allowing health professionals to get more in-depth pictures of their patients' conditions and act before things worsen.
- **Smart Implants:** Implantable IoT devices such as smart pacemakers, and smart insulin pumps will give real-time monitoring of the chronic conditions and would also be able to self-adjust the pace of regulating the diseases. These devices should directly speak to the health care providers, so that, any detected problems are promptly addressed.
- **IoT-Enabled Home Health Kits:** Health kits for homes that contain more than one IoT device will enable a patient to monitor their health more effectively from home. These kits could be a blood pressure monitor, glucose monitor, oximeter, and other related gadgets that are connected to a master system that reports to the doctors.

10.7.2 Integration of IoT with Other Disruptive Technologies

The integration of IoT with other disruptive technologies will create synergistic effects, further transforming healthcare delivery:

- **5G Connectivity:** 5G network solutions will greatly improve the IoT used in healthcare by delivering higher and more reliable connection speeds and lower latency. This will allow for the actual-time transfer of information that facilitates sensible operation such as remote surgery and real-time telemedicine consults, and better distant tracking.

- **Blockchain:** Embarking IoT with a blockchain system will improve its security, confidentiality, and credibility. Thus, the use of the technology can create a secure and unalterable system of records that health data belongs to or that can work as a key providing access to certain types of data. The following can enhance the level of trust and user adherence in the handling of health information.
- **Robotics:** Implementation of IoT and robotics can help in increasing the accuracy of surgeries, reducing the role of human intervention in monotonous tasks, and patient care solutions. For instance, IoT-integrated operating theatres are capable of delivering highly sensitive surgery through the use of data received from several sensors and imaging tools.
- **AI and ML**: IoT with AI and ML will allow for deeper and more analytical patterns and predictions in data and decision-making. Integration of the IoT with analytics powered by AI can reveal patterns and trends concerning the big data collected by IoT, which can be applied to developing individual therapy plans as well as forecasting when medical equipment requires maintenance.

10.7.3 Personalized and Precision Medicine Enabled by IoT

Devices including connected sensors will prove to be instrumental in the further development of personal and precision medicine, which target different characteristics of patients. Key opportunities include:

- **Genomic IoT Devices:** Personalized tools that could analyze and interpret genes will help doctors in the determination of treatment options depending on the patient's genotype. This can assist in determining the relevant treatments, if any, and preventative measures concerning each particular patient.
- **Real-Time Health Data Integration:** Incorporating real-time data from wearable IoT devices; patients' vital signs, behaviors, and factors in the environment they operate in will afford a complete picture of a patient's health. The above data will also promote precision medicine as the detailed results will help in providing accurate diagnosis as well as treatment.
- **Dynamic Treatment Adjustments:** The integration of IoT in healthcare systems makes it possible to observe patients' reactions to the prescribed treatments and alter the therapies as often as necessary. For example, smart drug delivery systems can adjust the concentrations of delivered medications in response to signals provided by biosensors in real time to ensure that therapeutic outcomes are maximized and therapies' toxicities are reduced.
- **Predictive Health Management:** In this segment, it is possible for healthcare givers to use analysis of data obtained from various IoT devices to evaluate the likely health trends or risks of the patient. Clinical intervention is excellent as it helps in early prevention hence the enhancement of a healthier lifestyle.

Various discussions indicate that the future of healthcare will be revolutionized by IoT and related innovative solutions. Integrated wearables for the patient, smart implantable devices, and IoT home health kits will improve the efficiency of patient care. There are notable growth prospects for healthcare from IoT, 5G, blockchain, robotics, and AI, where the system will enhance the delivery of healthcare, particularly through IoT & 5G networks, blockchain for security and personalized robotics, and AI for efficiency. Healthcare IoT will drive precise, targeted treatment, and earlier intervention with treatment measures, both goals that focus on the patient and the patient's health at the center of attention. As these trends and opportunities expand, the healthcare sector opens up for a revolutionary age fuelled by the adoption of technologies.

10.8 CONCLUSION

Healthcare 5.0 with the IoT joining the field of healthcare this year, the latest in medical practices, promises even more significant progress. This change is about actual time, data analysis, cool technology, smart devices, smooth interconnected patient care, the manner in which health is delivered, and various processes. This results in the efficiency of everything involved in healthcare, and IoT in its essence is a network of devices and systems used to cope with chronic diseases, monitor health ceaselessly, etc. Wearable or smart apparel, biosensors smart medical equipment, and remote patient monitoring help the patients or the healthcare individuals to have the health information with them at early stages and make it more patient-centric.

But hold your horses! Employing IoT in healthcare is not all upside. Since data may contain personal information for the users, it becomes essential that the data is protected from hackers and hence needs to be encrypted and restricted to a few people depending on the laws. In its current state, IoT means different tech and devices must work in harmony with one another. Furthermore, training the people and ensuring that they know the usefulness of the IoT techs through training and making the models as simple as possible is essential to gaining people's support. The future appears to be very promising when it comes to IoT applications in the healthcare industry! Estates, flashy accessories, and tiny healthcare kits might change the way patients are taken care of a great deal. Combining IoT with more technologies such as 5G, blockchain, robots, and AI may cause some cool shifts in telemedicine, precision medicine, and forecasting health requirements.

In the subsequent days, as IoT in healthcare gets more glamorous by the minute, a coordinated yet humanistic healthcare system that utilizes real-time data and glamour analytical instruments to convey customized care will be experienced. An emphasis will be placed on the individual approach as the specificity of each patient will finally provide better outcomes as a rule. The road to adopting IoT in Healthcare 5.0 is full of twists and turns but perks as well! There are solutions to these challenges, when all the above challenges are dealt with innovatively and when all the standards are followed closely – we can harness the full benefit of IoT to deliver very effective, tailor-made care to all of us as we are led to better health status collectively.

Summary of Key Points

1. **Introduction to Healthcare 5.0 and IoT:** Healthcare 5.0 is a symbolic representation of a new era in medicine through the incorporation of IoT as one of the technologies. The integration of these principles will focus on augmenting individualized, preventive, and anticipatory patient care, clinical and administrative effectiveness, and overall healthcare.
2. **IoT Applications in Healthcare 5.0**
   - **Remote Patient Monitoring:** Remote surveillance of patients' health status hence is easily detected and addressed as they stay at home saving on the number of times they must be admitted.
   - **Wearable Devices and Sensors:** Equip people to monitor health standards in real-time 'increasing patients' awareness of their health status.
   - **Smart Hospitals and Clinics:** Implement IoT for patient tracking, intelligent beds, and connected medical equipment hence improving the hospital functionality and improved patient care.
   - **Telemedicine and Telehealth:** Provide remote consultation and virtual follow-up and increase the reach of the health care services especially in rural areas.
   - **Chronic Disease Management:** Through constant supervision, scheduling, and analysis of feedback the health of patients with chronic diseases is enhanced.
   - **Medication Management and Adherence:** Smart pill bottles and automated dispensing systems enhance patients' compliance with regard to medication plans and regimens.
3. **IoT-Enabled Healthcare Ecosystem**:
   - **Interconnected Devices and Systems:** An arrangement of devices that can interconnect for a complete solution to health problems.
   - **Data Collection and Analysis:** Real-time data interchange An integrative framework for knowledge processing in decision support and targeted treatment.
   - **Cloud Computing and Storage:** Mobile and web applications that support massive and easy accessibility of health-related information and technology-driven secure storage systems.
   - **Artificial Intelligence and Machine Learning:** Per case diagnostic and predictive analytics, big data, IoT, and other technologies improve treatment and administrative outcomes.
4. **Challenges and Considerations**:
   - **Data Privacy and Security:** Maintaining sound procedures for handling patients, employees, and other health information while following the set laws and policies.
   - **Interoperability:** Some of the key issues include implementing systems to ensure protocol of communication and compiling a network of systems that interact harmoniously.

   - **Regulatory and Legal Issues:** As with any public health intervention, there are also issues with health regulations, ownership of data, and handling of liability issues.
   - **User Acceptance and Adoption:** User interface design, recommended approach which includes training and showing the benefits of IoT solutions.
5. **Case Studies and Examples**:
   - **Mayo Clinic:** Experiences with a chronic patient concerning remote patient monitoring for chronic disease management.
   - **Cleveland Clinic:** Introducing and or enhancing smart technologies to be used in delivering quality patient care in hospitals.
   - **Mercy Virtual:** Development of technology services that increase the reachability of healthcare services in remote areas.

Future Outlook for IoT in Healthcare 5.0

Speculations on the further developments of IoT in Healthcare 5.0 are marked by continued innovation and integration with other advanced technologies, promising transformative changes in the healthcare industry:

1. **Emerging IoT Technologies:** There will be progression in wearables, biosensors, and smart implants for enhanced and accurate health monitoring resulting in early diagnosis and timely treatment.
2. **Integration with Disruptive Technologies**:
   - **5G Connectivity:** Greater intimacy will facilitate faster transfer of actual-time data and complicated applications such as operation from a distance and more.
   - **Blockchain:** Better protection of the data through the distribution of health management across networks.
   - **Robotics:** Greater accuracy in the surgical procedures that are performed and also increased mechanization of processes, which increases productivity within facilities.
   - **AI and Machine Learning:** 'Smart' management of patient data and extraction of analytical and predictive patterns to design treatment regimens and preventive health care systems.
3. **Personalized and Precision Medicine**: IoT will also be seen to have an influential position in the future development of healthcare, especially through the concepts of precision and personalized medicine that will be in a position to customize care delivery through genomic IoT devices, real-time data integration in healthcare, dynamic treatment plans, and predictive healthcare.

Therefore, the use of IoT to advance the Healthcare 5.0 ecosystem will keep on developing, affording incomparable approaches to enhance patient care, operational effectiveness of healthcare systems, and healthcare delivery. With the continuation of these evolutions and improvements in these aforementioned technologies in healthcare, the world is already on the cusp of a more integrated, convenient, and patient-oriented medical world (Table 10.2).

REFERENCES

1. Mohanta, Bhagyashree, Priti Das, and Srikanta Patnaik. "Healthcare 5.0: A paradigm shift in digital healthcare system using artificial intelligence, IOT and 5G communication." In *2019 International Conference on Applied Machine Learning (ICAML)*. IEEE, 2019.
2. Chi, Hao Ran, et al. "Healthcare 5.0: In the perspective of consumer internet-of-things-based fog/cloud computing." *IEEE Transactions on Consumer Electronics* 69(4), 745–755 (2023).
3. Mbunge, Elliot, Benhildah Muchemwa, and John Batani. "Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies." *Global Health Journal* 5(4), 169–177 (2021).
4. Khan, Tahir Abbas, et al. "Secure IoMT for disease prediction empowered with transfer learning in healthcare 5.0, the concept and case study." *IEEE Access* 11, 39418–39430 (2023).
5. Wazid, Mohammad, et al. "Healthcare 5.0 security framework: applications, issues and future research directions." *IEEE Access* 10, 129429–129442 (2022).
7. Singh, Gyaneshwar, et al. "Blockchain-based access control architecture for enhancing authorized E-healthcare data sharing services in industry 5.0." *IEEE Transactions on Consumer Electronics* (2024).
6. Saraswat, Deepti, Pronaya Bhattacharya, Ashwin Verma, Vivek Kumar Prasad, Sudeep Tanwar, Gulshan Sharma, Pitshou N. Bokoro, and Ravi Sharma. Explainable AI for healthcare 5.0: Opportunities and challenges. *IEEE Access* 10, 84486–84517 (2022).
8. Rejeb, Abderahman, Karim Rejeb, Horst Treiblmaier, Andrea Appolloni, Salem Alghamdi, Yaser Alhasawi, and Mohammad Iranmanesh. The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things* 22, 100721 (2023).
9. Basulo-Ribeiro, Juliana, and Leonor Teixeira. The future of healthcare with industry 5.0: Preliminary interview-based qualitative analysis. *Future Internet* 16(3), 68 (2024).
10. Parihar, Akshay, Jigna B. Prajapati, Bhupendra G. Prajapati, Binti Trambadiya, Arti Thakkar, and Pinalkumar Engineer. Role of IOT in healthcare: Applications, security & privacy concerns. *Intelligent Pharmacy* 2(5), 707–714 (2024). https://doi.org/10.1016/j.ipha.2024.01.003
11. Almotairi, K. H. Application of internet of things in healthcare domain. *Deleted Journal* 14(1), 1–12 (2022).
12. Kumar, Mohit, Ashwani Kumar, Sahil Verma, Pronaya Bhattacharya, Deepak Ghimire, Seong-heum Kim, and ASM Sanwar Hosen. Healthcare internet of things (H-IoT): Current trends, future prospects, applications, challenges, and security iIssues. *Electronics* 12(9), 2050 (2023).
13. Javaid, Mohd, and Ibrahim Haleem Khan. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *Journal of Oral Biology and Craniofacial Research* 11(2), 209–214 (2021).
14. Thottempudi, Pardhu, and Vijay Kumar. The role of IoT in modern healthcare: Innovations and challenges in pandemic era. In *Technologies for Sustainable Healthcare Development*, Advances in medical technologies and clinical practice book series (pp. 57–80). IGI Global, 2024.

15. Wasswa, Shafik. Connected healthcare—the impact of internet of things on medical services: Merits, limitations, future insights, case studies, and open research questions." In *Artificial Intelligence and Internet of Things based Augmented Trends for Data Driven Systems* (pp. 181–217). CRC Press, 2024.
16. Jambli, Mohamad Nazim, et al. "5G-enabled IoT applications in healthcare: Transforming the industry 5.0 healthcare landscape." *The Future of Human-Computer Integration* (pp. 110–120). CRC Press, 2024.
17. Taimoor, Najma, and Semeen Rehman. "Reliable and resilient AI and IoT-based personalised healthcare services: A survey." *IEEE Access* 10, 535–563 (2021).
18. Chander, Bhanu, et al. "Artificial intelligence-based internet of things for industry 5.0." In *Artificial intelligence-based internet of things systems* (pp. 3–45). Springer, 2022.
19. Tuppad, Ashwini, and Shantala Devi Patil. "Super-smart healthcare system in society 5.0." In *Society 5.0: Smart Future Towards Enhancing the Quality of Society* (pp. 209–227). Springer Nature Singapore, 2022.
20. Avcı, Yasemin Demir, and Sebahat Gözüm. "The impact of industry 5.0: The artificial intelligence, IoT and blockchain revolution in home healthcare." In *Industry 5.0 for Smart Healthcare Technologies* (pp. 62–76). CRC Press, 2024.
21. Wu, Chenggang, et al. "Healthcare 5.0: A secure and distributed network for system informatics in medical surgery." *International Journal of Medical Informatics* 186, 105415 (2024).
22. Singh, Prabhdeep, and Devesh Pratap Singh. "Role of disruptive technologies in the smart healthcare sector of society 5.0." In *Artificial Intelligence and Society 5.0* (pp. 143–153). Chapman and Hall/CRC, 2024.
23. Deep, Gagan, V. Jyoti, and S. Anjali. "Innovating healthcare: Synergistic integration of AI, IoT, and blockchain for sustainable and efficient smart healthcare solutions." In *Industry 5.0 for Smart Healthcare Technologies* (pp. 248–264). CRC Press, 2024.
24. Kumar, S. N., et al. "Industry 5.0 in the smart healthcare sector." In *Industry 5.0 for Smart Healthcare Technologies* (pp. 1–13). CRC Press, 2024.
25. Suriyan, Kannadhasan, and R. Nagarajan. "Role of internet of things: Challenges and opportunities." In *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security* (pp. 22–31), IGI Global, 2024.

11 Role of 5G in Healthcare 5.0

V. Lakshmi and Sujatha Rajkumar

11.1 INTRODUCTION

The evolution of wireless communication technology brings people closer even though they may be physically far away. This evolution began in the 1970s and continues to date. A decade is referred to as one generation in communication technology. Now we are in the fifth generation. In this chapter, we will discuss each generation in detail [1, 2]. Figure 11.1 illustrates the evolution from the first to the fifth generation of wireless communication technology.

In the swiftly evolving fields of technology and communication, various terminologies and abbreviations are frequently used in this chapter. Table 11.1 summarizes some of the key terms and their full forms, which are essential for understanding the nuances of modern technological advancements in Healthcare 5.0.

11.1.1 1G (First Generation, 1970s–1980s)

In the 1970s and 1980s, 1G, or the first generation of wireless communication technology, was unveiled. NTT introduced the first commercial 1G network in Japan in 1979, an analog system with a speed of 2.4 kbps that primarily supported basic voice communication, using FDMA access techniques and FM modulation. It was not supported for data transmission. The technology was limited, with low capacity, incompatibility between European systems, and no mobile-assisted handover. The standards included AMPS (USA), TACS (Europe), and NMT (Scandinavia), each with its own set of limitations which results in poor call quality and frequent call drops and prone to call interference. Considering its weaknesses, 1G technology set the stage for the creation of further wireless generations, that have evolved over time due to technological breakthroughs.

11.1.2 2G (Second Generation, 1990s)

The second generation of wireless communication technology was first released in the early 1990s, it marked a substantial advancement over 1G. By using digital signals for transmission, it introduced data services and enhanced call quality. GSM (global system for mobile Communications), which supported numerous users and

 DOI: 10.1201/9781003532286-11

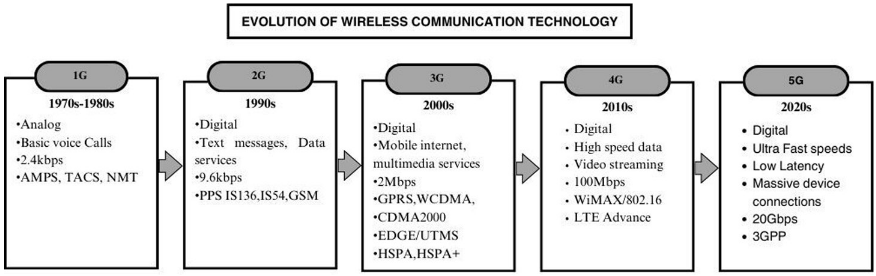


FIGURE 11.1 Evolution from the first to the fifth generation of wireless communication technology

data services, was the most extensively utilized 2G standard. Japan was the only country that used the 2G mobile telecommunications standard PDC (personal digital cellular). It was created as a competitor to NADC in Japan and was the primary standard used there until it was phased out in favor of 3G technologies such as W-CDMA and CDMA2000. Along with supporting circuit-switched data rates of up to 9.6 kbps and packet-switched data rates of up to 14.4 kbps, 2G systems also brought basic data services such as MMS and SMS and enabled internet access via WAP (wireless application protocol).

11.1.3 3G (Third Generation, Early 2000s)

The third generation of wireless communication technology, 3G, commenced in the early 2000s, advancing with a faster data transfer rate of 144 kbps by means of packet switching technology for the improvement and better voice quality compared to 2G and 2.5G networks. Different services benefited people around the world such as video calls, mobile TV, mobile broadband access, and improved voice quality. There was also a focus on the security of the data in transit which led to end-to-end encryption. To attain 3G technology, 2G was upgraded gradually to 2.5G and 2.75G, before it attained 3G. Enhanced data rates for GSM evolution networks were created, offering faster data transfer rates and better voice quality. It is based on a set of standards used for mobile devices and mobile telecommunications services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications set by the International Telecommunication Union. The UMTS (Universal Mobile Telecommunications System), standardized by 3GPP in 2001, was used in Europe, Japan, China (with a different radio interface), and other regions that had predominantly GSM-based 2G infrastructure. Meanwhile, the CDMA2000 system, standardized by 3GPP2 and first offered in 2002, was primarily used in North America and South Korea. The latest UMTS release, HSPA+, provided peak data rates of up to 56 Mbps downlink and 22 Mbps uplink, while CDMA2000's release, EVDO Rev.B, offered peak rates of 14.7 Mbps downlink. These advancements played a profound role in changing mobile connectivity and setting the stage for a future where mobile internet is indispensable.

TABLE 11.1
Evolving Connectivity in Healthcare: A Comparative Insight into Fourth- and Fifth-Generation Communication Systems, Challenges Faced, and Advantages Realized

Feature	4G	5G	Challenges of 4G	Advantages of 5G
Data Transmission and speed	Up to 100 Mbps	Up to 1 Gbps	Limited bandwidth, high latency	Faster data transfer, improved patient care
Latency	20–50 ms	1 ms	High, limited	Real-time communication, improved patient outcomes
IoT Support	Limited	Massive machine type communication (mMTC)	Limited scalability, high maintenance costs	Supports a large number of devices, improved healthcare operations.
Teleconsultation	Limited	Enhanced mobile broadband (eMBB)	Limited coverage, High latency	Improved remote consultations, enhanced patient care
Robot-Assisted Services	Limited	Time-sensitive networking (TSN)	Limited integration, high maintenance costs	Improved automation, enhanced patient care
Connected Ambulances	Limited	High-definition cameras, VR headsets	Limited range, high latency	Improved real-time monitoring and communication
Security	Limited	Enhanced security features	Limited security measures, high risk of data breaches	Improved data protection, enhanced patient care
Cost	High	High	High implementation costs, limited accessibility	Improved healthcare operations, enhanced patient care

11.1.4 4G (Fourth Generation, Late 2010s)

In the late 2010s, wireless communication technology evolved to its fourth generation, 4G. This technology used even faster data transmission speeds to support video streaming with high quality and additionally bandwidth-intensive applications. Key features of 4G include faster data transmission speeds, which enable users to stream high-definition video and use other bandwidth-intensive applications. 4G used LTE (long-term evolution) technology, which provided faster data transmission speeds and lower latency. Additionally, 4G enabled users to access mobile broadband services, which provided faster internet access and improved overall network performance. The downlink peak data rate for 4G was approximately 100 Mbps, making it significantly faster than its predecessors.

11.1.5 5G (Fifth Generation, 2020s)

In 2020 the fifth generation, 5G, evolved. 5G offers significantly faster speeds (up to 20 Gbps), lower latency (as low as 5 ms), and greater bandwidth compared to its predecessors, enabling the development of new and broad-ranging applications and use in services across numerous industries, such as IoT, industrial automation, gaming and entertainment, healthcare and telemedicine, transportation and autonomous vehicles, and smart cities and infrastructure [3, 4]. 5G networks use techniques such as 5G New Radio, cell sites, small cells, and millimeter wave (mmWave) spectrum to provide coverage and capacity, and are designed to be software-defined and virtualized for greater flexibility and scalability, with advanced technologies such as massive MIMO and edge computing to improve performance. Commercial 5G services began rolling out in 2019, with major carriers deploying 5G networks in different countries, offering various types of services including 5G cellular and private 5G [5].

11.2 ARCHITECTURE OF 4G LTE(LONG TERM EVOLUTION)

Figure 11.2 shows the 4G LTE network architecture, comprised of two sections E-UTRAN (evolved universal terrestrial radio access network) and EPC (evolved packet core). The user's equipment connects to the network through the eNode at the base station, comprised of remote radio units and baseband units; these components are connected by means of backhaul and fronthaul links. The EPC includes the mobility management entity (MME) which handles user mobility, the service gateway (SGW), which routes data packets, and the packet data network gateway (PGW), which connects to external networks such as the internet. External networks include the internet message service (IMS), which handles the multimedia services over an IP network, bridging to both the public switched telephone network (PSTN) and the wider internet. This architecture ensures seamless communication across various network elements for optimal connectivity and service distribution.

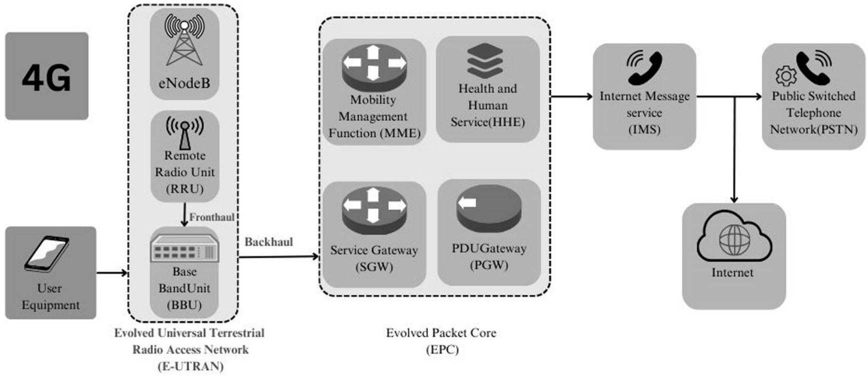


FIGURE 11.2 Architecture of a 4G network

11.3 ARCHITECTURE OF 5G NEW RADIO (NR)

Figure 11.3 illustrates the architecture of the 5G network, detailing the connection from user equipment (UE) to the active antenna unit (AAU) responsible for radio frequencies. The distributed unit (DU) oversees real-time operations such as scheduling, while the centralized unit (CU) manages non-real-time functions. Fronthaul links connect the AAU to the DU, and the midhaul links connect the DU to the CU, enabling smooth data flow. The virtualized edge, featuring the user plane function (UPF), processes data closer to users to minimize latency. The virtualized core network includes elements such as access and mobility management function (AMF) for mobile control, session management function (SMF) for session regulation,

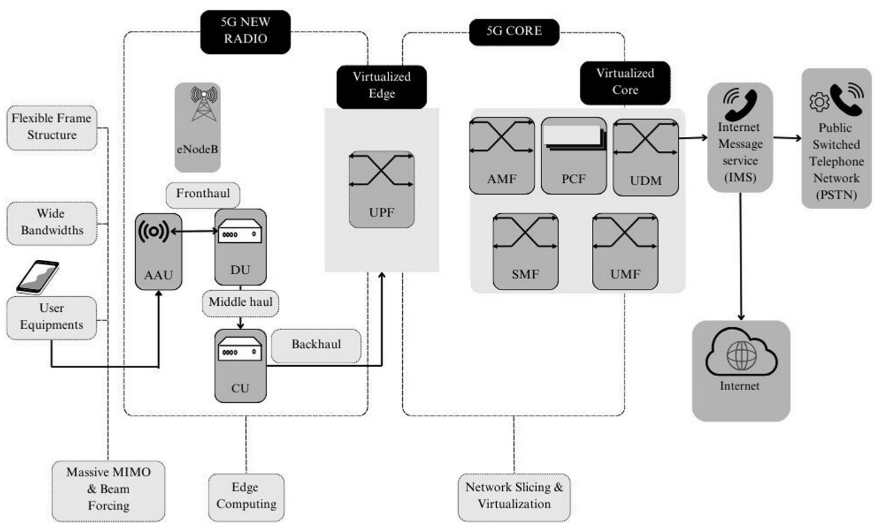


FIGURE 11.3 Architecture of a 5G network

policy control function (PCF) for policy enforcement, unified data management (UDM) for storing subscriber data, and another UPF for data handling. External networks such as the internet, internet message service (IMS) for multimedia, and the public switched telephone network (PSTN) for traditional telephone calls are connected to the system. Enhanced features such as flexible frame structures, wide bandwidths, massive MIMO and beamforming, edge computing, network slicing, and virtualization provide high speed, low latency, and reliable connections vital for Healthcare 5.0.

11.3.1 Edge Computing

Instead of transferring data to a central server or cloud, edge computing processes it locally. As a result, there is less latency, faster processing, and better real-time data processing. Stated differently, edge computing processes data at the point of creation rather than sending it to a remote server or cloud. This reduces latency, accelerates the process, and improves real-time data processing. Imagine having a little data center next to your wearables, sensors, or smart gadgets. They can work quicker and more consistently with this configuration. In healthcare, this is crucial for quick data analysis and immediate responses.

11.3.2 Frequency Ranges

Most 4G networks operate in frequency bands below 6 GHz. These lower frequency bands give good coverage, but they have limited bandwidth. In contrast, 5G networks encompass a wider range of frequencies, including lower frequency bands under 6 GHz, mid-range bands between 1 GHz and 6 GHz, and high-frequency bands (millimeter-wave frequencies) more than 24 GHz. The latter high-frequency bands allow for substantially more bandwidth and capacity, but they have a shorter range and need more advanced antenna technology.

11.3.3 Data Capacity and Speed

4G networks deliver high-speed mobile data with theoretical maximum download speeds reaching several hundred megabits per second. The actual user experience, however, can fluctuate based on factors such as network congestion and signal strength. In comparison, 5G networks boast much higher data rates and improved network capacity. They can achieve multi-Gbps peak data rates, facilitating remarkably fast downloads and uploads. Additionally, 5G networks can accommodate a vast number of IoT devices and sensors simultaneously.

11.3.4 Response Time or Latency

Latency in 4G networks generally falls within the range of tens to several tens of milliseconds. Although this latency is adequate for many applications, it may not satisfy the needs of highly sensitive latency applications. On the other hand, 5G networks are designed to achieve ultra-low latency, aiming for targets as low as 1 ms. This almost instantaneous responsiveness is essential for applications such as autonomous vehicles, remote surgeries, and industrial automation.

11.3.5 Virtual Network Solution

4G networks lack the capability for network slicing, a feature that enables the formation of multiple virtual networks on a single physical infrastructure. This limitation restricts the optimization of network resources and performance for specific applications. In contrast, 5G networks incorporate network slicing as a fundamental architectural feature. This innovation allows for the creation of dedicated, isolated virtual networks tailored to unique service requirements, delivering customizable performance, enhanced security, and specific service level agreements (SLAs).

11.4 5G IN HEALTHCARE 5.0

Wearable technology or remote patient monitoring can be used by healthcare practitioners to continually gather, report, and transmit crucial information to a remote monitoring center, the 5G network has a 100 times greater ability to interface with IoT devices over 4G networks. Figure 11.4 highlights the key components of 5G technology [6]. Enhanced mobile broadband (eMBB), massive machine-type communication (mMTC), and ultra-reliable low-latency communication (URLLC) are the three most significant components. These overviews how 5G technology underpins

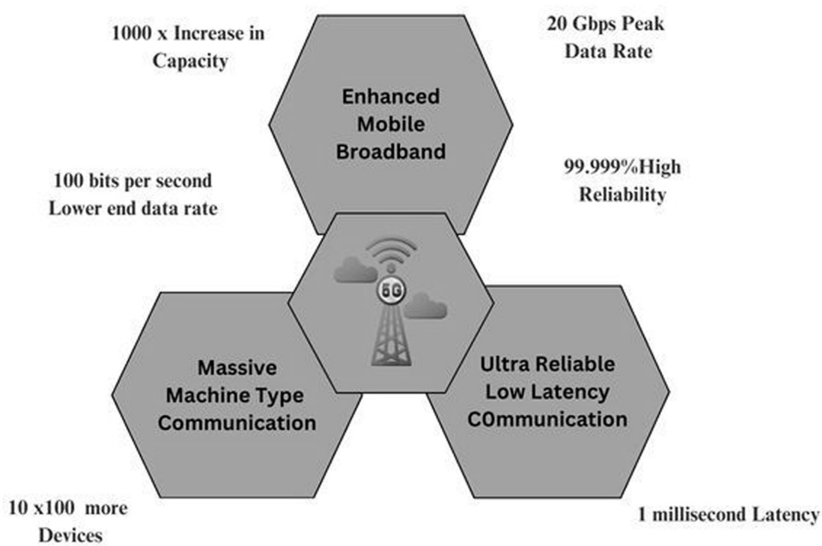


FIGURE 11.4 Significant components of 5G technology

cutting-edge applications, particularly in Healthcare 5.0, enabling innovative solutions and improved patient outcomes.

11.4.1 Ultra-Reliable Low-Latency Communication in 5G Networks

Ultrareliable low-latency communication (URLLC) is a main technology feature in 5G networks, intended to facilitate the transmission of mission-critical data with exceptional reliability and minimal latency. This capability is essential for applications such as remote surgery, autonomous vehicles, and real-time control systems, where quick and reliable data delivery is paramount.

11.4.1.1 Key Features and Techniques

URLLC achieves low latency typically less than 1 ms and a packet error rate below 10^{-5}, enabling the rapid and accurate transmission of critical messages even in scenarios where failure is unacceptable. To ensure seamless connectivity, techniques such as the dual active protocol stack (DAPS) handover allow for smooth transitions between cells, maintaining a stable connection without latency increases. Advanced methods employed in URLLC include sophisticated modulation techniques, such as differential and coherent modulation, alongside effective coding strategies. Network slicing enables dedicated communication channels, while guaranteed bit rates allow applications to reserve specific bandwidth and maintain consistent data transmission rates.

11.4.1.2 Redundancy Techniques for Reliability

Redundancy techniques are vital for maintaining high reliability and data integrity within the URLLC framework. Key methods include:

- **Hybrid Automatic Repeat Request (HARQ):** Combines error detection with retransmissions to enhance data reliability.
- **Incremental Redundancy (IR):** Sends additional bits to recover lost or corrupted data.
- **Soft Combining:** Merges multiple packet transmissions to improve overall signal quality.

11.4.2 Massive Machine-Type Communication in Healthcare 5.0

Massive machine-type communication (mMTC) plays a vital role in ensuring efficient and reliable connectivity for a vast array of IoT devices, particularly in high-density environments. By deploying several key techniques, mMTC enhances the functionality of diverse healthcare applications [7].

11.4.2.1 Key Techniques for Enhanced Connectivity

Narrowband IoT (NB-IoT) leverages a narrow bandwidth to sustain a large number of low-power devices, allowing them to operate effectively even in challenging conditions. Coverage enhancement (CE) significantly improves signal quality and device connectivity in hard-to-reach areas, such as deep inside buildings or in rural settings [8]. Additionally, efficient signaling protocols minimize the communication overhead, enabling smooth data transmission for numerous devices. resource management algorithms dynamically allocate network resources to optimize performance and prevent congestion, while power-saving modes such as extended DRX (eDRX) and power saving mode (PSM) help devices minimize power consumption while maintaining connectivity.

11.4.3 Transforming Healthcare Applications

These techniques allow mMTC to provide large-scale remote patient monitoring, allowing physicians to observe vital signs, ECGs, and other health information in real time. mMTC facilitates seamless communication among medical devices, including insulin pumps, pacemakers, and implantable cardioverter-defibrillators (ICDs). Furthermore, it improves connection for a variety of wearable devices, including trackers for fitness, smartwatches, and wellness monitors, promoting proactive health management [9]. In addition, mMTC plays a crucial role in advancing telehealth services by enabling video consultations, remote assessments, and virtual healthcare coaching. The deployment of IoT devices within healthcare facilities is also bolstered, with applications such as temperature, moisture, and air quality monitoring, all contributing to a more responsive and efficient healthcare ecosystem. In summary, mMTC represents a transformative force in Healthcare 5.0, ensuring that a multitude of IoT devices can operate seamlessly, reliably, and efficiently within the healthcare sector.

11.4.4 Enhanced Mobile Broadband (eMBB)

Enhanced Mobile Broadband (eMBB) is a vital feature of 5G technology that delivers more rapid data rates, higher capacity, and improved network efficiency, significantly transforming healthcare services in the context of Healthcare 5.0. eMBB enables high-speed connectivity essential for applications requiring rapid access to large datasets, such as high-definition medical imaging and telemedicine tools, which enhance patient experiences by allowing timely consultations with specialists regardless of geographical barriers. It supports mobile health (mHealth) applications that process large volumes of data quickly for actual-time monitoring of bodily functions and access to electronic health records (EHRs) while facilitating remote diagnostics by transmitting high-resolution imaging data for rapid analysis. Healthcare providers can also leverage eMBB for streaming live surgeries to training sessions, enhancing education and collaboration, and ensuring timely access to critical information in emergencies. Furthermore, eMBB promotes the interoperability of connected medical devices within the medical equipment connected to the internet, facilitating seamless communication crucial for remote monitoring and smart hospital systems. Nevertheless, challenges remain, such as data security issues regarding sensitive health information, ensuring reliable connectivity in less robust infrastructure areas, and the complexities of integrating new eMBB-enabled solutions with legacy systems. The overall implications of 5G on healthcare are profound, with eMBB enabling faster teleconsultations, real-time health monitoring, and connected ambulance services, while network slicing provides dedicated networks for critical applications, enhancing reliability and security. Increased efficiency and automation lower inventory levels and enhance patient experiences, transforming healthcare by supporting the use of IoT devices for real-time monitoring, which improves patient care, reduces costs, and enhances the overall healthcare experience.

11.4.5 Wearables in Healthcare 5.0

The field of healthcare has undergone a significant transition with the introduction of wearable devices. These innovative devices, equipped with enhanced sensors and accessibility have the ability to revolutionize patient monitoring, diagnosis, and treatment as shown in Figure 11.5. From tracking vital signs to enabling remote patient care, wearable devices are reshaping the landscape of healthcare delivery [10, 11]. A wearable spirometer is a device that measures lung function and can be used to track patients with respiratory conditions such as asthma or COPD. It can be worn on the wrist or as a patch on the chest, providing continuous monitoring and early detection of any respiratory distress.

A glucose monitor is a device that measures blood sugar levels, making it ideal for overseeing patients with diabetes. It can be worn on the wrist or applied as a patch on the skin, facilitating real-time monitoring and improved condition management. Similarly, a wearable blood pressure monitor assesses blood pressure and is designed for patients with hypertension. This device can be worn on the wrist or as an arm patch, providing healthcare providers with essential data to refine treatment plans.

A wearable oxygen saturation monitor evaluates oxygen levels in the blood and is beneficial for patients with respiratory issues such as COPD. This device can be worn on the wrist or as a finger patch, allowing for early detection of oxygen-related problems. Additionally, a wearable pulse monitoring system measures heart rate and aids in supervising patients with cardiovascular conditions. It can be worn on the wrist or as a patch on the chest, delivering real-time data to healthcare providers. A wearable body temperature sensor monitors body temperature and is advantageous for patients experiencing fever or other temperature-related concerns. It can be worn on the wrist or applied as a patch on the skin, enabling early detection and prompt intervention. An activity-tracking sensor records physical activity levels and targets patients with sedentary lifestyles. This can be worn on the wrist or as a skin patch, encouraging healthier habits among patients. Lastly, a range of motion sensors monitors joint movement and helps in assessing patients with musculoskeletal issues. It can be worn on the wrist or as a skin patch, providing valuable information for rehabilitation and recovery.

An assessment sensor is a device that measures various physiological parameters, including heart rate, blood pressure, and oxygen saturation. It can be worn on the wrist or applied as a skin patch, facilitating comprehensive health monitoring. An ECG patch is utilized to observe heart rhythm and is designed for individuals with heart-related issues. It can be placed on the chest or offered as a skin patch, enabling

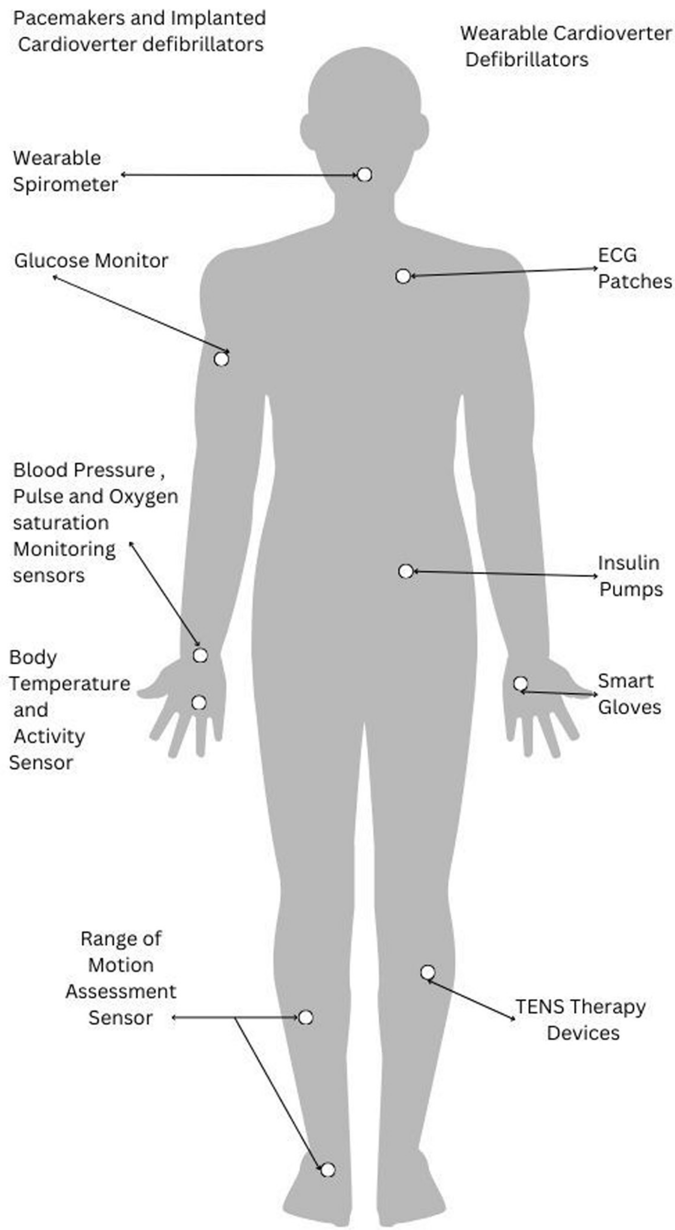


FIGURE 11.5 Wearable devices in healthcare: transforming patient monitoring and care

continuous observation and timely identification of any cardiac concerns. An insulin pump is a device that administers insulin to individuals with diabetes. It can be worn on the body or as a patch on the skin, providing a more convenient and effective method for managing the condition. A TENS (transcutaneous electrical nerve stimulation) therapy device delivers electrical impulses to the body for pain relief. It can be worn on the wrist or applied as a patch on the skin, offering a non-invasive approach to pain management. Smart gloves monitor hand movement and are suitable for evaluating individuals with musculoskeletal disorders. They can be worn on the hand, yielding valuable data for rehabilitation and recovery. A pacemaker regulates heart rhythm and supports individuals with heart-related issues. It can be implanted in the chest, offering a long-term solution for heart problems. An implanted cardioverter defibrillator also manages heart rhythm and is used for patients with heart conditions. This device can be implanted within the chest, providing a more advanced option for cardiac issues. A wearable cardioverter defibrillator similarly regulates heart rhythm and is intended for patients with heart concerns. It can be worn on the body, offering a more portable and accessible alternative for heart-related treatment. A folder monitor assesses muscle activity and is useful for tracking individuals with musculoskeletal conditions. It can be worn on the wrist or as a skin patch, providing essential information for rehabilitation and recovery.

The incorporation of these wearable devices into the healthcare ecosystem is likely to change how patient monitoring, assessment, and management are conducted. By providing real-time data, facilitating remote care, and encouraging patients to take a greater role in their health, wearable technologies are on the verge of transforming healthcare as we know it.

11.5 Healthcare 5.0 Use Cases

The healthcare sector is on the brink of a groundbreaking transformation, driven by the arrival of fifth-generation (5G) wireless technology. 5G is set to redefine the delivery of healthcare services, facilitating innovative applications that were once deemed impossible. This section delves into the substantial influence of 5G on the healthcare landscape, emphasizing the critical use cases that are designed to reshape the future of medical care.

11.5.1 Connected Ambulance

One of the most impactful applications of 5G in healthcare is the connected ambulance. This technology allows for instantaneous assessment of patients' health metrics, empowering medical professionals to make well-informed decisions before the ambulance arrives at the hospital. With low-latency, high-speed communication facilitated between ambulances, healthcare facilities, and medical staff, seamless collaboration and decision-making can occur. Ambulances connected via 5G feature advanced medical gear, patient monitoring systems, and telemetry devices that convey health information to the hospital in real time. They also include onboard cameras that deliver live visual feeds, allowing remote specialists to provide guidance during critical procedures. Moreover, 5G-connected ambulances can dramatically enhance patient care, particularly in emergency scenarios. This technology facilitates advanced healthcare from the moment a patient is encountered until they arrive at the hospital and enter the emergency room. It also streamlines response times in urgent situations, leading to timely and efficient patient care while alleviating some of the administrative burdens on healthcare providers. In India, 5G-connected ambulances have been successfully deployed, with Apollo Hospitals introducing them in various cities, including Bengaluru and Kolkata, to enhance emergency response capabilities. HealthNet Global has collaborated with Apollo Hospitals to launch these ambulances, allowing for immediate monitoring and communication between ambulances and hospitals. Thus, 5G-connected ambulances represent a revolutionary advancement in medical care, transforming real-time communication among ambulances, hospitals, and medical professionals, and aiming to improve patient care in critical moments.

11.5.2 Augmented Reality/Virtual Reality

The convergence of 5G, augmented reality (AR), and virtual reality (VR) is transforming the healthcare landscape by revolutionizing medical training and education, enhancing assessment and care planning, advancing remote care and telemedicine, and alleviating discomfort and anxiety for patients. The high-speed, low-latency capabilities of 5G facilitate immersive AR/VR experiences for healthcare professionals, allowing them to practice intricate medical procedures within safe, virtual environments, thereby enhancing their skills and expertise. Moreover, AR/VR technologies supported by 5G permit physicians to visualize complex anatomical structures in three dimensions, aiding in assessment and care strategies. This is accomplished by superimposing medical data, such as MRI and CT scans, onto a patient's body, which assists practitioners during procedures. Additionally, 5G-powered AR/VR can deliver high-quality, real-time video consultations and remote patient monitoring, thereby enhancing healthcare accessibility for individuals in rural or underserved regions. The seamless integration of 5G, AR/VR, and edge computing fosters instantaneous communication and data transmission among devices, medical equipment, and healthcare providers, simplifying remote collaboration and decision-making. This technology can also ease discomfort and anxiety for terminally ill or severely ill patients by providing soothing, distracting content. Overall, the combination of 5G, AR, and VR is revolutionizing the healthcare sector by enhancing medical training, advancing assessments and care, widening access to services, and enriching patient experiences. According to Verizon's Business Resources, the advanced visualization features of 5G can elevate patient care by allowing medical professionals to see complex anatomical structures in 3D. A study by health smart Taiwan (HST) outlines the capability of 5G-powered AR/VR to enhance diagnostic precision and minimize treatment errors. AT&T forecasts that 5G will enhance AR/VR for healthcare by promoting high-quality video consultations and remote patient monitoring. Tecknexus asserts that 5G will transform various sectors, including healthcare, through the integration of AI and AR/VR. Additionally, edge computing plays a vital role in optimizing the performance of AR/VR applications by facilitating data management closer to the user [12–16].

11.5.3 Telemedicine and Remote Consultations

The growth of 5G technology will transform telemedicine and healthcare delivery by providing low latency, high-speed internet access, and increased bandwidth. This development will facilitate real-time remote patient oversight, remote surgical procedures, and enhanced patient care. With the advantages offered by 5G, physicians will have the capability to oversee patients from a distance and conduct surgeries in real time, significantly improving the quality of care. The augmented bandwidth from 5G allows for the efficient transfer of substantial data volumes, including medical images and videos, thereby enhancing remote patient care by enabling physicians to access and analyze information swiftly. Additionally, 5G will revolutionize emergency management in smart cities through instantaneous communication and data exchange, enhancing response times and patient care quality. Data analytics will also see a boost from 5G, allowing for the collection and interpretation of large datasets to help healthcare providers make better-informed decisions. The enhanced mobile broadband (eMBB) aspect of 5G supports seamless video consultations between patients and healthcare practitioners, facilitating remote evaluations and treatment. This increases access to medical services, particularly for those in underserved or remote areas, while alleviating the strain on healthcare facilities.

11.5.4 Remote Patient Monitoring

The architecture of a 5G-driven remote patient monitoring (RPM) system involves several critical elements and technologies as shown in Figure 11.6. IoT devices and sensors, such as smartwatches or patches, track essential parameters such as heart rate, blood pressure, and glucose levels, along with sensors positioned at home or in medical facilities to observe patients' health states. The 5G network ensures high-speed, low-latency, and dependable internet access, allowing for seamless data transmission and real-time analyses.

Data from IoT devices and sensors is sent to centralized platforms for processing and evaluation, which can be integrated with electronic health records (EHRs) and

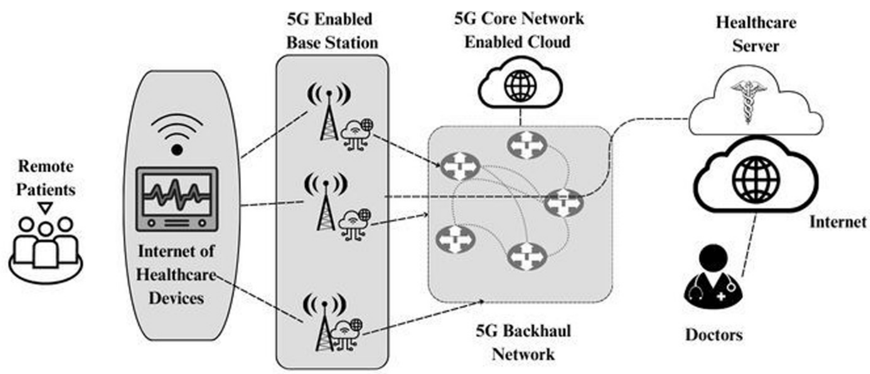


FIGURE 11.6 Architecture of 5G enabled remote patient monitoring system

various healthcare systems. Artificial intelligence (AI) and machine learning (ML) algorithms evaluate this information, identifying irregularities and alerting healthcare providers, as well as forecasting patient outcomes and suggesting personalized care plans. Patients can participate in video consultations with healthcare professionals through high-definition conferencing, which boosts engagement and reduces the necessity for in-person appointments. The analyzed data is visualized to give healthcare providers immediate insights into patient conditions, enabling more effective decision-making and improved health results. The 5G network also incorporates enhanced security measures, ensuring the confidentiality, integrity, and availability of patient data, with data encryption and secure storage being vital components of RPM systems. These systems are integrated into existing healthcare frameworks, such as EHRs and hospital information systems (HIS), allowing for smooth data sharing and coordination among various healthcare providers and facilities. Patients become active participants in their care through remote monitoring, fostering a proactive approach to health management, leading to better health outcomes and heightened patient satisfaction. Lastly, RPM systems are regularly evaluated and upgraded to assure optimal performance and patient health results [17, 18].

11.5.5 Remote Robotic Surgery

The 5G technology enables remote robotic surgery, allowing surgeons to perform procedures from a distance. Figure 11.7 shows the 5G-enabled remote robots which can perform surgery. This technology overcomes geographic constraints and provides access to specialized surgical expertise, even in remote or underserved areas [19–22]. Researchers in China have reported the first successful robot-assisted remote radical distal gastrectomy (stomach surgery) using 5G technology (International Telecommunication Union, 2007). The procedure was conducted with minimal delays and no packet loss, highlighting the viability and safety of 5G-powered remote surgery. The promising advantages of 5G remote robotic surgery include broadening the availability of advanced surgical treatments for patients in remote or underserved areas, enabling specialized surgeons to operate on patients situated far away, facilitating remote training and collaboration among healthcare professionals, and enhancing emergency response effectiveness (Healthcare in Europe, 2020). Nevertheless, there are challenges and barriers that must be overcome. The extensive implementation of 5G infrastructure in healthcare environments is still in progress, with larger, well-funded hospitals likely to be the first to incorporate it. Issues concerning data security and patient privacy must be resolved, alongside regulatory and liability matters related to remote surgical procedures. Looking ahead, as 5G technology progresses and becomes more widely integrated, remote robotic surgery is anticipated to gain greater traction. Innovations in areas such as haptic feedback and edge computing will further augment the functionalities of 5G-driven remote surgical systems.

The integration of 5G with other groundbreaking advancements, such as artificial intelligence and augmented reality/virtual reality, will drive further innovation in remote healthcare delivery. 5G-powered remote robotic surgery signifies substantial progress in healthcare, with the ability to enhance the availability of specialized treatments and revolutionize the provision of surgical services globally.

FIGURE 11.7 5G enabled Remote robots perform surgery

11.6 COMPARATIVE ANALYSIS OF FOURTH- AND FIFTH-GENERATION TECHNOLOGIES IN HEALTHCARE

Table 11.1 highlights the main distinctions between fourth- and fifth-generation communication systems within the healthcare sector. Aspects such as data transfer speed, latency, Internet of Things (IoT) support, teleconsultation, and robot-assisted services were examined.

11.6.1 Data Transmission and Speed

4G offers a data transmission rate of up to 100 Mbps, adequate for fundamental internet uses like website browsing and emailing. However, this performance falls short for applications that need rapid data movement, including video calls and streaming. On the other hand, 5G provides data transmission speeds reaching up to 1 Gbps, enabling it to accommodate more demanding use cases.

- **Latency:** 4G experiences latency rates of 20–50 ms, which may result in delays in live services such as video calls. In contrast, 5G boasts latency as low as 1 ms, allowing for quicker communication.
- **IoT Support:** 4G has limited capacity to support IoT devices, hindering their integration into healthcare frameworks. Conversely, 5G enables

massive machine-type communication (mMTC), capable of managing a vast array of IoT devices and enhancing healthcare functionalities.

- **Teleconsultation:** 4G offers only basic capabilities for teleconsultation, reducing the feasibility of remote consultations. In comparison, 5G enhances mobile broadband (eMBB), allowing for swift data movement and minimal latency, making it ideal for telehealth interactions.
- **Robot-Assisted Services:** 4G presents scarce support for robot-assisted technologies, complicating their incorporation into healthcare solutions. On the flip side, 5G facilitates time-sensitive networking (TSN), offering low latency and high reliability suitable for robotic assistance.
- **Connected Ambulances:** 4G's limited support for connected emergency vehicles hampers real-time monitoring and communication during crises. In contrast, 5G supports high-definition imaging and VR devices, providing immediate monitoring and communication capabilities in emergency situations.
- **Security:** While 4G has minimal security measures, making it susceptible to data breaches, 5G incorporates advanced security features, enhancing data protection and safety measures.
- **Cost:** 4G entails high setup costs and is not widely accessible, posing challenges for healthcare providers seeking integration. Conversely, while 5G also comes with considerable implementation expenses, it promises improved healthcare operations and better patient outcomes, making it a worthwhile investment for medical providers.
- Overall, this analysis underscores the substantial variations between 4G and 5G technologies concerning healthcare. 5G delivers quicker data transmission rates, reduced latency, better IoT integration, and fortified security features, rendering it a more appropriate choice for healthcare purposes.

11.7 MICROSEGMENTATION

Microsegmentation is a leading security technique tailored to the complexities of 5G-enabled healthcare environments. This method entails establishing smaller, distinct segments within the network, each managed by separate security protocols and access regulations. This granular segmentation allows organizations to better manage and protect sensitive data flows across the network [23].

In a 5G healthcare ecosystem, where multiple interconnected devices and applications coexist, the implementation of microsegmentation provides a robust security architecture. Should a security breach occur, microsegmentation limits the impact to the compromised segment, thereby minimizing the risk of lateral movement by malware or unauthorized users. This containment principle ensures that even if one segment is breached, the integrity and functionality of the rest of the network remain intact.

Microsegmentation can be achieved through several methodologies, each with distinct advantages:

1. **Network Segmentation:** This involves subdividing the network's physical and virtual infrastructure into distinct segments, ensuring that sensitive applications and data are isolated from other less secure segments.
2. **Agent-Based Solutions:** This approach deploys software agents on individual workloads, creating barriers that enforce strict access controls and maintain isolation between segments.
3. **Network-Based Solutions:** Utilizing existing network infrastructure—such as load balancers, switches, and software-defined networks (SDNs)—these solutions enforce security policies at the network level, providing a centralized mechanism to manage security configurations.
4. **Cloud-Native Controls:** Leveraging the capabilities of cloud service providers, these solutions offer additional layers of security by utilizing built-in security features inherent to the cloud environment.

The advantages of applying microsegmentation in 5G healthcare systems are substantial. It reduces the attack surface significantly by constraining the spread of malware and unauthorized access. Improved insight into network traffic facilitates the quick detection and response to possible security threats. Furthermore, microsegmentation makes it easier to adhere to regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA), by securely isolating sensitive information and systems.

11.7.1 Challenges in Microsegmentation Implementation

While microsegmentation provides a robust framework for enhancing network security, its implementation can present challenges. The complexity of modern network architectures and the diverse range of security protocols can complicate deployment. Other issues include the investment costs required for infrastructure upgrades and the need to ensure interoperability among various network components and devices. Healthcare organizations must strategically navigate these hurdles, often necessitating collaboration with cybersecurity professionals and investment in specialized training for staff.

11.8 ZERO-TRUST ARCHITECTURE (ZTA)

Zero-trust architecture is a contemporary framework which operates on the principle of treating every device and user with suspicion by default, irrespective of location within the network. Unlike traditional perimeter-based defenses, ZTA requires rigorous verification of identities and access permissions at every interaction point within the network. This ensures that even if an endpoint is compromised, attackers cannot move laterally throughout the network.

ZTA is particularly beneficial in 5G healthcare environments, characterized by a high volume of connected devices such as medical sensors, wearables, and IoT devices that create a substantial attack surface [24].

11.8.1 Key Principles of Zero-Trust Architecture

1. **Explicit Verification of Access:** All access requests are verified using multi-factor authentication (MFA) and real-time validation processes, ensuring that only legitimate users gain entry to the network.
2. **Minimal Access Rights:** Users and devices are granted only the essential permissions required for operations, thereby reducing exposure to sensitive information and decreasing potential attack surfaces.
3. **Assumed Breach:** The ZTA model operates on the assumption that a breach could occur at any time, leading to continuous monitoring and proactive security measures.
4. **Microsegmentation:** The network is divided into smaller, isolated segments, allowing for tailored security policies applicable to specific segments. This containment strategy hinders attackers from moving laterally even if they gain initial access.
5. **Ongoing Surveillance:** Real-time observation of user behavior and network traffic is crucial for the timely identification of irregularities and swift action against potential threats, ensuring a strong security framework in dynamic healthcare environments.

11.8.2 Fundamental Elements of Zero-Trust Architecture

- **Authentication and Access Control (AAC):** This system verifies user identities and implements access restrictions. AAC is essential for guaranteeing that only verified users can access particular resources.
- **Policy Enforcement Engine:** This element applies access control policies according to contextual variables, including user roles, device status, and data sensitivity, enabling real-time access determinations.
- **Secure Access Service Edge (SASE):** By integrating networking and security functions into a single cloud-delivered service, SASE enhances secure access to resources, enabling healthcare professionals to use various devices and locations without compromising security.

11.8.3 Benefits of Zero-Trust Architecture

1. **Improved Security:** ZTA reduces the exposure to potential vulnerabilities and implements stringent access restrictions, strengthening the organization's overall security framework. Segmentation and thorough verification processes collaborate to effectively mitigate potential threats.
2. **Enhanced Visibility:** Continuous monitoring and detailed logging of network traffic and user behaviors provide healthcare organizations with a clearer understanding of their security landscape, enabling better threat detection and mitigation.

3. **Increased Flexibility:** ZTA allows healthcare providers to adapt quickly to changing network and security requirements, supporting the integration of new devices and technologies without compromising security.
4. **Regulatory Compliance:** By safeguarding sensitive data and enforcing strict access controls, ZTA assists healthcare organizations in complying with regulations such as HIPAA, ensuring that patient information is adequately protected.

11.8.4 Challenges in Implementing ZTA

While the benefits of ZTA are significant, healthcare organizations face several challenges in its implementation:

1. **Complexity of Network Environments:** Transitioning to a ZTA model often requires a comprehensive overhaul of existing network infrastructures, which can be complex and resource-intensive. Healthcare organizations with legacy systems may find full integration particularly challenging.
2. **Scalability Issues:** As the quantity of connected devices keeps expanding in healthcare environments, ensuring that the ZTA framework can scale effectively to accommodate this growth can be daunting. Organizations must design solutions that can adapt to increasing complexity without sacrificing security.
3. **Resource Constraints:** Many healthcare organizations operate under tight budgets and limited IT resources, difficult to allocate resources for the essential technologies and staff to deploy
4. **User Training and Change Management:** Educating staff about the principles of ZTA and how to navigate the new protocols is crucial, yet it can be met with resistance or confusion. Effective change management strategies are essential to ensure that personnel are engaged and compliant.
5. **Interoperability with Legacy Systems:** Integration of ZTA in environments with numerous legacy systems poses significant challenges in terms of compatibility and coherence. Organizations must ensure that legacy applications can work within the ZTA framework without compromising security or functionality.

11.9 NETWORK FUNCTION VIRTUALIZATION (NFV)

NFV is a revolutionary idea that changes conventional networking by separating network functions from specialized hardware devices. By leveraging IT virtualization technologies, NFV allows these functions to be implemented as virtual machines (VMs) or containers that run on commercial off-the-shelf (COTS) servers, switches, and storage devices [25].

This innovative approach revolutionizes how service providers deploy and manage network services, facilitating rapid scaling of resources on-demand while reducing both capital and operational expenses typically associated with dedicated hardware.

11.9.1 Key Components of NFV

The backbone of NFV consists of three primary components:

1. **NFV:** These are applications that run on software to provide essential NFV management and orchestration (NFV-MANO) capabilities, such as firewalls, load balancers, and routing. VNFs substitute physical hardware devices, offering enhanced flexibility and scalability.
2. **NFV Infrastructure (NFVI):** This includes both the physical and virtual resources necessary to host VNFs. NFVI consists of computing power, storage, and networking resources, forming the basis on which VNFs operate.
3. **NFV Management and Orchestration (NFV-MANO**): This element oversees the lifecycle of VNFs and the NFVI. It guarantees smooth deployment, scaling, and administration of network operations and coordinates the interrelations among various VNFs to ensure optimal performance of services.

11.9.2 Benefits of NFV

NFV offers numerous advantages for the healthcare sector, including:

- **Increased Agility:** NFV allows healthcare providers to rapidly deploy new services and scale resources according to fluctuating business and user demands. This agility is crucial for adapting to evolving healthcare challenges and patient needs.
- **Cost Savings:** By decoupling network functions from proprietary hardware, organizations can significantly reduce both capital and operational expenses. NFV enables multiple VNFs to operate on a single server, improving resource efficiency and reducing the requirement for dedicated hardware.
- **Enhanced Security:** NFV creates a secure and isolated environment for VNFs, protecting network functions from unauthorized access and malicious attacks. This isolation is critical in a healthcare environment where sensitive patient data is frequently under threat.
- **Diverse Use Cases:** Offers several important use cases in healthcare. It enables virtualized mobile base stations, allowing for quick scaling and cost-effective mobile services. NFV also supports content delivery networks that ensure fast and secure distribution of medical content and data. Additionally, it provides security functions such as virtual firewalls and load balancers to manage data flows securely and efficiently. Furthermore, NFV enhances network performance and minimizes latency, which is vital for telemedicine and instantaneous patient monitoring.
- **Software-Defined Networking (SDN):** NFV can be deployed either on its own or in combination with software-defined networking. SDN divides the network control plane from the data forwarding plane, easing better adaptableness and programmability. When integrated with NFV, SDN offers a robust framework for developing and managing cost-effective, modern communication networks that can swiftly adapt to the evolving demands of the healthcare industry.

11.9.3 Challenges in Implementing NFV in Healthcare

Despite the considerable advantages of NFV, healthcare organizations face several challenges in its implementation:

1. **Complexity of Integration:** Transitioning from traditional networking to NFV can be complex, especially in environments with legacy systems. Organizations may struggle with integrating NFV solutions into their existing infrastructures.
2. **Resource Allocation:** NFV requires significant computational resources. Healthcare organizations must ensure they have adequate and appropriately configured COTS hardware to support the deployment and operation of VNFs and NFVI.
3. **Skill Gaps:** There exists a critical skills shortage for IT professionals familiar with NFV and virtualization technologies. This talent gap can hinder the successful implementation and ongoing management of NFV solutions.
4. **Security Concerns:** While NFV inherently offers enhanced security through the isolation of VNFs, new vulnerabilities may arise from misconfigurations and improper management. Organizations should implement robust security measures and conduct regular assessments to reduce these risks.
5. **Interoperability Issues:** With the proliferation of IoT devices and various applications, ensuring that VNFs can seamlessly interoperate with existing systems and maintain compliance with healthcare regulations (e.g., HIPAA) can be challenging.
6. **Latency and Performance Overhead:** Introducing virtualization can sometimes introduce latency or performance overhead, which is crucial to monitor, particularly in time-sensitive healthcare applications such as remote surgeries or real-time patient monitoring.

11.10 SOFTWARE-DEFINED NETWORKING

SDN has developed into a groundbreaking technology that strengthens the security infrastructure of Healthcare 5.0 networks. By decentralizing network management and enabling dynamic control over network resources, SDN addresses various security challenges unique to the healthcare sector [26].

11.10.1 Key Security Features of SDN in 5G Healthcare

Separation of Control and Data Planes: The fundamental architecture of SDN divides the control plane, which is responsible for decision-making and management, from the data forwarding plane, which handles the actual data transmission. This distinction allows for centralized management and oversight of network traffic, facilitating improved monitoring and control. It simplifies the process of identifying suspicious activities and responding to potential dangers instantly.

Centralized Network Management: With SDN, healthcare organizations can consolidate their network management processes. This unified approach allows for consistent enforcement of protection policies across the entire network. Administrators can more effectively implement and update security measures, which is crucial in a sector that must comply with strict data protection regulations.

Dynamic Policy Management: One of the standout features of SDN is its programmable interface that enables flexible policy changes. Network administrators can easily define and modify security protocols based on immediate conditions or emerging risks. This adaptability is important in a landscape where cyber dangers transform rapidly, allowing healthcare organizations to remain proactive rather than reactive.

Enhanced Response to Threats: SDN enables quicker identification and reaction to security incidents. By analyzing traffic patterns in real time, SDN can detect irregularities indicative of security violations. Once a potential danger is identified, network administrators can swiftly implement predefined response procedures to mitigate hazards.

Establishment of Secure Network Slices: With 5G technology, SDN supports the concept of network slicing, which allows for the establishment of several virtual networks within a single tangible network infrastructure. Each slice can be tailored to address specific protection needs, ensuring that confidential medical information is isolated from less critical traffic. This segmentation reduces the likelihood of data security incidents and improves overall protection.

Integrated Protection Functions: SDN simplifies the incorporation of advanced security features, such as firewalls, breach detection systems, and encryption protocols. Network administrators can implement these solutions seamlessly within the SDN architecture, delivering an improved layer of safety for sensitive healthcare information.

Facilitating Secure Remote Access: Healthcare professionals often require remote access to systems to provide care efficiently. SDN can create secure access points that allow medical professionals to connect to the network without compromising information security. This capability is especially important for virtual medicine and distance patient monitoring, where maintaining information integrity and confidentiality is crucial.

11.10.2 Challenges in Implementing SDN Security in Healthcare

While SDN offers numerous security benefits, there are hurdles that healthcare organizations must address:

Implementation Complexity: Transitioning to SDN from traditional network architectures may be intricate and demanding in terms of resources. Healthcare organizations must ensure their personnel is sufficiently trained and equipped with the tools needed to effectively oversee a software-defined network.

Evolving Threat Landscape: The constant emergence of advanced cyber threats necessitates continuous adaptation of security protocols. Organizations must stay alert and invest in solutions that prepare them to combat threats aimed at healthcare data.

Reliance on the Controller: In SDN frameworks, the controller serves as a central management unit. If the SDN controller is breached, it could present severe security vulnerabilities. Organizations must ensure their controllers are extremely secure and resilient against attacks.

11.11 BLOCKCHAIN FOR SECURING DATA EXCHANGE

The healthcare sector is experiencing a noteworthy shift with the introduction of 5G technology. With its ability to facilitate high-speed data transfer, minimal latency, and extensive connectivity, 5G is set to transform the delivery of healthcare services. However, as the dependence on digital information increases, the need for strong security protocols has intensified. This is where blockchain technology plays a crucial role, providing a secure and decentralized method to safeguard and oversee healthcare data. Blockchain has gained recognition in the healthcare sector due to its capacity to offer a secure and reliable method to safeguard healthcare data. Through the use of a distributed ledger, blockchain guarantees that data is resistant to tampering and accessible only to authorized users. This is vital in the healthcare field, where patient information is sensitive and requires stringent confidentiality.

The fusion of 5G and blockchain technology is revolutionary for the healthcare sector. With 5G's capability to enable rapid data transmission and minimal latency, blockchain can be utilized to securely safeguard and oversee extensive healthcare data. This is essential for remote patient tracking, where patients' information must be transmitted securely and efficiently. The integration of blockchain and 5G technology in healthcare presents numerous advantages: blockchain guarantees that healthcare information is tamper-resistant and accessible only to authorized users, offering a clear method to safeguard and oversee healthcare data, ensuring that all stakeholders share the same information. Furthermore, it automates various healthcare processes, lessening the reliance on manual data entry and enhancing efficiency. Additionally, it can improve patient care by providing healthcare professionals with instantaneous access to patient information, allowing them to make more knowledgeable decisions.

11.11.1 Challenges and Limitations

While the combination of blockchain and 5G advancements in healthcare presents numerous advantages, there are several obstacles and constraints to take into account. Blockchain can be sluggish and inefficient, especially when handling substantial volumes of data. Incorporating it with current healthcare infrastructures can be complex, necessitating considerable modifications to existing frameworks and procedures. Additionally, this solution must adhere to prevailing healthcare regulations, which can be daunting and labor-intensive. The confluence of blockchain and 5G in healthcare represents a groundbreaking method for secure data exchange. By offering a safeguarded and clear approach to managing and overseeing healthcare data, blockchain can enhance patient care, lower expenses, and boost operational efficiency. Although there are obstacles and constraints to acknowledge, the merits of combining blockchain with 5G in healthcare are undeniable, making it an intriguing and promising field for research and innovation [27].

11.11.2 Enhanced Data Encryption and Isolation

Data encryption is a powerful security method that converts sensitive details into an unreadable format, protecting them from unauthorized access, alteration, or theft. This complex process, referred to as cryptography, guarantees that only permitted individuals can interpret the encrypted content, making it inaccessible to malicious entities. In the healthcare sector, data encryption is an essential element of data protection. It safeguards sensitive patient details, such as medical files and personal information, keeping them confidential and shielded from unauthorized access. This is especially vital in healthcare, where patient privacy and safety are of utmost importance.

11.11.3 Types of Data Encryption

Symmetric and Asymmetric Encryption: In symmetric encryption, the identical key is utilized for both the processes of encryption and decryption, which enhances speed but reduces security. In contrast, asymmetric encryption utilizes a private key that is possessed by the data owner and a public key that is provided to the recipient. Providing a higher level of security due to the lack of private key sharing.

To ensure robust data encryption in healthcare, organizations should implement the following best practices. Utilize industry-standard encryption algorithms such as AES to ensure the highest level of security. Encrypt data stored on devices, servers, or databases, as well as during transmission using protocols such as transport layer security (TLS). Allow selective encryption of sensitive data to ensure that only necessary information is protected. Manage encryption keys securely and efficiently to avoid illegal access. Define and implement encryption guidelines automatically to ensure compliance with regulatory requirements. Although it has challenges in real-time practicality. Managing encryption keys is a critical part of encryption management, requiring careful planning and execution.

11.11.3.1 Ensuring Performance and Security in Healthcare Data Encryption

Maintain encryption without compromising system performance, as this is vital for the complete effectiveness of healthcare organizations. Implement strong security strategies to safeguard from various threats, including brute-force and side-channel assaults. Adhere to applicable laws, such as the Health Insurance Portability and Accountability Act (HIPAA), to avoid legal and financial repercussions. By adopting effective data encryption solutions, healthcare organizations can uphold the privacy, integrity, and authenticity of sensitive patient information, shielding it from unauthorized access while ensuring regulatory adherence. Real-time network security situational awareness involves actively monitoring network activity to quickly identify potential threats. This proactive strategy enables swift incident response, minimizing the impact of security breaches on healthcare services [28].

11.11.4 Continuous Identity Authentication

Authentication is essential for healthcare organizations to keep sensitive patient data safe. As cybersecurity is a major concern, strong authentication methods are needed to make sure only approved staff can access this information. Many healthcare providers use connected medical devices, which also need protection from cyber threats to ensure services run smoothly. Traditional password methods are not effective, as they are often weak or easily stolen. Passwordless authentication offers several advantages: it removes risks tied to passwords, reduces the hassle of remembering multiple passwords, and helps healthcare organizations comply with regulations such as HIPAA. This method allows for faster and more secure access to health information, improving patient care. The best way to authenticate in healthcare is through tap-and-login, which uses employee ID badges and smartphones as security keys. This system improves convenience and security, making sure only authorized personnel can view patient records. As the industry moves toward Healthcare 5.0, adopting passwordless authentication will be vital for protecting patient data [29].

11.11.5 Fine-Grained Access Control

Fine-grained access control allows organizations to manage access to specific resources and data based on user roles and permissions. This strategy ensures that only authorized individuals can access sensitive information and systems, significantly lowering the chance of unauthorized access and data breaches. Key components of fine-grained access control include assigning users specific roles and permissions aligned with their job functions and access needs. These roles specify which resources and data each user can access. Access control lists (ACLs) outline the permissions for each user or team, defining what actions—such as reading, writing, executing, or deleting—they can carry out on particular resources. Additionally, attribute-based access control (ABAC) takes into account user characteristics, permissions, and other relevant factors to establish access rights.

Mathematical representation for fine-grained access control process:

The fine-grained access control process can be represented mathematically as follows:

1. **User Features:** The attributes of a user are shown as a set $P = \{A_i : 1 \le i \le n\}$, where A_i is the i^{th} feature and n is the count of features.
2. **Authentication Information:** The authentication information for a user is represented as $UI = \{username, password, certificate, etc.\}$.

3. **Access Control Function:** The access control function $I(A)$ is defined as the configuring function of the user feature A, which satisfies: $I(A) = \sum_{i=1}^{n} I_i(A_i)$, where $I_i(A_i)$ is the configuring function of the i^{th} feature A_i.
4. **Access Identifier (AID):** The AID is generated based on the user feature A and is represented as $AID = I(P) = \sum_{i=1}^{n} I_i(A_i)$.

Fine-grained access (FGA) control offers several advantages, including the ability to significantly reduce the risk of unauthorized access and data breaches by managing access to particular resources and information. This control enables more accurate access management, eliminating the need for broad, generic permissions. It also assists organizations in meeting regulatory compliance by ensuring that access is granted based on clearly defined roles and permissions. Consequently, FGA control is an essential element of contemporary security frameworks. By regulating access to distinct resources and information according to user roles and permissions, fine-grained access control guarantees that only authorized personnel can access sensitive data and systems, further mitigating the risk of unauthorized access and data breaches [30].

11.11.6 Network Slicing

The advancement of 5G technology has introduced network slicing, allowing operators to create various virtual networks, or "slices," on a shared physical infrastructure. Each slice is tailored to specific use cases with unique resources and security settings. While network slicing enhances security by isolating slices from one another, it also brings challenges. Managing many slices increases the risk of human errors that can lead to vulnerabilities. Operators must secure numerous slices, each requiring careful configuration. This complexity can lead to weaknesses, with billions of potential attack points in a 5G network. To address security concerns, operators and security companies are developing solutions such as micro-segmentation and security-as-a-service (SECaaS). These strategies aim to simplify management and protect against risks. In healthcare, 5G also faces security challenges. Providers should adopt advanced techniques such as micro-segmentation, zero-trust architecture, and artificial intelligence–based security. Additional measures such as improved data encryption and continuous identity authentication are vital for safeguarding 5G healthcare systems [31–33].

11.12 FUTURE TRENDS AND RESEARCH DIRECTION

The future of 5G in healthcare is hopeful, with numerous key trends and research directions emerging. Widespread deployment of 5G networks, especially in underprivileged and rural areas, is crucial to ensure equitable access to 5G-enabled healthcare services. Leveraging 5G's low latency and high bandwidth will enable more seamless, high-quality virtual consultations and remote patient monitoring while integrating 5G-enabled wearables, sensors, and IoT devices will facilitate continuous monitoring and early intervention for chronic conditions [34].

Utilizing 5G's data handling capabilities will enable real-time analysis of large healthcare datasets using machine learning and artificial intelligence, allowing for the development of predictive models and personalized treatment plans. The exploration of AR/VR applications in healthcare, such as remote surgery, medical guidance, and patient rehabilitation, will also be enabled by 5G's low latency [35].

Cybersecurity and data privacy considerations are essential to protect sensitive patient data in 5G-enabled healthcare systems. Ensuring robust security measures and developing comprehensive data governance outlines and rules will address privacy concerns and regulatory compliance. Blockchain, edge computing, and digital twins will enhance 5G healthcare applications and services.

Establishing clear regulatory guidelines and policies will support the widespread and secure implementation of 5G in healthcare, addressing issues such as liability, data privacy, and patient safety. Promoting awareness and understanding comprehension of the benefits and contests of 5G in healthcare among healthcare professionals, policymakers, and the general public will also be crucial. By tackling these emerging trends and research priorities, the healthcare sector can fully leverage 5G to enhance patient outcomes, improve healthcare delivery, and foster innovation within the industry.

11.13 CONCLUSION

In summary, 5G technology has the potential to completely transform the healthcare sector by offering a dependable and strong framework for data transfer in real time, thereby facilitating telemedicine, remote patient monitoring, and other cutting-edge healthcare applications.

- By bridging the gap between patients and healthcare providers through latency at ultra-low, data transfer at high speed, and mMMC capabilities, 5G will bridge the gap between patients and healthcare providers, allowing for more efficient and effective care.
- Enable telemedicine and remote patient monitoring to increase underprivileged communities' access to healthcare.
- Support instantaneous communication between medical equipment and healthcare providers, enhancing patient care and reducing errors.
- Facilitate the development of precision medicine and personalized treatment plans through advanced data analytics and AI-driven insights.
- Improve emergency response times with real-time emergency dispatch and remote emergency services.
- Enhance patient engagement and empowerment through mobile health apps and wearables. In general, the implementation of 5G technology in the healthcare industry holds promise for revolutionizing the delivery of healthcare services, resulting in increased accessibility, efficacy, and efficiency. 5G will be significant in determining how healthcare is delivered in the future as the healthcare sector develops.

REFERENCES

1. Vora, L. J. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G. *International Journal of Modern Trends in Engineering and Research*, 2(10), 281–290 (2015).
2. Fagbohun, O. O. Comparative studies on 3G, 4G and 5G wireless technology. *IOSR Journal of Electronics and Communication Engineering*, 9(3), 88–94 (2014).
3. Hao, Y. Investigation and technological comparison of 4G and 5G networks. *Journal of Computer and Communications*, 9, 36–43 (2021).
4. Gopal, B. G., & Kuppusamy, P. G. A comparative study on 4G and 5G technology for wireless applications. *IOSR Journal of Electronics and Communication Engineering*, 10(6), 2278–2834 (2015).
5. Kumar, A., Dhanagopal, R., Albreem, M. A., & Le, D. N. A comprehensive study on the role of advanced technologies in 5G based smart hospital. *Alexandria Engineering Journal*, 60(6), 5527–5536 (2021).
6. Moglia, A., Georgiou, K., Marinov, B., Georgiou, E., Berchiolli, R. N., Satava, R. M., & Cuschieri, A. 5G in healthcare: from COVID-19 to future challenges. *IEEE Journal of Biomedical and Health Informatics*, 26(8), 4187–4196 (2022).
7. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. 5G technology for healthcare: Features, serviceable pillars, and applications. *Intelligent Pharmacy*, 1(1), 2–10 (2023).
8. HealthNet Global Introduces 5G Connected Ambulance at Apollo Hospital, Bengaluru. The Economic Times, 16 Dec. 2022. Available at: https://health.economictimes.indiatimes.com/news/hospitals/healthnet-global-introduces-5g-connected-ambulance-at-apollo-hospital-bengaluru/106729890
9. The 5G Connected Ambulance: Leading the UK's First Remote Diagnosis. Ericsson, 2 Dec. 2020. Available at: https://www.ericsson.com/en/cases/2020/the-5g-connected-ambulance
10. Dunn, J., Runge, R., & Snyder, M. Wearables and the medical revolution. *Personalized Medicine*, 15(5), 429–448 (2018).
11. Tana, J., Forss, M., & Hellsten, T. *The use of wearables in healthcare–challenges and opportunities* (2017).
12. Apollo Launches 5G-Connected Ambulance Service in Kolkata. ETTelecom, 18 Feb. 2023. Available at: https://telecom.economictimes.indiatimes.com/news/industry/apollo-launches-5g-connected-ambulance-service-in-kolkata/100703298
13. AT&T. 5G expected eventually to improve AR/VR for healthcare (n.d.). Retrieved from https://www.business.att.com/learn/top-voices/5g-expected-eventually-to-improve-ar-vr-for-healthcare.html
14. HST. Advanced visualization for patient care (2021). Retrieved from https://www.hst.org.tw/en/story/content/4051
15. STL Partners. Edge computing: 5G-edge AR/VR use cases (n.d.). Retrieved from https://stlpartners.com/articles/edge-computing/5g-edge-ar-vr-use-cases/
16. Tecknexus. Connected enterprise: How 5G, AI, and AR/VR are transforming vertical industries (2023). Retrieved from https://tecknexus.com/5g-network/shaping-future-connectivity-tech-5g-magazine-may-2023/connected-enterprise-how-5g-ai-and-ar-vr-are-transforming-vertical-industries/
17. Verizon. 5G business use cases: Workforce productivity: Advanced visualization for patient care (n.d.). Retrieved from https://www.verizon.com/business/resources/5g/5g-business-use-cases/workforce-productivity/advanced-visualization-patient-care/
18. Astej. *Remote Patient Monitoring: A Review of the Current State of the Art*, V06(04), P06 (2020).

19. Oleshchuk, V., Fensli, R. Remote Patient Monitoring Within a Future 5G Infrastructure. Wireless Pers Commun 57, 431–439 (2011)
20. Fan, Yuxin et al. “5G Remote Robot-Assisted Hepatobiliary and Pancreatic Surgery: A Report of Five Cases and a Literature Review.” The international journal of medical robotics + computer assisted surgery : MRCAS vol. 21,1 (2025)
21. Healthcare in Europe. *World's First Remote Operation Using 5G Surgery, HuaweiTech* (2020).
22. Medical Device Network. *5G Remote-Controlled Robots Will Enable Surgery from Afar* (2020).
23. Piya, K., Au, Q. A., Shrestha, S., Singh, A., & Mohd, T. K. IoT in health care industry: a promising prospect. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0466–0474). IEEE (2021, December).
24. Almuseelem, W. Continuous And Mutual Lightweight Authentication for Zero-Trust Architecture-Based Security Framework in Cloud-Edge Computing-Based Healthcare 4.0. *Journal of Theoretical and Applied Information Technology*, 102(1) (2024).
25. Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167, 106984 (2020).
26. Trivisonno, R., Guerzoni, R., Vaishnavi, I., & Soldani, D. SDN-based 5G mobile networks: architecture, functions, procedures and backward compatibility. *Transactions on Emerging Telecommunications Technologies*, 26(1), 82–92 (2015).
27. Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, 35(4), e4329 (2024).
28. Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., & Alkhassawneh, H. M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications*, 16(5), 421–432 (2022).
29. Wu, G., Wang, J., Zhang, Y., & Jiang, S. A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors*, 18(1), 179 (2018).
30. Ai, Z., Liu, Y., Chang, L., Lin, F., & Song, F. A smart collaborative authentication framework for multi-dimensional fine-grained control. *IEEE Access*, 8, 8101–8113 (2019).
31. V. P. Singh, M. P. Singh, S. Hegde and M. Gupta, "Security in 5G Network Slices: Concerns and Opportunities," in IEEE Access, vol. 12, pp. 52727–52743 (2024).
32. Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira J.. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine*, 55(5), 80–87 (2017).
33. Jiang, M., Condoluci, M., & Mahmoodi, T. Network slicing in 5G: An auction-based model. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE (2017, May).
34. Khan, A., Dhar, S. P., Shanmugasundaram, R., & Chemparathy, J. *5G Networks: An Overview of Architecture, Design, Use Cases and Deployment* (2024).
35. Whig, P., Kouser, S., Bhatia, A. B., Nadikattu, R. R., & Alkali, Y. J. Modeling Virtual Worlds Using IoT: Applications and Challenges. *Modelling of Virtual Worlds Using the Internet of Things*, Edition 1, 1–18 (2024).

12 Role of Blockchain in Healthcare 5.0

Britant Sharma

12.1 INTRODUCTION

Blockchain's usefulness extends far beyond just digital currencies such as Bitcoin. Think about how the identical technology that facilitates decentralized financial transactions might transform the oversight of medical records, clinical studies, and pharmaceutical distribution networks. Fundamentally, blockchain offers a permanent, clear, and distributed ledger system that can dramatically transform our perspectives on trust, privacy, and efficiency within the healthcare sector.

During a period when the surge of patient information, rising expenses, and increasing cybersecurity risks burden healthcare systems, blockchain has the potential to act as a revolutionary technology that tackles several of the sector's essential issues [1]. By providing secure and immutable solutions, blockchain could enhance the focus on patients, reliance on data, and credibility in healthcare.

The healthcare industry faces numerous urgent challenges that influence not only providers but also patients, insurers, and policymakers. A primary concern is the security of data. Medical records are among the most private forms of personal information, and as a result, they frequently become targets for cyberattacks. In 2020, breaches in healthcare data affected more than 22 million people globally, leading to a loss of patient trust, disruptions in care, and considerable financial repercussions for hospitals and insurance companies [2]. Existing methods of data storage, whether utilizing centralized cloud systems or traditional paper formats, are vulnerable to hacking, unauthorized access, and human error.

One significant challenge is interoperability. Usually, data does not flow smoothly between hospitals, laboratories, insurance companies, and pharmacies. This fragmentation of information results in care delays, unnecessary testing, and miscommunication among professionals, thus potentially hindering a patient's treatment. Although we have seen improvements in electronic health record (EHR) systems, interoperability still faces obstacles [3].

Global healthcare systems deal with issues such as payment delays, bottlenecks, and opaque pharmaceutical supply chains. These issues may lead to increased expenses, fraud, and hold-ups in getting necessary prescription drugs. It is difficult for current procedures to promote responsibility and confidence between various healthcare facilities, especially when it comes to managing patient permission and the validity of clinical trials [4].

 DOI: 10.1201/9781003532286-12

Figure 12.1 illustrates the distribution of blockchain technology usage across various sectors [5], with a specific emphasis on the healthcare sector.

- **Healthcare** is highlighted as a significant sector, accounting for **25%** of blockchain usage.
- **Finance** remains the dominant sector of blockchain implementation.
- The **Supply chain** sector also shows substantial use of blockchain.

In this chapter, we will discuss how blockchain technology can transform the healthcare industry focusing on the key propositions of how blockchain can help address some of the most significant challenges facing the healthcare system, including inefficiencies, security of data, and interoperability.

Finally, this chapter will analyze some use cases of blockchain in various medical areas. It will emphasize the current uses of blockchain in areas such as clinical trials, pharmaceutical supply chains, and electronic health records. Through these case studies, readers will learn about the current state of healthcare blockchain technology and its potential for future development.

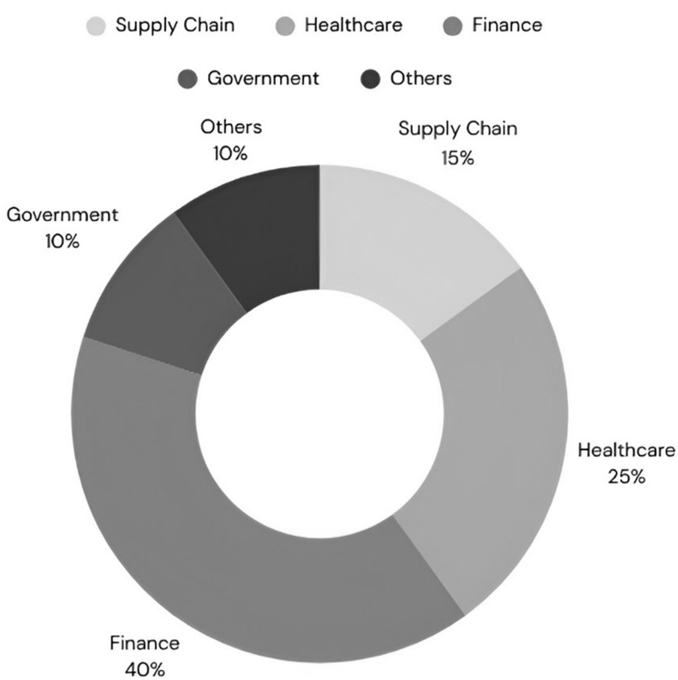


FIGURE 12.1 Blockchain usage by sector

12.2 BLOCKCHAIN'S ROLE IN ELECTRONIC HEALTH RECORDS (EHRS)

Electronic health records (EHRs) have transformed the management, access, and sharing of patient data between distinct healthcare institutions [6, 7]. Electronic health records (EHRs) allow authorized clinicians to see a patient's full digital health record, diagnosis, treatments, lab findings, etc. [8]. This data streamlining reduces mistakes and ensures that the current and complete patient information is utilized to steer healing choices. Although offering numerous benefits, EHRs remain plagued by major issues: security, privacy, interoperability, and patient control over their own data [9]. Emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) are helping healthcare systems grow both in sophistication and data demand, thus prompting questions concerning the efficacy and sustainability of current EHR systems.

One of the major concerns about conventional EHR systems is security. The majority of EHR systems currently in use are centralized in nature, meaning they can be hacked from a single point, allowing their data to be erased or accessed by any number of unauthorized third parties. Threat actors typically target the healthcare sector to obtain financial records, medical history, insurance details, and personally identifiable information (PII). In recent years, millions of patients have had their personal data compromised by high-profile breaches in the healthcare sector, revealing the urgent need for tighter security protocols. Additionally, since hospitals or other healthcare providers manage and maintain patient medical information, patients often have limited control over who can access their data.

Blockchain technology presents a promising solution to the challenges faced by traditional EHR systems. Blockchain's decentralized structure offers an innovative way to organize, share, and protect medical data. Its essential characteristics—distributed design, encryption, and consensus-based validation—make it particularly suitable for safeguarding sensitive health information and maintaining data integrity within healthcare systems. By addressing many of the core issues associated with EHRs, blockchain can help establish a more patient-centered, transparent, and secure system for storing medical records [10, 11]. The distinction between blockchain-based and conventional EHR systems is covered in Figure 12.2.

Several real-world examples show the potential of blockchain in enhancing EHRs. Estonia, one of the pioneers in digital healthcare, has successfully integrated blockchain technology into its national healthcare system. More than a million patient records in Estonia are protected by blockchain technology, which guarantees that all medical data is secured and kept in a decentralized fashion. A new patient-centric approach to data management is being established in Estonia, where patients have complete control over their medical data and can provide access to healthcare professionals using cryptographic keys [12]. Another illustration is the blockchain-based platform MedRec, which was created by MIT researchers. With MedRec, patients can keep control of their medical records and only share them with those who need to know.

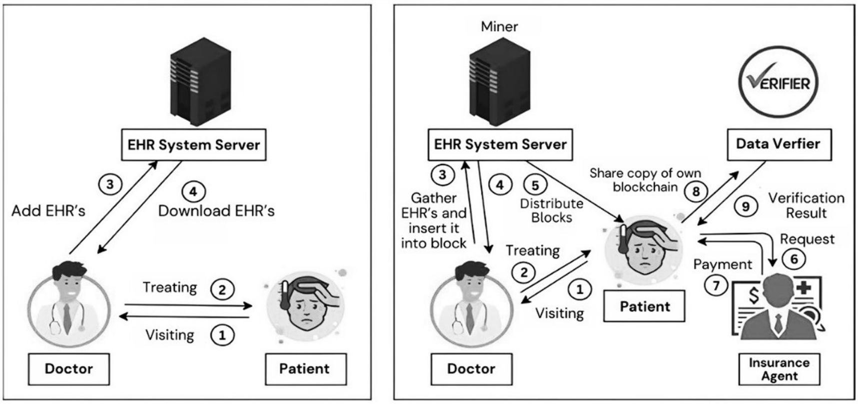


FIGURE 12.2 Traditional vs blockchain-based EHR

12.3 BLOCKCHAIN-BASED EHRS AND INTEROPERABILITY

Another significant problem facing the healthcare sector is the interoperability of conventional EHR systems. Frequently, disparate healthcare providers manage patient records using incompatible systems, which makes effective data sharing challenging or impossible. Incomplete medical histories, redundant testing, treatment delays, and misunderstandings between healthcare professionals can all arise from this fragmented patient data caused by a lack of interoperability [13, 14]. Critical information on the patient's care may be lost or delayed if, for instance, a patient visits several medical facilities for various treatments and these facilities are unable to exchange information easily. In addition to decreasing the quality of care, the fragmented nature of current systems puts more administrative strain on healthcare workers, who have to manually transfer or re-enter data into different systems. Figure 12.3 explains the challenges of EHR interoperability in healthcare.

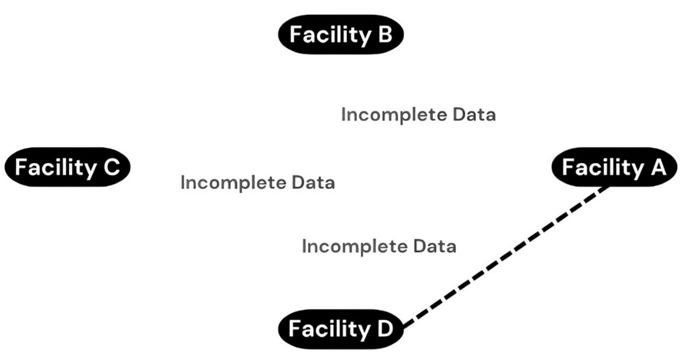


FIGURE 12.3 Challenges of EHR interoperability in healthcare

Data integrity remains a crucial aspect of conventional EHR systems. Ensuring the precision and validity of patient records in healthcare is essential, as even minor inaccuracies or omissions can lead to misdiagnoses, incorrect treatments, or other negative consequences [15]. Nonetheless, contemporary systems permit data manipulation, whether on purpose or by accident, without proper audit trails. A lack of transparency can result in disputes regarding record accuracy. Moreover, this diminishes the trust patients have in their healthcare providers.

Many of these challenges are addressed through blockchain's decentralized architecture. By utilizing a network of nodes for data sharing, blockchain diminishes the necessity for a central authority to manage patient records, thereby lowering the chances of data breaches and unauthorized access. Each transaction or update to patient records is encrypted and validated through a consensus mechanism among varied nodes, removing the risk of a single party modifying or tampering with the data undetected [16]. This ensures that patient records are secure and unaltered. Additionally, blockchain empowers patients to manage their medical information. Patients can retrieve their health records at any time they wish. They have the right to share their records with whoever they choose or to restrict access. The paradigm shift from doctor-oriented to patient-centered qualitative data governance is consistent with the vision of Healthcare 5.0, and advocates for a more individualized and patient-driven healthcare system [17].

In terms of interoperability, blockchain presents a solution by building a universal and decentralized framework that different healthcare providers can adopt irrespective of the EHR system they use. The decentralized ledger under blockchain technology enables the presence of multiple parties to access and edit records in real time. This would allow for easy data communication between clinics, hospitals, labs, pharmacies, and other healthcare organizations. For example, a blockchain could be used to securely log a patient's entire medical history across various providers. This would allow authorized physicians to access the data whenever they needed to, regardless of the systems that other providers use. Another feature of some blockchain constructs is smart contracts, which are self-executing contracts in which the terms of the agreement between buyer and seller are directly written into lines of code; their execution can ensure the sharing of sensitive patient information with the right individuals or organizations under the right context [18, 19].

Data entered into the blockchain is immutable, meaning data cannot be changed or tampered with retroactively, creating an audit trail tracing back to the source. One of its main features is verifying the authenticity of information such as patients' files. Every update or change in a record is time-stamped and connected to the prior transaction, creating a transparent, verifiable record of all the changes to a patient's medical information. Since this level of traceability means that every change is always transparent and verifiable, it can help healthcare providers settle disputes about the accuracy of records, as well as help those providers demonstrate compliance with legal and regulatory requirements and adherence to the standards of care and treatment, thereby contributing to more accountability for the healthcare system.

12.4 LITERATURE REVIEW

Patient data management is one of the most significant areas where Blockchain can contribute to Healthcare 5.0. For instance, a blockchain system stores encrypted medical records in a decentralized ledger which secures access to data only to authorized parties such as patients and healthcare providers with the help of cryptographic keys. Medical information is protected from exposure, breaches are prevented, and patients can access and manage their medical information. The papers [1, 5, 9] give a broad survey on healthcare data security and their novel trends for addressing real-world challenges. The authors described the different prominent cryptography, biometrics, watermarking, and blockchain-based security approaches for healthcare applications. The authors in [2, 10] have surveyed information breaches that can occur on healthcare data and indirectly raise healthcare costs. During clinical trials, blockchain provides an innovative means of reducing operational burdens such as data breaches, enabled by the features discussed in paper [4, 20]. It raises key challenges including data integrity, transparency, and trust of patients. Smart contracts can reduce administrative overhead by automating regulatory compliance through reference to preset procedures. Following the principles of Healthcare 5.0, these features contribute to more efficient, safer, and patient-centric clinical trial procedures. The papers [8, 9] discuss the privacy and security concerns of electronic health record storage, and the authors in the papers [10, 13] proposed blockchain as a cure to answer these concerns. As per the research published in [15, 11, 18] interoperability is also an important factor in electronic health records. The **National Alliance for Health Information Technology** defines interoperability as the ability of information technology systems and software applications to communicate, and exchange data accurately, effectively, and consistently, and to use the information that has been exchanged to provide better healthcare services. This includes seamless EHR (electronic health records) and other health data integration enabling a real-time and comprehensive patient health profile to all relevant stakeholders. Interoperability, at its core, should enable data to flow freely between different providers of care and ultimately improve patient care, ensure patient safety, lower unnecessary costs, and improve workflow. It allows various components of the data flow—hospitals, clinics, pharmacies, laboratories, and insurance companies to seamlessly and efficiently share and use data without additional work [12].

The current state of interoperability and data sharing in healthcare is characterized by significant challenges and advancements. Partial patient data collection can cause issues when an individual patient needs to switch their primary care providers or when they are referred to a specialist, as their records are kept in a centralized system and often poorly connected to their medical history [21]. The 21st Century Cures Act and similar regulations aim to advance better data sharing, but pervasive barriers such as inconsistent data standards, privacy issues, and outdated infrastructure prepare us to miss widespread, seamless interoperability [22]. Blockchain technology is proving to potentially overcome these challenges by allowing for secure, decentralized, and immutable information sharing, from multiple organizations

[23]. It provides DLT (distributed ledger technology), which allows the sharing of data about patients among various healthcare providers while ensuring the privacy, security, and integrity of the data. The entire data is encrypted, verified, and stored in a series of nodes in a peer-to-peer network. Smart contracts enabled by blockchain, or automatic agreements, could determine who has access to private health information. By avoiding any modifications or alterations, blockchain becomes a secure pathway for managing electronic health records (EHRs), ensuring data integrity, accountability, and transparency [24, 25].

Healthcare delivery relies heavily on data, and data sharing and interoperability are vital for optimizing care delivery, driving patient safety, and overall operational efficiency. Clinicians can call up patient data from different health systems, assuring that the healthcare decision that needs to be made can utilize the best data available [26]. This further reduces the need to duplicate diagnostic efforts, reduces the risk of medical errors, and enables smooth transitions between different healthcare settings. One of the major problems with EHRs—existing cyber threats and data breaches—is tackled by blockchain technology from a security standpoint. Since healthcare data is highly sensitive as well as the number of data breaches also continues to increase thus a more secure and resilient system is needed to protect it. Since blockchain is a decentralized technology, it is almost impossible for any malicious agent to tamper with the data, providing better privacy and security. In addition, blockchain personnel remove the need for intermediaries from various transactions, thus decreasing administrative costs and even improving the sharing

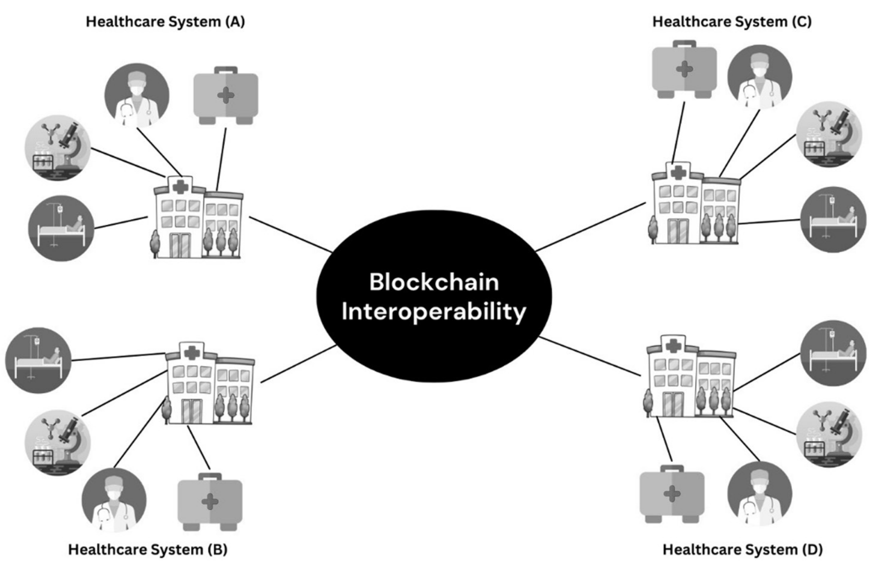


FIGURE 12.4 Blockchain interoperability facilitating secure data exchange

of information across healthcare systems [27]. Regulations such as HIPAA in the United States require organizations to protect health information and encourage secure, professional data sharing between systems [22]. This ledger-ability makes it easier for healthcare organizations to facilitate compliance with data protection regulations without compromising on data privacy, as blockchain exhibits a clear audit trail (Figure 12.4).

12.5 ROLE OF BLOCKCHAIN IN CLINICAL TRIALS

Arguably the biggest benefit of utilizing blockchain within clinical trials is the implementation of an immutable ledger of all transactions performed during the trial. Each transaction, whether it is patient consent, data entry, or analysis, is then stored in a block which connects to its previous block, creating an unbroken chain of blocks—hence the name blockchain. Unlike a conventional database, this chain operates in a distributed manner such that no single organization oversees the data. Therefore, blockchain can minimize the risk of data manipulation, fraud, or selective reporting which, in the past, has compromised trust in clinical trials [6, 7, 11].

By making the same records available to all users, transparency is improved in blockchain. In a typical clinical trial, patient information is collected and stored in a centralized database that is often overseen by the sponsor or research group. In contrast, blockchain technology relies on several nodes that each maintain an entire copy of the ledger. This setup preserves the integrity of the trial statistics by ensuring that the other nodes will rapidly detect any attempt to change the information in one node [28].

One of the key features of blockchain technology is smart contracts, self-executing contracts with the terms of the agreement directly written into lines of code. These smart contracts can simplify three processes in clinical trials: patient enrollment, consent management, and data sharing as shown in Figure 12.5. As an illustration, a smart contract may be created to allow for the automatic enrollment of a patient in a trial immediately after they have consented to do so, conditional on the meeting of all legal and ethical requirements before trial initiation [29].

Moreover, smart contracts facilitate data sharing among stakeholders. At present, sharing clinical trial data can be complex and slow among researchers, sponsors, and regulatory agencies, often requiring many middlemen. Using distributed ledger technology, blockchain can eliminate delays and ensure that all parties have access to the most up-to-date information, allowing for this process to be completed more quickly in a real-time manner with instant access to the latest information for all parties involved.

Smart contracts can enforce protocol adherence in trials, as well. For example, assume a clinical trial states a particular analysis must be performed once a certain number of patients have been enrolled in the study, the smart contract will automatically trigger the analysis once that threshold has been hit. This reduces the risk of data dredging or selective outcome reporting by making sure that the trial is conducted according to the pre-defined plan as shown in Figure 12.5.

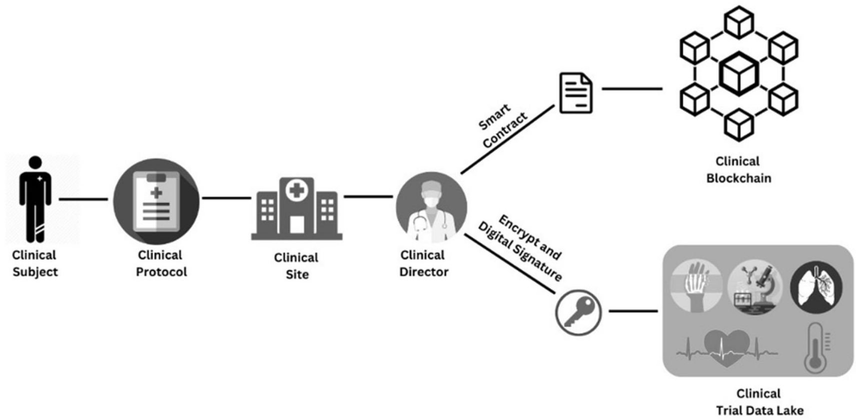


FIGURE 12.5 Smart contracts in clinical trials

Patient consent is one of the most complex problems in clinical trials. For both ethical and legal reasons, it is important that patients fully understand what the trial involves and consent to participate. Until now, there are a few challenges in patient consent that blockchain can solve. After patients consent to join a trial, their consent is stored on the blockchain, making it easy for researchers, regulators, and auditors to see that patients agree to the trial. This is to maintain that patients' rights are upheld during the trial [30].

In addition, by providing patients with greater control over their data, blockchain is able to empower them. Patients often lose both control and visibility over the usage of their data after submission in traditional clinical trials. Using the blockchain, patients retain control of their data and can grant or restrict access as they please. This is consistent with the 21st-century movement toward patient-centered care, which sees people taking a more active role in deciding how and in what way their health care and health [31].

12.6 BLOCKCHAIN-BASED SMART CONTRACTS FOR SECURE REMOTE PATIENT MONITORING IN HEALTHCARE

Remote monitoring systems and digital tools are values being accommodated by the Healthcare 1.0 industries to improve management outcomes. Once only in the hands of healthcare professionals, remote patient monitoring (RPM) has become widespread in its ability to monitor real-time investor health information outside the walls of the typical healthcare environment, increasing the efficiency of health delivery. Yet the rapid proliferation of Internet of Things (IoT) devices, especially wearable medical sensors, has created new challenges regarding data security, privacy, and interoperability. These devices—often called the Internet of Medical Things (IoMT)—produce vast amounts of sensitive medical information that must be securely transmitted, stored, and analyzed.

IoMT systems also have privacy and security issues, but the supporting technology—blockchain—has emerged as a promising solution [3, 4]. Originally conceived as a decentralized ledger for the exchange of cryptocurrencies, the technology behind blockchain has been implemented in various sectors, including healthcare. The important property of blockchain is keeping secure, unalterable records, which is suitable for controlling protected health information (PHI). The objective of this chapter is to cover how the data transfer between the users and service providers could be securely processed, monitored, and privacy compliant when using blockchain-based smart contracts in a remote patient monitoring (RPM) system [32, 23].

Essentially, blockchain technology is a distributed ledger that records transactions securely and in an unbreakable way across thousands of nodes. In the healthcare field, this technology is useful to record and authenticate patient data, ensuring data cannot be altered after it has been placed into the system. With a decentralized system, blockchain has enabled more secure and intact health data with no need for a central authority or third party to verify transactions. Besides that, blockchain is a public ledger that enables patients and healthcare providers to monitor all the activity related to medical records, resulting in greater public and professional accountability for the healthcare system [33].

Blockchain systems can be divided into three main types: public, private, and consortium. Public blockchains (such as the ones underlying the Bitcoin cryptocurrency) are fully decentralized and permissionless. On the other side, private blockchains are limited to one organization, and consortium blockchains are controlled by crosswise approved members. In healthcare, consortium blockchains tend to be the most favored because they provide more control of access and privacy while keeping the benefits of decentralization.

Another important element of blockchain in healthcare is smart contracts. These are self-executing contracts with the terms of the agreement directly written into lines of code. Through smart contract automation, processes can be automated; this includes activating alerts or recording transactions when specified guidelines are met without any human intervention as shown in the Figure 12.6. For example, in the field of healthcare, smart contracts can verify that all patient data from IoMT devices are securely processed and sent to the relevant healthcare professionals in real time [34, 35].

Remote patient monitoring is the continuous health gathering of measurable data via wearable or implanted medical devices. These devices monitor vital signs such as blood pressure, heart rate, and glucose levels, sending the information to medical professionals for analysis. Real-time health monitoring made possible by RPM systems has improved patient outcomes, but there are serious issues with data security, privacy, and dependability [36].

The addition of smart contracts to RPM systems ensures the secure and efficient handling of patient data by healthcare providers. Smart contracts work on executing predetermined rules if some conditions are fulfilled. A contract could be set up, for example, to sound an alarm when a patient's heart rate exceeds a preset threshold. As well as ensuring that event-specific medical intervention occurs in real time,

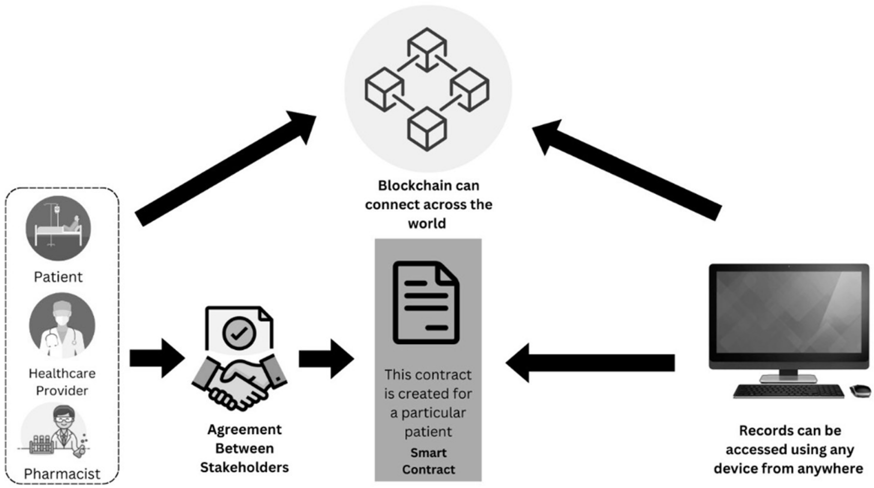


FIGURE 12.6 Smart contracts automating agreements and transactions in blockchain networks

these contracts also log each and every action taken onto the blockchain, creating an auditable and immutable record of the event [37, 38, 39].

In a consortium blockchain, the data written by the smart contracts is only accessible to authorized users (such as hospitals, medical professionals, and equipment manufacturers). The controlled access allows multiple organizations to utilize the technology while still keeping their patients secure. Also, the smart contracts here can be personalized according to each patient's monitoring and medical needs [40].

Security and Privacy: One of the key benefits of blockchain technology in RPM systems is the ability to add security and privacy. Traditional systems using on-cloud data storage and communication of health data are susceptible to hacking, data breaches, and helpful access. However, the decentralized aspect of blockchain means it is extremely hard to manipulate. All data written to blockchain is immutable, therefore health information will always remain accurate and up-to-date.

In addition, blockchain systems can help anonymize patient data. In the proposed model, patients are represented by anonymous addresses on the blockchain., with which it is impossible to directly associate the health information about them. Such a requirement is essential for complying with privacy regulations such as HIPAA which requires that personally identifiable health information is protected from unauthorized demonstration.

Blockchain has the potential to not just augment patient data security but also promote transparency in healthcare. Patients can access their medical records and track all activities related to their data from the moment it is collected by an Internet of Medical Things (IoMT) device until it is analyzed and used in making medical decisions. Such transparency allows patients to be in charge of their healthcare and instills trust between patients and their providers [41].

12.7 CONCLUSION

This study examined the utilization of blockchain technology in addressing key challenges in healthcare, including transparency, interoperability, and data security. Ever-present problems such as data breaches, information fragmentation, and inefficiencies across supply chains, clinical trials, and other areas call for creative approaches. Blockchain offers patients increased autonomy along with a secure, decentralized layer for processing medical data. The headline findings reveal how blockchain could improve EHRs, ensure transparency in clinical trials, reduce the risk of counterfeit products in the pharmaceutical supply chain, and enhance data security in remote patient monitoring systems. These applications demonstrate the way blockchain can directly cut costs and encourage trust while creating a more effective, patient-centered healthcare ecosystem. However, additional study is needed to tackle some challenges including scalability, regulatory obstacles, and integration with emerging tech. Nonetheless, there are still challenges such as scalability, regulatory hurdles, and integration with emerging technologies that are yet to be explored. Research in the future must seek to elude those obstacles in order to streamline the utilization of Blockchain. The blockchain-centric approach can seamlessly skyrocket the healthcare systems toward a more secure, transparent, and patient-first approach that would help us in forming a potentially equitable future.

12.8 FUTURE DIRECTIONS

With blockchain technology evolving, there are several opportunities for further research and development in education, especially in healthcare. One possible avenue is the combination of blockchain technology with other emerging fields such as big data analytics and artificial intelligence (AI). Integrating AI with blockchain allows healthcare providers to access more in-depth information on patients, such as their medical history and genetic makeup, for personalized treatment and care options. AI also has the potential to automate key management processes which will help manage a very high number of IoMT devices more efficiently.

Another area of future research is the development of more efficient consensus algorithms for blockchain systems. Existing consensus methods, including Proof of Work (PoW), are resource-intensive and sluggish in nature. For such systems, new algorithms are being designed that would aid consensus more quickly and in a more energy-efficient manner for blockchain to be more applicable in real-time and operational applications such as RPM and practical Byzantine fault tolerance (PBFT).

REFERENCES

1. Singh, A. K., Anand, A., Lv, Z., Ko, H., and Mohan, A. A Survey on Healthcare Data: A Security Perspective. *ACM Transactions on Multimidia Computing Communications and Applications*, 17(2s), 1–26 (2021).
2. Sung, J., Choi, M., Johnson, E., and Lee, J. An Event Study of Data Breaches and Hospital IT Spending. *Health Policy and Technology*, 9(3), 372–378 (2020).

3. Torab-Miandoab, A., Samad-Soltani, T., Jodati, A. *et al.* Interoperability of Heterogeneous Health Information Systems: A Systematic Literature Review. *BMC Medical Informatics and Decision Making*, 23, 18 (2023).
4. Omar, I. A., Jayaraman, R., Salah, K. *et al.* Applications of Blockchain Technology in Clinical Trials: Review and Open Challenges. *Arabian Journal for Science and Engineering*, 46, 3001–3015 (2021).
5. Ali, O., Jaradat, A., Kulakli, A., and Abuhalimeh, A. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access*, 9, 12730–12749 (2021).
8. Basil, N. N., Ambe, S., Ekhator, C., and Fonkem, E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus, 14(10), e30168 (2022). https://doi.org/10.7759/cureus.30168
9. Keshta, I., and Odeh, A. Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal*, 22, 177–183 (2021).
10. Shahnaz, A., Qamar, U., and Khalid, A. Using Blockchain for Electronic Health Records. *IEEE Access*, 7, 147782–147795 (2019).
13. Jabbar, R., Fetais, N., Krichen, M., and Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, 2020.
15. Sreenivasan, M., and Chacko, A. M. Chapter 2 - Interoperability issues in EHR systems: Research directions. In: Kun Chang Lee, Sanjiban Sekhar Roy, Pijush Samui, Vijay Kumar (Eds.), *Data Analytics in Biomedical Engineering and Healthcare*, Academic Press, 2021, pp. 13–28.
17. Zarour, M., Alenezi, M., Ansari, T. M., Pandey, A., Ahmad, M., Agrawal, A., … & Khan, R. A. Ensuring Data Integrity of Healthcare Information in the Era of Digital Health. *Healthcare Technology Letters*, 8(3), 66–77 (2021).
18. Rasel, M., Bommu, R., Shovon, R. B., and Islam, M.A. Ensuring Data Security in Interoperable EHR Systems: Exploring Blockchain Solutions for Healthcare Integration. *International Journal of Advanced Engineering Technologies and Innovations*, 1(1), 212–232 (2023), accessed on Oct. 23, 2024.
12. Soares, B., Ferreira, A., and Mota Veiga, P. The Benefits and Challenges of Blockchain Technology and eHealth Implementation in Estonia - A Literature Review. *Appl Med Inform*, 45(4), 118–131 (2023).
24. Han, Y., Zhang, Y., and Vermund, S. H. Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, 19, 15577 (2022).
25. Schmeelk, S., Kanabar, M., Peterson, K., and Pathak, J. Electronic Health Records and Blockchain Interoperability Requirements: A Scoping Review. *JAMIA Open*, 5(3), ooac068 (2022).
26. Savage, M., and Savage, L. Doctors Routinely Share Health Data Electronically Under HIPAA, and Sharing With Patients and Patients' Third-Party Health Apps is Consistent: Interoperability and Privacy Analysis. *Journal of Medical Internet Research*, 22(9), e19818 (2020).
27. Shelke, P., Sable, N. P., Dedgaonkar, S., and Mirajkar, R. Applications of Blockchain: A Healthcare Use Case. In: Anter, A. M., Elhoseny, M., and Thakare, A. D. (Eds.), *Nature-Inspired Methods for Smart Healthcare Systems and Medical Data*. Cham: Springer (2024).
20. Bapatla, A. K., et al. PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain. *IET Networks*, 12(2), 53–76 (2023).

32. Khan, D., Jung, L. T., and Hashmani, M. A. Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, 11(20), 9372 (2021).
11. Xi, P., Zhang, X., Wang, L., Liu, W., and Peng, S. A Review of Blockchain-Based Secure Sharing of Healthcare Data. *Applied Sciences*, 12(15), 7912 (2022).
6. Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., and Javaid, N. Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Applied Sciences*, 10(2), 488 (2020).
7. Gaynor, M., Gillespie, K., Roe, A., Crannage, E., and Tuttle-Newhall, J. E. Blockchain Applications in the Pharmaceutical Industry. *Blockchain in Healthcare Today*, 7, 10.30953/bhty.v7.298 (2024).
14. Esmaeilzadeh, P. Benefits and Concerns Associated With Blockchain-Based Health Information Exchange (HIE): a qualitative study from physicians' perspectives. *BMC Medical Informatics and Decision Making*, 22, 80 (2022).
16. Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W., and Ali, I. An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT Images for the Hospitals. *Computerized Medical Imaging and Graphics*, 87, 101812 (2021).
19. Li, T., Wang, H., He, D., and Yu, J. Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT. *IEEE Internet of Things Journal*, 9(16), 15138–15149 (2022).
21. Liu, J., Li, X., Ye, L., Zhang, H., Du, X., and Guizani, M. BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. In *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1–6. https://doi.org/10.1109/GLOCOM.2018.8647713
22. Bhosale, K. S., Nenova, M., and Iliev, G. A study of Cyber Attacks: In the Healthcare Sector. In *2021 Sixth Junior Conference on Lighting (Lighting)*, Gabrovo, Bulgaria, 2021, pp. 1–6. https://doi.org/10.1109/Lighting49406.2021.9598947
23. Kumar, A., Singh, A.K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P.K., Alissa, K.A., Bajaj, M., Ur Rehman, A. and Tag-Eldin, E. A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security against Cyberattacks in Healthcare. *Sensors*, 22(15), 5921 (2022).
33. Nwosu, A. U., Goyal, S. B., Bedi, P. Blockchain Transforming Cyber-Attacks: Healthcare Industry. In: Abraham, A., Sasaki, H., Rios, R., Gandhi, N., Singh, U., and Ma, K. (Eds.), *Innovations in Bio-Inspired Computing and Applications. IBICA 2020.* Advances in Intelligent Systems and Computing, Vol. 1372. Cham: Springer (2021).
34. Guimarães, T., Duarte, R., Cunha, J., Silva, P., and Santos, M. F. The Role of Blockchain Technology in Ensuring Security and Immutability of Open Data in Healthcare. In: Machado, J.M., et al. (Eds.), *Blockchain and Applications, 5th International Congress. Blockchain 2023.* Lecture Notes in Networks and Systems, Vol. 778. Cham: Springer (2023).
35. Kumar, R., and Tripathi, R. Secure Healthcare Framework Using Blockchain and Public Key Cryptography. In: Choo, K. K., Dehghantanha, A., and Parizi, R. (Eds.), *Blockchain Cybersecurity, Trust and Privacy. Advances in Information Security*, Vol. 79. Cham: Springer (2020).
36. Apostolaros, M., Babaian, D., Corneli, A. et al. Legal, Regulatory, and Practical Issues to Consider When Adopting Decentralized Clinical Trials: Recommendations From the Clinical Trials Transformation Initiative. *Therapeutic Innovation & Regulatory Science* 54, 779–787 (2020).
37. Omar, I. A., Jayaraman, R., Salah, K. et al. Applications of Blockchain Technology in Clinical Trials: Review and Open Challenges. *Arabian Journal for Science and Engineering* 46, 3001–3015 (2021).

28. Omar, I. A., Jayaraman, R., Salah, K. et al. Ensuring Protocol Compliance and Data Transparency in Clinical Trials Using Blockchain Smart Contracts. *BMC Medical Research Methodology* 20, 224 (2020).
29. Hang, L., Kim, B., Kim, K., and Kim, D. A Permissioned Blockchain-Based Clinical Trial Service Platform to Improve Trial Data Transparency. *BioMed Research International*, 2021, 5554487 (2021).
30. de-Melo-Diogo, M., Tavares, J., and Nunes Luís, Â. Data Security in Clinical Trials Using Blockchain Technology. In I. Management Association (Ed.), *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 607–625). IGI Global (2023).
31. Hang, L., Chen, C., Zhang, L., and Yang, J. Blockchain for Applications of Clinical Trials: Taxonomy, Challenges, and Future Directions. *IET Communications*, 16, 2371–2393 (2022).
38. Badri, N., Nasraoui, L., Azouz Saïdane, L. A Comprehensive Review of Blockchain Integration in Remote Patient Monitoring for E-Health. *International Journal of Network Management*, 34(2), e2254 (2024).
39. Kazmi, H. S. Z., Nazeer, F., Mubarak, S., Hameed, S., Basharat, A., and Javaid, N. Trusted Remote Patient Monitoring Using Blockchain-Based Smart Contracts. In: Barolli, L., Hellinckx, P., Enokido, T. (Eds.), *Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2019.* Lecture Notes in Networks and Systems, Vol. 97. Cham: Springer (2020).
40. Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A. I., and Abid, M. Secure and Privacy-Aware Blockchain-Based Remote Patient Monitoring System for Internet of Healthcare Things. In *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Bologna, Italy, 2021, pp. 200–205.
41. Hossain Faruk, M. J., Shahriar, H., Valero, M., Sneha, S., Ahamed, S. I., and Rahman, M. Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring. In *2021 IEEE International Conference on Digital Health (ICDH)*, Chicago, IL, USA, 2021, pp. 299–308. https://doi.org/10.1109/ICDH52753.2021.00054

13 Security Challenges and Mitigating Strategies of Digital Twin in Healthcare 5.0

A Review

Deep Solanki

13.1 INTRODUCTION

A digital twin (DT) is a virtual representation of a physical object, system, or process. It is a virtual counterpart or virtual replica of an actual physical entity. The digital twin is fed with real-time data gathered from actual physical entities with the help of sensors, cameras, recorders, and other equipment to replicate the actions and behaviors of real objects with the aim of reducing the errors in physical entities and identifying the improvements. The concept of digital twins was first introduced in 2003 as a part of a course on product lifecycle management [1]. In 2012, researchers at NASA identified the need for digital twins for certification, fleet management, and sustainment of aerospace vehicles and formalized the concept of digital twins [2]. By using the advancements in the Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI), digital twins can significantly improve real-time monitoring, optimizing resources, predictions, and decision-making in various sectors [3]. Digital twins are a critical part of Industry 4.0 as they offer remarkable efficiency and sustainability across various sectors as shown in Figure 13.1. Applications of digital twins are extensive as they include sectors such as manufacturing, where manufacturers can optimize production. In urban planning, a digital twin simulation can help in identifying unsustainable errors and flaws in planning. In healthcare, organs and medical equipment can be virtualized for better and personalized treatment [4]. However, along with the numerous benefits of digital twins, many security risks are also attached, which must be addressed to prevent the misuse of digital twins and maximize the potential of this technology. Some of the security risks are highlighted in Figure and Table 13.2.

Technological advancements in the healthcare sector are significantly transforming the treatment process. The technology of digital twins is one of those developments

DOI: 10.1201/9781003532286-13

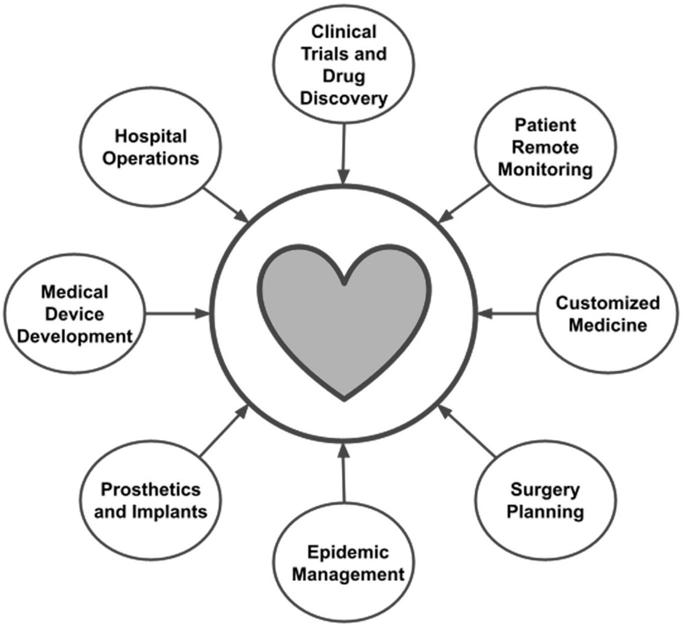


FIGURE 13.1 Benefits of digital twins in the healthcare sector [38]

that can truly revolutionize personal treatment. A digital twin can virtually represent the state of organs or the behavior of medical devices on a patient which is integrated with computational models to simulate the conditions and predict the outcomes that enable better decision-making and improvised and personalized healthcare experience [5]. Data for digital twins can be extracted from a variety of sources such as wearable devices (consisting of health sensors to detect heart rate, blood pressure, sugar level, oxygen level, etc.), imaging devices (such as X-ray machines, CT scans, MRI scans, etc.), and previous electronic health records. We can use this data for patient-specific treatments, precise diagnosis, simulate surgical procedures, predict the course of particular medical treatment, and avoid potential side effects. For example, researchers have developed cardiac digital twins to model heart behavior, allowing precise diagnostics and therapy adjustments for different heart conditions [6]. Also as long-term chronic diseases increase globally, digital twins offer a proactive way to monitor, manage, and predict the health of patients [7]. Even though digital twins in healthcare have enormous benefits, there are various security challenges which has to be considered as any cyber attack on the digital twin can directly harm the health of a person and it can have grave consequences in sensitive sectors such as healthcare [8].

While the advantages of digital twins are desirable, the security challenges cannot be ignored. Digital twins are based on sensitive real-life and real-time data that can be manipulated by a cyber attack. Unauthorized access, data breaches, and ransomware attacks on these systems can have life-threatening consequences, disrupt medical work, and compromise patient safety [9]. Confidential information related to a person or digital resources can be compromised even if databases are encrypted if authentication and authorization mechanisms are weak which can reveal private and sensitive data critical for patient safety [10]. Further, researchers in the paper [11] classified four layers in the digital twin domain that are vulnerable to cyber-attacks. Digital twins have serious security concerns as they can be vulnerable to software attacks such as, privilege escalation, rogue virtual resources, virtual resource tampering, extraction of private information, man-in-the-niddle, and denial of service along with many other attacks [11].

In this chapter, we have focused on identifying methods and procedures in healthcare where digital twins can be used and identifying some of the major security risks associated with digital twin technology. We have also provided a table of remedies consisting of prevention and mitigation strategies for such risks. Our aim is to critically examine the utilization of digital twins in healthcare and enhance security architectures for the safe usage of the technology.

13.2 ORGANIZATION OF THE CHAPTER

In Section 13.1, we gave a brief introduction to digital twins, their utilization in the healthcare sector, and the security challenges associated with such systems. In Section 13.3, we have given the literature survey of the existing schemes for the different use cases of DTs and analyzed various security risks associated with DTs in the healthcare sector. In Section 13.4, we have analyzed different protection mechanisms that exist to secure the DTs. Section 13.5 is the conclusion of our chapter and finally, in Section 13.6, we have included references.

13.3 LITERATURE SURVEY

Digital twin technology in healthcare can revolutionize the health industry. The concept of digital twins was first envisaged in 2003 [1] and it was formalized by NASA for regulation and certification of its aeronautical fleet [2]. Ever since, various

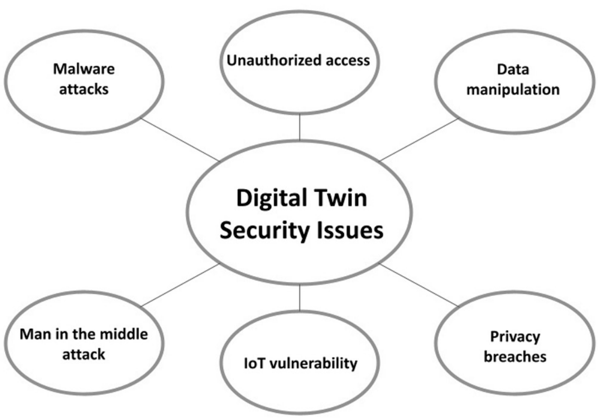


FIGURE 13.2 Security issues with digital twins

industries have found the usefulness of digital twins in their respective domains such as oil and gas [12], smart grids [13, 14], production control [15], water treatment systems [16], manufacturing [17–21], automotive [22–25], and healthcare [3–8, 26–32] along with many other sectors.

In the healthcare sector, digital twins could become an essential part of daily health services [33] due to their ability to clone physical organs and medical equipment. Different twin clones could be used to examine the test results of various medications and their effectiveness over a long period [5]. We can use this technology to simulate surgeries and treatment outcomes, for example, cardiac digital twins can show the changes happening in the heart and preventive measures that can be taken and it can also simulate the effective medications and treatments before a physical twin is damaged [6]. Development of medicine requires years of trials on both animals and humans which has many ethical and health challenges. A digital twin can help us not only to quickly develop medicines and treatment procedures but also reduce other dilemmas [8].

Although the concept and development of digital twins are still in their infant phase, many researchers have worked toward the development of digital twins of human organs. Such digital replicas of individual patients can help us study the nature of these organs in more detail and find novel treatment procedures. In the paper [26], researchers have developed a digital twin of liver development and the discovery of drugs. In the paper [6], the authors have identified ways to develop and utilize digital twins for the purpose of cardiology. The authors of the paper [28] used sensors to gather data and used IoT and AI models to generate virtual representations of lungs. In the paper [29], researchers followed machine learning, artificial intelligence, and statistical analysis–based approaches to use digital twins and they were able to improvise the diagnosis the eye diseases. The authors of [30] worked on bone-based digital twins to gain knowledge on different states of bone tissues. The researchers in [31] have categorized the mechanisms to accurately model the digital twin of skeletal muscle and areas of improvement needed for precise virtual replication. In the paper [32], the digital twin of a brain is conceptualized to fill the gap between the human brain and artificial intelligence where they have used brain functions, brain dysfunctions, and external interventions to model their digital twin. Table 13.1 contains works made in the area of developing digital twin organs.

However, these advancements are not stand alone as there are a number of security risks associated with the concept of digital twins especially in the healthcare sector. We have analyzed the security risks and their impact in Table 13.2. Along with security risks, various methods of prevention and mitigation are also described in Table 13.3 that can help in understanding mechanisms to defend against such threats.

13.4 ANALYSIS

In healthcare, digital twins are highly vulnerable as they are dependent on real-time data from interconnected sensors and devices, and manipulation of resources could lead to harm to the health of a person. Some of the major risks associated with digital twin technology and their impact on healthcare are mentioned in Table 13.2,

TABLE 13.1
Works on Digital Twin Models of Organs

Paper	Work Toward Digital Twin Organ
[26]	Liver
[6, 27]	Heart
[28]	Lungs
[29]	Eyes
[30]	Bones
[31]	Skeletal muscle

TABLE 13.2
Security Risks Associated with DTs in the Healthcare Sector

Paper	Security Risks	Explanation of Risk Impact on the Healthcare Sector
[4]	Unauthorized access	Attackers gain access to - Identity theft sensitive patient data. - Misuse of patient data leading to compromised patient safety
[11]	Data manipulation	Modification of medical - Could lead to misdiagnosis data or outputs in digital - Incorrect treatment plans twins - Risk to patient safety
[34]	Privacy breaches	Unauthorized exposure of - Leakage of confidential medical history patient or operational data. - Social stigmatization
[35] [36] [37]	IoT vulnerability Man in the middle attack Malware attacks	Exploit interconnected - Faulty medical simulations devices to feed inaccurate - Inefficient device performance data to sensors - Delayed emergency responses Attackers intercept - Unauthorized modification of critical treatment data communication between - Service disruption digital twin systems. DTs are insecure to - System shutdowns traditional malware like - Loss of critical patient records ransomware, worms, - Financial and reputational damage spyware, trojans, etc.

As described in Table 13.2, unauthorized access, data manipulation, privacy breaches, IoT vulnerability, man-in-the-middle attacks, and malware attacks are major threats and they can have severe impacts on health, monetary damages, sensitive data leakage, service disruptions, and reputational damages along with other consequences.

Having an understanding of attack vectors is not enough as the development of countermeasures against such attacks is also important to secure our digital and

TABLE 13.3
Prevention and Mitigation Strategies in the Healthcare Sector

Security Risk	Prevention Strategy	Mitigation Strategy
Unauthorized access [4]	- Role-based access controls (RBAC) [38] - Multi-factor authentication (MFA) [39]	- Revoke and reset the credentials [40]
Data manipulation [11]	- Encryption [41] - Blockchain [42]	- Data Hashing [43]
Privacy breaches [34]	- Encryption [41] - Secure access control [44]	- Isolation and containment [45]
IoT vulnerability[35]	- Segmentation of IoT network [46] - Secure authentication mechanism [47]	- Implement Security Orchestration, Automation, and Response (SOAR) in DTs [48]
Man in the middle attack [36]	- Implement IDS/IPS [49] and firewalls [50]	- Cryptography based solutions [51]
Malware attacks [37]	- Vulnerability management [52] - Host hardening [53]	- Threat mitigation [54, 55]

physical assets. We have identified the strategies for the prevention and mitigation of an attack on digital twins which are grouped in Table 13.3.

As described in Table 13.3, prevention and mitigation strategies are listed for major attacks, unauthorized access, data manipulation, privacy breaches, IoT vulnerability, man-in-the-middle attacks, and malware attacks mentioned in Table 13.2.

13.5 PREVENTION STRATEGIES

Prevention strategies are those sets of steps and actions that we use to prevent attacks from happening. It describes a plan that can be utilized to stop different types of attacks from occurring. For each vulnerability mentioned in Table 13.2, we have identified certain preventive measures.

For each mentioned attack in Table 13.2, we have identified the preventive mechanisms to secure our digital twin assets shown in Figure 13.3.

13.5.1 Unauthorized Access

13.5.1.1 Role-Based Access Control (RBAC)

We can implement role-based access control (RBAC) [38] which is a mechanism to secure the authorization process. Figure 13.4 shows the role based access control mechanism to prevent unauthorized access. It allocates role-based permissions to users which makes users utilize only those parts of data to which they are authorized. Permissions are given based on the user's role in the organization. So if the

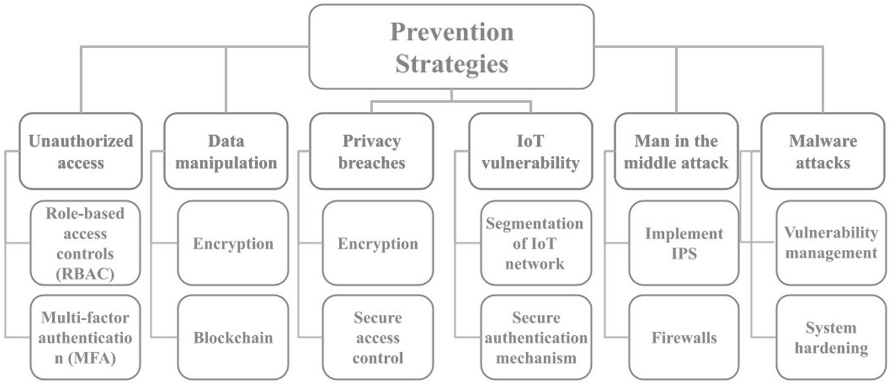


FIGURE 13.3 Prevention strategies for security risks in digital twins

patient wants to access their data they can access it using their role as patient but they can not use any other data. Similarly, doctors can access the data of their particular patients only but they can not access the data of other patients of other doctors. In the same way, digital twin model engineers can access the technical details but they can't access patient's data. However, above mentioned is just an example in reality, who is authorized for which data depends on the policy of access control [56].

13.5.1.2 Multi-Factor Authentication

Another way to prevent unauthorized access is to implement multi-factor authentication (MFA). MFA is a process to authenticate the user multiple times using multiple methods as shown in Figure 13.5 [39]. It is possible that the attacker might be able to bypass the normal user-id and password mechanism by exploiting some

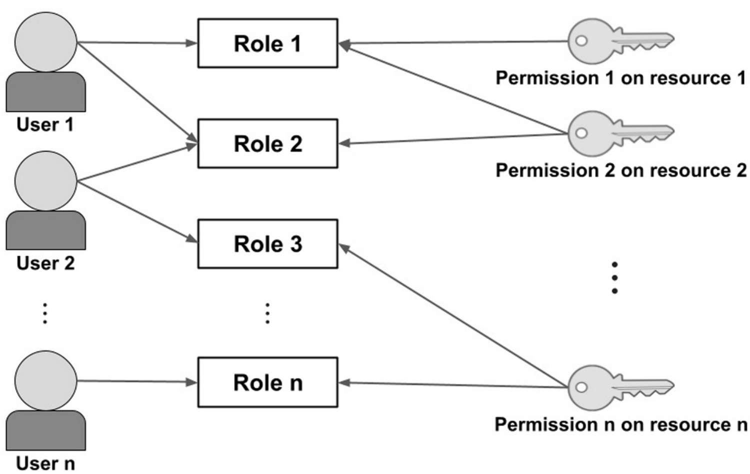


FIGURE 13.4 Prevention strategy—role-based access control (RBAC) [56]

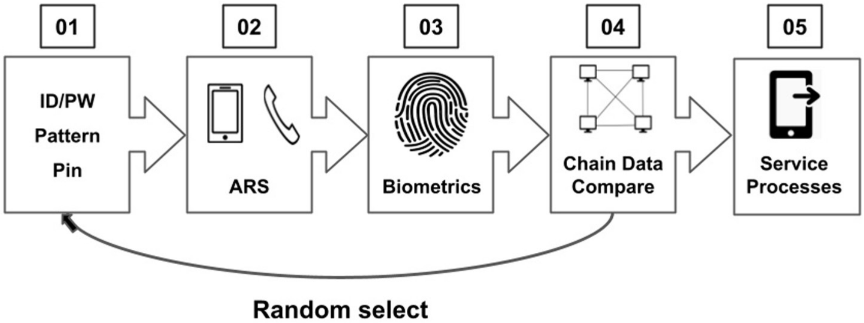


FIGURE 13.5 Prevention strategy—multi-factor authentication [57]

vulnerability. Therefore, having another layer of authentication such as biometrics or email/phone one-time password (OTP) can stop the attacker from gaining access to digital twin resources even after bypassing the first layer of defense [57].

13.5.2 Data manipulation

13.5.2.1 Encryption

One of the most effective ways to prevent data manipulation is to encrypt the data with cryptographically secure algorithms. By encrypting the data, we are preventing the attackers from understanding and analyzing the data Figure 13.6 shows the symmetric and asymmetric cryptographic schemes for preventing data manipulations [41]. This makes it impossible to extract any meaningful information and change it according to the attackers' wishes. We can use both symmetric key (uses the same key for encryption and decryption) and asymmetric key (uses two separate keys known

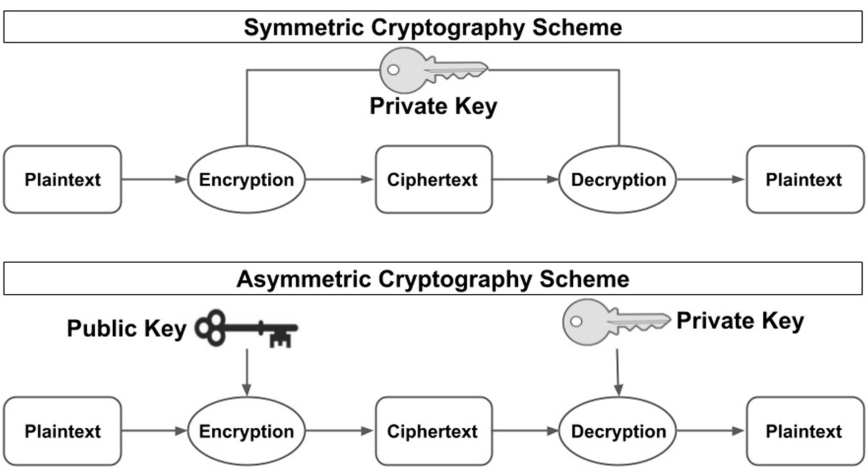


FIGURE 13.6 Prevention strategy—encryption [58]

as public key and private key for encryption and decryption) for securing our data based on the requirement [58]. Encrypting the data not only prevents data manipulation but also prevents privacy violations and misuse of data.

13.5.2.2 Blockchain

Blockchain is a newly emerging technology where we are using a distributed database for storing our data. Every change that we commit in the database will be reflected in the shared ledger across various devices [42]. An authorized change in one device will be inconsistent with ledgers of other devices and we can identify the attempt of manipulation [59]. Figure 13.7 shows the secure data storage mechanism. Blockchain is secure and decentralized records of transactions (changes) and digital twins can utilize it to maintain the integrity of the databases across various platforms and prevent data manipulations.

13.5.3 Privacy breaches

13.5.3.1 Encryption

As discussed in Section 13.3.2.1, encryption converts the data into an unreadable format. Without having a decryption key [41], it is nearly impossible to crack cryptographically secure encryption algorithms. Hence, even if our database is revealed to an unauthorized entity, it can not extract sensitive information about patients, sensors, system configurations, or even metadata.

13.5.3.2 Secure Access Control

It involves creating a policy of access control along with a secure encryption model. It is similar to role-based access control (RBAC) where we limit the permissions to access data based on their role in the organization. Apart from RBAC, relationship-based access control and attribute-based access control are other ways to secure access control as explained in given Figure 13.8.

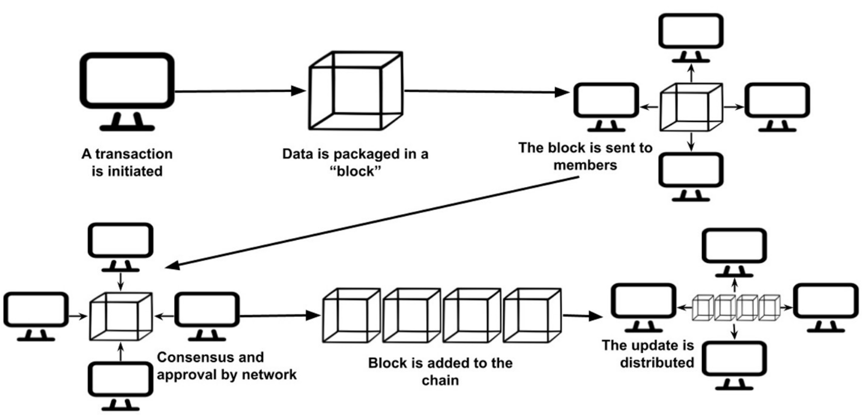


FIGURE 13.7 Prevention strategy—blockchain [59]

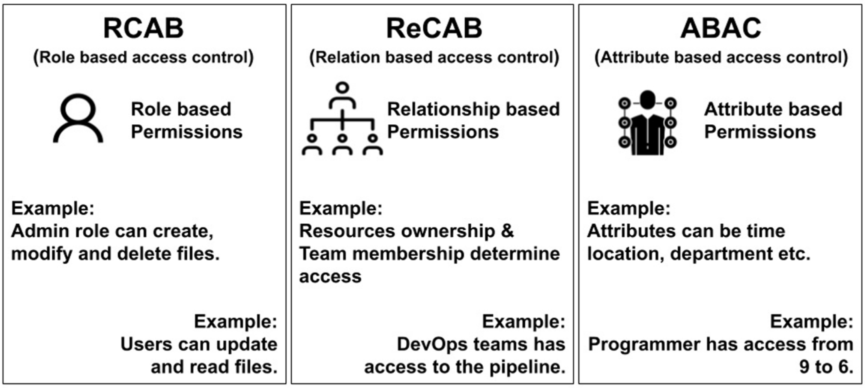


FIGURE 13.8 Prevention strategy—secure access control [65]

13.5.4 IoT Vulnerability

13.5.4.1 Network Segmentation

Segmentation of the network is about dividing the larger network space into smaller subnets. By doing so, we are able to separate the devices from each other into different subnets that prevent the attacker from compromising the entire network of IoT even if a single device gets violated [46]. By segmenting our digital twin derived from a network of IoT sensors we reduce the attack scope of a cyber attack. Network segmentation enhances the security of the network but it could also put additional administrative burden [60]. Figure 13.9 demonstrates how network segmentation can be implemented to enhance the security of a medical campus.

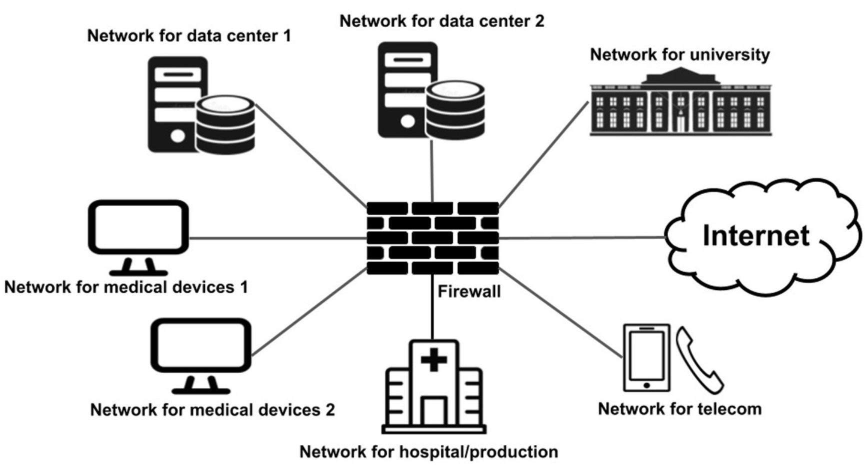


FIGURE 13.9 Prevention strategy—network segmentation [60]

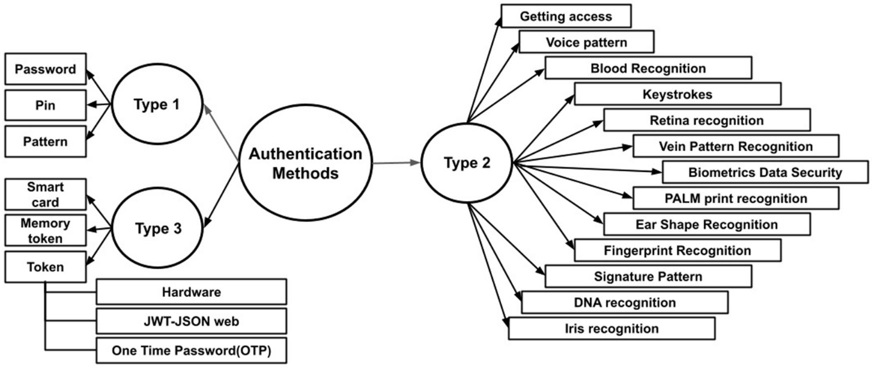


FIGURE 13.10 Prevention strategy—secure authentication mechanism [61]

13.5.4.2 Secure Authentication Mechanisms

In IoT-based digital twins, data is fed to the virtual twin through devices and sensors. Each device can have its own vulnerabilities and can pose serious threats to the overall network and patient health. Access to each device must be secured with a suitable authentication mechanism to prevent the attackers from exploiting vulnerabilities in IoT devices' networks. Authors in the paper [47] have developed a privacy-preserving authentication mechanism for digital twins using decentralized identity. Depending upon the requirement, various mechanisms for authentication are categorized into three types as described in Figure 13.10 [61].

13.5.5 Man-in-the-Middle Attacks

13.5.5.1 IDS in Digital Twins

Intrusion detection systems are used to identify malicious activities happening in the system host or network. IDS for digital twins is a relatively new idea where we identify signatures-based and statistical anomaly-based models to identify intrusion in the resources supporting virtual replicas. Given Figure 13.11 shows how IDS interacts with various layers. Man-in-the-middle attacks usually target the network channels to intercept the communication. Signature-based IDS uses the existing signatures of attacks to detect and prevent future intrusion while statistical anomaly-based IDS marks the behavioral patterns in normal conditions to identify variations (anomalies) that occur during the attack [49].

13.5.6 Malware Attacks

13.5.6.1 Vulnerability Management

Malware refers to malicious software designed to harm digital resources. Malware is designed to exploit the existing vulnerabilities in the system. There are many types

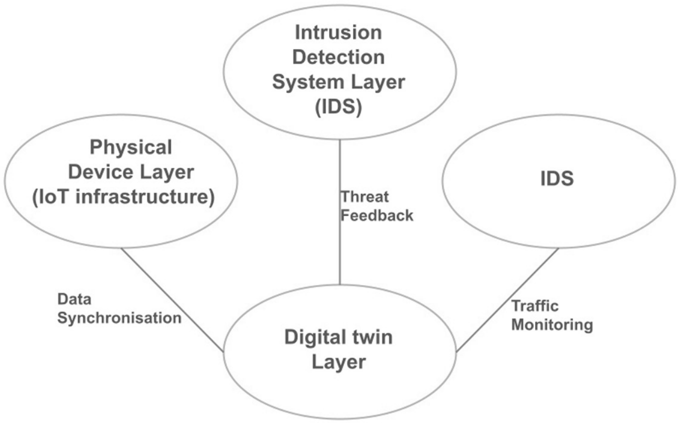


FIGURE 13.11 Prevention strategy—IDS in digital twin [66]

of malware such as viruses, worms, ransomware, spyware, trojans, etc. where each has different functionality and exploits different types of vulnerabilities existing in the system [52]. To prevent these malware attacks we can implement vulnerability management. Figure 13.12 shows vulnerability prevention strategy. To secure the digital twins, patch management has to be implemented to remove such vulnerabilities and secure our system resources [62].

13.5.6.2 System Hardening

It is a mechanism to limit the default permissions of the system. Figure 13.13 displays different methods that we can implement for system hardening. In the case of digital twins, we can limit the functionality of the virtual system by removing unnecessary features that can potentially be exploited by malware attacks [53]. It involves closing open ports, blocking unrequired protocols, enforcing password complexity and password updation at regular intervals, removing unnecessary libraries, giving limited capabilities to users, allowing only updated versions of software, etc.

13.6 MITIGATION STRATEGIES

Mitigation strategies are those sets of steps and actions that we use to prevent attacks from happening. It describes a plan that can be utilized to stop different types of

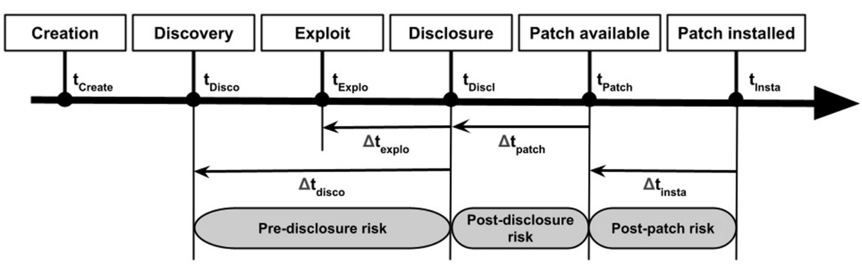


FIGURE 13.12 Prevention strategy—vulnerability management [62]

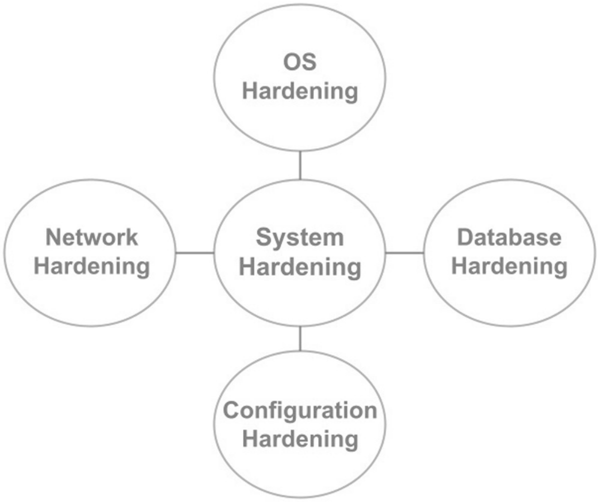


FIGURE 13.13 Prevention strategy—system hardening

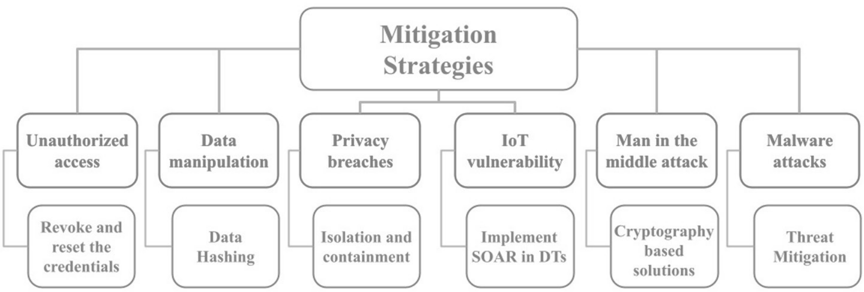


FIGURE 13.14 Mitigation strategies for security risks in digital twins

attacks from occurring. For each vulnerability mentioned in Table 13.2, we have identified certain preventive measures.

Prevention strategies are useful to prevent attacks while mitigation strategies are used when an attack has happened in our system and now we have to quickly eliminate the threat and minimize the damage. Below, we have discussed mitigation plans that can be used if our digital twin is compromised. Figure 13.14 provides categories of mitigation techniques that we can utilize to counter different attacks.

13.6.1 Unauthorized Access

13.6.1.1 Revoke and Reset the Credentials

If suspicious activities of unauthorized access are confirmed, we should immediately revoke the existing credentials of users and assign them a new set of credentials [40]. Figure 13.15 demonstrates how we can revoke and reset credentials with immediate effect in the case of unauthorized access. If unauthorized access is caused due to

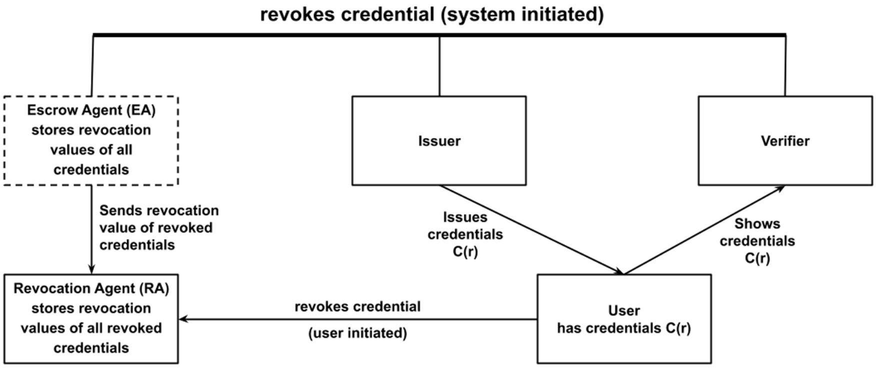


FIGURE 13.15 Mitigation strategy—revoke and reset the credentials [67]

credential leakages then we'll be able to mitigate the threat immediately. However, if another vulnerability is exploited for unauthorized access then we'll need a different strategy.

13.6.2 Data Manipulation

13.6.2.1 Data Hashing

One of the best ways to identify the manipulation in data is by using irreversible hash functions such as SHA-256, MD-5, etc. to generate the hash value. Further, we can integrate blockchain to improve the integrity of medical data in digital twins [43]. Even a single bit of data integrity violation will result in a completely different value of hash using which we can detect the violation in the data integrity. In case of manipulation, we can use data backup to restore to the point where the data was not manipulated and integrity was maintained. As shown in the given Figure 13.16, a minor change in the password field leads to a completely different value of hash which we can compare and identify manipulation in data.

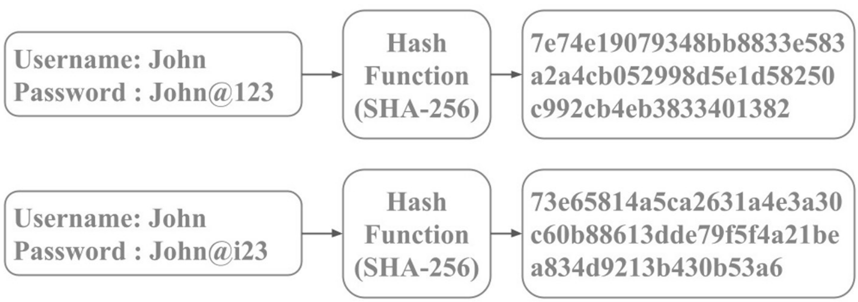


FIGURE 13.16 Mitigation strategy—data hashing

13.6.3 Privacy Breaches

13.6.3.1 Isolation and Containment

Once a privacy breach occurs we can not fully reverse the effect as data is now available to attackers who might generate multiple copies of breached data. However, we can reduce the effect of breaches by taking certain actions to stop the further spread and misuse of data such as isolating the databases, resetting credentials, restricting digital twins from accessing further sensitive data, contacting legal authorities to punish the culprits, and reducing the spread of the breach [45]. An incident response plan should be prepared to initiate the damage control and removal of threats quickly.

13.6.4 IoT Vulnerability

13.6.4.1 Implement SOAR in DTs

SOAR is an acronym for security orchestration, automation, and response and it is used for managing digital tools and resources. SOAR is a combination of manual and automatic responses to cyber attacks used to counter continuously emerging cyber threats. Countermeasures are defined in the "playbook" for different attacks to reduce the time of response action and mitigate the attack quickly. IoT devices used for digital twins are made up of multiple endpoint devices and sensors with complicated networks. A framework to utilize SOAR in IoT devices for digital twins is designed in the paper [63]. Here, Figure 13.17 shows how these mechanisms can be utilized together to provide robust security posture.

13.6.5 Man-in-the-Middle Attacks

13.6.5.1 Cryptography-Based Solutions

Using digital certificates, digital signatures, hashing, steganography, protocols, and encryption mechanisms can mitigate the security issue of man-in-the-middle attacks as shown in Figure 13.18 [64]. Physical entities and their digital twins are connected

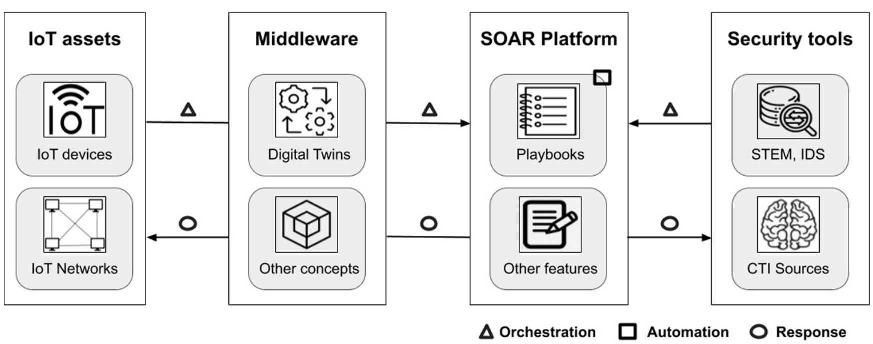


FIGURE 13.17 Mitigation strategy—implement SOAR in DTs [63]

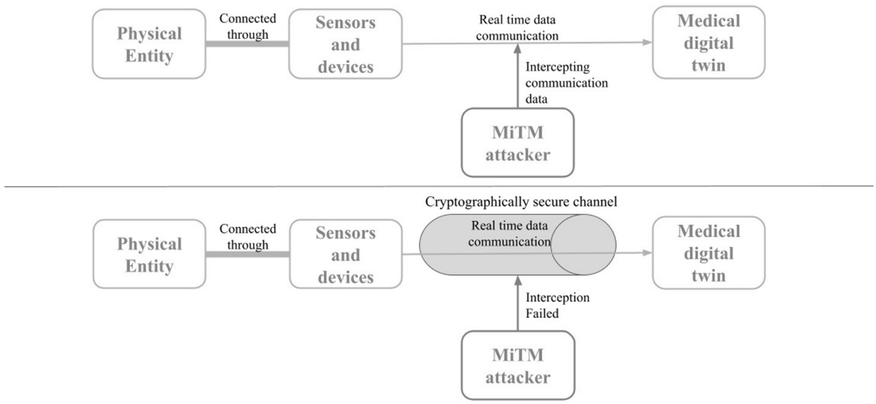


FIGURE 13.18 Mitigation strategy—cryptographic solutions

through sensors and devices. Any communication changes in sensors attached to digital twins could result in unreliable and false digital twin outcomes. To mitigate the attack, we can deploy cryptographic algorithms to establish confidentiality and verify the integrity of the communicated data.

13.6.6 Malware Attacks

13.6.6.1 Threat Mitigation

Different types of malware can sabotage the digital twin infrastructure in various ways. Such as ransomware can encrypt all the functionalities of digital twins for ransom, wiper malware can delete all the files and critical data, spyware can steal sensitive patient and model information, rootkits can grant unauthorized access to

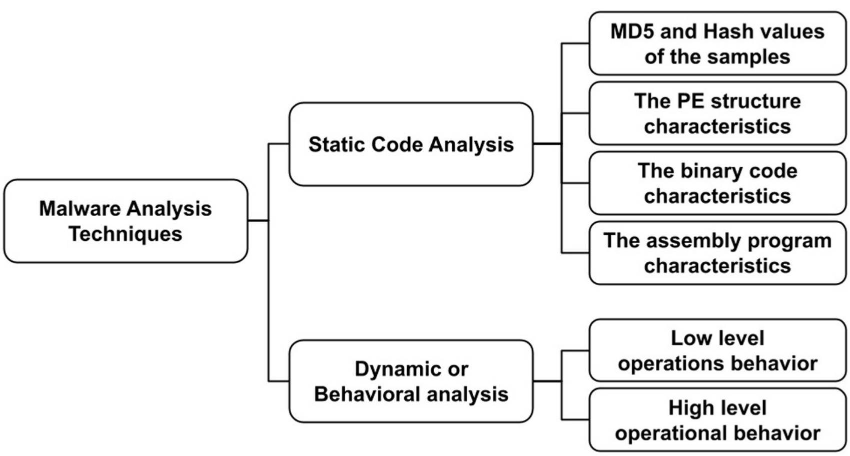


FIGURE 13.19 Mitigation strategy—malware threat mitigation [55]

attackers, and many more [54]. Malware can be best mitigated by patching the vulnerability itself. Static and dynamic analysis can help identify and analyze the existing threats and mitigate them [55]. We can use forensic malware analysis methods presented in Figure 13.19 to understand, analyze, remove and recover from malwares and their negative effects in the digital twin infrastructure.

13.7 CONCLUSION

In conclusion, we can say that it is clear that digital twins have tremendous potential to revolutionize the healthcare domain. It can replicate the physical organs, medical devices, and treatment procedures in the virtual space which will improve our decision-making and reduce the errors in the actual physical domain. However, there are several security challenges as well that can cause serious harm to patients if not taken seriously. Some of the major and critical challenges are analyzed in detail in the analysis. We also analyzed their prevention and mitigation strategies in detail which can be a guide for further development of other preventive and mitigation measures and strategies. Digital twins are still a new technology whose security aspects have not yet been explored in depth. Many unidentified challenges could still exist which is a scope of future study. If we can achieve a secure environment for digital twins to thrive then it can change the face of medical treatment forever. There are still many vulnerable aspects to discover and resolve before we fully adopt the technology. We hope that our work was helpful to readers in understanding the security issues of digital twins in healthcare and inspired them to work further in this field.

REFERENCES

1. Grieves, Michael. “Digital twin: manufacturing excellence through virtual factory replication.” White paper 1.2014 (2014): 1–7.
2. Glaessgen, Edward, and David Stargel. “The digital twin paradigm for future NASA and US Air Force vehicles.” In *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA*; 2012.
3. Tao, Fei, et al. “Digital twin in industry: State-of-the-art.” *IEEE Transactions on Industrial Informatics* 15(4), 2405–2415 (2018).
4. Fuller, Aidan, et al. “Digital twin: Enabling technologies, challenges and open research.” *IEEE Access* 8, 108952–108971 (2020).
5. Bruynseels, Koen, Filippo Santoni de Sio, and Jeroen Van den Hoven. “Digital twins in health care: ethical implications of an emerging engineering paradigm.” *Frontiers in Genetics* 9, 31 (2018).
6. Corral-Acero, Jorge, et al. “The ‘Digital Twin’to enable the vision of precision cardiology.” *European Heart Journal* 41(48), 4556–4564 (2020).
7. Sun, Tianze, Xiwang He, and Zhonghai Li. “Digital twin in healthcare: Recent updates and challenges.” *Digital Health* 9, 20552076221149651 (2023).
8. Papachristou, Konstantinos, et al. “Digital Twins’ Advancements and Applications in Healthcare, Towards Precision Medicine.” *Journal of Personalized Medicine* 14(11), 1101 (2024).
9. Suhail, Sabah, Raja Jurdak, and Rasheed Hussain. “Security attacks and solutions for digital twins.” *arXiv preprint arXiv:2202.12501* (2022).

10. Schroeder, Greyce N., et al. “A methodology for digital twin modeling and deployment for industry 4.0.” *Proceedings of the IEEE* 109(4), 556–567 (2020).
11. Alcaraz, Cristina, and Javier Lopez. “Digital twin: A comprehensive survey of security threats.” *IEEE Communications Surveys & Tutorials* 24(3), 1475–1503 (2022).
12. Analogi. “ATOM: Digital Twin of Siemens Gas Turbine Fleet Operations.” (2020).
13. Olivares-Rojas, Juan C., et al. “Towards cybersecurity of the smart grid using digital twins.” *IEEE Internet Computing* 26(3), 52–57 (2021).
14. Min, Qingfei, et al. “Machine learning based digital twin framework for production optimization in petrochemical industry.” *International Journal of Information Management* 49, 502–519 (2019).
15. Örs, Evrim, et al. “A conceptual framework for AI-based operational digital twin in chemical process engineering.” In *2020 IEEE international conference on engineering, technology and innovation (ICE/ITMC)*. IEEE, 2020.
16. Sugumar, Gayathri, and Aditya Mathur. “Assessment of a method for detecting process anomalies using digital-twinning.” In *2019 15th European Dependable Computing Conference (EDCC)*. IEEE, 2019.
17. Anylogic. *Digital Twin of a Manufacturing Line: Helping Maintenance Decision-Making*, CNH Industries and Fair Dynamics, 2020.
18. Vachálek, J., L. Bartalský, O. Rovný, M. Morháč, and M. Lokšík, “The Digital Twin of an Industrial Production Line Within the Industry 4.0 Concept,” In *2017 21st international conference on process control (PC)* (pp. 258–262). IEEE, 2017.
19. Semenkov, Kirill, et al. “Validation of complex control systems with heterogeneous digital models in industry 4.0 framework.” *Machines* 9(3), 62 (2021).
20. Khan, Abid, et al. “Toward smart manufacturing using spiral digital twin framework and twinchain.” *IEEE Transactions on Industrial Informatics* 18(2), 1359–1366 (2020).
21. Bevilacqua, Maurizio, et al. “Digital twin reference model development to prevent operators’ risk in process plants.” *Sustainability* 12(3), 1088 (2020).
22. Damjanovic-Behrendt, Violeta. “A digital twin-based privacy enhancement mechanism for the automotive industry.” In *2018 International Conference on Intelligent Systems (IS)*. IEEE, 2018.
23. Magargle, Ryan, et al. “A Simulation-Based Digital Twin for Model-Driven Health Monitoring and Predictive Maintenance of an Automotive Braking System.” In *Modelica* (Vol. 132, p. 35), 2017.
24. Veledar, Omar, Violeta Damjanovic-Behrendt, and Georg Macher. “Digital twins for dependability improvement of autonomous driving.” In *European Conference on Software Process Improvement*. Cham: Springer International Publishing, 2019.
25. Almeaibed, Sadeq, et al. “Digital twin analysis to promote safety and security in autonomous vehicles.” In *IEEE Communications Standards Magazine* 5(1), 40–46 (2021).
26. Subramanian, Kalyanasundaram. “Digital twin for drug discovery and development—the virtual liver.” *Journal of the Indian Institute of Science* 100(4), 653–662 (2020).
27. rayanova, Natalia A., and Adityo Prakosa. “Up digital and personal: How heart digital twins can transform heart patient care.” *Heart Rhythm* 21(1), 89–99 (2024).
28. Avanzato, Roberta, et al. “Lung-DT: an AI-powered digital twin framework for thoracic health monitoring and diagnosis.” *Sensors* 24(3), 958 (2024).
29. Iliuţă, Miruna-Elena, et al. “Digital Twin Models for Personalised and Predictive Medicine in Ophthalmology.” *Technologies* 12(4) 55 (2024).
30. Dimbath, Elizabeth, Anup Pant, and Ali Vahdati. “Digital twins for understanding the mechanical adaptation of bone in disease and postsurgery.” *Digital Human Modeling and Medicine*, 493–513 (2023).

31. Liu, Dan, et al. "Advances in digital twins technology of human skeletal muscle." *Sheng wu yi xue Gong Cheng xue za zhi= Journal of Biomedical Engineering= Shengwu Yixue Gongchengxue Zazhi* 40(4), 784–791 (2023).
32. Xiong, Hui, et al. "The digital twin brain: A bridge between biological and artificial intelligence." *Intelligent Computing* 2, 0055 (2023).
33. Scoles, Sarah. "*A digital twin of your body could become a critical part of your health care*." Brooklyn, NY, USA: Slate, 2016.
34. Masison, Joseph, et al. "A modular computational framework for medical digital twins." *Proceedings of the National Academy of Sciences* 118(20), e2024287118 (2021).
35. Pirbhulal, Sandeep, Habtamu Abie, and Ankur Shukla. "Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications." In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*. IEEE, 2022.
36. Jameil, Ahmed K., and Hamed Al-Raweshidy. "AI-Enabled Healthcare and Enhanced Computational Resource Management With Digital Twins Into Task Offloading Strategies." *IEEE Access* 12, 90353–90370 (2024).
37. Al-Dalati, Issam. "Digital twins and cybersecurity in healthcare systems." In *Digital Twin for Healthcare* (pp. 195–221). Academic Press, 2023.
38. Alshammari, Kaznah. "Access management for digital twins in the built environment." Diss. Cardiff University, 2021.
39. Sain, Mangal, et al. "A survey on the security in cyber physical system with multi-factor authentication." In *2021 23rd international conference on advanced communication technology (ICACT)*. IEEE, 2021.
40. Satsangi, Ankit, Pankaj Dashore, and Rachana Dashore. "Secure Digital Identity Cards With Blockchain and Digital Twins Approach." In *Ensuring Security and End-to-End Visibility Through Blockchain and Digital Twins* (350–361). IGI Global, 2024.
41. Stergiou, Christos L., Maria P. Koidou, and Konstantinos E. Psannis. "IoT-based big data secure transmission and management over cloud system: A healthcare digital twin scenario." *Applied Sciences* 13(16), 9165 (2023).
42. Dai, Yueyue, et al. "Blockchain empowered access control for digital twin system with attribute-based encryption." *Future Generation Computer Systems* 160, 564–576 (2024).
43. Yi, Haibo. "Improving cloud storage and privacy security for digital twin based medical records." *Journal of Cloud Computing* 12(1), 151 (2023).
44. Saeed, Mamoon Mohammed Ali, Rashid A. Saeed, and Zeinab E. Ahmed. "Data Security and Privacy in the Age of AI and Digital Twins." In *Digital Twin Technology and AI Implementations in Future-Focused Businesses* (99–124). IGI Global, 2024.
45. Damjanovic-Behrendt, Violeta. "A digital twin-based privacy enhancement mechanism for the automotive industry." In *2018 International Conference on Intelligent Systems (IS)*. IEEE, 2018.
46. Bellavista, Paolo, et al. "Digital twin oriented architecture for secure and QoS aware intelligent communications in industrial environments." *Pervasive and Mobile Computing* 85, 101646 (2022).
47. Patel, Chintan, et al. "User-empowered secure privacy-preserving authentication scheme for Digital Twin." *Computers & Security* 140, 103793 (2024).
48. Empl, Philip, et al. "SOAR4IoT: securing IoT assets with digital twins." In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (p. 46). 2022.
49. Gupta, Deepti, et al. "Hierarchical federated learning based anomaly detection using digital twins for smart healthcare." In *2021 IEEE 7th international conference on collaboration and internet computing (CIC)*. IEEE, 2021.

50. Salim, Mikail Mohammed, David Camacho, and Jong Hyuk Park. "Digital Twin and federated learning enabled cyberthreat detection system for IoT networks." *Future Generation Computer Systems* 161, 701–713 (2024).
51. Bhushan, Bharat, Ganapati Sahoo, and Amit Kumar Rai. "Man-in-the-middle attack in wireless and computer networking—A review." In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017.
52. Bajpayi, Pragya, Smita Sharma, and Madhu Sharma Gaur. "AI Driven IoT Healthcare Devices Security Vulnerability Management." In *2024 2nd International Conference on Disruptive Technologies (ICDT)*. IEEE, 2024.
53. Lo Bianco, Davide. "Cybersecurity assessment and host hardening policies for virtualization technologies." Diss. Politecnico di Torino, 2022.
54. Franco, Javier, et al. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23(4), 2351–2383 (2021).
55. Kumar, Manish. "Scalable malware detection system using big data and distributed machine learning approach." *Soft Computing* 26(8), 3987–4003 (2022).
56. Abdelfattah, Doaa, Hesham A. Hassan, and Fatma A. Omara. "A novel role-mapping algorithm for enhancing highly collaborative access control system." *Distributed and Parallel Databases* 40(2), 521–558 (2022).
57. Kim, Semin, Hyung-Jin Mun, and Sunghyuck Hong. "Multi-factor authentication with randomly selected authentication methods with DID on a random terminal." *Applied Sciences* 12(5), 2301 (2022).
58. Thabit, Ahmed A., and Hadi T. Ziboon. Improving probability of detection using CFAR and adaptive threshold for cognitive radio (CR), International Journal of Engineering and Advanced Technology, Vol 4, Issue 5. 2015
59. Goni, Nasim Al, Sherif Saad Ahmed, and Ahmed Ibrahim. "A P2P Optimistic Fair-Exchange (OFE) Scheme for Personal Health Records Using Blockchain Technology." In *3rd International Conference on Wireless, Intelligent and Distributed Environment for Communication: WIDECOM 2020*. Springer International Publishing, 2020.
60. Johansson, David, et al. "Information Technology and Medical Technology Personnel's Perception Regarding Segmentation of Medical Devices: A Focus Group Study." In *Healthcare* (Vol. 8, No. 1, p. 23). MDPI (2020).
61. Pooyandeh, Mitra, Ki-Jin Han, and Insoo Sohn. "Cybersecurity in the AI-Based metaverse: A survey." *Applied Sciences* 12(24), 12993 (2022).
62. Jimmy, F. N. U. "Understanding Ransomware Attacks: Trends and Prevention Strategies." *Journal of Knowledge Learning and Science Technology* 2(1), 214 (2023). https://doi.org/10.60087/jklst.vol2.n1.p214.
63. Empl, Philip, et al. "SOAR4IoT: securing IoT assets with digital twins." In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1–10). 2022.
64. Katz, Jonathan. *Efficient cryptographic protocols preventing "man-in-the-middle" attacks*. Columbia University, 2002.
65. Vanessa Villa. "RBAC vs ReBAC vs ABAC: Comparison and Guide on how to get started." Available at: https://pangea.cloud/blog/rbac-vs-rebac-vs-abac/
66. El-Hajj, Mohammed. "Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures." *Electronics* 13(19), 3941 (2024).
67. Lueks, Wouter, et al. "Fast revocation of attribute-based credentials for both users and verifiers." *Computers & Security* 67, 308–323 (2017).

14 Pilot Projects of Digital Twin and Blockchain Fusion for Healthcare 5.0

Munish Kumar

14.1 INTRODUCTION

Digital transformation of the healthcare industry has been on an accelerated pattern since the COVID-19 pandemic led healthcare professionals across the world to adopt new ways of delivering care without exposing themselves and their patients to unnecessary risk of face-to-face visits. With this digital healthcare revolution comes one of its emerging trends—the combination of blockchain technology and digital twin technology, which has the potential to completely revolutionize the sector and become the cornerstone of Healthcare 5.0.

Digital twins, which are virtual representations of physical assets, processes, or systems, have already demonstrated their worth in various industries, including manufacturing and infrastructure. In the healthcare setting, digital twins can be used to create personalized models of patients, allowing for more accurate diagnosis, treatment, and monitoring. New healthcare highlights patient-centered care, which requires secure communication among multiple participants. Ensuring the safe exchange of patient data is critical but can often be a time-consuming and complex process.

By automating the data-sharing mechanism, a patient digital twin can simplify how the involved actors in care delivery (not only the providers but also the payers, administrators, government agencies, community-based organizations, etc.) interact with each other while accelerating the realization of preventive and predictive interventions all while protecting patient data [18]. Blockchain's intrinsic properties of decentralization, immutability, and transparency make it a compelling technology for healthcare applications, particularly in the areas of electronic medical record management, supply chain tracking, clinical trials, and patient data management. Serious errors in the medical domain, including some that may do more harm than good, are reliably detectable, using data from blockchain-based software. This, in turn, can potentially improve the effectiveness, safety, and transparency of medical data sharing in the healthcare system.

The study in [2] explains the Internet of Things (IoT)-based blockchain along with digital twins along with the concept and architecture of this solution. The author explains the significance of this solution, mentioning the data integrity, security, and

DOI: 10.1201/9781003532286-14

transparency. The use of digital twins with blockchain can also enhance interoperability within healthcare systems, enabling patients and different providers to seamlessly exchange information. However, due to the complex nature of healthcare systems and the novelty of these technologies, their effective deployment necessitates careful planning and validation.

Pilot projects play a critical role in bridging the gap between theoretical promise and real-world implementation by providing a controlled environment for testing and refining these technologies. Pilot projects demonstrate the impact of blockchain and digital twin technologies on clinical outcomes and operational efficacy, thereby providing a basis for assessing their feasibility in specific healthcare environments. They also provide a low-risk environment in which to identify potential issues and remedy them before wider roll-out. Because pilot projects hold the promise of facilitating stakeholder engagement and buy-in, they provide bureaucrats an opportunity to evaluate the impact of blockchain on data management and physicians a chance to see firsthand how digital twins improve patient care.

Pilots are needed to test interoperability and integration with existing medical equipment, electronic health records (EHRs), and other digital systems. They also ensure compliance with strict legal requirements, such as the GDPR in Europe or the HIPAA (Health Insurance Portability and Accountability Act of 1996) in the United States. The feasibility of the pilot programs is another key element such as planning resources and scalability. Learnings and best practices from successful pilot projects, including documentation on technology integration, workflow modifications, stakeholder training, and impact measurement, can be applied for future implementation. Additionally, they promote an innovative culture that regularly explores and tests new concepts and technology [1, 4].

14.2 ARCHITECTURE OF DIGITAL TWIN AND BLOCKCHAIN-BASED HEALTHCARE SYSTEM

With the healthcare industry turning toward blockchain and digital twin technology, a smooth and secure workflow is ensured. First, patients' data such as medical records, diagnostic information, and real-time sensor data need to be securely stored in a blockchain network. This blockchain-enabled data-storage mechanism will enable transparency and trust in the healthcare system through data integrity and transparency of the data tracing process. This blockchain data is then used in conjunction with other relevant information to create a digital twin, a digital representation of the patient. By acting as a thorough model of the patient's current state of health, this digital twin enables medical professionals to model, examine, and anticipate possible problems. [3]cancer

Healthcare providers can access the digital twin of the patient and interact with it to guide personalized treatment protocols and make adjustments. The underlying blockchain technology ensures that every interaction and change with the digital twin is recorded and immutable, enhancing accountability and providing a secure audit trail. Figure 14.1 is an architectural diagram for the healthcare blockchain-based digital twin showing interactions between different components.

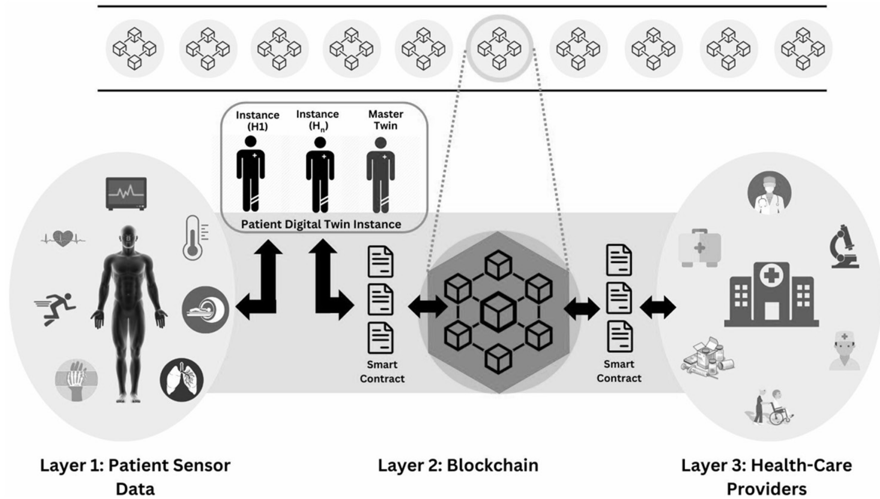


FIGURE 14.1 Architectural diagram of the blockchain-based digital twin for healthcare

14.3 PILOT PROJECTS OF DIGITAL TWINS AND BLOCKCHAIN FUSION FOR HEALTHCARE 5.0

Many pilot engagements in recent years have been related to blockchain and digital twin convergence in healthcare. These pilot projects explore ways in which this combination can be used to address the opportunities and challenges posed by the new Healthcare 5.0 paradigm. One of these pilot projects focused on a transparent and secure way of tracing pharmaceutical products in the supply chain using blockchain technology and digital twins [7].

This was a pilot project to boost the integrity and admissibility of the pharmaceutical supply chain and ultimately help patients by leveraging digital twins' real-time monitoring and control features along with blockchain's heightened security and transparency [5, 7, 8]. A separate pilot study examined the potential of blockchain and digital twins for decentralized management of healthcare data, enabling individuals to own and control their personal data and facilitate the exchange of data between healthcare providers in a secure manner.

Patients will gain greater control over their health information, which may encourage accountability and transparency in the healthcare system [5–7]. By enabling the seamless exchange of information between different healthcare providers and patients, the integration of blockchain technology and digital twins can also enhance the interoperability of healthcare systems.

14.3.1 Project (No. 2018AAA067): Chronic Disease Management via Digital Twin and Blockchain

Chronic disease management (CDM) is one of the most significant challenges in global healthcare systems. Traditional methods of managing diseases such as diabetes, hypertension, and cardiovascular illnesses require constant monitoring, timely interventions, and data management. However, with advancements in digital technologies, innovative approaches, for example, digital twins, virtual replicas of physical systems, enabling real-time analysis and simulations, enhancing decision-making and operational efficiency, and blockchain for security and transparency [9] have emerged to address these challenges. One such transformative initiative is taken by the National Natural Science Foundation of China (No. 81974355 and No. 82172525), the National Intelligence Medical Clinical Research Center (No. 2020021105012440), and the Hubei Province Technology Innovation Major Special Project (No. 2018AAA067) project [10]**,** which leverages digital twin and blockchain technologies to revolutionize chronic disease management. A digital twin is a virtual representation of a physical system, in this case, a human body. For chronic disease management, a digital twin can replicate a patient's biological processes, continuously collecting real-time data from wearable devices, sensors, and medical records. The digital twin then uses AI and machine learning algorithms to simulate how the patient's condition might evolve, predict potential complications, and suggest personalized treatment plans.

The project harnesses the potential of digital twins to improve the management of chronic conditions by simulating disease progression, digital twins can forecast the likely future outcomes of a patient's condition, allowing for preventive measures before symptoms worsen.

Based on real-time vital sign monitoring and other pertinent health data, each patient's digital twin can assist medical professionals in developing a customized treatment plan. Because their health data is continuously monitored remotely, patients do not need to attend clinics on a regular basis. This improves patient outcomes while lessening the strain on healthcare systems. The effectiveness of treatment can be assessed instantly. In order to maximize patient care, changes can be taken right once if a treatment plan is not producing the expected outcomes.

Making sure that data flows securely and transparently is one of the major issues in managing chronic diseases. This is addressed by blockchain technology, which offers a decentralized, impenetrable record that guarantees data confidentiality, transparency, and integrity. Because blockchain technology is decentralized, patient data is safe, unchangeable, and impossible for unauthorized parties to alter. When handling private health data, this is essential. Blockchain makes it possible for various insurance companies, healthcare providers, and other stakeholders to efficiently and securely access patient data. The smooth exchange of information improves patient care coordination. Blockchain gives individuals greater control over who can access their health information and when. People are now empowered to actively manage their conditions thanks to the shift toward patient-centered data management. An overview of the information processing is shown in Figure 14.2.

The authors in [10] conducted a case study focusing on chronic diseases, for example, cardiovascular diseases, diabetes, and pulmonary diseases. The patient uses **wearable** devices [14] to monitor and gather health-related data continuously. These devices, equipped with smart technology and embedded intelligence, serve as a bridge between the physical and digital aspects of healthcare. By leveraging **edge**

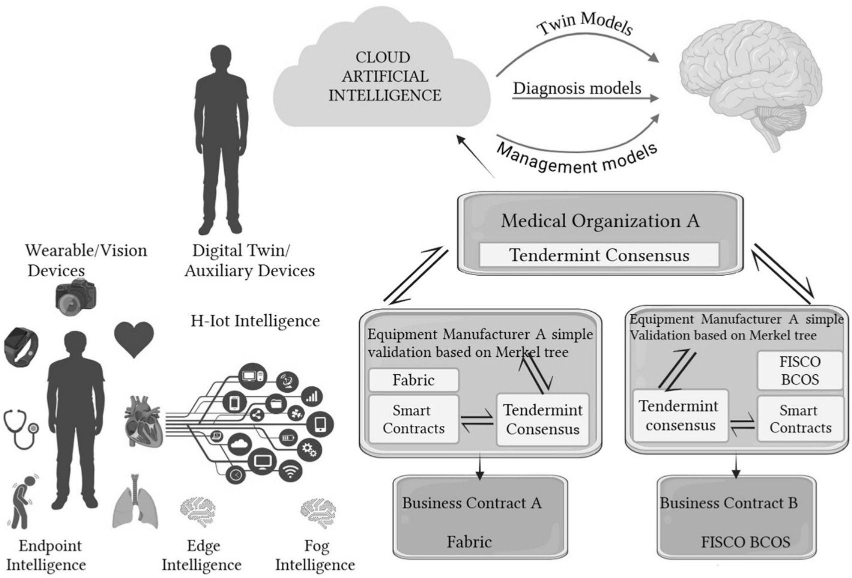


FIGURE 14.2 Flow of information in digital twin and blockchain-based healthcare system [10]

and fog computing, **blockchain** technology, and **cloud-based digital twin models**, healthcare providers can not only monitor patients in real time but also predict potential health risks and devise personalized treatment plans.

14.3.1.1 Wearable Devices: A Source of Smart Data

Wearable devices, such as smartwatches, fitness trackers, and health monitoring sensors, have become integral tools in modern healthcare. Numerous physiological data, including heart rate, body temperature, blood oxygen levels, sleep patterns, and physical activity, can be monitored by the sensors built into these devices. These wearables are unique because of their inherent intelligence, which enables them to analyze information locally, react to changes, and adjust to the wearer's surroundings.

The data generated from wearable devices is rich in detail. It offers constant, up-to-date data on a patient's condition, enabling prompt actions as needed. An important development is the move to continuous monitoring from periodic data gathering, which is usually observed in conventional healthcare settings. Wearable technology gathers data continuously, providing medical professionals with information about a patient's changing health that was previously impossible to obtain through routine examinations.

14.3.1.2 Edge and Fog Computing: Optimizing Analytics

Effective data processing is needed in light of the huge amount of data generated by wearable technology. Fog computing and edge computing come in handy in this case. Real-time analysis and faster decision-making are enabled by these paradigms of computing, which bring data processing nearer to the source.

- **Edge computing** is a method in which data is processed directly on the wearable device or on a local node in the vicinity (such as a smartphone or a specialized gateway). This is especially useful for low-latency applications that must analyze data immediately. To guarantee that critical health events are dealt with in real time, a wearable device, for example, can immediately ring an alarm if it recognizes an abnormal heartbeat.
- **Fog computing** introduces an intermediary layer between the edge devices and the cloud, fog computing builds upon the concept of edge computing. Distributed data processing facilitated by this layer lightens the load of the cloud and improves productivity. Fog computing is often used when more complex analytics that cannot be processed on the edge are needed or when there are limitations on the computational capability of the edge devices. This model directs data through local network infrastructure instead of processing it on the wearable device directly.

Both edge and fog computing improve the responsiveness of healthcare systems by reducing the latency with data transmission to central cloud servers. Healthcare providers can decide whether analytics be done in the fog layer or at the edge depending on the data being harvested and the resource requirements. Although more complex tasks, such as pattern detection in long-term data, may be done in the fog or even shipped to the cloud, less complex tasks, such as monitoring a patient's heart rate, may be conducted on the edge.

14.3.1.3 Medical Blockchain: Secure Data Storage

Maintaining data privacy and security is a top priority while dealing with medical data. Sensitive health information is being gathered continuously by wearable technology, so protecting this data from tampering and unauthorized access is essential. A decentralized, immutable ledger for storing patient data is offered by a medical blockchain. An open and secure history of a patient's medical record is guaranteed by the fact that the blockchain cannot be altered or deleted once data has been input. Since blockchain technology is distributed, data is not stored in a single location, which minimizes the possibility of hacking or data breaches.

Blockchain technology enables ensuring that patient data is traceable and unpenetrable when it comes to wearable technologies. Healthcare professionals and other approved individuals can access the secure record formed when wearable devices send information to a blockchain. This maintains the integrity of the patient's medical records and ensures accountability. Healthcare providers are certain that the original data is secure even in the case that cloud servers get hacked by saving it on the blockchain before uploading it to the cloud. Also, smart contracts enabled by blockchain can make certain healthcare procedures automated, such as notifying physicians if a patient's vital signs stray outside a safe range.

14.3.1.4 Digital Twin, Diagnosis, Management Models on Cloud

The information is transferred to the cloud for processing and analysis once it has been stored securely on the blockchain. Cloud is the optimal platform for digital twin model building because it is necessary for the handling of vast amounts of information that require lots of processing capabilities. A digital twin is a virtual image of an actual person, in this instance a patient. Healthcare providers can simulate a patient's health, predict potential outcomes, and enhance treatment protocols by creating a digital twin of the patient. The patient's medical history, lifestyle habits, and environmental conditions are some of the other relevant medical information that the digital twin integrates with the information from the wearable devices. The cloud facilitates easier creation of management models, diagnostic modes, and twin models, which are which are essential for personalized medicine. These models enable health professionals to:

- Simulate different treatment options to see how a patient might respond.
- Diagnose potential health issues by comparing the patient's current data with historical patterns.
- Manage chronic diseases by continuously monitoring the digital twin and adjusting treatment plans in real time.

For example, if a patient with diabetes wears a continuous glucose monitor, the data from the device is sent to the cloud, where the digital twin can simulate the patient's metabolic responses to different foods, medications, and lifestyle changes. Based on these simulations, healthcare providers can recommend personalized treatment plans tailored specifically to the patient's unique needs.

14.3.1.5 Personalized Treatment Plans

Digital twins are expected to create personalized treatment plans as the end goal. Rather than follow generalized treatment protocols, doctors can customize interventions tailored to a detailed understanding of the patient's health, as modeled by their digital twin. Medical professionals can:

- Adjust medications based on real-time data.
- Recommend lifestyle changes that are backed by predictive analytics.
- Monitor patients remotely, allowing for early detection of potential complications.

The combination of real-time data from wearable devices, advanced analytics via cloud-based digital twins, and secure data storage through blockchain creates a powerful system for managing **chronic diseases** and improving patient outcomes. Personalized treatment plans can be adjusted dynamically based on the latest data, ensuring that each patient receives the best possible care tailored to their specific health conditions.

14.3.1.6 Findings of the Case Study

Making full use of scattered real-time multidimensional data requires the establishment of structured and intelligent multidisciplinary integration as well as the iteration and innovation of machine learning and AI for the high-performance calculation of data [11], yet there are challenges in handling different formats:

- Integrating data streams (e.g., heart rate and glucose levels) collected at different timescales presents difficulties in synchronization and alignment for analysis.
- Determining gait abnormalities from movement data is computationally complex and requires advanced analytics.
- Environmental data may need to be integrated with physiological and behavioral data to make sense of certain conditions (e.g., increased heart rate due to hot weather). Establishing these relationships is complex, especially when trying to assess the combined impact of environmental factors on health.
- Finding correlations between different types of data, such as how physical activity affects glucose levels or how environmental temperature impacts heart rate, requires sophisticated analytics. These relationships are often nonlinear and context-dependent, adding further complexity to the integration process.
- In addition to sensor-based data, many wearable platforms allow patients to enter data manually. Self-reported data can be inconsistent and subjective. Patients may not log data accurately or may provide data at irregular intervals, making it difficult to integrate with objective sensor-based data. The data may be incomplete or missing, which can lead to gaps in the analysis and complicate efforts to build a comprehensive health profile [12].

14.3.2 Project BreathEasy: Digital Twins of Lungs to Improve COVID-19 Patient Outcomes

The onset of the COVID-19 pandemic placed unprecedented stress on healthcare systems worldwide, with respiratory complications, particularly those requiring ventilator support, being at the forefront of patient management challenges. Project BreathEasy was born out of the need to improve outcomes for patients with severe respiratory issues caused by COVID-19. This innovative project, led by OnScale, revolves around the use of **digital twin technology** to model patient lungs and optimize the use of ventilators.

By simulating various ventilation strategies for each patient, the project aims to personalize treatment regimens, minimize the potential harm associated with putting patients on ventilators, and ultimately save more lives [13].

Digital twins are virtual replicas of real-life objects or systems, updated to reflect data in real time, to accurately represent their physical counterparts. In healthcare, this concept is extended to create digital replicas of organs, tissues, or entire physiological systems. Project BreathEasy aims to construct highly detailed, patient-specific digital models of lungs. Using patient-specific data—for example, medical imaging, lung capacity, and disease severity—the project constructs simulations that are capable of predicting how various treatments will affect individual patients, especially mechanical ventilation.

Advanced fluid dynamics simulations are used to generate the digital twin models. Such data-driven models enable a dynamic and real-time representation of airflow and gas exchange in the lungs of ICU patients, which could also help clinicians decide on appropriate ventilator settings. Conventional strategies in the management of ventilator mechanics are based on broad guidelines that do not necessarily account for the individual-specific respiratory mechanics and result in impeding rather than facilitating optimal care. This more personalized strategy is only enabled by the digital twin approach.

14.3.2.1 The Critical Role of Ventilators in COVID-19 Care

For patients whose lungs cannot operate well on their own, mechanical ventilators are life-saving devices. However, inappropriate or extended ventilator usage can result in ventilator-induced lung damage (VILI), which makes recovery even more difficult for patients, especially those with acute respiratory distress syndrome (ARDS), a serious and frequent COVID-19 consequence.

Ventilators function by forcing oxygen into the lungs and assisting patients in releasing carbon dioxide; however, depending on the patient's state, settings such as the air delivery pressure and volume must be carefully adjusted. Unfortunately, a one-size-fits-all approach to ventilator settings might result in difficulties like inflammation in the sensitive lung tissues or over-inflation of the lungs. Project BreathEasy can help with this by testing different ventilation techniques on digital twins before they are actually used on patients. Figure 14.3 explains the importance of the BreathEasy Project.

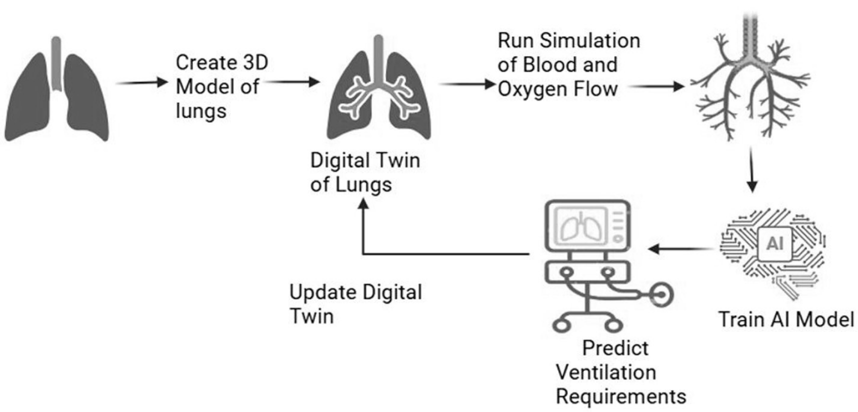


FIGURE 14.3 BreathEasy Project [13]

The first step in Project BreathEasy's methodology is collecting comprehensive physiological data from COVID-19 patients, especially those with serious lung problems. This information comes from clinical measures such as ventilator settings, oxygen saturation levels, and lung compliance as well as medical imaging methods such as CT scans and X-rays. The information is entered into OnScale's simulation platform, which models the patient's lung function using sophisticated fluid and airflow dynamics. After creating the digital twin, medical professionals can use the virtual model to simulate various ventilator settings and forecast the patient's lung response. They can see the consequences of real-time variations in inspiratory flow rates, positive end-expiratory pressure (PEEP), and tidal volume thanks to the digital twin. In this way, it assists physicians in adjusting ventilator settings to achieve optimal oxygenation while minimizing the risk of lung injury.

This approach has several advantages:

- **Personalized Care:** Each digital twin is unique to the patient, ensuring that ventilator settings are tailored to their specific physiological needs.
- **Reduced Risk of Injury:** By simulating the impact of different settings, the risk of over-ventilation and VILI (ventilator-induced lung injury) is reduced.
- **Real-Time Adaptability:** As patient conditions change, so too can the digital twin. If a patient's lung compliance improves or worsens, the twin updates, and clinicians can adjust ventilation strategies accordingly.

14.3.2.2 The Technology Behind BreathEasy

At the core of Project BreathEasy is **OnScale's cloud-based simulation technology**, which is capable of handling the complex computational demands of creating and updating digital twins. OnScale uses **finite element analysis (FEA)** and **computational fluid dynamics (CFD)** to simulate lung behavior under different conditions. The company's platform is built to scale, allowing it to process thousands of simulations quickly and efficiently.

The use of cloud computing is critical, as it provides the computational power needed to run these detailed simulations in real time. Additionally, the project leverages **machine learning** algorithms to continuously improve the accuracy of the digital twin models based on new data. As more patient data is processed, the system becomes better at predicting outcomes, further enhancing its utility in clinical decision-making.

14.3.2.3 Findings of the Case Study

- The digital twin models allowed for customized ventilator settings based on the unique respiratory mechanics of each COVID-19 patient. This resulted in more effective oxygenation and minimized the risk of ventilator-induced lung injury (VILI).
- By simulating various ventilation strategies, clinicians were able to fine-tune settings that helped reduce the overall duration patients spent on ventilators, improving recovery rates.

- The personalized treatment approach significantly reduced mortality among severe COVID-19 patients with acute respiratory distress syndrome (ARDS), a common and fatal complication of the virus.
- Since **Project BreathEasy** deals with highly sensitive medical data, blockchain could be used to securely manage the real-time data being collected from patients. Using blockchain's decentralized ledger, each transaction of data (such as updates to the digital twin model) could be recorded and verified, ensuring that only authorized parties (healthcare providers, patients, or relevant stakeholders) have access to the data. This would prevent unauthorized access or tampering, which is critical in healthcare.

14.3.3 Frederick National Laboratory for Cancer Research: Digital Twin–Based Pilot Projects in Cancer Care

Digital twin technology is increasingly being applied in healthcare, and **cancer care** is a promising area where it can significantly improve patient outcomes [15, 19]. The core idea behind using digital twins in cancer care is to create virtual models of a patient's biological systems, enabling clinicians to simulate various treatment strategies and predict outcomes before administering them in real life. The Frederick National Laboratory for cancer research has given a grant to five research groups to develop a prototype of a digital twin–based cancer care system. Each group is working on different cancer to record the parameters and how the digital twin of the patient cancer tumors reacting to the treatment plan. For example, a digital twin of a breast cancer patient can be created using data from biopsies, imaging scans, and genetic profiles. The twin can then be used to predict how the cancer cells will respond to different drugs or therapies, allowing for highly individualized treatment plans that minimize side effects and improve efficacy as highlighted in Table 14.1.

Project 1: Simulating One Million Pancreatic Cancer Patient Digital Twins to Plan Precision Medicine Treatment Strategies and Improve Long-Term Survival—Lead Institution—Georgetown University

The goal of the project was to create methodologies that link data from pancreatic cancer patients to computational simulations of tumor evolution. Specifically, it aimed to integrate three aspects:

1. **Progression:** The natural course and development of pancreatic cancer in patients.
2. **Therapeutic Interventions:** The treatments administered to patients, such as chemotherapy or surgery.
3. **Outcomes:** The results of these treatments, such as survival rates or tumor reduction.

These patient data were intended to be compared or connected to **simulation results** generated by a mathematical or computational model of **subclonal tumor evolution**.

TABLE 14.1
Pilot Projects in Cancer Care Worldwide [15]

Project Title	Project Aim	Principal Investigator
Simulating One Million Pancreatic Cancer Patient Digital Twins to Plan Precision Medicine Treatment Strategies and Improve Long-term Survival	Simulate one million pancreatic cancer patient digital twins (CPDT) in a models repository by parameterizing input from real patient trajectories for drug sensitivity and resistance [16, 17]	Matthew McCoy, Ph.D. Assistant Professor, Innovation Center for Biomedical Informatics, Georgetown University
An Adaptive Digital Twin Approach for Monitoring Treatment Response and Resistance	Advance the hypothesis that optimal pathways for a specific cancer patient can be selected by exploring the treatment pathway space through a dynamical, multiscale digital twin derived by harnessing patient's own data and leveraging data from similar patients in the population.	Olivier Gevaert, Ph.D. Assistant Professor in Medicine, Stanford University
Dynamic Multiscale Digital Twin for a Lung Cancer Patient	Build the first prototype of an individualized digital twin of non-small cell lung cancer for identifying the optimal treatment pathway and adaptive treatment monitoring, leveraging the population information and new test results.	Qi Wang, Ph.D. Professor of Mathematics, University of South Carolina
Prototyping a Self-learning Digital Twin Platform for Personalized Treatment in Melanoma Patients	Rapidly prototype a 3D multiscale model of melanoma metastases that interact with the host immune system with or without treatment (autologous vaccine immunotherapy)—and verify that it recapitulates a broad variety of clinically relevant patient trajectories.	Paul Macklin, Ph.D. Associate Professor of Intelligent Systems Engineering, Indiana University
My Virtual Cancer	Combine mechanistic, machine learning, and stochastic modeling approaches to create a DT platform that utilizes biological, biomedical, and EHR data sets. Will focus on one common cancer—breast cancer—and one rare cancer—uveal melanoma— to evaluate the performance of the DT for both common and rare cancers.	Leili Shahriyari, Ph.D. Assistant Professor, Mathematics and Computer Science, University of Massachusetts Amherst

Subclonal tumor evolution refers to the genetic diversity within a tumor, where different subgroups of cells (subclones) evolve and respond differently to treatments.

By bridging real-world patient data and simulated tumor models, the project seeks to better understand the dynamics of pancreatic cancer, optimize treatment strategies, and predict outcomes based on various therapeutic interventions. The scientists are continuously working on improving the outcomes of the project as the exact approximation of such difficult systems is very difficult.

Project 2: Self-Learning Platforms for Personalized Treatment of Melanoma—Lead Institution—Indiana University

This project represents the foundational phase of an ambitious initiative to create **clinically actionable computational patient digital twins (CPDTs)** for immunotherapy planning in patients with metastatic melanoma. The key elements are as follows:

1. **Multiscale Tumor-Immune Interaction Models:** The team developed advanced models that simulate interactions between tumors and the immune system across multiple scales, focusing specifically on melanoma metastases in the lungs.
2. **Use of Canine Data**: Canine models were incorporated to accelerate the refinement of these multiscale simulations, leveraging similarities in tumor progression between canines and humans.
3. **High-Performance Computing (HPC):** HPC resources were utilized to explore the models comprehensively, ensuring that they accurately replicate critical clinical scenarios, including:
    - Spontaneous tumor regression.
    - Tumor growth arrest at subclinical sizes.
    - Progression to detectable clinical sizes.
4. **Artificial Intelligence (AI) Integration:** AI techniques were employed to analyze simulated patient trajectories, extract meaningful patterns, and develop adaptable CPDT templates. These templates are essential for tailoring the models to the unique characteristics of individual patients.

This project aims to bridge biological complexity and computational modeling, laying the groundwork for personalized and predictive tools that can guide immunotherapy decisions in metastatic melanoma care.

Project 3: An Adaptive Digital Twin Approach for Monitoring Treatment Response and Resistance—Lead Institution—Stanford University

This project focuses on creating an adaptive **computational patient digital twin (CPDT)** for lung cancer treatment by integrating various data types (e.g., demographic, imaging, pathology, and genomics). The CPDT uses baseline and real-time data to predict treatment responses, monitor resistance mechanisms, and adjust therapies dynamically. Key features include:

- **Predictive Modeling:** Utilizes AI to forecast therapy outcomes, enabling treatment changes if predictions fail.
- **Maintenance Phase:** Tracks resistance mechanisms, toxicity, and effectiveness for further optimization.
- **Modular Approach:** Initial modules are being developed for essential data types, with retrospective datasets used to train and test the model.
- **Deep Learning Integration:** Combines multi-modal data into a unified adaptive model.

This CPDT aims to guide treatment decisions, monitor responses, and dynamically adapt strategies for lung cancer management. The project's future work involves developing a **multiscale model** of lung cancer lesions by integrating individual modules (e.g., imaging, pathology, and genomics) through a **late fusion strategy**. This model aims to predict tumor size under two treatment modalities: **anti-EGFR treatment** and **immunotherapy**.

Project 4: A Patient-Specific Multiscale Digital Twin for the Exploration of Optimal Treatment Pathways for Non-Small Cell Lung Cancer—Lead Institution—University of South Carolina

This project aims to create a **cancer patient digital twin (CPDT)** for **non-small cell lung cancer (NSCLC)** patients. A CPDT is a virtual model that represents an individual patient, built using their medical data and information from similar patients. Its purpose is to help optimize cancer treatment by:

1. **Personalized Care:** Tailoring treatments specifically for the patient by analyzing their unique medical history and comparing it with population data.
2. **Dynamic Treatment Exploration:** Simulating different treatment options in real time to find the best pathway for managing the patient's condition.
3. **State Tracking:** The CPDT acts as a digital mirror, recording the patient's **past state**, tracking their **current health**, and predicting possible **future outcomes**.

The project has made significant strides in developing a digital twin (DT) for non-small cell lung cancer (NSCLC). The team has compiled patient data from both the Yale–New Haven Health System cohort and publicly available databases, laying a solid foundation for model development. Progress has been achieved on the physiological module within the multiscale digital twin, which is crucial for simulating patient-specific conditions. Deep learning techniques, including long short-term memory (LSTM) networks and neural dynamical systems, are being utilized to conduct similarity analyses among patients, enabling personalized insights. Additionally, initial work on modeling protein network dynamics has commenced, aiming to understand the cellular mechanisms driving cancer progression. These advancements collectively contribute to creating a robust framework for precision medicine in NSCLC treatment.

Project 5: Virtual Cancer Digital Twin Approaches Lead Institution—University of Massachusetts, Amherst

The creation of a **cancer patient digital twin (CPDT)** aims to predict the unique evolution of each patient's cancer, given that cancers respond differently to treatments due to their distinct characteristics. By leveraging computational modeling, the CPDT helps predict how cancer will progress in each individual, guiding clinicians to detect aggressive tumors early, perform timely surveillance, and select the most effective treatments. This personalized approach combines **mechanistic models**, **machine learning**, and **stochastic modeling** to create the "My Virtual Cancer" platform. The platform updates dynamically based on the patient's data, continuously refining predictions about the disease's evolution and its impact on other organs, especially in the context of targeted therapies.

The CPDT incorporates **quantitative systems pharmacology (QSP)**, a computational method that integrates biochemistry, biophysics, and pharmacokinetic–pharmacodynamic (PK–PD) models to simulate the entire body's response to cancer treatments. One challenge of QSP is parameter estimation, as the data used to calibrate models often come from various sources rather than a single curated dataset. The team is addressing this by using **patient-specific data** to personalize the CPDT, ensuring its predictions are tailored and more reliable for individual treatment planning.

The team conducted an analysis of **1,218 primary breast tumors** from the **TCGA (the cancer genome atlas) project** and **1,904 tumors** from the **METABRIC (molecular taxonomy of breast cancer international consortium)** datasets. They employed a **digital cytometry** method on gene expression profiles of these tumors to characterize their immune profiles and estimate variables for a mathematical model. This led to the development of a **data-driven ordinary differential equation (ODE)** model for human breast tumors, identifying **five distinct immune patterns** and examining the dynamics of each.

14.3.3.1 Key Findings from the Projects

- The projects demonstrate how **biological and clinical knowledge**, **machine learning**, and **mechanistic modeling** can combine to create **modular, reusable CPDT frameworks**.
- Advanced techniques such as **AI-driven analysis** and **large-scale model exploration** are essential for addressing challenges in model calibration and feature extraction. [20]
- The CPDT field is transitioning from theoretical concepts to **clinical reality**, with promising results emerging from pilot projects.

14.4 CONCLUSION

The pilot projects on **digital twin (DT)** and **blockchain** technologies are advancing healthcare innovation by combining virtual patient replicas and secure data management. These digital models rely on **AI** and **machine learning** to refine predictions as new data emerges, making them more adaptive to individual patient needs. However, the success of these projects is contingent on the availability of high-quality, longitudinal data.

Blockchain technology plays a crucial role by ensuring secure, tamper-proof data sharing across various stakeholders in healthcare, facilitating real-time collaboration without compromising patient privacy. Despite the potential, challenges such as integrating diverse data sources and regulatory compliance remain. These pilot projects emphasize the importance of interdisciplinary collaboration, with efforts such as the

envisioning computational innovations in cancer challenges (ECICC) community fostering partnerships across academia, healthcare, and industry.

In the future, these efforts will likely lead to more disease-specific, data-driven digital twins, which will enhance personalized treatment strategies. As **AI**, **machine learning**, and **blockchain** technologies evolve, they will be critical in overcoming current limitations, and shaping the future of precision medicine. These technologies offer a promising path forward in transforming healthcare by making treatment plans more precise and data sharing more secure.

REFERENCES

1. Rani R, Kumar R, Mishra R, and Sharma SK. Digital health: A panacea in COVID-19 crisis. *Journal of Family Medicine and Primary Care*, 10(1), 62–65 (2021). https://doi.org/10.4103/jfmpc.jfmpc_1494_20
2. Hemdan EED, El-Shafai W and Sayed A. Integrating digital twins with IoT-based blockchain: Concept, architecture, challenges, and future scope. *Wireless Personal Communications*, 131, 2193–2216 (2023).
3. Haleem A, Javaid M, Pratap Singh R, Suman R, and Rab S. Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, 2, 130–139 (2021).
4. Lu Q, Chen L, Xie X et al. Framing blockchain-integrated digital twins for emergent healthcare: a proof of concept. *Proceedings of the Institution of Civil Engineers – Engineering Sustainability*, 176(4), 228–243 (2023).
5. Khezr S, Moniruzzaman M, Yassine A, and Benlamri R. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences*, 9, 1736 (2019).
6. Hussien HM, Yasin SM, Udzir NI, Ninggal MI, Salman S. Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, 22, 100217 (2021).
7. Ullah, H. Sami, and Samia Aslam. "Blockchain in healthcare and medicine: A contemporary research of applications, challenges, and future perspectives." arXiv preprint arXiv:2004.06795 (2020).
8. Ben Fekih, Rim, and Mariam Lahami. "Application of blockchain technology in healthcare: a comprehensive study." In The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18, pp. 268–276. Springer International Publishing, 2020.
9. Zhen, Zhen, and Yanqing Yao. "The confluence of digital twin and blockchan technologies in Industry 5.0: Transforming supply chain management for innovation and sustainability." Journal of the Knowledge Economy (2024): 1–27.
10. Xie Y, et al. Integration of artificial intelligence, blockchain, and wearable technology for chronic disease management: a new paradigm in smart healthcare. *Current Medical Science*, 41(6), 1123–1133 (2021).
11. Chae SH, Kim Y, Lee KS, et al. Development and clinical evaluation of a web-based upper limb home rehabilitation system using a smartwatch and machine learning model for chronic stroke survivors: Prospective comparative study. *JMIR mHealth and uHealth*, 8(7), e17216 (2020).
12. Sun T, He X, and Li Z. Digital twin in healthcare: Recent updates and challenges. *Digital Health*, 9, 20552076221149651 (2023).

13. https://onscale.com/project-breatheasy-digital-twins-of-lungs-to-improve-covid-19-patients-outcomes/
14. Dai N, Lei IM, Li Z, Li Y, Fang P, and Zhong J. Recent advances in wearable electromechanical sensors—Moving towards machine learning-assisted wearable sensing systems. *Nano Energy*, 105, 108041 (2022).
15. https://frederick.cancer.gov/news/digital-twins-cancer-care-exploring-cross-disciplinary-innovative-approach
16. Stahlberg EA, et al. Exploring approaches for predictive cancer patient digital twins: Opportunities for collaboration and innovation. *Frontiers in Digital Health*, 4, 1007784 (2022).
17. Hernandez-Boussard T, Macklin P, Greenspan EJ, et al. Digital twins for predictive oncology will be a paradigm shift for precision cancer care. *Nature Medicine*, 27, 2065–2066 (2021).
18. Amofa S, Xia Q, Xia H, Obiri IA, AdjeiArthur B, Yang J, et al. Blockchain-secure patient Digital Twin in healthcare using smart contracts. *PLoS One*, 19(2), e0286120 (2024).
19. Stahlberg EA, Abdel-Rahman M, Aguilar B, Asadpoure A, Beckman RA, Borkon LL, Bryan JN, Cebulla CM, Chang YH, Chatterjee A, Deng J, Dolatshahi S, Gevaert O, Greenspan EJ, Hao W, Hernandez-Boussard T, Jackson PR, Kuijjer M, Lee A, Macklin P, Madhavan S, McCoy MD, Mohammad Mirzaei N, Razzaghi T, Rocha HL, Shahriyari L, Shmulevich I, Stover DG, Sun Y, Syeda-Mahmood T, Wang J, Wang Q, and Zervantonakis I. Exploring approaches for predictive cancer patient digital twins: Opportunities for collaboration and innovation. *Frontiers in Digital Health*, 4, 1007784 (2022).
20. Meijer C, Uh HW, and El Bouhaddani S. Digital twins in healthcare: Methodological challenges and opportunities. *Journal of Personalized Medicine*, 13(10), 1522 (2023).

Index