Computer Science Review 60 (2026) 100909

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

# AI-driven blockchain technology in smart healthcare system: Opportunities, challenges and future implications

Yunsheng Zhang [a,1], Syed Muhammad Mohsin [b,c,**], Hana Mujlid [d], Muhammad Sadiq [a,1], Syed Muhammad Abrar Akber [e], Sheraz Aslam [f,g], Junwei Liang [a,*]

[a] Shenzhen University of Information Technology, Shenzhen, China
[b] Department of Computer Science, University of Wah, Quaid Avenue, Wah Cantt 47040, Pakistan
[c] Standard College of Modern Sciences, Virtual University of Pakistan, Lahore 55150, Pakistan
[d] Department of Computer Engineering, Taif University, 21944, Taif, Saudi Arabia
[e] Faculty of Physics and Applied Computer Science, AGH University of Krakow, al. Mickiewicza 30, 30-059, Krakow, Poland
[f] Department of Computer Science, American University of Cyprus, Larnaca, Cyprus
[g] Department of Computer Science, CTL Eurocollege, 3077 Limassol, Cyprus

ARTICLE INFO

*Keywords:*
AI-driven smart healthcare
Blockchain
Security and privacy
Patient data
Opportunities and challenges

ABSTRACT

Blockchain technology in conjunction with artificial intelligence (AI) is transforming smart healthcare systems, by providing enhanced data security, interoperability, and transparency. Integration of AI along with blockchain into smart healthcare systems offers numerous benefits, including supporting decision-making processes, reducing administrative burdens, improving coordination of patient care and automated, trust-based execution of healthcare agreements. This study presents applications of AI-based blockchain technology in the field of smart healthcare and analyzes the state of affairs, highlights the key issues, and identifies perspectives to strengthen the reliability and trustworthiness of future medical systems. The study uses a structured framework to analyze the effectiveness of blockchain in healthcare by contrasting its advantages and disadvantages. Blockchain systems benefit healthcare by improving data security, streamlining data processing, ensuring trust, facilitating telemedicine and remote monitoring, and enabling efficient consent management, automated workflows and medication traceability. In this context, the study introduces a conceptual model namely the trust–automation–interoperability (TAI) synergy framework to guide the design, analysis, and deployment of AI-enabled blockchain solutions for smart healthcare aiming to achieve a sustainable digital health ecosystem by strengthening three fundamental dimensions: trust, automation, and interoperability. However, challenges such as scalability, interoperability, legal ambiguities, security concerns, user experience, acceptance barriers, long-term data storage, connectivity issues, discrepancies between data formats, user identity management, and cost considerations emphasize the importance of strong solutions.

## 1. Introduction

The rapid advancements in modern technologies such as internet of things (IoT), machine learning (ML), artificial intelligence (AI), and blockchain are reshaping the healthcare industry [1–3]. Blockchain technology, which was originally developed for cryptocurrencies, is revolutionizing healthcare systems by providing security, interoperability, and transparency [4–6]. Blockchain technology has the potential to be used in each decision- making process of healthcare systems to securely store and distribute medical information, improve interoperability, and enable decentralized and transparent patient data management [7]. By 2030, it is anticipated that the worldwide medical cloud computing market will reach a value of $197.45 billion [8]. Blockchain system is predicted to save up to $150 billion annually in counterfeit drug costs by 2025 [9].

* Corresponding author.
** Corresponding author at: Department of Computer Science, University of Wah, Quaid Avenue, Wah Cantt 47040, Pakistan.
*Email addresses:* zhangys@sziit.edu.cn (Y. Zhang), syedmmohsin9@gmail.com (S.M. Mohsin), hmujlid@tu.edu.sa (H. Mujlid), sadiq@sziit.edu.cn (M. Sadiq), abrar@agh.edu.pl (S.M.A. Akber), aslam.sheraz@aucy.ac.cy (S. Aslam), jwliang@sziit.edu.cn (J. Liang).

[1] Yunsheng Zhang and Muhammad Sadiq contributed equally to this work.

https://doi.org/10.1016/j.cosrev.2026.100909
Received 13 September 2025; Received in revised form 20 December 2025; Accepted 15 January 2026
Available online 30 January 2026

Decision- making process of the traditional healthcare organizations faces several challenges, including fragmented medical records, lack of interoperability among healthcare providers, permanent storage of sensitive data, inability to guarantee data accuracy, vulnerability to data linkage attacks that can compromise patient privacy, and prevention of illegal drug use [10]. Blockchain technology can help address these challenges by providing a decentralized and secure platform for storing and exchanging patient data between different healthcare providers and ensuring interoperability through defined data formats and smart contracts [11]. By tracing the origin of medicines, ensuring authenticity, and reducing the incidence of counterfeit drugs, blockchain can further increase transparency in the drug supply chain [12].

Many healthcare systems are centralized control systems where access to information is granted by third parties, such as the government or professionals who require previous records. Patients may have multiple consultants who require information about the patient's medical history. This increases the likelihood that information will be leaked, which can have serious consequences for the patient's privacy and the system's reputation. Blockchain technology can protect against such situations and is helpful in explaining previous examinations and procedures [13]. Blockchain provides an option for smart contracts and focuses on multiple elements within the contracting process that facilitate understanding of contract terms [10]. Furthermore, it protects and manages data across all participants and creates an integrated health record that can be accessed globally by physicians, practitioners, pharmacists and other stakeholders who can manage the patient's health [14].

The blockchain paradigm has transformed the healthcare industry by bringing significant advancements such as e-health, prescription medication data, and insurance information [15]. These technologies can reduce the need for routine hospital visits, and home connections can help prevent hospitalizations or readmissions [9]. It facilitates access to disease symptoms and diagnoses for providing immediate treatments to patients provides control over problematic situations and notifies doctors to view previous information about the patient [16]. Blockchain technology can eliminate counterfeit drugs protect patients from taking ineffective drugs, keep digital records, and ensure the quality of medicines [17]. The Gcoin blockchain system [18] plays a key role in healthcare as it helps with drug transactions and increases transparency.

Furthermore, blockchain technology also enables medical devices to make a proper assessment through trigger messages and diagnoses before the situation becomes dangerous. The sensors installed in the various devices of the patients help to collect information and send it to the physician for analysis. These systems have led to continuous innovations in the healthcare industry. Blockchain based data preservation system [19] could provide a storage solution that guarantees originality and verifiability to users. This provides an additional feature of notification when there is an attempt at tampering [13]. The security of blockchain can prove the accuracy, security, and privacy of healthcare systems and the critical points in the system [20].

A healthcare system that is distributed across different medical facilities makes it challenging to access the private information of patients [9]. A typical organization of a smart healthcare system is shown in Fig. 1. A blockchain-based smart healthcare system (SHS) is a secure and decentralized platform that uses blockchain technology to enable the safe storage and exchange of patient medical records and data across several healthcare providers. SHS maintains data integrity and interoperability, improves patient privacy, and promotes efficient and transparent healthcare services using smart contracts and decentralized consensus methods [21,22]. It offers several key advantages, as it provides an immutable platform for storing and sharing medical records and patient data.

In artificial intelligence (AI), the integration of blockchain technology appears to be a decisive factor in changing the landscape of data

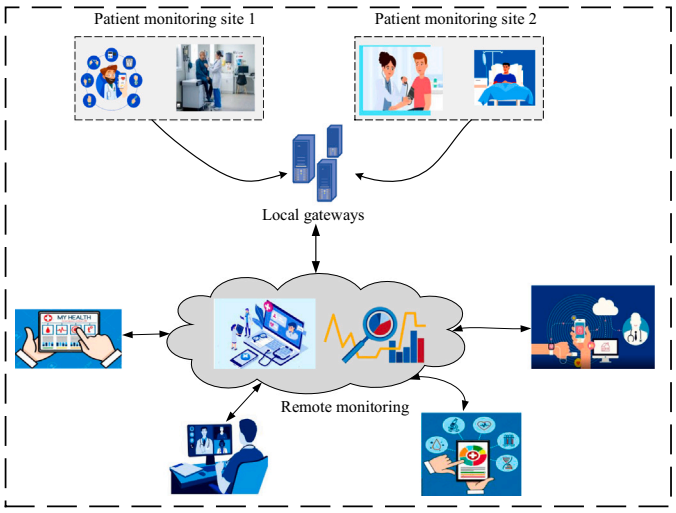


**Fig. 1.** A typical organization of smart healthcare architecture.

management, security, and usage. At its core, blockchain provides a decentralized, immutable data set that serves as the basis for creating trust and transparency in digital transactions [23]. In combination with AI systems, blockchain not only ensures the integrity and confidentiality of large data sets but also strengthens the reliability and verifiability of AI algorithms and their conclusions. This synergistic combination of AI and blockchain has enormous potential to revolutionize a wide range of industries by providing AI applications with reliable data sources, faster transactions, and strengthened security standards [24,25]. Companies are able to unlock unprecedented innovation opportunities and manage risks by leveraging the combined strengths of AI and blockchain [26,27].

This study explores the potential of blockchain technology in the healthcare sector, as well as the opportunities and challenges, through an examination of the existing literature. The study aims to assess the challenges associated with the implementation of blockchain technology in the healthcare industry. It also aims to identify the barriers to the adoption of the technology and ways to overcome them. It highlights previous literature and extracts key information to understand the outcomes of SHS and blockchain implementation. The study concludes that interoperability between healthcare organizations is very important for health information, patient identification, data access authorization, and health data management. The key motivations and objectives of the study are mentioned in the following.

1. To provide an in-depth discussion of blockchain features and their benefits in the smart healthcare system based on 50+ recent studies from 2019–2025.
2. To discover opportunities offered by blockchain systems in the smart healthcare industry.
3. To discuss challenges that prevent the effective and efficient application of blockchain technology in smart healthcare systems and to present future recommendations.
4. To propose a conceptual model, namely Trust–Automation–Interoperability (TAI) Framework, intended to guide the design, analysis, and deployment of AI-enabled blockchain solutions for smart healthcare.

Rest of the article is organized as follows. Background terms and technologies related to the blockchain enabled smart healthcare system and implementation details of blockchain technology in smart healthcare systems are described in Section 2. The detailed discussion and

critical analysis of state-of-the-art literature are presented in Section 3. Opportunities and research challenges of blockchain implementation in smart healthcare systems are discussed in Section 4. Our proposed trust-automation-interoperability (TAI) synergy framework is elaborated in Section 5. Brief limitations of the study are presented in Section 6, whereas Section 7 concludes this study. At the end, Section 8 highlights the future implications.

## 2. Preliminaries and implementation of blockchain technology in smart healthcare

### 2.1. Preliminaries

To provide a solid foundation for the discussion, this section introduces key concepts, terminology, and technologies underlying blockchain-enabled smart healthcare systems. Understanding these preliminaries is essential for appreciating the implementation strategies discussed in the subsequent section.

#### 2.1.1. Blockchain technology

Blockchain technology is a distributed ledger system that records and verifies transactions over a network of computers (nodes) [28,29]. When a new transaction is created, it is combined with existing transactions to form a block. The network's nodes collaborate to authenticate the transaction's validity and integrity using complex cryptographic techniques before adding the block to the chain. After reaching consensus, the block is added to the chain in chronological sequence, becoming a permanent part of the blockchain. Each succeeding block has a distinct cryptographic reference to the prior block, resulting in an unbroken chain of transactions. Because the blockchain is distributed among several nodes, it ensures transparency, immutability, and security, making it impervious to manipulation and serving as a reliable foundation for various applications [13].

Blockchain technology is capable of reducing expenses, improving overall healthcare delivery, and making it efficient. The blockchain technology is used to securely encrypt patient data to control the outbreak of dangerous diseases. Blockchain is a decentralized, immutable database that facilitates asset tracking and transaction recording in an enterprise network [30]. A blockchain system consists of an extended collection of documents called blocks. The blocks are securely linked through encryption. They also consist of transaction information, a timestamp, and a cryptographic hash of the previous block. In addition, the timestamp records the transaction data at a particular point in time [31]. The blocks form a chain that is interdependent and contains information that is then transmitted and recorded.

#### 2.1.2. Decentralization

Unique features and prospective advantages of blockchain technology are largely defined by the concept of decentralization, which is a fundamental component of the blockchain technology. Decentralization is the practice of distributing power, authority, and decision making throughout a network of participants (nodes) as opposed to keeping them concentrated in the hands of a single central body or authority. With decentralization, there are multiple entities that control data, increase security, and prevent unauthorized tampering [32]. Blockchain technology is decentralized in terms of its data replication and storage, intermediary disruption, decentralized network, open access, consensus mechanisms, censorship resistance and ownership. Although decentralization offers several advantages, it also has drawbacks, including issues with scalability, energy consumption, and governance [33].

#### 2.1.3. Smart healthcare system

The smart healthcare system using blockchain technology enables secure and efficient sharing of patient data with various healthcare professionals. Blockchain technology ensures data integrity and privacy to maintain control over health data and grants access to authorized healthcare professionals. The smart healthcare system is able to improve the transparency and reliability of clinical trials by verifying and securely recording study data and ensuring the authenticity of results [34,35]. Supply chain management is also managed by the smart healthcare system to improve traceability and transparency of pharmaceutical supply chains. It provides better insight by enabling real-time tracking of medical products from the pharmaceutical industry to the patient, improving patient safety and regulatory compliance [36].

### 2.2. Implementation details of blockchain technology in smart healthcare

Building on the foundational concepts, this subsection explores how blockchain technology is implemented in smart healthcare systems, highlighting practical architectures, workflows, and integration with AI for enhanced security and efficiency.

#### 2.2.1. Data management

At the heart of the smart healthcare system is patient data, which is available to professionals in real time to review and analyze the available data [37]. Blockchain technology includes wearable devices to capture such patient-specific data. Healthcare data is characterized by high volume, heterogeneity, and velocity, and since patient data is highly personal, its privacy must be ensured [4,38,39].

- Data collection and storage: Data collection and storage are crucial for the accuracy and integrity of a smart healthcare system. In the consensus algorithm of a Blockchain system, participants agree on the validity of transactions or data entries. It also simplifies the process of audits and regular data validation to ensure data quality within blockchain technology [14]. Researchers of [4], have discussed the use in blockchain technology for data collection and storage. Data is stored in blocks, which consist of a set of information that is subsequently transmitted from one block to another. The information transmitted is of great importance to the other parties. For example, the pharmacist needs a diagnosis from the doctor and a prescription.

  Another study [16], highlighted the use of IoT for data collection and storage in blockchain blocks. The study mentioned that patient-centric data is highly sensitive and it is secured with the help of encryption. Challenges associated with data collection and storage for a blockchain-based healthcare system include the non-uniformity of patient data, the heterogeneity of variables, and the need for real-time data analysis [38]. Such challenges may lead to the inaccessibility of useful data and ineffective diagnosis of diseases [40].
- Data sharing: Data sharing is critical in a blockchain-based healthcare system to allow authorized healthcare providers safe and reliable access to the patient information. In [41] authors explained the potential sharing of data through blockchain technology and various cases are described where it has proven to be very useful. Physicians are able to connect with other consultants to gain access to medical records and support, even if the patient is unable to visit the clinic. Doctors are able to identify the previous diagnosis and perform various other tests or treatments based on the judgments. In [31], the researchers explained the lessons learned from using blockchain technology to improve data sharing during the pandemic. The COVID-19 cases were monitored through real-time data sharing in different countries. Health systems using blockchain benefited from data sharing capabilities like the research and development team.

  The study in [42] discussed cases of transparent data sharing among various government agencies, including healthcare. The study highlights the potential of blockchain and data privacy. The study explains that the shared data is considered important to make better decisions when patients and their diseases are delayed. A study [43] mentioned the Blockchain-based solution enhancing the security of healthcare documents in IoT-enabled digital healthcare ecosystems (EHDHE). The study explained the mechanism

of blockchain and the way it exchanges data. Privacy, integrity, and access control issues are addressed in the transfer of sensitive information.

In addition, Hajian et al. [44] discussed blockchain-based information sharing systems in electronic health records. It helps in facilitating and securing efficient data sharing among various stakeholders in healthcare. The authors emphasize that blockchain technology helps to improve information flow and increase trust in the healthcare system. The research in [18] presents blockchain-based privacy solutions for IoT-enabled healthcare systems. Encryption of data at each step of data exchange enables high security. The framework enables secure and privacy-friendly data exchange to enhance trust among participants involved in the blockchain healthcare system. Data sharing is also discussed in [45,46], where the transformative capabilities of blockchain technology are highlighted. It improves business process innovation and enables data sharing and security. An innovative approach is possible when information is shared, and there is continuous improvement in healthcare work. Whether it's medical devices or new drugs, innovation is possible through data sharing.

- Data interoperability: Interoperability is defined as a mechanism to optimize and standardize the quality of a healthcare system [32]. Interoperability in healthcare is critical because there are multiple sources of patient-related information, such as patient history, medical examination results, data from wearable IoT devices and genomic data. Blockchain technology is capable of improving the data exchange system and solving the interoperability problem in the healthcare industry. In blockchain technology, patients are marked as hash ID which are unique identifiers. The ID can be unique and help protect user privacy. Patients would have the right to share their decryption key, which contains their data and medical information. The process increases security and privacy and creates a patient-centered system [13]. Blockchain technology can help in data sharing and comprehensive medical records.

The healthcare system needs to be interoperable so that patients' medical records can be shared for assessments and better decision making [17]. Electronic health record (EHR) exchange must be comprehensive because inefficiencies in the system may cause problems. The study [17] highlighted two challenges that may arise from inefficient interoperability, namely difficulty in identifying patients, and information blockage when healthcare providers inappropriately restrict the exchange of patient data or electronic health records [47]. The study further stated that there is a lack of recognized patient identifiers and various information blocking practices have distorted the entire healthcare system. The study in [20] recommended improving the flow of innovation in healthcare to enable remote monitoring and telemedicine for physicians around the world.

- Data security issues: Several healthcare organizations store valuable information in a central location that is vulnerable to cyberattacks. These organizations have minimal protection for detailed patient data [48]. Each year, organizations spend millions of dollars to protect their data and improve their security systems. There have been several reports of fraud and cyberattacks where data has been corrupted or used for various illegal activities. Therefore, security will always be a risk in online processes. In the case of healthcare, patients have almost all of their information on credit cards, insurance information, medical reports, payment plans, and appointments. Access to these records could cause great harm not only to the patient but to the entire system [49].

Authors of [50] explored the future possibilities of blockchain platforms for industrial healthcare. The study stated that the benefits of blockchain technology are to improve the security, privacy, and efficiency of healthcare systems. It highlighted the areas such as medical records, patient consent, drug supply chain and medical device tracking. Challenges related to regulatory compliance and integration with existing healthcare systems are also highlighted. Content analysis of blockchain data management is summarized in Table 1.

#### 2.2.2. Enabling technologies for blockchain-based smart healthcare

Enabling technologies help the ideas come into existence. In the following subsection enabling technologies for blockchain enabled smart healthcare systems are discussed.

- Internet of Things: Internet of things devices are the basic data sources to generate patient-specific health data. In smart healthcare, blockchain and IoT may be used to provide a safe and efficient environment for storing patient data, monitoring health parameters, and enhancing healthcare services. Wearable health trackers, remote patient monitoring sensors, and medical equipment are examples of IoT devices that create real-time data that can be safely stored on a

**Table 1**
Content analysis of blockchain data management.

| Ref. | Year | Study & methodology | Benefits | Challenges |
|---|---|---|---|---|
| [41] | 2019 | Literature review | Increased security and improved efficiency in government services. | Scalability problem and interoperability issues |
| [4] | 2020 | Case Study | Opportunities in healthcare systems for research and discovering ways for treatments, enhanced security and privacy, data integrity | Challenges in adoption in different healthcare mechanisms and problems in scalability |
| [14] | 2020 | Literature review | Improved patient care, increased data sharing, and enhanced transparency and trust | Regulatory and legal challenges with technical complexities |
| [16] | 2020 | IoT cases with Blockchain | Improved security and privacy, interoperability, and tamper proof records | Mechanisms problem for consensus |
| [17] | 2020 | Literature review | Enhanced data security, efficient, efficient healthcare system and enhanced patient privacy | Technical problems while implementing, expensive updates and scalability limitations |
| [31] | 2020 | Report analysis | High security and enhanced performance of healthcare staff | Challenges of interoperability and integration complexities |
| [50] | 2020 | Case study | Improved patient care, increased data sharing, and enhanced transparency and trust. | Regulatory and legal challenges with technical complexities. |
| [47] | 2020 | System analysis of the pharmaceutical company | Build the credibility of medicines from manufacturing to the end user | Higher cost and interoperability |
| [51] | 2021 | Remote monitoring to elderly persons | Long operating times, resilience to network problems, security | Latency and higher cost |
| [44] | 2022 | Literature review | Enhanced information sharing, improved security | Adoption challenge and integration complexity |
| [45] | 2022 | Comparative analysis of systems | Business process innovation, enhanced efficiency and improved security | Integration challenges and technical complexities |
| [18] | 2023 | Analysis for privacy | Privacy preservation and improved security | Integration & scalability challenges |
| [43] | 2023 | Comparative analysis of systems | Enhanced information sharing, improved security | Scalability & adoption challenges |

blockchain [4,52]. As a result, blockchain secures the data's integrity and immutability, prohibiting illegal access and alteration of patient data.

Blockchain and IoT enable decentralized and patient-centric health data management. Patients have complete control over their medical information and may choose which healthcare professionals have access to specific data, ensuring privacy and consent-driven data sharing. Interoperability standards enable easy communication between various IoT devices and healthcare systems, resulting in the creation of a complete and linked healthcare network. This integration of blockchain and IoT in smart healthcare has the potential to transform healthcare delivery, improve data accuracy, improve patient outcomes, and drive medical research and innovation [53,54]. Furthermore, IoT also works with blockchain to facilitate the integration of medical devices, which enables real-time monitoring and provides remote access to telemedicine and extends its reach.

- Big Data Analytics: Blockchain and big data may be used to build a safe and scalable infrastructure for managing massive volumes of patient data in smart healthcare. Big data analytic can handle and analyze massive amounts of healthcare data provided by IoT devices, electronic health records, and other sources, yielding significant insights for individualized therapies, illness prediction, and population health management [55,56]. This sensitive patient data may be securely maintained using blockchain technology, assuring data integrity, privacy, and transparent access control.

  In Kamble et al. [38], the authors explained the need to integrate blockchain with big data analytic. This means that both technologies must be used simultaneously to create information that can be evaluated by physicians and all other members of the Blockchain system. Big data analytic shares the information about consumer behavior with multiple stockholders. In addition, Big Data analytics and blockchain together can create and transform data in real time and eliminate the risk of commercialization.
- Artificial Intelligence: Artificial Intelligence, in conjunction with blockchain technology, facilitates the advanced diagnosis, production of personalized medications, and predictive analysis in smart healthcare systems [19]. Consequently, AI helps improve patient health. Enabling technologies work together to create patient-centered care that can deliver healthcare to every corner of the world. The use of AI in healthcare helps make better decisions and analyze the external and internal environment. During the pandemic of COVID-19, such technologies helped to monitor patient information and refer infected patients directly to isolation. Organizations are encouraged to use such advanced technologies by leveraging digital platforms and mobile applications.

  AI significantly enhances blockchain security by introducing intelligent monitoring and early-warning capabilities that go beyond traditional rule-based checks. Machine-learning models can rapidly analyze transactions and network behavior to identify anomalies such as double-spending attempts, Sybil attacks, or unusual node activity. AI also contributes to safer smart-contract deployment by detecting logical flaws and potential vulnerabilities in the code. In healthcare settings, where data sensitivity and system reliability are critical, AI supports real-time threat detection, device behavior analysis, and more adaptive access-control decisions. Collectively, these capabilities make blockchain systems more resilient and better equipped to respond to evolving security challenges.

Fig. 2 presents a high-level view of how artificial intelligence and blockchain work together within a smart healthcare system. Data generated from patients, such as electronic health records, wearable and internet of medical things (IoMT) devices, laboratory results, and clinical reports, is first gathered and organized through a data acquisition and integration layer. This prepared data is then analyzed by the AI/ML layer to support tasks such as risk prediction, early warnings, diagnosis support, and personalized care recommendations, with explanations provided to assist clinical decision-making.

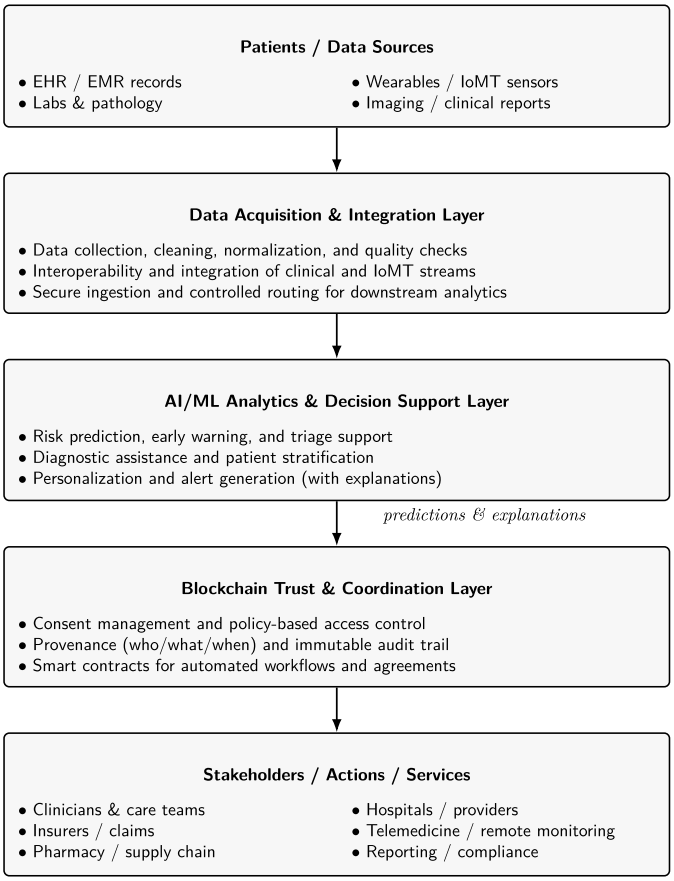


**Fig. 2.** AI–blockchain integration enabling trusted data sharing and actionable healthcare insights.

Running alongside this process, the blockchain layer acts as a foundation of trust by managing patient consent, maintaining tamper-proof audit trails, and coordinating automated workflows through smart contracts. By combining intelligent analytics with secure data governance, the model enables reliable decision-making and smooth collaboration among healthcare stakeholders, including clinicians, hospitals, insurers, and telemedicine services.

- Data Security in Transforming the Healthcare Sector: The discussion in [19] focuses on the change that technology has brought to the health sector. One important area is data security in the financial industry. The systems are decentralized and have an immutable ledger. Even though the system is highly encrypted and offers a high level of data protection, there are still concerns. Research has shown that continuous change and adoption of systems can improve data sharing and interoperability. Healthcare systems in developed countries allow seamless access to patient records and monitoring of their health. In addition, blockchain-based solutions reduce errors, reduce paperwork and claims processing, and increase efficiency.
- Smart Healthcare System in Weak Economies: Enabling technologies have not only changed the way healthcare works, but also the way the financial system works. When it comes to healthcare, finance is very different because there can be no compromise on the health of the patient. Blockchain technology has gained prominence due to its increased security. The financial situation in many countries is not as good as in developed economies. In low economic countries where healthcare is weak, sick people lose their lives due to lack of financial support [57], and the treatments that Blockchain offers can be beneficial for them as well.
- Supply Chain: In terms of supply chain, the blockchain system is being revolutionized in the healthcare industry [58]. Stakeholders

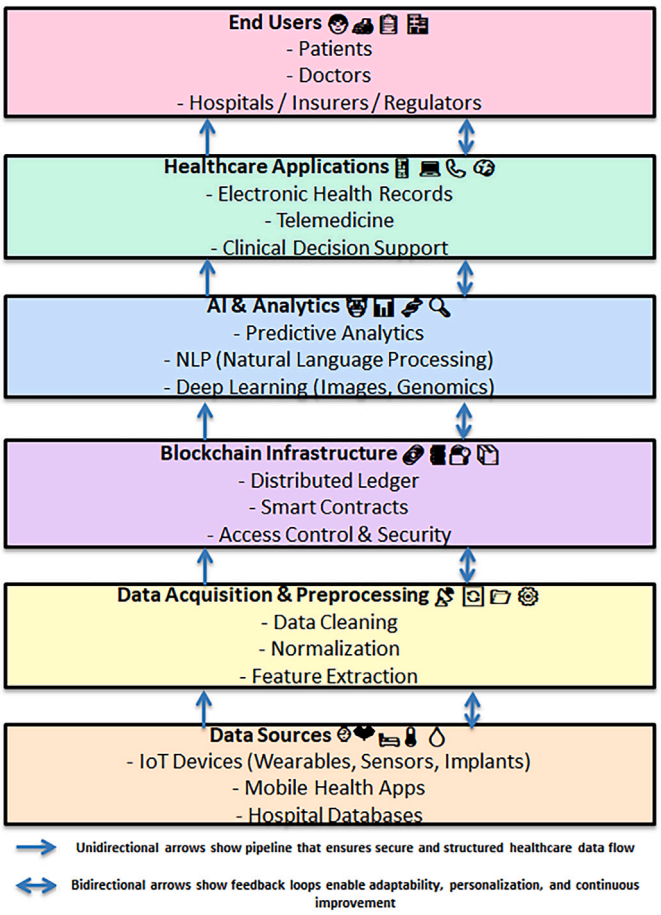


**Fig. 3.** Layered model of blockchain in smart healthcare.

can improve integrity and ensure the delivery of drugs and medical devices. SHS can help reduce problems related to medicines and improve the quality of care. Patients have more control over their health data by monitoring the supply chain system in the blockchain and can secure it for future use.

A layered model illustrating the implementation of blockchain technology in smart healthcare is presented in Fig. 3.

## 3. Critical analysis of state-of-the-art literature

With the implementation details in mind, this section presents a critical analysis of recent studies, comparing different approaches, identifying their strengths and limitations, and evaluating their impact on healthcare applications. The most commonly observed strengths throughout the literature in Table 2 are data quality and privacy. A detailed discussion on the strengths of blockchain technology in smart healthcare systems can be divided into the following four main areas.

1. Data integrity
2. Organizational issues
3. Health data handling costs
4. Collaboration among pharmacists

### 3.1. Data integrity

The study in [69] reported that there have been many incidents where power holders have forged medical test results, resulting in court cases in their favor. However, such cases are not highlighted in the studies. Therefore, the lack of information security is the fundamental problem that can be overcome by blockchain. Moreover, the authors of [73,75] discussed only the problems with the originality of the medicines. Many people who are less privileged do not receive original medicines, which leads to problems and sometimes death. Blockchain technology has helped many people authenticate medications at every step so that everyone has access to the actual medication.

Many healthcare organizations, such as community health systems in the United States, have fallen victim to digital crimes due to a failure to ensure cybersecurity [49]. Many healthcare systems use manual methods to access digital medical records. This system is outdated and can be altered with fraudulent intent. The study in [38] explains that medical records can also be lost due to disruptions or natural disasters. Blockchain technology eliminates the risk of data theft or mishandling of stored data. The damage caused by a natural disaster to a medical facility is avoided because the data is available in multiple locations and there is no central point of failure. Therefore, blockchain technology in a smart healthcare system is an effective means to ensure data integrity.

### 3.2. Organizational issues

Data in medical data centers and insurance carriers are fragmented in several areas [58,94–96]. Similar comments were made by the authors of [33] where they reported that insurance companies and healthcare institutions pursue their own interests and manipulate data. In [34], the authors mentioned that blockchain is excellent for collecting patients' medical history, creating contracts, and preserving all previously stored data to exclude people's involvement. So, if a diabetic patient suffers an accident, doctors and practitioners would have his medical history and could immediately seek advice from the pharmacist and physicians. This is possible if the data are kept up-to-date, traceable, and tamper-proof [64]. A counter-argument in [73] explains that data can be accurate if it is frequently updated or real-time assessments are implemented within blockchain technology.

Data quality and protection are considered critical in healthcare systems as they directly impact patient privacy and overall data integrity [97,98]. Blockchain technology has proven to be an effective solution as it improves security, data sharing, and trust. In [43], the author explained that the shared information about the patient can be used in various ways by leveraging the immutability and decentralization of the blockchain. Also in [71], it is pointed out that the information sharing systems in electronic health records improve data quality, build trust among stakeholders, and enable secure information exchange. In addition, Fusco et al. [31] highlighted that data quality can improve nurse management scenarios through a collaborative environment.

### 3.3. Health data handling costs

The costs associated with blockchain technology are a major concern in the healthcare industry. The transfer of patient data from the existing system to the blockchain system is a point of concern. The reason is the higher number of entries that need to be added to the system, and the medical record is divided into different departments [38]. Authors of [48] have mentioned that the patient who was once under medical treatment does not need to have a record and can be considered as a new patient at the next visit. Such strategy would help reduce the data handling cost however the administration and physician would not be able to see the patient history. It can be very costly to enter the past years' medical records into the system to better monitor the patient's current situation. Therefore, it is pointed out in [33,47,63,67] that capturing patient information in a manual system is time-consuming and costly. The person receiving the data must manually feed it into the system to be forwarded to the appropriate person.

**Table 2**
Comparative analysis of existing literature.

| Ref. | Year | Study & methodology | Benefits | Challenges |
|---|---|---|---|---|
| [10] | 2019 | Computing activity analysis | Decentralization of information and access during high alerts | Scalability issues |
| [19] | 2019 | Preferred reporting items for systematic reviews and meta-analysis (PRISMA) | Data protection is strong. | Scalability, latency and interoperability |
| [33] | 2019 | Real-time patient information | Safety and privacy, diagnostic precision, efficient therapies | Response time, heterogeneous data |
| [38] | 2019 | Literature review analysis databases within the ISI Web of Science | Improved quality of life, disease diagnosis, treatment, and healthcare service delivery system | Non-uniform data, large number of variables, and need for real-time data analysis |
| [48] | 2019 | Research article | Usage of health care for purchasing original products | High cost |
| [59] | 2019 | Patient-centered model | Improved patient care, increased data sharing, and enhanced security and privacy of patient data | Heterogeneity and scalability issue |
| [60] | 2019 | Literature review | Increased security and improved efficiency in healthcare industry | Technical challenges and legal complexities |
| [61] | 2019 | Literature review | High security and enhanced performance of healthcare staff | Less control over data |
| [13] | 2020 | Healthcare supply chain case study | Detailed discussion on data transparency, security and integrity | Massive data generation in supply chain |
| [15] | 2020 | Comparative analysis | Literature review on data security and integrity | Scalability and interoperability issues |
| [58] | 2020 | Access to the patient data | Management of patient groups, gathering data in real-time, and alert for emergencies | Data breach and security concerns |
| [62] | 2020 | Survey for attacks and security issues | Enhanced data security, efficient healthcare system and enhanced patient privacy | Scalability problem and interoperability issues |
| [63] | 2020 | Analyzing a company system | Transactions are validated, and authenticity is sealed until the material is encrypted, digitally signed, and saved | Costly as some parts do not integrate with same system |
| [64] | 2020 | Systematic review on overview of Blockchain, | Data security, storage, and payments through smart contracts. Store and retrieve the reports and prescriptions anytime | Complexity in scalability |
| [65] | 2020 | Study on patient feedback analysis | Timely support, and immediate responses | Inaccessible when traveling to different parts of the world |
| [66] | 2021 | Literature review | Focused on data security, privacy and efficiency of healthcare system | Scalability problem and interoperability issues |
| [67] | 2021 | Literature review | Information is authentic and legitimate and preserves users' privacy | Data handling and processing |
| [68] | 2021 | Systematic review | Telecare medicine information system and e-health | Challenges include data sharing, clinical trials and big data |
| [30] | 2021 | Analysis of database management system | Scalability, data processing, data security and interoperability | Adoption challenge and integration complexity |
| [69] | 2021 | Interoperability analysis of control groups | Improved patient care, increased data sharing, and enhanced transparency and trust | challenges of interoperability and integration complexities |
| [70] | 2021 | Comparative analysis | Increased security and improved efficiency in government services | Regulatory and legal challenges with technical complexities |
| [71] | 2021 | Systematic literature review | Blockchain-based e-healthcare ecosystems | Cyber crime, medical diagnostics and policy making |
| [72] | 2021 | Analysis of electronic records | High security and enhanced performance of healthcare staff | Integration complexity |
| [73] | 2022 | Used medical data and cases for investigation | Direct access to data for patients and a more robust data-sharing infrastructure. | Privacy, security, and full ecosystem interoperability |
| [74] | 2022 | Review article | Enhanced data sharing and data integrity | Technical challenges and legal complexities |
| [75] | 2023 | Survey | Better patient management | Problems in real time response and data encryption |
| [76] | 2023 | System analysis | Improved security and privacy, efficient learning systems and enhanced collaboration | Scalability limitations |
| [77] | 2023 | Survey | Security in healthcare systems and enhanced privacy is focused | Big medical data and its storage |
| [78] | 2023 | Analysis of health records | Interoperability of healthcare records, improved patient care | Adoption complexity, lack of technical support |
| [79] | 2023 | Systematic analysis of e-health system | Privacy-preserving control, enhanced security and improved healthcare | Scalability and interoperability |
| [27] | 2024 | Review article | Application, benefits and challenges of blockchain technology in healthcare | Regulatory hurdles, energy consumption, interoperability and scalability |
| [80] | 2024 | Traditional blockchain-related attacks in healthcare | Security vulnerabilities related to medicine traceability and records management are handled | Data storage and adoption complexities |
| [81] | 2024 | Topical review | Blockchain technology with IoT healthcare | Big IoT generated medical data storage |
| [82] | 2024 | Review article | Applications, solutions and performance issues of blockchain in healthcare | Cross-border data transfer, Throughput, scalability, interoperability and energy consumption |
| [83] | 2024 | Survey paper | Integration of blockchain and cloud computing in healthcare | Communication latency and data heterogeneity |
| [84] | 2024 | Research Article | Application of blockchain technology in IoT disciplines related to healthcare | Blockchain integration with latest technologies |
| [85] | 2025 | Survey paper | Blockchain and Generative AI | Scalability, privacy, energy consumption |
| [86] | 2025 | Survey paper | Blockchain technology and AI for EHRs | Interoperability, user interface complexities and data security |
| [87] | 2025 | Research article | Blockchain-distributed ledger technology and explainable artificial intelligence | Privacy protection, optimization, bias-mitigation |
| [88] | 2025 | Survey paper | Integration of AI and blockchain | Seamless interoperability, cost reduction, AI-Blockchain convergence |
| [89] | 2025 | Systematic Literature Review | Convergence of decentralized artificial intelligence, blockchain technology, and smart contracts | Trustworthiness, incentive alignment, transparency, accountability |
| [90] | 2025 | Research paper | Healthcare decision-making using blockchain and AI | Interoperability and scalability |
| [91] | 2025 | Research paper | Binary spring search technique for IoMT using blockchain and AI | Big IoT generated medical data storage |
| [92] | 2025 | Research paper | AI integrated blockchain in healthcare supply chain using F-AHP | Scalability, heterogeneity of data, evidence-based treatments |
| [93] | 2025 | Research paper | EffiIncepNet, an ensemble deep learning network, for health data categorization and blockchain security | Scalability, energy consumption, IoMT data processing and storage |

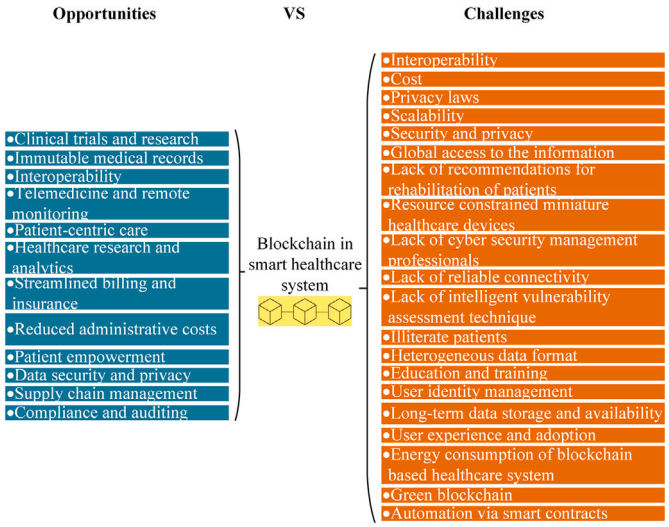


**Fig. 4.** Opportunities and challenges of blockchain technology in smart healthcare system.

Economies with small populations can easily handle their blockchain technology based smart healthcare systems as compared to the countries with large populations. If economies are able to manage their blockchain systems, blockchain technology can massively reduce administrative costs [44]. The records are secured in the smart contracts as digital fingerprints. Moreover, Myrzashova et al. [76] explained that the records are not only stored with credibility, but are secured at every level by identity verification and authentication of all participants and uniform authorization patterns [99]. Thus, once a manageable technology emerges, it can reduce the cost of smart healthcare systems.

### 3.4. Collaboration among pharmacists

Pharmacists can collaborate with patients and provide health care professionals with tools for interaction and individualized medical advice. Pharmacists can access comprehensive medical records and patient medication history, helping them make informed decisions. Real-time information available through the blockchain system provides valuable insights into patients' allergies, past side effects, and medical preferences [47]. Blockchain technology also facilitates knowledge and financial management for healthcare facilities. It reduces the environmental impact and minimizes the cost and time required for data transformation.

## 4. Opportunities and challenges

Following the critical review, this section examines the opportunities and challenges associated with deploying AI-enabled blockchain in smart healthcare, providing insights into research gaps and areas requiring further development. These opportunities and challenges present significant obstacles that must be carefully addressed in order to fully leverage the technology. A graphical representation of the opportunities and challenges of blockchain technology in smart health systems can be seen in Fig. 4. Details of each point are provided in the later part of this section.

### 4.1. Opportunities

When integrated into a smart healthcare system, blockchain technology offers a wide range of exciting possibilities. Its potential impact on healthcare ranges from promoting patient-centered care to improving data security. In this subsection, the study explores the key prospects that blockchain offers for the healthcare industry.

#### 4.1.1. Clinical trials and research

Handling clinical trial data can be made more efficient and secure with blockchain. By ensuring the accuracy and traceability of data, researchers can facilitate the review of trial results and accelerate the development of new treatments.

#### 4.1.2. Immutable medical records

When medical data is stored in a blockchain, it is immutable and resistant to tampering. As a result, there are fewer errors and discrepancies in the accuracy and integrity of patient information over time.

#### 4.1.3. Interoperability

Interoperability of data between different healthcare providers, systems, and devices can be facilitated by blockchain. This allows patient data to be easily and securely shared between different healthcare organizations, improving care coordination and reducing duplicate tests and procedures.

#### 4.1.4. Telemedicine and remote monitoring

Blockchain can help telemedicine interactions and remote patient monitoring become more secure and private. Sensitive information can be confidently exchanged between patients and healthcare professionals.

#### 4.1.5. Patient-centric care

Blockchain enables patient-centric care by ensuring that medical records follow the patient, allowing medical professionals to make decisions based on the whole medical history of a patient.

#### 4.1.6. Healthcare research and analytics

Blockchain networks provide secure access to a massive database of anonymized patient data, allowing researchers to perform advanced analytics and gain important insights into the patterns of diseases and the effectiveness of treatments.

#### 4.1.7. Streamlined billing and insurance

Blockchain can securely record and verify claims, which will streamline and automate the billing and insurance procedures. This can reduce administrative expenses and prevent erroneous claims.

#### 4.1.8. Reduced administrative costs

Blockchain's automation and efficiency enhancements can reduce healthcare administration costs, which can then be allocated towards patient care and research.

#### 4.1.9. Patient empowerment

More control over their medical records can be given to patients, who can also grant or revoke access as necessary. Individuals are empowered to actively engage in healthcare decisions and share their personal information with healthcare professionals of their choice.

#### 4.1.10. Data security and privacy

The security and privacy of healthcare data can be improved through blockchain. In order to reduce the risk of data breaches and unauthorized access, patient records, treatment histories, and personal information can be securely maintained and accessed only by authorized parties. Patients can exercise greater control over their health information by authorizing specific individuals or organizations to access it.

#### 4.1.11. Supply chain management

Pharmaceutical and medical device supply chains can be tracked via blockchain, ensuring product quality and authenticity. Patient safety is improved and the chance of fake pharmaceuticals entering the market is decreased.

#### 4.1.12. Compliance and auditing

Healthcare organizations can use blockchain to help them stay in compliance with legal regulations like HIPAA in the US. The transparency and effectiveness of auditing and reporting increase.

### 4.2. Challenges

In addition to advantages, blockchain technology also has some limitations. The main ones identified in the literature are security, privacy, scalability, interoperability, and lack of laws and policies. In addition, the risk of error, the complexity of the patient's condition, and the structural design are the main problems of blockchain technology. For example, a weak or incorrect diagnosis is usually re-evaluated by physicians and recognized through experience. The technology cannot analyze the condition based on the severity [62]. The private keys are also vulnerable to security breaches due to the risk of being stolen or lost. In both cases, this would result in unauthorized individuals gaining access to the health data [10]. There are growing security concerns regarding future technologies such as quantum computing that require encrypted access, which could lead to security issues. Even when an organization makes changes in technology and software updates, they require access to the information, which can also lead to privacy breaches and security issues. A few prominent research challenges of blockchain enabled smart healthcare systems are discussed in this section.

#### 4.2.1. Interoperability

Interoperability in blockchain based healthcare systems is not limited to sending information, but also includes sending reports to all professionals to efficiently search for solutions [14]. However, only 60% of hospitals can use the incoming data and integrate it into their electronic health records. Research in [34] has shown that state and federal governments around the world are working to improve the healthcare system, its interoperability and have complementary regulations working towards a common vision. In addition, work on standardization and regulatory matters also affects the interoperability issue of blockchain technology.

The study by Shaikh et al. [133] explains interoperability in the healthcare sector. Blockchain technology in healthcare represents secure and seamless information exchange, but its lack of interoperability makes it difficult. It is complicated because it consists of information about the patient that involves multiple stakeholders, providers, consumers, and payers. The Office of the National Coordinator for Health Information Technology (ONC) outlined a roadmap to help people and organizations. In doing so, ONC called on IT stakeholders to formulate and develop designs and approaches to achieve the ability to share data without fear of information loss [42]. As a result, blockchain technology requires significant investment.

Lack of universal adoption of blockchain will increase the challenge of interoperability. There are no universal standard rules or systems for healthcare information because the internal mechanisms and applications are different [13]. Literature review reveals the existence of different methodologies from different suppliers on different platforms and dissimilarities among applied algorithms. Such heterogeneity also complicates the issue of interoperability. Therefore, it should be noted that there exists no standardization for the transfer of information from one format to another. There are different providers or platforms that may not be interoperable [58]. As a result, blockchain networks are not capable of ensuring consistency of patient information and transfer of records. The study in [58] explores that the three blockchain systems that were worked on were different, making it difficult for a person to access their medical record in another country.

Less attention was paid to the differences in prototypes and proofs-of-concept. For COVID-19, this was also a challenge because the medical record could not be accessed if the person wanted to travel [63]. The systems may cause problems because there are differences in the smart contract functions, transaction processes, and models [67]. A comparison of HealthChain and Hyperledger Fabric shows that the functions within the same concept are different [47]. Hyperledger uses the Ethereum blockchain platform, which has different internal functions and is distinct. Both systems manage electronic health records (EHRs) on different platforms. However, sharing information between one EHR system and the other platform is challenging [33,47,100]. Therefore, interoperability among blockchain networks is a significant challenge when it comes to sharing health related stored data.

#### 4.2.2. Cost

Implementing strategies to overcome interoperability or to create a global system for eliminating legal regulations would increase costs [38]. Different nations, regions, or locales have various blockchain systems that are tailored to their economic structures. As a result, the healthcare system is created in the same way. If adjustments were made to establish a single, universal system, the cost would be greater. In addition, the agreements and approvals from different agencies would create a complicated situation for all parties involved [48,101]. This could also lead to disruptions in the current healthcare system. Patients would not be able to wait for data to be processed and would face long waiting times. This would not only affect the cost but also the time. Therefore, cost is one of the biggest challenges of blockchain technology.

In addition, the cost of setting up a digitized system is still considered high even when applied to a single region. Evaluating and implementing a new technology would increase costs. In addition, changing the technology or adding drugs to the system would mean having a dedicated team for research and development [36]. The cost of processing the credibility of each element in the system would require significant investment. The healthcare system is based on the blockchain, which requires resource availability, upgrades, and backups. Therefore, the system has the problem of higher operational costs [47,67].

#### 4.2.3. Privacy laws

Another challenge is ensuring that blockchain technology is compatible with the country's privacy laws [13]. The lack of clarity on compliance is a challenge that discourages healthcare organizations from implementing the system. The study states that work is still being done on the rules and regulations for blockchain. The organization needs to monitor the regulations and the system as it is still in its early stages. The research suggests that healthcare organizations should be directly involved in collecting information from local regulatory authorities regarding privacy laws. Policies vary among countries regarding the blockchain system. For example, Singapore and Switzerland use token systems to speed up the system [10]. On the other hand, the United States has different policies for different regions [10]. In [38], it is suggested that technology in the healthcare industry needs to work on blockchain policies and practices to make blockchain technology mainstream.

In addition, when working with blockchain technology, it is challenging when an external participant has limited information about regulatory requirements. Newly introduced laws and regulations have implications for blockchain-based healthcare systems. Multi-national companies operating in the healthcare industry need to be aware of legal developments in order to understand the healthcare related information. Companies need to keep abreast of regulatory developments to continuously monitor them [20]. For example, if companies use a drug that is banned in a country, this can lead to legal issues. The challenge of the supplier not being part of the system can lead to legal violations. Therefore, navigating the legal requirements can be a problem for the external partner.

#### 4.2.4. Scalability

One of the prominent challenges of blockchain technology in smart healthcare systems is scalability, which hinders its popularity [70]. The

blockchain system is capable of executing multiple transactions simultaneously, which makes it easier for physicians to progress. In [32], it is mentioned that the database stores information such as profile data, financial information, and various other important details. Storage of large health data leads to data replication issues that ultimately require significant storage capacity. The large storage requirement is a scalability issue of blockchain technology in smart healthcare systems [9,48]. There are limitations in transferring large biomedical data as it leads to significant performance degradation [63,102]. The scalability challenge is directly related to processing speed. Blockchain technology is adversely affected by latency, which is a limiting factor for system scalability. Higher delays may lead to lower processing speeds [33]. Therefore, scalability of the blockchain applications can be problematic and challenging for large organizations.

#### 4.2.5. Security and privacy

Security and privacy are the key elements of blockchain technology that enable trust and improve the use of information by healthcare participants. Blockchain technology has attracted the attention of all stakeholders because it enables decentralized, immutable, and transparent data management. Several studies [18,45,72,78] have highlighted how blockchain nodes create a secure environment for patients, promote trust among participating nodes and facilitate secure information exchange. Blockchain technology, with its cryptographic techniques and decentralized architecture, offers the potential to address privacy concerns by enabling secure data exchange while maintaining confidentiality for patients [41].

The ever-accelerating growth in IoT devices leads to the generation of gigantic data volumes. Due to the limited computational and memory capacity of these devices, local storage is not feasible, leading to data outsourcing [103]. Cloud-based data storage has rapidly gained popularity in recent years. Data outsourcing to the cloud introduces security risks, including cloud pooling [104,105]. Patient privacy and confidentiality are critical concerns, especially when sharing sensitive health information like cancer and HIV reports. Privacy concerns arise when patient records are shared with third-party service providers [103]. Inadequate security measures, misconfigured devices, and network vulnerabilities can compromise patient data privacy and confidentiality [106]. Additionally, cloud service providers store data from smart devices but may not guarantee that the received data remains unaltered.

#### 4.2.6. Global access to the information

Existing medical records for data sharing are not as efficient, as they do not provide global access to information. The study by [16] examined current medical records and how they are shared. A centralized system stores patient records. In a centralized system, data exchange may be simpler because manual systems were time consuming and had complicated procedures. These centralized systems might be problematic in healthcare, where a huge number of emergencies are received every day. Furthermore, systems administration may be delayed owing to changing legislation, incompatible technologies, and fragmented information. This challenge is due to a lack of collaboration and a problematic storage system. The current system makes it difficult to analyze data in real time to make immediate assessments and provide immediate care to the patient [51].

#### 4.2.7. Lack of recommendations for rehabilitation of patients

To provide for their care and treatment, the aging population of the globe has a large demand for trained healthcare professionals [107,108]. As a result, especially during an epidemic like COVID-19, a shortage of trained medical professionals might significantly increase the death rate. Smart medical devices have been created to track the many aspects of patients' health, including glucose monitoring, Parkinson's disease monitoring, and heart-rate monitoring. Additionally, remote patient monitoring (RPM) is now possible thanks to these devices. These tools do not, however, provide suggestions for immediate rehabilitative therapy. These devices track, collect, and share information with medical specialists so they can propose more treatments, which slows down and stresses hospitals. Therefore, the only way to determine an accurate and timely course of treatment is through a brief patient evaluation.

The benefits of suggested breast cancer treatment based on machine learning have not been well investigated [109,110]. However, these intelligent wearables fall short in developing corrective methods for the future assessments of the collected data. Such gadgets have to incorporate advanced artificial intelligence (AI), genetic algorithms (GA), ant colony optimization (ACO), and simulated annealing (SA), which may be used for data analysis and suggestion of the optimum solution [111]. The use of smart devices for self-recommendation treatment may help patients recover more quickly and relieve hospital pressure.

#### 4.2.8. Resource constrained miniature healthcare devices

Patients can have microscopic-sized smart medical devices implanted inside them to monitor their health. These tiny gadgets often feature 64KB to 640KB of memory, weak computational capability, and low battery life, all of which impact performance and require frequent recharging. For manufacturers and software developers, adopting advanced security solutions may be difficult due to these restrictions. In the event that the security of these smart devices is compromised, patients might find themselves in a number of risky scenarios. However, there hasn't been a study done on the advancement of the lightweight cryptographic techniques discussed in [112]. There is a need for extensive study to develop resource-constrained cryptography algorithms for smart medical devices [113,114]. These devices also need to have longer battery lives in order to prevent network failure [114,115].

#### 4.2.9. Lack of cyber professionals

The ecosystem of smart health-care consists of several intelligent implanted and wearable technologies that continually monitor the patients' health whether they are receiving care at home or at the hospital. The ecosystem, however, is still in its infancy and vulnerable to several security and privacy risks. The health of patients in intensive care units (ICUs) must be continuously monitored. The hospital IoT network is particularly vulnerable to DDoS assaults and other attacks that require significant resources and effort to defend the systems. In the healthcare sector, cyberattacks have become more frequent [116]. Additionally, network interruptions brought on by these assaults might result in patient fatalities. Consequently, the hospital needs cybersecurity management specialists who can quickly restore the environment.

#### 4.2.10. Lack of reliable connectivity

In comparison to doctors, the number of patients worldwide is rising quickly. The lack of qualified medical professionals forces health care organizations to remotely check patients' conditions. Smart gadgets transfer data to the cloud, where doctors may access and review the patient records. Additionally, the online telemedicine system contributes to the efficient and prompt delivery of medical treatments [117]. However, for ongoing data exchange and monitoring, these smart gadgets require a reliable internet connection. Patients who are in critical condition must remain in locations with internet access. The patient may experience a catastrophic scenario as a result of minor internet connection latency [118]. In nations with unstable connections, the idea of telemedicine and the monitoring of cloud-based data may be challenging. As a result, the benefits of smart healthcare may only be available to wealthy nations, leaving developing nations without access to them.

#### 4.2.11. Lack of intelligent vulnerability assessment technique

The small size and limited processing and memory capacities of smart gadgets make it challenging to develop cryptographic methods. Additionally, the varied nature of these devices makes it difficult for researchers to design automated vulnerability identification and recovery methods [119,120]. It is challenging for researchers to find

real-time datasets with sufficient availability for security vulnerability identification and prompt remediation. Similarly, the researcher faces a significant hurdle due to the network's constantly changing functionality and the need for a single automated binary fix. The database that keeps track of exploits and vulnerabilities and records that structured data is still in its infancy.

#### 4.2.12. Illiterate patients

Medical equipment has a number of smart characteristics. The wearable smart gadget has an accelerometer, pedometer, and can track various activities in addition to blood pressure and heart rate. However, the uneducated patient may find it challenging to grasp these gadgets' usage of medical terms like systolic and diastolic. It may be difficult to comprehend, absorb, and assess the information displayed on smart gadgets [121]. The developing world has a higher rate of illiteracy than the industrialized world [122]. Additionally, not every patient will be able to comprehend the terms and scales used in medicine to quantify the health of various bodily parts [123]. If there is no doctor around to monitor the patient's condition, it may be difficult to grasp medical terminology. [123]. As a result, the vendor of smart devices should provide a brief course-based tutorial in the patient's native tongue on how to operate these gadgets. Additionally, the gadget should be capable of understanding urgent patient situations and alerting rescue services if necessary. This would facilitate efficient pandemic management. The current Covid-19 epidemic has had an impact on several nations in terms of the lack of awareness and early illness diagnosis.

#### 4.2.13. Heterogeneous data format

Data management presents a number of issues due to the heterogeneous format of data originating from wearable or implanted sensors. These gadgets function differently for various bodily areas and gather data in various formats. Diverse smart medical devices have diverse ranges, natures, volumes, and rates [124]. For examples the data from Electro Cardio Graphic (ECG) devices may be recorded in XML format which may differ from other data recordings. The evaluation of the patient's health is delayed as a result of the collection and processing of heterogeneous data, which presents major data management challenges. However, there is a framework that gathers data from all wearable or implanted devices and then categorizes the acquired data to provide a single report. Practitioners have worked in a variety of fields to accomplish data protocols [125].

For the physicians to analyze the overall health of the body, all the devices must report the gathered data through a unified interface. This can aid in the doctor's medication recommendation. In the past, a patient would just mention one illness, and the doctor would then prescribe the appropriate medication. There are a number of negative consequences this technique has on patient health. In contrast, if the system displays the health state of every body part to the doctor, this may help the doctor comprehend the patient's overall health and administer medication without causing negative side effects on other body parts.

#### 4.2.14. Education and training

Healthcare professionals and IT staff must be trained on the technology in order to effectively use and maintain healthcare systems built on blockchain technology [41]. Research should explore possibilities for education and training to narrow the knowledge gap. One of the IoT industry's fastest-growing ecosystems, with healthcare gadgets expected to reach 176 billion by 2026, is the IoT market. The use of these smart gadgets in hospitals, particularly in the intensive care unit (ICU), offers both patients and medical professionals a number of opportunities. The management of this ecosystem requires a skilled IT staff due to the complexity of these devices and the heterogeneous network architecture [126]. The adoption and assessment of these smart devices can be supported by a sizable pool of competent IT professionals who have a thorough understanding of the patient and the healthcare system. A little carelessness when using these gadgets might have a major negative impact on the health of the patient. Additionally, a lack of highly skilled IT professionals in the medical industry may lead to poor purchases of these smart gadgets. Therefore, before putting these gadgets into use and testing them, the operational team members need to be trained.

#### 4.2.15. User identity management

Healthcare systems need to ensure reliable and secure management of patient identification [21,127]. To authenticate patient IDs on the blockchain without compromising privacy, research is needed to develop trusted and accessible techniques [128].

#### 4.2.16. Long-term data storage and availability

Healthcare-related data must be stored securely and long-term. Exploring techniques to maintain data integrity and ensure its availability on the blockchain over extended periods of time still requires research [129].

#### 4.2.17. User experience and adoption

A number of parties, including patients, healthcare professionals, insurers, and regulators, need to work together to adopt blockchain technology in the healthcare industry [14]. Strategies to drive user adoption and provide a frictionless user experience should be the subject of research.

#### 4.2.18. Energy consumption of blockchain based healthcare system

Proof-of-work (PoW) based blockchain networks like Bitcoin are known to consume a lot of energy [130]. Developing consensus mechanisms that are acceptable for medical applications should be the main goal of research.

#### 4.2.19. Green blockchain

Fossil fuel based energy generation leads to higher carbon emissions that is in turn an environmental challenge. The use of renewable energy to power the blockchain based healthcare system is another research area to be focused on [131].

#### 4.2.20. Automation via smart contracts

Smart contracts can automate and streamline a number of healthcare procedures, but their complexity and irreversibility require careful planning and testing [132]. Research is needed to create reliable and secure smart contracts that accurately execute healthcare agreements without unintended consequences. A brief strengths, weaknesses, opportunities and threats (SWOT) analysis of blockchain implementation in the smart healthcare system is shown in Fig. 5.

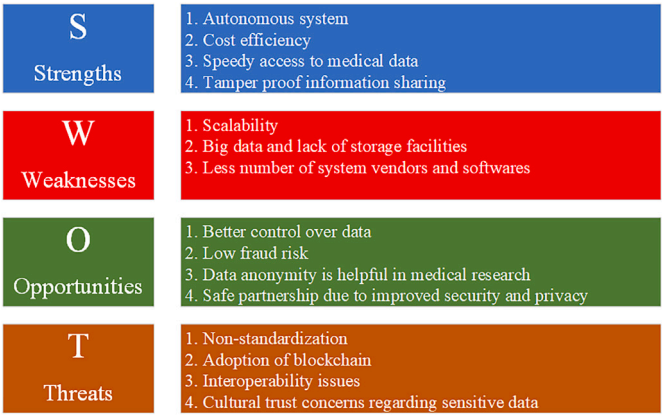


**Fig. 5.** SWOT analysis of blockchain implementation in smart healthcare system.

## 5. Proposed trust-automation-interoperability (TAI) synergy framework

Although prior studies have thoroughly examined the individual advantages and limitations of blockchain and artificial intelligence in healthcare, they largely fall short of explaining the value that emerges when these technologies are combined as elements of a broader ecosystem. To address this gap, this study introduces the Trust–Automation–Interoperability (TAI) Framework, a conceptual model intended to guide the design, analysis, and deployment of AI-enabled blockchain solutions for smart healthcare. The framework is grounded in the premise that a robust and sustainable digital health ecosystem can only be achieved by jointly strengthening three fundamental dimensions: trust, automation, and interoperability.

### 5.1. Trust

Trust represents the confidence that healthcare data and system processes are reliable, secure, private, and open to verification. In this context, blockchain plays a foundational role by ensuring that records cannot be altered, data exchanges are cryptographically protected, and all activities are transparently logged through decentralized consensus mechanisms. Artificial intelligence further reinforces trust by making system decisions more understandable through explainable AI and by continuously monitoring the system to identify security threats or unusual behavior. Together, these capabilities help answer a central concern in smart healthcare: how to reliably safeguard sensitive data, ensure fairness in automated decisions, and build lasting confidence among patients, healthcare professionals, and regulatory authorities.

### 5.2. Automation

Automation reflects the system's ability to carry out tasks, enforce rules, and generate meaningful insights with little or no human intervention. Blockchain supports this capability through smart contracts that automatically execute predefined actions, such as processing insurance claims, managing patient consent, and verifying healthcare supply chains in a secure and reliable manner. At the same time, artificial intelligence strengthens automation by enabling predictive analytics, streamlining routine administrative work through robotic process automation, and assisting clinicians with intelligent diagnostic and decision-support tools. Together, these technologies help reduce administrative overhead, speed up clinical and operational workflows, and shift healthcare delivery toward more proactive, data-driven care.

### 5.3. Interoperability

Interoperability refers to the capacity of different healthcare systems, devices, and organizations to seamlessly share, understand, and use data in a meaningful way. Blockchain contributes to this goal by providing a standardized and shared ledger that acts as a trusted single source of truth, enabling secure data exchange across institutional and organizational boundaries. Artificial intelligence further enhances interoperability by using natural language processing (NLP) to extract insights from unstructured clinical notes and machine learning techniques to align diverse data formats with common standards and ontologies. Together, these capabilities address a fundamental challenge in healthcare by breaking down data silos, supporting comprehensive and longitudinal patient records, and enabling more coordinated and continuous care.

The strength of the TAI Framework lies in the close interconnection of its three dimensions, where progress in one area naturally reinforces the others. Trust serves as the foundation for automation, as confidence in data integrity and the security of smart contracts is essential before automated clinical and administrative processes can be widely adopted. In turn, automation supports interoperability by enabling automated data harmonization and smart contract–based data-sharing mechanisms that help overcome technical and organizational barriers. Interoperability then feeds back into trust by ensuring access to complete and consistent data, which is critical for training reliable and unbiased AI models and for maintaining accurate, longitudinal patient records. An effective AI-blockchain healthcare system therefore operates in the central "synergy zone" of the TAI model, where trust, automation, and interoperability evolve together. In contrast, many existing solutions focus on only one dimension, e.g., blockchain-based supply chain systems that achieve strong trust guarantees but fall short in AI-driven automation or broad interoperability.

To capture the relationship among these dimensions, this study adopts the Trust–Automation–Interoperability (TAI) Synergy Framework (Fig. 6). The model offers a straightforward way to understand how different healthcare solutions, ranging from traditional information systems to AI-enabled blockchain platforms, align with or

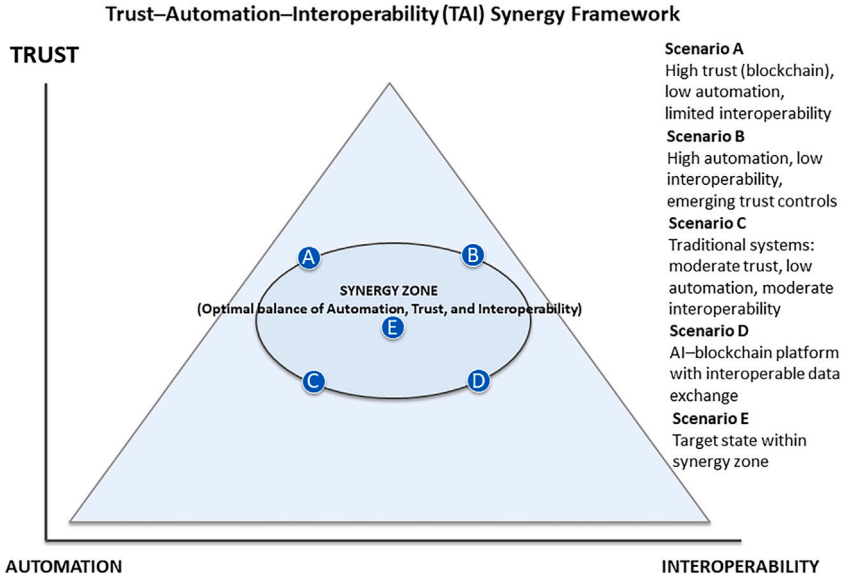


**Fig. 6.** Trust-Automation-Interoperability (TAI) Synergy Framework illustrating a balance among trust, automation, and interoperability.

fall short of the balance needed for reliable smart healthcare delivery. By positioning various system scenarios within a triangular space, the framework illustrates how robust trust mechanisms, intelligent automation, and seamless data exchange must reinforce one another to achieve a resilient and trustworthy health ecosystem.

In this context, blockchain contributes verifiable data integrity and transparent access control, while AI supports intelligent decision-making, workflow automation, and predictive capabilities. Interoperability binds these strengths together by ensuring that data, once secured and processed, can be meaningfully shared across institutions. The synergy zone represents the point where these three qualities are well aligned, reflecting the kind of system maturity envisioned in emerging healthcare architectures.

The conceptual arrangement of trust, automation, and interoperability is illustrated in Fig. 6, which outlines how varying levels of maturity and integration shape the effectiveness of AI-enabled blockchain systems in healthcare. The synergy zone represents the optimal intersection where AI-enabled blockchain solutions can support secure, automated, and smoothly interconnected healthcare workflows.

An illustrative example of our proposed TAI Framework in practice is an AI-augmented telemedicine platform. In such a system, trust is established by using blockchain to securely record video consultations and patient vital data, while explainable AI helps physicians understand and confidently act on AI-generated diagnostic recommendations. Automation is achieved through smart contracts that manage appointment scheduling and payments, alongside AI-based triage systems that prioritize patients by analyzing reported symptoms. Interoperability is addressed by adopting Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) standards, with blockchain oracles enabling the secure retrieval of patient histories from hospital electronic health record (EHR) systems. From a TAI perspective, this platform is highly effective when trust, automation, and interoperability are fully integrated; however, its impact is significantly reduced if it functions as an isolated application that lacks meaningful data exchange with the broader healthcare ecosystem.

Another practical application of our proposed TAI Framework can be seen in clinical trial data management. In this setting, blockchain establishes trust by immutably recording trial protocols, patient consent, and outcome data, thereby reducing the risk of data tampering and research fraud. Automation is introduced through AI systems that continuously monitor trial data to detect early safety concerns or emerging efficacy signals, while smart contracts automatically release payments to trial sites once predefined milestones are verified. Interoperability is achieved by integrating data from multiple electronic data capture (EDC) platforms and wearable sensors into a single, unified trial ledger. From a TAI standpoint, this use case clearly demonstrates how the combination of automation and trust, supported by interoperable data flows, addresses longstanding challenges in clinical research.

## 6. Limitations

While this study offers a broad overview of current work in the field, it still faces a few limitations. Much of the available literature is based on early-stage models, small pilot projects, or controlled test settings, which do not always reflect the complexities of real healthcare environments. Differences in regulations, data practices, and system compatibility between countries also make it difficult to apply the findings universally. Because AI and blockchain continue to develop at a fast pace, some observations may change as newer methods and tools appear. These points show that more real-world testing, collaboration across healthcare institutions, and longer-term studies are needed to build a clearer picture of how these systems will perform at scale.

## 7. Conclusion

Drawing on the preceding discussions, this study highlights the role of blockchain in enhancing smart healthcare systems by improving data security, privacy, transparency, and decision-making processes. The review of state-of-the-art literature reveals both the benefits and limitations of blockchain adoption, including stronger data integrity, reduced human error, and cost efficiency, alongside challenges such as interoperability, regulatory uncertainty, patient identity management, implementation costs, and global accessibility. By analyzing these factors, the study provides a clear overview of current applications, identifies key obstacles, and suggests directions for future research and practical deployment. Overall, this work demonstrates how blockchain can support more reliable, efficient, and trustworthy healthcare infrastructures while offering a foundation for addressing remaining technical, operational, and regulatory challenges.

## 8. Future implications

The study highlights potential future directions and implications for both research and practical applications, showing how AI and blockchain can continue to enhance healthcare systems. Looking ahead, these technologies could support healthcare networks that are secure, automated, and interoperable, enabling real-time patient monitoring, early diagnostics, and more personalized treatment pathways. Blockchain can ensure that medical records remain tamper-proof and transparent, while AI can interpret large and complex healthcare datasets to support more accurate decision-making and better resource allocation.

Integrating AI explainability will make AI-driven insights clearer and more trustworthy for clinicians and patients, ensuring that automated recommendations can be understood and validated. In addition, the emergence of federated blockchain models offers a way to maintain strong data privacy while still enabling collaborative analytics across multiple healthcare institutions.

These advancements can also encourage greener healthcare practices by reducing paper-based processes, minimizing unnecessary hospital visits, and improving the energy efficiency of digital platforms. Moreover, they can strengthen telemedicine services, simplify administrative workflows, and enhance patient privacy and consent management. As standards, scalability approaches, and regulatory frameworks evolve, AI-enabled blockchain solutions have the potential to become the foundation of resilient, reliable, efficient, and environmentally sustainable smart healthcare infrastructures.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Funding

This work is supported by the Science and Technology Ph.D. Research Startup Project (Grant No. SZIIT2023KJ016, received by Dr. Muhammad Sadiq), and by Guangdong Basic and Applied Basic Research Foundation (Grant No. 2023A1515110070, received by Dr. Junwei Liang).

## Data availability

All used data and material is cited in the article.

## References

[1] E. Fazel, M.Z. Nezhad, J. Rezazadeh, M. Moradi, J. Ayoade, IOT convergence with machine learning & blockchain: a review, Internet Things (2024) 101187.
[2] A. Thacharodi, P. Singh, R. Meenatchi, Z.H. Tawfeeq Ahmed, R.R.S. Kumar, V. Neha, S. Kavish, M. Maqbool, S. Hassan, Revolutionizing healthcare and medicine: the impact of modern technologies for a healthier future—a comprehensive review, Health Care Sci. 2 (5) (2024) 329–349.
[3] A.S. Bale, T.P. Purohit, M.F. Hashim, S. Navale, Blockchain and its applications in industry 4.0, A Roadmap for Enabling Industry 4.0 by Artificial Intelligence (2022) 295–313.

[4] P.P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for iot-based healthcare: background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) (2021) 85–94.
[5] G. Wu, S. Wang, Z. Ning, B. Zhu, Privacy-preserved electronic medical record exchanging and sharing: a blockchain-based smart healthcare system, IEEE J. Biomed. Health Inform. 26 (5) (2021) 1917–1927.
[6] S. Srividhya, K. Pradeepa, Blockchain technology, Industry 5.0 for Smart Healthcare Technologies: Utilizing Artificial Intelligence, Internet of Medical Things and Blockchain (2024) 77.
[7] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, A. Abraham, Securing ai-based healthcare systems using blockchain technology: a state-of-the-art systematic literature review and future research directions, Trans. Emerg. Telecommun. Technol. 35 (1) (2024) e4884.
[8] F.B. Insights, Healthcare Cloud Computing Market Size, Share & Industry Analysis, Report Id: Fbi109897, Tech. rep., 2025.
[9] C. Arsene, The Global "blockchain in Healthcare" Report: the 2022 Ultimate Guide for Every Executive, Tech. rep., 2022.
[10] N. Islam, Y. Faheem, I.U. Din, M. Talha, M. Guizani, M. Khalil, A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services, Futur. Gener. Comput. Syst. 100 (2019) 569–578.
[11] S. Khan, M.B. Amin, A.T. Azar, S. Aslam, Towards interoperable blockchains: a survey on the role of smart contracts in blockchain interoperability, IEEE Access 9 (2021) 116672–116691.
[12] S. Dhingra, R. Raut, K. Naik, K. Muduli, Blockchain technology applications in healthcare supply chains–a review, IEEE Access 12 (2024) 11230–11257.
[13] M. Reda, D.B. Kanga, T. Fatima, M. Azouazi, Blockchain in health supply chain management: state of art challenges and opportunities, Procedia Comput. Sci. 175 (2020) 706–709.
[14] M. Attaran, Blockchain technology in healthcare: challenges and opportunities, Int. J. Healthc. Manag. 15 (1) (2022) 70–83.
[15] A.A. Mazlan, S.M. Daud, S.M. Sam, H. Abas, S.Z.A. Rasid, M.F. Yusof, Scalability challenges in healthcare blockchain system—a systematic review, IEEE Access 8 (2020) 23663–23673.
[16] S.V. Akram, P.K. Malik, R. Singh, G. Anita, S. Tanwar, Adoption of blockchain technology in various realms: opportunities and challenges, Secur. Priv. 3 (5) (2020) e109.
[17] R.G. Shukla, A. Agarwal, S. Shukla, Chapter 10 - blockchain-powered smart healthcare system, in: Handbook of Research on Blockchain Technology, Academic Press, 2020, pp. 245–270.
[18] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, R.G. Crespo, Blockchain-based privacy preservation for iot-enabled healthcare system, ACM Trans. Sens. Netw. 19 (3) (2023).
[19] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: a systematic review, Healthcare 7 (2) (2019).
[20] D.O. Ogundipe, The impact of big data on healthcare product development: a theoretical and analytical review, Int. Med. Sci. Res. J. 4 (3) (2024) 341–360.
[21] A.K. Tyagi, R. Seranmadevi, Blockchain for enhancing security and privacy in the smart healthcare, Digit. Twin Blockch. Smart Cities (2024) 343–370.
[22] H. Omidian, Synergizing blockchain and artificial intelligence to enhance healthcare, Drug Discov. Today (2024) 104111.
[23] Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J.P. Tsai, C.-R. Shyu, A patient-centric health information exchange framework using blockchain technology, IEEE J. Biomed. Health Inform. 24 (8) (2020) 2169–2176.
[24] D. Bhumichai, C. Smiliotopoulos, R. Benton, G. Kambourakis, D. Damopoulos, The convergence of artificial intelligence and blockchain: the state of play and the road ahead, Information 15 (5) (2024) 268.
[25] N.K. Shinde, A. Seth, P. Kadam, Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and IOT for diverse applications, Mach. Learn. Optim. Eng. Des. (2023) 85–119.
[26] Z. Qu, W. Shi, B. Liu, D. Gupta, P. Tiwari, Iomt-based smart healthcare detection system driven by quantum blockchain and quantum neural network, IEEE J. Biomed. Health Inform. 28 (6) (2024) 3317–3328, https://doi.org/10.1109/JBHI.2023.3288199
[27] A. Atadoga, O.A. Elufioye, T.T. Omaghomi, O. Akomolafe, I.P. Odilibe, O.R. Owolabi, et al., Blockchain in healthcare: a comprehensive review of applications and security concerns, Int. J. Sci. Res. Arch. 11 (1) (2024) 1605–1613.
[28] A.K. Tyagi, S. Tiwari, K. Naithani, Distributed systems and distributed ledger technology-an introduction, Artif. Intell.-Enabled Digit. Twin Smart Manuf. (2024) 103–123.
[29] W.Y. Leong, Y.Z. Leong, W. San Leong, Blockchain technology in next generation energy management system, in: 2024 7th International Conference on Green Technology and Sustainable Development (GTSD), IEEE, 2024, pp. 15–19.
[30] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, M. Abid, Healthblock: a secure blockchain-based healthcare data management system, Computer Networks 200 (2021) 108500.
[31] A. Fusco, G. Dicuonzo, V. Dell'Atti, M. Tatullo, Blockchain in healthcare: insights on Covid-19, Int. J. Environ. Res. Public Health 17 (19) (2020).
[32] K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: review and open research challenges, IEEE Access 7 (2019) 10127–10149.
[33] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, Blockchain-based remote patient monitoring in healthcare 4.0, in: IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 87–91.
[34] F.A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A.A. Alwan, A. Jabbari, R.G. Sonkamble, R.A. Dziyauddin, Blockchain-based framework for interoperable electronic health records for an improved healthcare system, Sustainability 15 (8) (2023) 6337.
[35] Z. Zhao, X. Li, B. Luan, W. Jiang, W. Gao, S. Neelakandan, Secure internet of things (IOT) using a novel brooks iyengar quantum byzantine agreement-centered blockchain networking (biqba-bcn) model in smart healthcare, Inf. Sci. 629 (2023) 440–455.
[36] L. Zhou, L. Wang, Y. Sun, Mistore: a blockchain-based medical insurance storage system, J. Med. Syst. 149 (2018).
[37] M.U. Tariq, Revolutionizing health data management with blockchain technology: enhancing security and efficiency in a digital era, in: Emerging Technologies for Health Literacy and Medical Practice, IGI Global Scientific Publishing, 2024, pp. 153–175.
[38] S.S. Kamble, A. Gunasekaran, M. Goswami, J. Manda, A systematic perspective on the applications of big data analytics in healthcare management, Int. J. Healthc. Manag. 12 (3) (2019) 226–240.
[39] E.P. Adeghe, C.A. Okolo, O.T. Ojeyinka, Evaluating the impact of blockchain technology in healthcare data management: a review of security, privacy, and patient outcomes, Open Access Res. J. Sci. Technol. 10 (2) (2024) 013–020.
[40] L. Chen, T. Chen, T. Lan, C. Chen, J. Pan, The contributions of population distribution, healthcare resourcing, and transportation infrastructure to spatial accessibility of health care, INQUIRY: The Journal of Health Care Organization, Provision, and Financing 60 (2023) 00469580221146041.
[41] Y.Y. Ghadi, T. Mazhar, T. Shahzad, M. Amir khan, A. Abd-Alrazaq, A. Ahmed, H. Hamam, The role of blockchain to secure internet of medical things, Sci. Rep. 14 (1) (2024) 18422.
[42] A. Alketbi, Q. Nasir, M.A. Talib, Blockchain for government services — use cases, security benefits and challenges, in: 15th Learning and Technology Conference (L&T), 2018, pp. 112–119.
[43] P. Sharma, S. Namasudra, R. Gonzalez Crespo, J. Parra-Fuente, M. Chandra Trivedi, Ehdhe: enhancing security of healthcare documents in iot-enabled digital healthcare ecosystems using blockchain, Inf. Sci. 629 (2023) 703–718.
[44] A. Hajian, V.R. Prybutok, H.-C. Chang, An empirical study for blockchain-based information sharing systems in electronic health records: a mediation perspective, Comput. Hum. Behav. 138 (2023) 107471.
[45] D. Aloini, E. Benevento, A. Stefanini, P. Zerbino, Transforming healthcare ecosystems through blockchain: opportunities and capabilities for business process innovation, Technovation 119 (2023) 102557.
[46] A. Bathula, S. Muhuri, S.K. Gupta, S. Merugu, Secure certificate sharing based on blockchain framework for online education, Multimed. Tools Appl. 82 (11) (2023) 16479–16500.
[47] P. Bhattacharya, S. Tanwar, U. Bodkhe, S.T.N. Kumar, Bindaas: blockchain-based deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw. Sci. Eng. 8 (2) (2021) 1242–1255.
[48] N. Singh, Blockchain for healthcare: use cases and applications, Retrieved December 4 (2019) 2020.
[49] B. Curran, Looking Ahead to Blockchain Interoperability: Issues & future Solutions, Tech. rep., 2018.
[50] A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: vision and future opportunities, Comput. Commun. 154 (2020) 223–235.
[51] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula, Health-blockedge: blockchain-edge framework for reliable low-latency digital healthcare applications, Sensors 21 (7) (2021).
[52] F. Hu, H. Yang, L. Qiu, X. Wang, Z. Ren, S. Wei, H. Zhou, Y. Chen, H. Hu, Innovation networks in the advanced medical equipment industry: supporting regional digital health systems from a local–national perspective, Front. Public Health 13 (2025) 1635475.
[53] I. Alrashdi, A. Alqazzaz, Synergizing AI, IOT, and blockchain for diagnosing pandemic diseases in smart cities: challenges and opportunities, Sustain. Mach. Intell. J. 7 (2024) 1–6.
[54] P. Whig, R. Gera, A.B. Bhatia, R. Reddy, Convergence of blockchain and IOT in healthcare, Convergence of Blockchain and Internet of Things in Healthcare 277 (2024).
[55] M. Karatas, L. Eriskin, M. Deveci, D. Pamucar, H. Garg, Big data for healthcare industry 4.0: applications, challenges and future perspectives, Expert Syst. Appl. (2022) 116912.
[56] M.A. Haq, M.A. Rahim Khan, Dnnbot: deep neural network-based botnet detection and classification, Comput. Mater. Contin. 71 (1) (2022).
[57] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inform. Assoc. 24 (6) (2017) 1211–1220.
[58] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics 9 (1) (2020).
[59] H.S. Chen, J.T. Jarrell, K.A. Carpenter, D.S. Cohen, X. Huang, Blockchain in healthcare: a patient-centered model, Biomed. J. Sci. Tech. Res. 20 (3) (2019) 5017–15022.
[60] A. Siyal, A. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: challenges and future perspectives, Cryptography 3 (1) (2019) 1–3.
[61] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—a scoping review, Int. J. Med. Inform. 134 (2020) 104040.
[62] J. Sengupta, S. Ruj, S. Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IOT and iiot, J. Netw. Comput. Appl. 149 (2020) 102481.
[63] B. Reddy, Madhushree, P.S. Aithal, Blockchain as a disruptive technology in healthcare and financial services - a review based analysis on current implementations, Int. J. Appl. Eng. Manag. Lett. 4 (1) (2020) 142–155.

[64] M. Gupta, S. Tanwar, S. Badotra, A. Rana, A Systematic Review on Blockchain in Transforming the Healthcare Sector, Springer International Publishing, Cham, 2022, pp. 181–200.
[65] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inf. Secur. Appl. 50 (2020) 102407.
[66] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, G. Dhiman, Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives, Artif. Intell. Food Qual. Improv. (2021) 11475–11490.
[67] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A survey on blockchain for information systems management and security, Inf. Process. Manag. 58 (1) (2021).
[68] H.M. Hussien, S.M. Yasin, N.I. Udzir, M.I.H. Ninggal, S. Salman, Blockchain technology in the healthcare industry: trends and opportunities, J. Ind. Inf. Integr. 22 (2021) 100217.
[69] F. Reegu, S.M. Daud, S. Alam, Interoperability challenges in healthcare blockchain system - a systematic review, Ann. Rom. Soc. Cell Biol. (2021) 15487–15499.
[70] O. Ali, A. Jaradat, A. Kulakli, A. Abuhalimeh, A comparative study: blockchain technology utilization benefits, challenges and functionalities, IEEE Access 9 (2021) 12730–12749.
[71] A. Tandon, A. Dhir, A.K.M.N. Islam, M. Mäntymäki, Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda, Comput. Ind. 122 (2020) 103290.
[72] U. Chelladurai, S. Pandian, A novel blockchain based electronic health record Automation system for healthcare, J. Ambient Intell. Humaniz. Comput. 13 (2022) 693–703.
[73] M.S. Arbabi, C. Lal, N.R. Veeraragavan, D. Marijan, J.F. Nygård, R. Vitenberg, A survey on blockchain for healthcare: challenges, benefits, and future directions, IEEE Commun. Surv. Tutor. 25 (1) (2023) 386–424.
[74] R. Jayaraman, Y. Al-Hammadi, I. Yaqoob, K. Salah, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. 34 (2022) 11475–11490.
[75] K.N. Rani, K. PRavallika, S.K. Nadiya, T. Poojitha, K. Greeshma, Blockchain technology in healthcare: challenges and opportunities, Int. J. Health Care Biol. Sci. 3 (3) (2022) 51–55.
[76] R. Myrzashova, S.H. Alsamhi, A.V. Shvetsov, A. Hawbani, X. Wei, Blockchain meets federated learning in healthcare: a systematic review with challenges and opportunities, IEEE Internet Things J. (2023) 1.
[77] E.R.D. Villarreal, J. García-Alonso, E. Moguel, J.A.H. Alegría, Blockchain for healthcare management systems: a survey on interoperability and security, IEEE Access 11 (2023) 5629–5652.
[78] D. Aloini, E. Benevento, A. Stefanini, P. Zerbino, Blockchain-based framework for interoperable electronic health records for an improved healthcare system, Sustainability 15 (8) (2023).
[79] H. Naser Alsuqaih, W. Hamdan, H. Elmessiry, H. Abulkasim, An efficient privacy-preserving control mechanism based on blockchain for e-health applications, Alex. Eng. J. 73 (2023) 159–172.
[80] N. El Madhoun, B. Hammi, Blockchain technology in the healthcare sector: overview and security analysis, in: 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2024, pp. 0439–0446.
[81] W.A.N.A. Al-Nbhany, A.T. Zahary, A.A. Al-Shargabi, Blockchain-iot healthcare applications and trends: a review, IEEE Access 12 (2024) 4178–4212.
[82] M.S.B. Kasyapa, C. Vanmathi, Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies, Front. Digit. Health 6 (2024) 1359858.
[83] L.J.R. Lopez, D. Millan Mayorga, L.H. Martinez Poveda, A.F.C. Amaya, W. Rojas Reales, Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: a review, Computers 13 (6) (2024) 152.
[84] J. Almalki, State-of-the-art research in blockchain of things for healthcare, Arab. J. Sci. Eng. 49 (3) (2024) 3163–3191.
[85] T. Mazhar, S. khan, T. Shahzad, M.A. khan, M.M. Saeed, J.B. Awotunde, H. Hamam, Generative AI, IOT, and blockchain in healthcare: application, issues, and solutions, Discov. Internet Things 5 (1) (2025) 5.
[86] N. Rathore, A. Kumari, M. Patel, A. Chudasama, D. Bhalani, S. Tanwar, A. Alabdulatif, Synergy of AI and blockchain to secure electronic healthcare records, Secur. Priv. 8 (1) (2025) e463.
[87] A.A. khan, R. Ghodhbani, A. Alsufyani, N. Alsufyani, M.A. Mohamed, Leveraging blockchain-integrated explainable artificial intelligence (XAI) for ethical and personalized healthcare decision-making: a framework for secure data sharing and enhanced patient trust, J. Supercomput. 81 (15) (2025) 1353.
[88] I. Alim, N. Imtiaz, A. Al Prince, M.D.A. Hasan, AI and blockchain integration: driving strategic business advancements in the intelligent era, J. Eng. Comput. Intell. Rev. 3 (2) (2025) 38–50.
[89] M.S. Al Jasem, T. De Clark, A.K. Shrestha, Toward decentralized intelligence: a systematic literature review of blockchain-enabled AI systems, Information 16 (9) (2025) 765.
[90] N. Rathore, G. Soni, B. Khandelwal, R. Kashyap, B.P. Kasaraneni, R. Nair, Leveraging AI and blockchain for scalable and secure data exchange in iomt healthcare ecosystems, in: 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, IEEE, 2025, pp. 1–6.
[91] R. Mounira, M. Majda, B. Abdelmadjid, B.S. Oumaima, M. Derdour, Comprehensive survey on blockchain, federated learning, and AI for securing the internet of medical things, in: 2025 International Conference on Networking and Advanced Systems (ICNAS), IEEE, 2025, pp. 1–8.
[92] N. Seifi, E. Ghoodjani, S.S. Majd, A. Maleki, S. Khamoushi, Evaluation and prioritization of artificial intelligence integrated block chain factors in healthcare supply chain: a hybrid decision making approach, Comput. Decis. Mak. 2 (2025) 374–405.
[93] A.A. Almazroi, Innovative AI ensemble model for robust and optimized blockchain-based healthcare systems, Netw. Model. Anal. Health Inform. Bioinform. 14 (1) (2025) 6.
[94] G. Xu, X. Fan, S. Xu, Y. Cao, X.-B. Chen, T. Shang, S. Yu, Anonymity-enhanced sequential multi-signer ring signature for secure medical data sharing in iomt, IEEE Trans. Inf. Forensics Secur. 20 (2025) 5647–5662.
[95] J. Jin, M. Wu, A. Ouyang, K. Li, C. Chen, A novel dynamic hill cipher and its applications on medical IOT, IEEE Internet Things J. 12 (10) (2025) 14297–14308.
[96] J. Li, J. Li, C. Wang, F.J. Verbeek, T. Schultz, H. Liu, Outlier detection using iterative adaptive mini-minimum spanning tree generation with applications on medical data, Front. Physiol. 14 (2023) 1233341.
[97] P. Hao, Z. Yan, H. Wen, Privacy-preserving NILM: a self-alignment source-aware domain adaptation approach, IEEE Trans. Instrum. Meas. 74 (2025) 1–12.
[98] M. Zhang, E. Wei, R. Berry, J. Huang, Age-dependent differential privacy, IEEE Trans. Inf. Theory 70 (2) (2023) 1300–1319.
[99] S. Namasudra, S. Das, S. Datta, R.G. Crespo, D. Taniar, An advanced blockchain-based mutual authentication technique for the internet of vehicles environment, J. Supercomput. 81 (15) (2025) 1445.
[100] A. Bathula, S.K. Gupta, S. Merugu, L. Saba, N.N. Khanna, J.R. Laird, S.S. Sanagala, R. Singh, D. Garg, M.M. Fouda, et al., Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review, Artif. Intell. Rev. 57 (9) (2024) 238.
[101] T. Ashfaq, R. Khalid, A.S. Yahaya, S. Aslam, A.T. Azar, S. Alsafari, I.A. Hameed, A machine learning and blockchain based efficient fraud detection mechanism, Sensors 22 (19) (2022) 7162.
[102] J. Xiang, J. Zhang, Y. Zhao, F.-X. Wu, M. Li, Biomedical data, computational methods and tools for evaluating disease–disease associations, Brief. Bioinform. 23 (2) (2022) bbac006.
[103] L.M. Haji, S. Zeebaree, O.M. Ahmed, A.B. Sallow, K. Jacksi, R.R. Zeabri, Dynamic resource allocation for distributed systems and cloud computing, TEST Eng. Manag. 83 (May/June 2020) (2020) 22417–22426.
[104] T. Kumar, P. Kumar, S. Namasudra, User revocation-enabled access control model using identity-based signature in the cloud computing environment, Int. J. Interact. Multimed. Artif. Intell. 9 (1) (2024) 127–136.
[105] A. Gupta, S. Namasudra, P. Kumar, A secure VM live migration technique in a cloud computing environment using blowfish and blockchain technology, J. Supercomput. 80 (19) (2024).
[106] S. Sonune, D. Kalbande, A. Yeole, S. Oak, Issues in IOT healthcare platforms: a critical study and review, in: 2017 International Conference on Intelligent Computing and Control (I2C2), IEEE, 2017, pp. 1–5.
[107] R. Shah, A. Chircu, IOT and AI in healthcare: a systematic literature review, Issues Inf. Syst. 19 (3) (2018).
[108] A. Alanazi, IOT and AI in healthcare: a systematic literature review, PLOMS AI 1 (1) (2021).
[109] M. Bahl, R. Barzilay, A.B. Yedidia, N.J. Locascio, L. Yu, C.D. Lehman, High-risk breast lesions: a machine learning model to predict pathologic upgrade and reduce unnecessary surgical excision, Radiology 286 (3) (2018) 810–818.
[110] S. Merugu, M.C.S. Reddy, E. Goyal, L. Piplani, Text message classification using supervised machine learning algorithms, in: International Conference on Communications and Cyber Physical Engineering 2018, Springer, 2018, pp. 141–150.
[111] N.A.A. Bakar, W.M.W. Ramli, N.H. Hassan, The internet of things in healthcare: an overview, challenges and model plan for security risks management process, Indones. J. Electr. Eng. Comput. Sci. 15 (1) (2019) 414–420.
[112] M. Jammula, V.M. Vakamulla, S.K. Kondoju, Performance evaluation of lightweight cryptographic algorithms for heterogeneous IOT environment, J. Interconnect. Netw. 22 (Supp01) (2022) 2141031.
[113] M.A.F. Al-Husainy, B. Al-Shargabi, S. Aljawarneh, Lightweight cryptography system for IOT devices using DNA, Comput. Electr. Eng. 95 (2021) 107418.
[114] J. Wang, X. Kang, Y.-C. Liang, S. Sun, An energy harvesting chain model for wireless-powered IOT networks, in: 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2018, pp. 1–6.
[115] M. Schöffel, F. Lauer, C.C. Rheinländer, N. Wehn, Secure IOT in the era of quantum computers—where are the bottlenecks? Sensors 22 (7) (2022) 2484.
[116] I. Ponemon, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Tech. rep., Technical Report, 2016.
[117] A.F. Hussein, M. Burbano-Fernandez, G. Ramírez-Gonzalez, E. Abdulhay, V.H.C. De Albuquerque, et al., An automated remote cloud-based heart rate variability monitoring system, IEEE Access 6 (2018) 77055–77064.
[118] A. Tissaoui, M. Saidi, Uncertainty in IOT for smart healthcare: challenges, and opportunities, 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, Springer, 2020, pp. 232–239.
[119] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, N. Kumar, IOT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges, IEEE Access 8 (2020) 168825–168853.
[120] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, C. Xu, Handling a trillion (unfixable) flaws on a billion devices: rethinking network security for the internet-of-things, in: Proceedings of the 14th ACM Workshop on Hot Topics in Networks, 2015, pp. 1–7.

[121] N.H. Esha, M.R. Tasmim, S. Huq, M. Mahmud, M.S. Kaiser, Trust ioht: a trust management model for internet of healthcare things, in: Proceedings of International Conference on Data Science and Applications: ICDSA 2019, Springer, 2021, pp. 47–57.
[122] V.M. Rohokale, N.R. Prasad, R. Prasad, A cooperative internet of things (IOT) for rural healthcare monitoring and control, in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE, 2011, pp. 1–6.
[123] M. Karamali, M. Yaghoubi, A. Parandeh, Scientific mapping of papers related to health literacy using co-word analysis in medline, Iran. J. Health Educ. Health Promot. 9 (3) (2021) 280–295.
[124] E. Ahmed, I. Yaqoob, I.A.T. Hashem, I. Khan, A.I.A. Ahmed, M. Imran, A.V. Vasilakos, The role of big data analytics in internet of things, Computer Networks 129 (2017) 459–471.
[125] A. Shahid, T.-A.N. Nguyen, M.-T. Kechadi, Big data warehouse for healthcare-sensitive data applications, Sensors 21 (7) (2021) 2353.
[126] L. Menvielle, A.-F. Audrain-Pontevia, W. Menvielle, The digitization of healthcare: new challenges and opportunities, Palgrave Macmillan, London, 2017, pp. 454.
[127] M.S. Al-Otaibi, S. Asiri, R.M. Al-Mutairi, A.F. Al-Shammari, S.R. Al-Dhafiri, A.M. Al-Muthabt, T. Al-Mutairi, A.M. Al-Hazmi, M.A. Al-Dosari, M.M.A. Al-Dossary, et al., The role of health security in healthcare settings: a comprehensive review, J. Int. Crisis Risk Commun. Res. (2024) 2517–2521.
[128] R. Hanumantharaju, K.N. Shreenath, B.J. Sowmya, K.G. Srinivasa, Fog-driven approach for distributed intrusion detection system in auditing the data dased on blockchain-cloud systems, Cloud Comput. Data Sci. (2024) 97–107.
[129] M.I. Hossain, T. Steigner, M.I. Hussain, A. Akther, Enhancing data integrity and traceability in industry cyber physical systems (icps) through blockchain technology: A comprehensive approach, arXiv preprint arXiv:2405.04837, 2024.
[130] N. Lasla, L. Al-Sahan, M. Abdallah, M. Younis, Green-pow: an energy-efficient blockchain proof-of-work consensus algorithm, Comput. Netw. 214 (2022) 109118.
[131] A. Rejeb, K. Rejeb, I. Zrelli, E. Süle, M. Iranmanesh, Blockchain technology in the renewable energy sector: a co-word analysis of academic discourse, Heliyon 10 (8) (2024).
[132] T.K. Vashishth, V. Sharma, K.K. Sharma, P. Sethi, T. Chaudhary, A. Bhardwaj, Future implications of blockchain for biomedical and healthcare, in: Blockchain for Biomedical Research and Healthcare: Concept, Trends, and future Implications, Springer, 2024, pp. 367–404.
[133] M. Shaikh, S.A. Memon, A. Ebrahimi, U.K. Wiil, A systematic literature review for blockchain-based healthcare implementations, Healthcare 13 (9) (2025) 1087.