Blockchain-Based Framework for Secure Medical Information in Internet of Things System

Joseph Bamidele Awotunde, Sanjay Misra, Oluwafisayo Babatope Ayoade, Roseline Oluwaseun Ogundokun, and Moses Kazeem Abiodun

1 Introduction

Like other fields, healthcare system has benefited from the blockchain technology due to its built-in features like authentication, security, distributed ledger, and immutability. The blockchain have moved beyond cryptocurrency to practical application in other fields especially in healthcare system [1–2]. Due to severe regulatory restrictions, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), in healthcare sector, the application of blockchain needs severe record sharing authentication and interoperability requirements. Researchers in academia and industry have begun to investigate solutions aimed toward healthcare use, based on existing blockchain technologies. Smart contracts, fraud detection, and identity verification are examples of these applications.

Blockchain stores information in decentralized recording ledgers that are distributed across all computer devices that are part of the blockchain architecture [3]. The blockchain works having both network users who take part in transactions and facilitate the transactions in a distributed ledger; thus, the infrastructure is peer-to-peer networks. Cryptographic techniques are employed by all miner, and the

J. B. Awotunde (✉) · O. B. Ayoade
Department of Computer Science, University of Ilorin, Ilorin, Nigeria
e-mail: awotunde.jb@unilorin.edu.ng; 15-68hg004.pg@students.unilorin.edu.ng

S. Misra
Department of Computer Science and Communication, Østfold University College (HIOF), Halden, Norway
e-mail: sanjay.misra@covenantuniversity.edu.ng

R. O. Ogundokun · M. K. Abiodun
Department of Computer Science, Landmark University, Omu Aran, Nigeria
e-mail: ogundodun.roseline@lmu.edu.ng; moses.abiodun@lmu.edu.ng

S. Misra, A. Kumar Tyagi (eds.), *Blockchain Applications in the Smart Era*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-89546-4_8

transaction is maintained in a decentralized set of nodes built by all these miners [4]. Furthermore, because it is built utilizing consensus methods, digital signatures, and hash chains, the blockchain ledger provides extremely reliable storage capabilities [5]. The services deliver by blockchain are in various ways like security, integrity, traceability, and non-repudiation using privacy-preserving manner while keeping all information in a public and in a decentralized manner [6].

In recent years, blockchain technology has demonstrated its tremendous adaptability as a range of healthcare sectors have found ways to incorporate its capabilities into their operations. Although much of the emphasis has been on the financial services sector so far, many projects are starting to shift in other service-related fields to included blockchain technologies [4]. Blockchain is a rapidly evolving technological innovation that has piqued the imagination of people all around the world. This technology enables computerized medical information transfer easier and safer than the traditional technique. It's a common knowledge that blockchain can make healthcare data more secure and accessible. For healthcare system, blockchain help in building a secure application because of the increased security and privacy provided in healthcare platforms. A decentralized database that is continuously kept up-to-date transactions information provides the healthcare sector with many benefits. When various parties require access to the same information, these benefits become particularly interesting. For instance, in the area of healthcare monitoring, access to healthcare records, transfers of vital documents like x-ray are vital areas in healthcare system where Blockchain technology can create additional level of security [4].

There has been a huge research breakthrough in finance and banking sectors unlike healthcare that has lately begun to gain significant interest in terms of blockchain-based applications [7–10]. Various researchers and medical scholars have highlighted the potential of blockchain application in the healthcare sector, and there is evidence that it can help to solve current security problems [7] [11–12]. The healthcare special security and privacy issues were able to be resolved using additional legal responsibilities in securing patients' medical information using blockchain technology. The risk of malicious attacks keeps on increasing in this era of Internet connectivities most especially as cloud storage and the proliferation of mobile health devices increase in sharing medical records and data. This has exposed the chance of private information during sharing to be compromised [13].

The sharing and privacy become an issue as smart devices are used to access health information, but there is no doubt these have help in reducing the number of patients that visit doctors. The healthcare sector is facing various challenges like data sharing, authentication, interoperability, and the transfer of medical information using mobile health applications [14]. Medical data from body sensors and other applications include patient physiological signs and symptoms and patient files and medical data. There is a need for proper security as medical records transition from paper to digital formats; role-based privileges must be implemented to preserve data and the security of healthcare records. There is a need to make sure that only authorized users are allowed to access medical data and records on the cloud databases, for example, and such access should be enforced and monitored. The

query methods must be rigorous and must be audited regularly to reduce the danger of tampering or copying healthcare records, and rigorous access controls must be implemented [15–16].

Therefore, this chapter presented a blockchain-based framework for a secure healthcare system. When collaborating with smart healthcare systems, privacy and authenticity are crucial. The concept employed the blockchain distributed ledger to provide authenticity and endorsement while maintaining anonymity through approved management of consortia and anonymized accounts. The chapter is prearranged as follows: The IoT-based applications in healthcare system are discussed in Sect. 2. In Sect. 3, the chapter look at how blockchain can be used in the healthcare sector. Section 4 discusses various challenges of implementing blockchain technology in IoT-based system to secure the medical information. The architecture for a secure smart healthcare monitoring system using blockchain is presented in Sect. 5. Finally, Section 6 brings the chapter to a close by discussing the future work on implementing the framework.

2 Application of the Internet of Things in Healthcare System

Digital wellness advances offer significant incentives for reshaping existing healthcare programs. From the advent of automated therapeutic annals to portable medical equipment to other new technology, digital health advances have enhanced the quality of care at a lower cost. Politicians are constantly exploring, embracing, and adopting information and communication technologies as part of healthcare policies (ICT) [13]. It influences how individuals and patients see and communicate with eHealth system. The path to digital medical care (eHealth) is a systemic evolution of the traditional medical care system that includes a variety of features, such as universal access to automated medical records, online tracking systems, inmate services, wearable devices, portable medical apps, data analytics, and other transformative innovations [13–14].

Due to the global spread of the pandemic, it is critical to make an effective use of contemporary technologies. The Internet of Things (IoT) is widely recognized as one of the most revolutionary breakthroughs, with enormous potential for combating disease outbreaks [17]. The IoT consists of a sparse network, where the IoT systems feel the world and transmit valuable data across the network. The IoT-based system generates a massive amount of data known as big data, which influences the development and expansion of more personalized healthcare systems. Active surveillance capabilities in wearable medical devices can collect a large quantity of medical data, resulting in big data, from which clinicians can predict the patient's future state [18]. These observational study and information extraction are a dynamic process that necessitates improved security approaches [19]. The use of AI on generated big data from IoT-based systems opens up a number of possibilities for healthcare systems ([19]. The use of AI in the big data generation process has the potential to greatly improve global healthcare systems [15].

The Internet of Things-based system has been utilized to lower the worldwide cost of disease prevention. The IoT-based technology can help patients with self-administration therapies by capturing data in real time. In IoT-based sensor data collecting for telemedicine and mHealth systems, mobile app integration is a commonplace [20]. One of the important tasks in creating health fairness is to use IoT-based expertise to swap different sections of present medical services. Cloud and IoT-based systems meet consumer demand in a timely manner, take into account the patient's current state of health, improve contact between physicians and sick people, and reduce the time spent waiting for therapeutic care, all of which will increase client loyalty while also maximizing hospital performance. With the right telemedicine, a standardized standard might be achieved.

Wearable technology for the IoT-based system has opened up a new potential in the medical area, thanks to the new emerging technologies such as medical sensors for remotely monitoring patients. WBANs (wireless body area networks) are a type of IoT healthcare pattern. Various embedded and implanted technologies have lately been utilized to monitor the essential physiological parts of the human body, such as detecting heart rates and glucose levels in real time. Other devices and sensors, similar to an actuator's measurement, can provide automated care and therapy. The data report sent to a mobile phone functions as a storage device and sends the information to healthcare staff in real time, allowing them to respond quickly to users' demands. This remote monitoring eliminates the need for doctors' visits and allows patients to move around more freely in their daily life [21].

Remote patient monitoring is becoming more common; in 2016, 7.1 million out-patients in the United States outsourced their health care plan to remote monitoring, with that number predicted to rise to 50.2 million by 2030 [14, 22]. Furthermore, the US Centers for Medicare and Medicaid Programs (CMSP) announced the new payment incentives on January 1, 2018, to encourage the use of "active feedback loop" devices that provide real-time observation [23]. As the field of remote patient monitoring expands, there are worries about the accuracy and security of medical data transfer. To enable integrated health monitoring, measurements from numerous sensors must be aggregated, structured, and analyzed together. Because health data is a primary target for hackers, there is a need for government regulation to protect the transmission of personal health information (PHI). As a result, patient privacy must be protected, and electronic health records (EHRs) must be easily controllable and portable.

With pinpoint accuracy and eluate in the data collected, an IoT has the capacity to monitor specimens, equipment, people, supplies, and even service animals. To measure various vital signs, sensors can be fitted on the patient's body with various biometric data. This allows physician to provide better care to the patients, allowing problems to be diagnosed more quickly and resources to be used more efficiently. To detect body temperature and blood pressure from any patient, sensors can be placed in the patient's room in a hospital or home care setting. These sensors can also be used to detect the odor of vomit within an area in hospital or home care premises. The use of sensors and IoT devices can detect fast walking activity against

the normal walk habit and the excessive cardiac training. This information could be useful in the diagnosis and treatment of the condition.

In today's healthcare, safety and violence are the major concerns. There have been numerous reports of horizontal violence, including nurse against nurse, as well as violence directed at healthcare providers or patients by visitors or family members. An IoT can be used to enforce a zero-tolerance policy as video surveillance systems are installed in healthcare facilities to perform these vital functions. Tracking the movements of employees, patients, and visitors, for example, could provide early alerts of unusual or threatening conduct. People visiting or residing in these situations could be monitored using biometric sensors to detect indicators of aggressiveness or stress. To charge patient account becomes easier with the use of barcode tags or low-cost RFID tags by a pharmacy. This helps to tag for scanning for an acute or long-term care setting for their various supplies. The IoT-based system can also be used to track and check such supplies from a repository or administered to a patient. An item could be located more rapidly in some circumstances where an RFID tag is utilized. For instance, goods like bandages, catheters of various types, and personal care items, are likely to be trackable. Medical products could be labeled with RFID tags in a home environment to track usage and warn the home care team when an item is being overused or the supply is running short. Many more IoT healthcare applications, according to researchers and practitioners, might significantly improve patient care, maximize resource usage, and save large sums of money if only the systems could be developed.

Recent technological advancements have drastically altered people's perceptions of how they should go about their daily lives. In the real world, the IoT has to be a growing trend in various industries, including healthcare. This rapid IoT revolution, however, has raised several questions and worries regarding the security of data held in various linked devices. It gets more difficult to ensure comprehensive data protection and privacy when the number of items, such as sensors and computers, grows. These security and privacy issues are the result of a decrease in the efficacy of IoT-based healthcare systems, which has a negative impact on individual's sensitive health information. Because healthcare data is so valuable and sensitive, the IoT healthcare paradigm's security and privacy protections exacerbate the situation. While growing IoT paradigms in the medical system help to develop the present healthcare systems, end users must face a number of privacy and security concerns. End users may be vulnerable to malicious threats if they grant authorization for potentially insecure or leaky third-party applications. Because the data is sent to the cloud, it travels across insecure communication networks, many of which are vulnerable to attack [19]. Furthermore, when data is uploaded to the owner's cloud storage facility, there are additional data security concerns.

However, the sheer number of connected devices (Fig. 1) and the massive amounts of sensory statistics generated by those devices have created new issues in terms of information security and confidentiality. Cyberattacks have evolved in tandem with the rapid development of IoT, resulting in a new channel of intrusion and risk for the whole medical business. Many research investigated IoT's multiple privacy and security vulnerabilities, as well as device flaws in

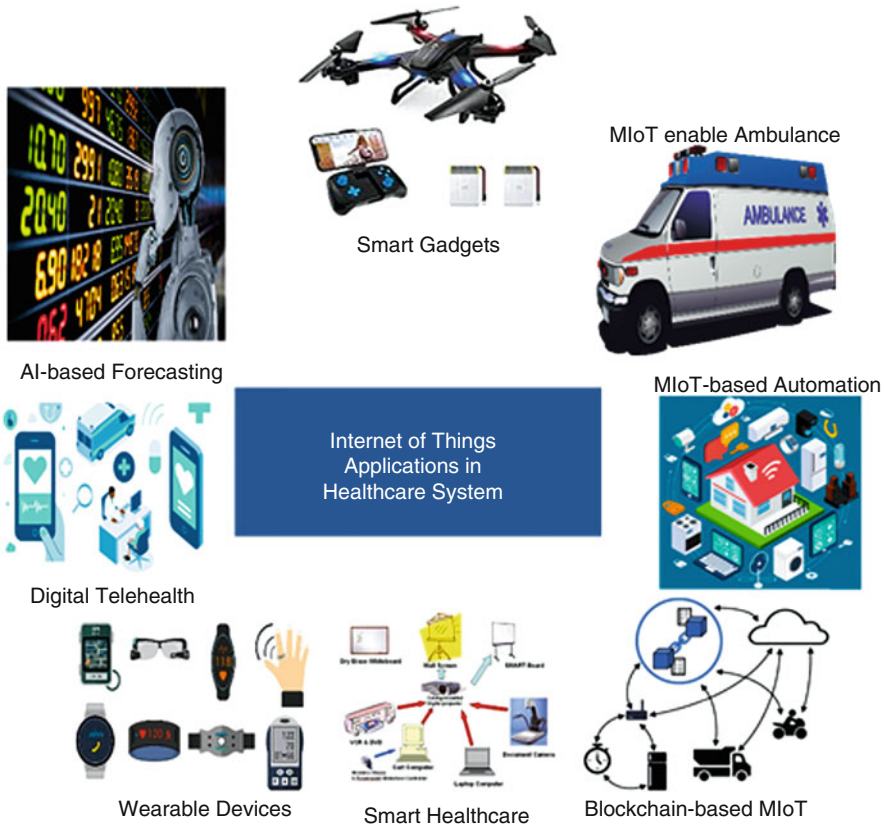

Fig. 1 Applications of the Internet of Things in healthcare system

cloud and fog computing settings pertinent to the IoT-based medical management gadgets [24–25]. The security and confidentiality of patient records are two critical considerations. When we talk about record safety, we mean that records are stored and communicated in a secure manner to preserve their absoluteness, genuineness, and legitimacy. The term "record confidentiality" refers to the fact that records can only be accessed and used by those who are allowed to see and use them [25–27]. An aggregate signature-based trust routing for data gathering in sensor networks can be used to create security and communication networks. Security and Communication Networks. With distinct objectives and specifications in mind, more reasonable security methods may be devised. The widespread use of IoT devices provides better guarantee of an individual's health [28], but it also creates a high demand on record security and concealment.

3 Applications of Blockchain in Internet of Things

The various aspects of healthcare systems can be improved using blockchain technology, and the security and privacy of patients with their well-being can be expanded and has the potential to improve various aspects of healthcare and well-being. Device tracking, clinical trials, pharmaceutical tracing, and health insurance are just a few examples. Hospitals can track their assets on a blockchain infrastructure, including throughout the device's whole life cycle. The information gathered can then be used to improve patient safety and do post-market analysis to save money. Current research has focused on pharmaceutical traceability, data interchange, clinical trials, and device tracking. With its immutability, fraud prevention, and ability to transport data between firms without requiring trust, healthcare is primed for revolution.

Bell et al. (2018) [29] improved the device identification and tracking that is a critical problem in healthcare sectors tagging medical equipment with a usable ID. For instance, device tracking can be used to disclose the cause of problem when a device malfunctions, thus saving cost and unnecessary repurchasing of lost items. A strong trust infrastructure based on the identification of medical equipment is expected to decrease these risks. With hospitals due to security and privacy concerns, just 20% to 30% of medical equipment are connected, according to the survey. Blockchain can assist the pharmaceutical business in overcoming the rising risks of counterfeit and unapproved pharmaceuticals. Smart contacts for pharmaceuticals can be formed with integrated GPS and chain-of-custody logging and then identified, just like a device tracking.

Blockchain can be used within clinical trials to address issues such as falsified results and data removal by researchers that contradict the funding source's objective. Clinical studies will be more reliable as a result of this. It also enables for the creation of an irreversible log of trial subject consent. Almost $200 billion was saved using a chain of custody in the supply chain in the pharmaceutical sector [29]. A trustworthy record of events around the patient journey would be beneficial to several sectors of health insurance like improved incident reporting and automated underwriting operations. Contracts could also be carefully written and then executed, such as automated payments for stages of the patient journey.

In healthcare services, information security, privacy, completeness, and access must be considered very seriously. Another area that the huge healthcare business might look into is the increased necessity of healthcare cost control. With the promise of blockchain mixed with IoT-based application layers built atop, healthcare services have enjoyed ultimate security and privacy, ensuring that applicable users may access a continuous record of information. By eliminating the third-party brokers' involvement in any financial transactions, blockchain has enhanced stakeholders' access to medical information and lowered costs, potentially lowering healthcare expenses and providing better results [30]. The researchers are interested in using blockchain technology to solve real-world issues, such as healthcare diagnostic and monitoring systems, centralizing research data, lowering

healthcare overhead costs, and organizing patient data from massive input big data. The abovementioned examples of blockchain technology deployment in healthcare systems touch on near-term potential and obstacles [31].

Blockchain technology has been utilized for money exchange transactions to eliminate the requirement for a trustworthy third party to validate and notarize transactions, as well as to protect data confidentiality and privacy throughout those transactions. The innovation has been restructured to meet the needs of various industries, such as healthcare, education, transportation, electricity, and tourism. Over the next decade, healthcare systems based on the IoT are expected to generate trillions of dollars [32]. More importantly, smart healthcare has resulted in a significant decrease in death rates and healthcare costs, as well as enhancing the quality of the healthcare system and reducing emergency room visits and hospital stays [33].

Medical records are saved in a cloud database that is weighty to allow knowledge sharing and quick access among many healthcare stakeholders [34]. Cloud storage also offers security and privacy features, which are bolstered by data longevity. There is no interoperability between different healthcare providers and treatments in cloud storage. Furthermore, there is no way to confirm the data's quality or veracity. Blockchains play an important role in improving the trustworthiness, accuracy, and validity of medical data that is stored and exchanged. By monitoring and ensuring allowed access to personal medical information, blockchains ensure the security of sensitive data [35]. Blockchains operate as a distributed database to protect medical data from modification [36–37]. To addresses the safety concerns in IoT-based systems, blockchains used a distributed trust mechanism to distribute patient records on the cloud storage database that could be handled by various users and advisors like caregivers, physicians, clinic experts, pharmacies, patients themselves, and insurance providers.

Blockchains rely on hashing and public cryptography techniques to preserve confidentiality, integrity, and accessibility of past transactions relating to the records of scattered patients. This prevents unauthorized users from destroying, falsifying, or accessing the papers. Patient records in blockchains can only be appended to the database, not deleted. Cryptographic hashing allows new data to be securely linked to a previous record. The majority of miners in the network must agree before records may be added to the blockchain. Miners are a group of special nodes that work together to verify new transactions added to a blockchain. Miners compete to solve a difficult mathematical task known as proof of work (POW), which takes an average of 10 minutes to add a record to a blockchain. This will help ensure that no single entity is able to alter or tamper with checked records. Furthermore, caregivers will be able to supply patients with encrypted alias focused on personalized health advice without having to reveal their names, thanks to blockchains.

Blockchain technology is still in its infancy and, particularly in the healthcare industry, must be linked with existing policies and processes. The National Research Council of Canada's Industrial Research Assistance Program (NRC-IRAP) has used the blockchain and its associated immutability, clarity, and distribution to coordinate and disseminate public knowledge about its operations and companies, recognizing

that operating within government restrictions is a significant challenge in and of itself [38]. The success of the effort demonstrates that public blockchain may be used to protect government data, resolve administrative issues, and pave the way for more complicated data integration, particularly in smart healthcare [39]. The projects' enormous success creates a productive approach to record important data, exchange valuable data, and serve as a crucial building stone for future, more sensitive initiatives.

The distributed database management system (DDBMS) is technically centralized (i.e., users believe a centralized database is running, but the underlying machines can be physically distributed), whereas blockchain is a peer-to-peer, decentralized database management system (i.e., each node runs independently while adhering to the protocols) [40]. As a result, blockchain is excellent for applications in which biomedical/healthcare stakeholders (e.g., hospitals, suppliers, patients, and payers) may communicate with one another without relying on a central management middleman [41–42].

IoT-based devices must be securely logged using orders issued to actuator nodes, in addition to maintaining the integrity of patients and maintaining an accurate timeline of occurrences, as both records and treatment for a patient must be approved by medical specialists [43–44]. When it comes to wearing medical devices, this solution would provide patients with piece of mind by offering an immutable ledger and automatic health incident updates in a secure manner. Medical experts receive real-time information on their patients, furthering the practice of precision medicine. Smart contacts aid in the automation of health alarms from multiple devices into a centralized cloud storage location, resulting in a game-changing solution that allows healthcare practitioners to easily implement new medical technologies.

By placing data in the hands of individuals, blockchain has the potential to change healthcare. Patients and physicians can access an immutable log of medical records using MedRec is one particularly interesting step in this direction [45–46]. In exchange for maintaining the network, miners are compensated with anonymized healthcare data, which is a novel technique of incentivizing miners. MedRec maps patient-provider relationships (PPRs) using smart contracts, in which the contract displays a list of references indicating the relationships between nodes on the blockchain [29]. It also gives patients control over PPRs, allowing them to accept, reject, or change partnerships with healthcare providers like hospitals, insurers, and clinics.

By generating a decentralized ledger of acknowledged fact in medical records that is available to all healthcare practitioners, blockchain enables interoperability in healthcare systems [42, 47]. This means that, while user interfaces may vary, all providers' basic ledgers will remain the same. The current state of health records across providers, which contain large amounts of the same data under different IDs that may or may not be linked, is a roadblock. As the blockchain expands in size, this produces duplication, and performance degrades as a result. Deduplication would be required to maintain a reasonably performant system with unique, anonymized identities to identify patients across all services [48]. Implementing a distributed

ledger medical record is a practical difficulty in and of itself, but it's important to note that health data would not be created from the ground up as they'd have to replace the old infrastructure, which raises challenges [49–51].

Another option is drug monitoring on the blockchain, which takes advantage of the data integrity of nodes that are connected for tracking and chain of custody from the maker to patient. Discover, a chain of custody model that shows where a medicine was created, is being developed by Chronicled, a technological business. It has been proved that leveraging on blockchain's error-handling capabilities can prevent pharmaceutical fraud during distribution of drugs to various clients and patients [52]. This allows hospitals to meet current medical criteria in terms of pharmaceutical sustainable development, with a focus on provider connectivity. The Counterfeit Medicines Project was recently formed by Hyperledger [53], to combat the problem of illegal drugs; the Open-Source Blockchain Working Group was also formed. Blockchain can be used to track down the origins of counterfeit pharmaceuticals and eliminate them from the supply chain. The inherent democratization of faith and legitimacy in the technology's principles gives blockchain an advantage over traditional techniques in drug monitoring. While central authority can be influenced or faked, influencing a distributed ledger unanimity is significantly more challenging.

4 The Challenges of Using Blockchain in the Internet of Things in Healthcare Systems

Medical information, as well as medical information such as clinical information, can be obtained using body sensors and other applications. Additional security and participation credentials must be established as health information shifts from traditional to digital versions in order to maintain data and the confidentiality of health information. Only authorized individuals should be allowed to access healthcare records housed in databases, for example, and such access should be enforced and monitored. To decrease the risk of interfering with or duplicating hospital documents, as well as requests to get those records, the query must be audited and rigorous access controls must be implemented [16].

Confidentiality of patient history (e.g., electronic patient records (EHR, EMR) and personal health record (PHR)) can also be difficult if conventional cryptographic standards are utilized in multiple platforms [54–56]. Current methods for protecting and securing records have proven ineffective, and the public disclosure of a patient's medical information might have real-world ramifications (for instance, challenges to clients' anonymity in the form of hostile assaults, which can impact the status and financially linked with those records) [57–59].

Some of the privacy concerns that connected health solutions confront include identification confidentiality, identity management, enquiry privacy, trace privacy, and proprietor privacy [60–65]. Third-party cloud providers face a variety of

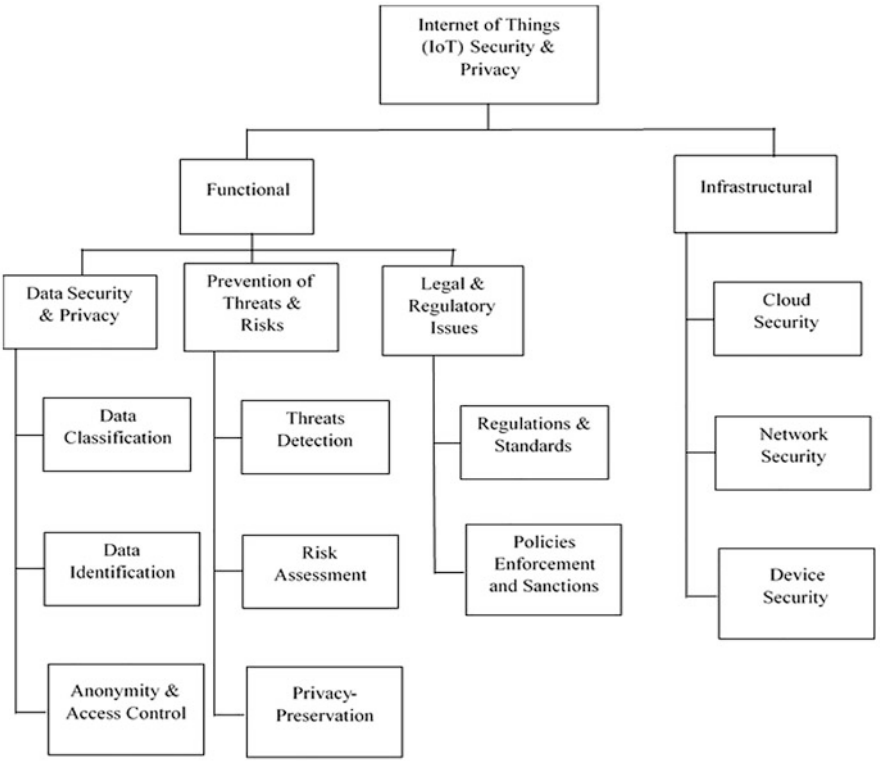

Fig. 2 The security and privacy in smart healthcare system

privacy issues when it comes to sharing medical information between various medical institutions [61]. One of these privacy issues is unauthorized access of medical information and patient data that is used and handled by third-party service providers [54, 61]. In addition to the privacy considerations of access control, IoT technologies also pose a risk of inference assaults [66]. Malicious actors utilize a mixture of wireless interception techniques and data mining to infer the value of a particular communication or signal, which is known as an inference attack [66]. The inferred information can then be utilized to further breach the account by using a phishing attack to get beyond authentication obstacles [66]. Cyber criminals can use data tampering, deception, spying, and material replay to target wireless devices in both active and passive ways [67]. A graphical demonstration of IoT security and privacy issues in smart healthcare system is shown in Fig. 2.

The use of blockchain technologies in healthcare is only getting started, and there are a lot of roadblocks to overcome and huge decisions to make in the future. In light of the issues that we faced a decade ago, our social understanding of privacy has evolved, and blockchain technology has the potential to uphold these boundaries if accepted. If deciding whether or not to use blockchain-based solutions, the trade-

off between the risk of data loss and the ability to control one's data (assuming no big data leaks) should be examined. The new repositories created by cloud computing have given birth to big data, which can then be analyzed by AI to create a personalized healthcare plan that doctors and policymakers can use.

If low-quality and wrong data is published on the blockchain, the blockchain will remain fair to its users; the chain will remain with low-quality and inaccurate information because immutability and decentralization can be trusted [68–69]. There are a number of new options for blockchain and supporting technologies, but attention must be paid to the implementation process as well as what information has been gained [70–71]. Vigilance about the information being processed is one of the interoperability options, as is providing responses to solve inconsistencies and distribute confidence to diverse forms of information. With the arrival of quantum computing and its predicted ability to overcome current encryption mechanisms, there is a new restricted possibility in blockchain technology [72]. Although it is unclear when this will occur, it appears to be within the next decade. If quantum computing's resistance to encryption is not resolved by then, we will face a number of problems, because storing all health data on publicly accessible servers on blockchain puts the data at danger.

In blockchain, a key with a certain sequence of characters is the ability to access data. However, if a key is lost, the information accessed by it becomes irretrievable. Then, it becomes unfair since consumers lose access to a lifetime's worth of health records simply because one of these keys is missing. Then, in order to reconnect users with their data, new approaches or techniques must be established. With existing solutions creating back doors to accessing the blockchain's private data, these methods will now be substituting one question with another. Another issue with blockchain technology is that if the decentralization of a blockchain is disturbed, one agent will become the only consensus agent and would be able to change the blockchain keys, which is in violation of the virtue of immutability. To guard against this possibility, new consensus mechanisms and government oversight of blockchain monopolization may be necessary [73].

The goal of blockchain technology is to allow for efficient information sharing with stakeholders while guaranteeing data confidentiality and patient privacy. This will motivate and empower individuals all over the world to make healthy choices in order to improve their health. With the blockchain model, the world's data is being protected more than ever before. Beyond the hoopla, skeptics are concerned about the complexities, and many established and invested parties are likely to oppose the shift, not to mention legal, regulatory, and technological aspects that have yet to be determined.

If the problems of standardization are continually overcome, reliable privacy established anonymization mechanisms constructed, and consensus gained on the kind of contracts required to manage information, a new era of healthcare may be on the horizon. These are significant obstacles, but as previously said, corporations have already made significant progress toward overcoming them. The use of artificial intelligence to learn from data has already demonstrated that the technology is prepared to provide revolutionary new insights with the massive data created by

the healthcare system, with privacy and patient control as a fundamental premise. The sectors are moving toward a disruptive event known as the health singularity, in which personalized healthcare is provided based on a comprehensive understanding of each individual's biology.

Other significant hurdles of implementing blockchain in the healthcare field are transparency and confidentiality. Increased openness and reduced secrecy, such as open data transparency during the transition, are commonly considered blockchain limitations because "everyone can see everything on a blockchain network" [74–75]. Also, even though a user is "anonymized" by using hash values as addresses, the user can still be identified by reviewing and analyzing publicly accessible transaction information on the blockchain. Because patient-related information (protected health information) is crucial, this issue is significant for healthcare applications.

One of the most distinguishing characteristics of blockchain systems is their immutability, and decentralized storage, which allows users to transfer data across several applications without relying on a centralized service provider [76]. A fundamental disadvantage of hierarchical structures is the prospect for privacy leakage from the public ledger that is propagated across the blockchain system. When a user receives his or her data, he or she is required to submit a private key in order to verify and decode the information from cypher text to plain text, potentially exposing personal information. Because the data is not stored locally, as it would be in a centralized database, the public key must be present on the network when the verification and decryption process begin. Due to the stringent requirements of the healthcare industry, this is a concern.

Because blockchain technology is still undeveloped and restively a new technology, there is no standardization, which impedes adoption and slows development [77]. Blockchain technology is being considered by many countries for use in government contexts, such as voting [78–79]. Countries like Estonia are seeking to achieve e-residency by combining residence rules with blockchain technology. This is the process of setting up an online account to verify a citizen's citizenship in a certain state and enable them to vote using that account [7]. To support all of these varied datacenters, there must be a high level of standardization across the numerous parties involved. The issue of standardization and regulations will become increasingly more crucial as more governments use blockchain as a solution [80, 82].

5 Blockchain-Based Framework for Secure Medical Information in Internet of Things System

The crust of the entire framework is the combination of the detection approach in the behavior of the patient's health data using the IoT, blockchain, and machine learning (ML). The shown methodology is essentially a system that requires the

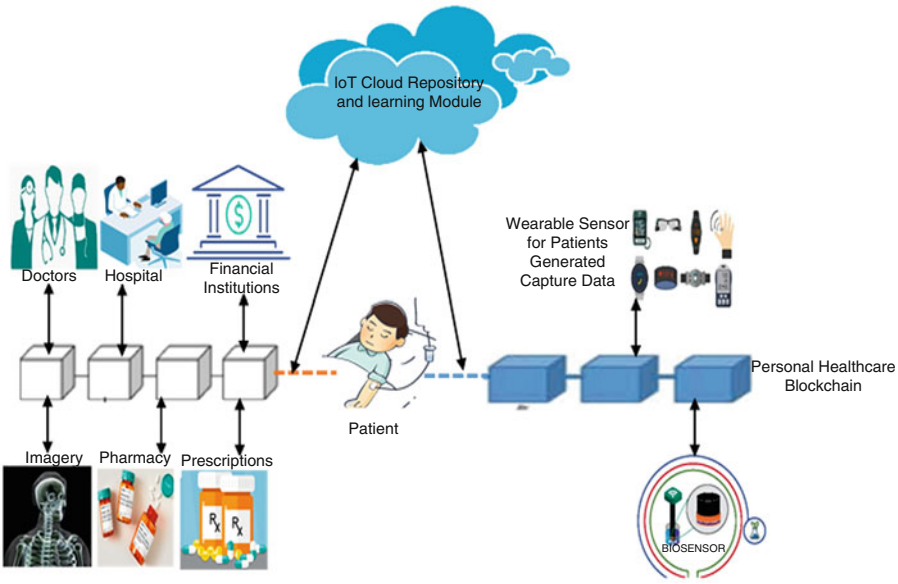

Fig. 3 The proposed blockchain-based Internet of Things for healthcare system

usage of an IoT module to intercept and retrieve data generated by the patient's wearable gadgets. The blockchain system presented is ideally suited for storing and keeping patient data in the form of multiple transactions, as well as providing access control to various stakeholders [81]. Furthermore, the blockchain framework is utilized to support medical research by maintaining the pseudo-anonymity of the patient's identity while yet providing permitted and reliable data for more accurate research. The ML model is mostly utilized for the detection of anomalies and the forecasting of future scenarios by evaluating data based on parameters provided by doctors for the basic diagnosis of the diseases that patients encounter (Fig. 3).

As a result, an effective IoT development must place a high priority on security and secrecy. Despite the fact that most healthcare organizations do not allocate sufficient funding to protect safety and secrecy, there is no doubt that safety and confidentiality play an important role in the IoT. IoT devices generate an increasing number of increasingly complicated real-time records, which is exceedingly delicate. On the one hand, the collapse of health organizations or system security could be disastrous. On the other hand, all levels of record processing, record transfer, cloud storage, and record republication have access to the patient's personal information. The framework was made up of three components, each of which has a distinct role to play:

IoT-Based Wearable Devices: These tools are used in real time to capture the symptoms of patients and monitor their status. These devices are made up of a number of sensors that detect the patient's vitality and atmosphere (like temperature, blood pressure, pulse rate, heart rate, humidity, ECG, etc.). When these criteria

are violated, physicians and clinicians are notified in real time (from the permitted limits). Short message services are utilized to report any cases to the appropriate physicians, and the messages are delivered via smart devices. In a more obvious sense, if a patient is getting some moderate therapy and is being followed up with some medical tests, a wearable sensor is an excellent approach to track the data generated by the patient at every second. Heart rate, calorie release, breath strengthening, and sleep stage monitoring are examples of data that might be considered based on the wearable worn by the patient. If blood pressure sensors are employed, or if pacemakers are installed in the patient, such data can also be accessed remotely via the IoT application module. Now, if the patient is bedridden or confined to the hospital, there is a huge demand for IoT sensors or biosensors that can recognize environmental conditions and take appropriate actions.

Blockchain Transaction and Access Management: The storage of the massive amount of data created by the patient must be managed and processed while adhering to a secure methodology. Furthermore, when there are several stakeholders involved with the data being generated, a vital module called an access management system must be created, which the blockchain network addresses. We've outlined the use of two critical blockchain networks in the suggested architecture: The personal healthcare (PHC) blockchain and the external record management (ERM) blockchain. The patient typically maintains the personal healthcare blockchain since it perceives and gathers data via personal wearable devices. The doctor will be given access to the data, which will be used for proper medicine and comprehension of the disease that the patient is suffering from. The data created by the wearable devices is then kept in a third-party cloud database that is governed by the blockchain network. Immutable storage blocks are used to hold transactional data. Only authorized users have access to the information. We can use blockchain technology to create privacy-preserving and fundamentally secure data exchange networks that allow participating agencies to readily access archived and real-time patient data using smart contracts that eliminate the need for data reconciliation completely. In a typical blockchain, there is no single administrator; therefore, it is a distributed system of control and access with some level of interest in each member, and everyone has equal rights and power.

Machine Learning (ML) Layer: The ML layer examines the data generated by the patient to look for anomalies. Anomaly detection may be greatly improved by using the model to extract abnormalities from the data being generated. When an abnormality is discovered, a notification is sent to the doctor, who can then take appropriate action based on the situation. The suggested system employs two-level blockchain technology. Internal healthcare agencies, such as service providers, physicians, inventory, and other internal stakeholders, employ a private blockchain. A public blockchain is utilized to communicate with other entities, such as patients, pharmacies, insurance providers, and so on. The usage of a two-level blockchain implementation allows for separation of distinct entities, resulting in a safe, privacy-preserving, consistent, and transparent workflow.

To discover responses to security breaches or system coercions, the blockchain layer processed data collected from overall terminal status data as well as network

traffic. This was done to discover various attack circumstances to device trends in real time and set up safeguards against them. This can be done by combining the incursion activity pattern with an access control strategy based on the IoT-based environment's acquired protection status data. The analysis tool searches for events or trends that may indicate that a device is vulnerable to security attacks. At this stage, malicious conduct analysis and rule-based analysis are carried out.

6 Results and Discussion

The implementation of the proposed framework was executed using Core i5 processor system with 8 GB RAM, running on Windows 8 with a 64-bit operating system. NetBeans 8.2, JDK 1.8, Tomcat 8.0.15, Jelastic cloud platform, and MySql 5.7 were used for the development of the framework. The proposed technique is compared to the closest traditional approaches using the Yahoo! Cloud Serving Benchmark (YCSB) and small bank datasets.

The proposed system was evaluated and expresses using average delay, success rate, and system execution time for the proposed mechanism. In comparison to conventional methods, it was discovered that using the proposed strategies reduces average latency and SET (system execution time) and enhances SR (success rate). How can we attain privacy efficiency while maintaining system compatibility, with the lowest possible error rate, the shortest possible execution time, and the highest possible success rate?

Table 1 displays the result of the proposed framework with the traditional methods. As shown in Table 1, the traditional approaches used are Ethereum [83], Hyperledger [83–84], and Parity [83] with the used metrics success rate (SR), system execution time (SET), and average delay (AD) all in (%) values from various research studies. From the obtained results, the proposed framework performed better than the existing methods based on the several metrics used for the observation like average delay, system execution time, and success rate for small bank dataset and the YCSB.

From Fig. 4, the results show that the proposed system performed best when compared with the conventional methods used on the YCSB and small bank dataset based on success rate (%).

Table 1 The performance of the proposed system against the traditional methods

	YCSB			Small bank		
Methods	SR (%)	AD (%)	SET (%)	SR (%)	AD (%)	SET (%)
Ethereum	27.4	10.5	12.52	29.5	13.4	X
Hyperledger	46	4.9	4.01	49	6.9	4.32
Parity	65	4.8	2.9	69	6.1	3.05
Proposed method	89	1.6	1.03	93	2.95	1.04

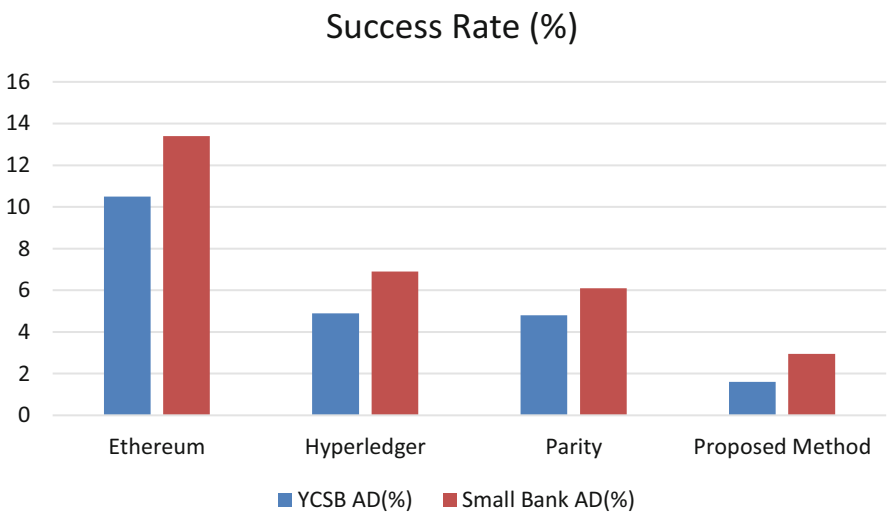

Fig. 4 The results of YCSB and small bank dataset by success rate (%)

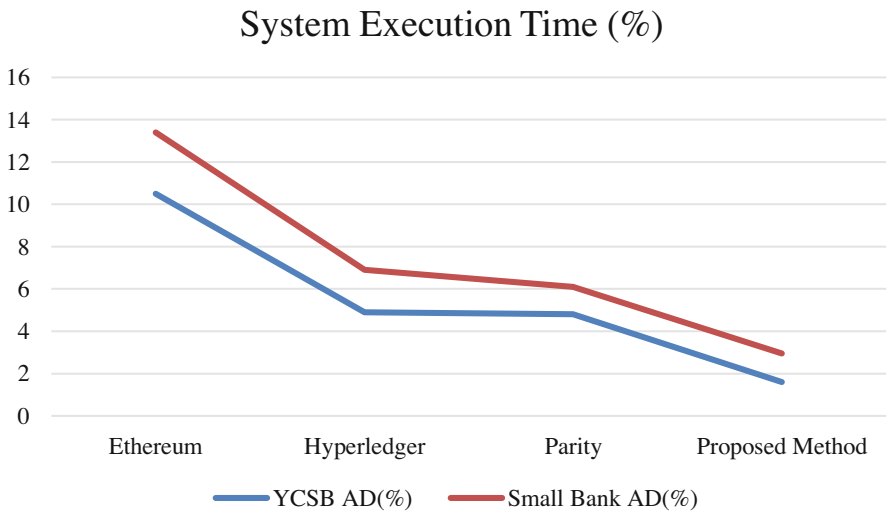

Fig. 5 The results of the YCSB and small bank dataset by system execution time (%)

From Fig. 5, the results show that the proposed system performed best when compared with the conventional methods used on the YCSB and small bank dataset based on system execution time (%).

From Fig. 6, the result show that the proposed system performed best when compare with the conventional methods used on the YCSB and small bank dataset based on Average Delay (%).

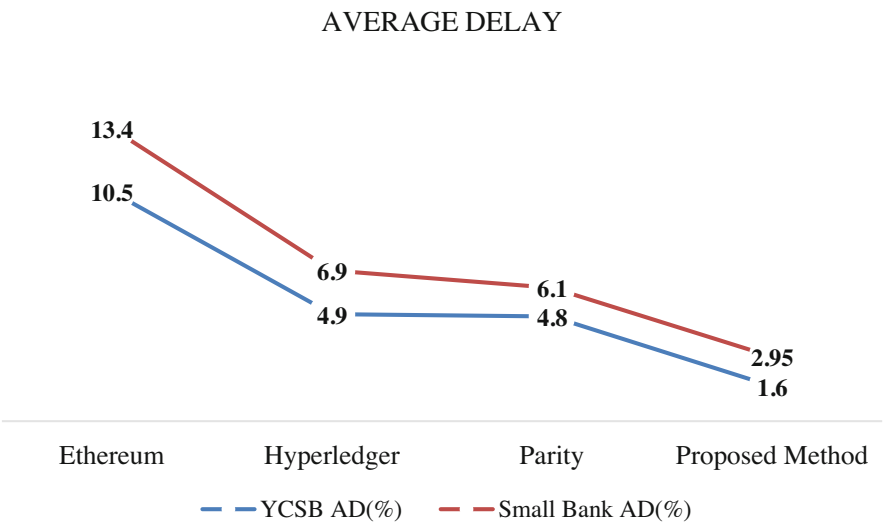

Fig. 6 The results of YCSB and Small Bank dataset by Average Delay (%)

7 Conclusion and Future Directions

In today's healthcare sector, the application of blockchain in healthcare systems is crucial. It can lead to automated data collecting and verification processes, as well as correct and aggregated data from diverse sources that is immutable, tamper-resistant, and safe, with a lower risk of cybercrime. It also allows distributed data, as well as system redundancy and failure tolerance. As a result, using blockchain technology, this chapter presented a secure smart healthcare system. The proposed approach was used to transform a concentrated and vulnerable smart system into a distributed, transparent, and safe system, thereby raising the standard of medical-related services on the smart healthcare system. There are various theories on why blockchain could be used to improve the healthcare system. First, it provides clear data to all stakeholders while safeguarding the privacy of patients. It also safeguards sensitive medical records from theft and eavesdropping by malicious attackers. In the proposed system, mathematical derivation is used to evaluate the efficiency, security, and cost-effectiveness of sharing healthcare data. The suggested framework is compatible with a cloud platform and completely independent for secure data transmission and recovery. The proposed system has reduced 1.6 AD in seconds and 1.03 SET in seconds and improves 25% SR. Finally, when compared to the traditional methods, the suggested methodology outperforms them on each parameter and dataset. The proposed framework's complete implementation will be carried out in the future. The lack of blockchain awareness among healthcare stakeholders is a key roadblock to its implementation, which will be addressed in the future to ensure that blockchain is properly implemented in the healthcare system.

References

1. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62–75.
2. Awotunde, J. B., Ogundokun, R. O., Jimoh, R. G., Misra, S., & Aro, T. O. (2021). Machine Learning Algorithm for Cryptocurrencies Price Prediction. In Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities (pp. 421–447). Springer, .
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557–564). IEEE.
4. Awotunde, J. B., Ogundokun, R. O., Misra, S., Adeniyi, E. A., & Sharma, M. M. (2020). Blockchain-Based Framework for Secure Transaction in Mobile Banking Platform. Advances in Intelligent Systems and Computing, 2021, 1375 AIST, pp. 525–534.
5. Nawari, N. O., & Ravindran, S. (2019). Blockchain and the built environment: Potentials and limitations. *Journal of Building Engineering, 25*, 100832.
6. Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences, 491*, 151–165.
7. Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review, 33*(4), 470–481.
8. Awotunde, J. B., Bhoi, A. K., & Barsocchi, P. (2021). Hybrid cloud/Fog environment for healthcare: an exploratory study, opportunities, challenges, and future prospects. Intelligent Systems Reference Library, 2021, 209, pp. 1–20.
9. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027–1038.
10. Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems, 68*, 1–13.
11. Shae, Z., & Tsai, J. J. (2017). On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 1972–1980). IEEE.
12. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). How blockchain could empower ehealth: An application for radiation oncology. In *VLDB workshop on data management and analytics for medicine and healthcare* (pp. 3–6). Springer.
13. Sanjukta, B., Sourav, B., & Chinmay, C. (2019). IoT-based smart transportation system under real-time environment. *IET: big data-enabled internet of things: Challenges and opportunities* (Ch. 16) (pp. 353–373). ISBN 978–1–78561-637-2.
14. Chakraborty, C., Banerjee, A., Kolekar, M. H., Garg, L., & Chakraborty, B. (Eds.). (2020). *Internet of things for healthcare technologies*. Springer.
15. Ho, C. W., Ali, J., & Caals, K. (2020). Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance. *Bulletin of the World Health Organization, 98*(4), 263.
16. Suzuki, S., & Murai, J. (2017). Blockchain as an audit-able communication channel. In *2017 IEEE 41st annual computer software and applications conference (COMPSAC)* (Vol. 2, pp. 516–522). IEEE.
17. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems, 78*, 659–676.
18. Chen, P. T., Lin, C. L., & Wu, W. N. (2020). Big data management in healthcare: Adoption challenges and implications. *International Journal of Information Management, 53*, 102078.
19. Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2021). An efficient lightweight cryptographic algorithm for IoT security. *Communications in Computer and Information Science, 2021*(1350), 41–53.
20. Albahri, A. S., Alwan, J. K., Taha, Z. K., Ismail, S. F., Hamid, R. A., Zaidan, A. A., ... Alsalem, M. A. (2021). IoT-based telemedicine for disease prevention and health promotion: State-of-the-art. *Journal of Network and Computer Applications, 173*, 102873.

21. Akkaş, M. A., Sokullu, R., & Çetin, H. E. (2020). Healthcare and patient monitoring using IoT. *Internet of Things, 11*, 100173.
22. Lee, S. M., & Lee, D. (2021). Opportunities and challenges for contactless healthcare services in the post-COVID-19 era. *Technological Forecasting and Social Change, 167*, 120712.
23. Daniel, J. G., & Uppaluru, M. (2017). New reimbursement for remote patient monitoring and telemedicine.
24. Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and privacy on the internet of medical things: Taxonomy and risk assessment. In *2017 IEEE 42nd conference on local computer networks workshops (LCN workshops)* (pp. 112–120). IEEE.
25. Mutlag, A. A., Ghani, M. K. A., Arunkumar, N. A., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems, 90*, 62–78.
26. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. *Security and Communication Networks, 2018*.
27. Tang, J., Liu, A., Zhao, M., & Wang, T. (2018). An aggregate signature-based trust routing for data gathering in sensor networks. *Security and Communication Networks, 2018*.
28. Sun, W., Cai, Z., Liu, F., Fang, S., & Wang, G. (2017). A survey of data mining technology on electronic medical records. In *2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom)* (pp. 1–6). IEEE.
29. Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. *Blockchain in healthcare today, 1*(8).
30. Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors, 20*(8), 2195.
31. Basha, S. M., Janet, J., & Balakrishnan, S. (2020). A study on privacy-preserving models using blockchain technology for IoT. In *Blockchain, big data and machine learning* (pp. 265–290). CRC Press.
32. Cancarevic, I., Plichtová, L., & Malik, B. H. (2021). Healthcare systems around the world. In *International medical graduates in the United States* (pp. 45–79). Springer.
33. Islam, M., Usman, M., Mahmood, A., Abbasi, A. A., & Song, O. Y. (2020). Predictive analytics framework for accurate estimation of child mortality rates for internet of things enabled smart healthcare systems. *International Journal of Distributed Sensor Networks, 16*(5), 1550147720928897.
34. Trivedi, S. A., Patel, M., & Patel, S. (2021). Health care cube integrator for health care databases. In *Web semantics* (pp. 129–151). Academic Press.
35. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security, 101966*.
36. Jia, Q. (2021). Research on medical system based on blockchain technology. *Medicine, 100*(16).
37. Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021). A Blockchain-based secret-data sharing framework for personal health records in emergency condition. In *Healthcare* (Vol. 9, p. 206). Multidisciplinary Digital Publishing Institute.
38. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications, and services (Healthcom)* (pp. 1–3). IEEE.
39. Khurshid, A. (2020). Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. *JMIR Medical Informatics, 8*(9), e20477.
40. Esmat, A., de Vos, M., Ghiassi-Farrokhfal, Y., Palensky, P., & Epema, D. (2021). A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Applied Energy, 282*, 116123.
41. Arani, S. A., Nawab, M. R. I., Rahman, M. T., & Zaman, M. (2020). A blockchain-based approach to prevent hidden contagion of COVID-19. *Compiler, 9*(2), 71–84.

42. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297.
43. Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications, 102857*.
44. Habibzadeh, H., Dinesh, K., Shishvan, O. R., Boggio-Dandry, A., Sharma, G., & Soyata, T. (2019). A survey of healthcare internet of things (HIoT): A clinical perspective. *IEEE Internet of Things Journal, 7*(1), 53–71.
45. Stafford, T. F., & Treiblmaier, H. (2020). Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. *IEEE Transactions on Engineering Management, 67*(4), 1340–1362.
46. Chanchaichujit, J., Tan, A., Meng, F., & Eaimkhong, S. (2019). Blockchain technology in healthcare. In *Healthcare 4.0* (pp. 37–62). Palgrave Pivot.
47. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62–75.
48. Sun, Z., Sun, R., Lu, L., & Mislove, A. (2021). Mind your weight (s): A large-scale study on insufficient machine learning model protection in mobile apps. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.
49. Dubovitskaya, A. (2021). Blockchain applications in healthcare. In *The emerald handbook of Blockchain for business*. Emerald Publishing Limited.
50. Duy, P. T., Hien, D. T. T., Hien, D. H., & Pham, V. H. (2018). A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. In *Proceedings of the Ninth International Symposium on Information and Communication Technology* (pp. 200–207).
51. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–the overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change, 158*, 120166.
52. Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)* (pp. 772–777). IEEE.
53. Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017). Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)* (pp. 253–255). IEEE.
54. Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation, 2*(1), 1–9.
55. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A review. *Procedia Computer Science, 113*, 73–80.
56. Khan, S. I., & Hoque, A. S. L. (2016). Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In *2016 International Conference on Networking Systems and Security (NSysS)* (pp. 1–6). IEEE.
57. Vithanwattana, N., Mapp, G., & George, C. (2016). mHealth-Investigating an information security framework for mHealth data: Challenges and possible solutions. In *2016 12th International Conference on Intelligent Environments (IE)* (pp. 258–261). IEEE.
58. Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access, 5*, 14757–14767.
59. Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation, 2*(1), 1–9.
60. Ding, D., Conti, M., & Solanas, A. (2016). A smart health application and its related privacy issues. In *2016 Smart City Security and Privacy Workshop (SCSP-W)* (pp. 1–5). IEEE.

61. Fernando, R., Ranchal, R., An, B., Othman, L. B., & Bhargava, B. (2016). Consumer oriented privacy preserving access control for electronic health records in the cloud. In *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)* (pp. 608–615). IEEE.
62. Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: State of the art and future challenges. *Journal of Medical Systems, 40*(6), 155.
63. Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In *Advances in healthcare informatics and analytics* (pp. 19–50). Springer.
64. Panigrahi, R., Borah, S., Bhoi, A. K., & Mallick, P. K. (2020). Intrusion detection systems (IDS)—an overview with a generalized framework. Cognitive Informatics and Soft Computing, 107–117.
65. Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain Technology for Secured Healthcare Data Communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics, 10*(12), 1437.
66. Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2016). A framework for personal data protection in the IoT. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 384–391). IEEE.
67. Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal, 25*(2), 315–329.
68. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain-ready manufacturing supply chain using a distributed ledger. *International Journal of Research in Engineering and Technology, 5*(9), 1–10.
69. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.
70. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. *Challenges and opportunities. Future generation computer systems, 88*, 173–190.
71. Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next internet technology*. Wiley.
72. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wireless Communications and Mobile Computing, 2021, 7154587
73. Song, H., Zhu, N., Xue, R., He, J., Zhang, K., & Wang, J. (2021). Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information Processing & Management, 58*(3), 102507.
74. Greenspan, G. (2015). Multichain private blockchain-white chapter. URL: http://www.multichain.com/download/MultiChain-White-Chapter.pdf.
75. De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production, Issue, 7*.
76. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)* (pp. 468–477). IEEE.
77. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics, 231*, 107831.
78. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software, 35*(4), 95–99.
79. Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access, 7*, 24477–24488.
80. Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer law & security review, 34*(3), 550–561.
81. Chakraborty, S., Aich, S., & Kim, H. C. (2019). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260–264). IEEE.

82. Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. Internet of Things, 2021, pp. 105–134.
83. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30*(7), 1366–1385.
84. Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *Journal of Ambient Intelligence and Humanized Computing*, 1–9.