Hindawi
Journal of Food Quality
Volume 2021, Article ID 7608296, 20 pages
https://doi.org/10.1155/2021/7608296

Review Article

Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives

Pranav Ratta,[1] **Amanpreet Kaur**,[1] **Sparsh Sharma**,[2] **Mohammad Shabaz**,[3] **and Gaurav Dhiman**[4]

[1]*University Institute of Computing, Chandigarh University, Patiala, Punjab, India*
[2]*Department of Computer Science & Engineering, NIT Srinagar, Srinagar, J&K, India*
[3]*Arba Minch University, Arba Minch, Ethiopia*
[4]*Government Bikram College of Commerce, Patiala, Punjab, India*

Correspondence should be addressed to Mohammad Shabaz; mohammad.shabaz@amu.edu.et

Received 19 April 2021; Revised 1 May 2021; Accepted 6 May 2021; Published 25 May 2021

Academic Editor: Rijwan Khan

Internet of Things (IoT) is one of the recent innovations in Information Technology, which intends to interconnect the physical and digital worlds. It introduces a vision of smartness by enabling communication between objects and humans through the Internet. IoT has diverse applications in almost all sectors like Smart Health, Smart Transportation, and Smart Cities, etc. In healthcare applications, IoT eases communication between doctors and patients as the latter can be diagnosed remotely in emergency scenarios through body sensor networks and wearable sensors. However, using IoT in healthcare systems can lead to violation of the privacy of patients. Thus, security should be taken into consideration. Blockchain is one of the trending research topics nowadays and can be applied to the majority of IoT scenarios. Few major reasons for using the Blockchain in healthcare systems are its prominent features, i.e., Decentralization, Immutability, Security and Privacy, and Transparency. This paper's main objective was to enhance the functionality of healthcare systems using emerging and innovative computer technologies like IoT and Blockchain. So, initially, a brief introduction to the basic concepts of IoT and Blockchain is provided. After this, the applicability of IoT and Blockchain in the medical sector is explored in three major areas—drug traceability, remote patient-monitoring, and medical record management. At last, the challenges of deploying IoT and Blockchain in healthcare systems are discussed.

1. Introduction

The Healthcare sector is an essential concern for all the developing as well as developed countries because this sector is directly concerned with the social welfare and lives of people. Research and development in the Healthcare sector should be an ongoing process, as it will help to improve the quality of living by fighting various health issues and diseases. With the advancement and recent developments in technology, the improvement in the Healthcare sector can be seen easily. The existing capabilities of the Healthcare and Medical Sector can be further improved by the introduction of the latest and innovative computer technologies in the Healthcare sector. These advanced computer technologies can assist doctors and medical practitioners in the early diagnosis of various diseases. The accuracy of detecting diseases in the early stages can also be improved considerably using these advanced computer technologies.

Various emerging and revolutionary computer technologies are already being used in other sectors with miraculous results. These technologies include the IoT, Blockchain, Machine Learning, Data Mining, Natural Language Processing (NLP), Image Processing, Cloud Computing, and many more.

IoT means connecting everything with the Internet. Everything here includes vehicles, home appliances, and other items embedded with electronics, and software, sensors, actuators, and connectivity that enable these things to connect, collect, and exchange data. Kevin Ashton is considered the father of IoT [1], which involves Internet connectivity beyond standard devices, such as desktops, laptops, smartphones, and tablets, to any range of traditionally dumb or noninternet-enabled physical devices and everyday objects. The leading technologies used in the Internet of things are sensors, cloud, wireless technology, and security.

The basic life cycle of IoT consists of four parts: (1) to gather the data through devices with the help of sensors; (2) the gathered data are stored in the cloud for the analysis; (3) the analyzed data are then sent back to the device; and (4) the device acts accordingly [2]. IoT is applicable in many domains, thereby making our life comfortable. The main applications of IoT are Smart Homes, Smart City, Agriculture, Smart Retail, Driverless Cars, and Healthcare. Security remains a crucial aspect of every technology and plays a vital role in the smooth functioning of IoT networks. Some ongoing projects for enhancing IoT security include methods for providing data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. The security problem in IoT arises due to careless program designing that leads to vulnerabilities, which is an important reason for network security issues.

In IoT architecture, proper initialization of IoT is done at the physical level so that any unauthorized receiver cannot access the system. IoT architecture consists of five layers: the Perception layer, Network layer, Middleware Layer, Application layer, and Business layer [3]. Each layer has its objective and issues. The main security goals crucial in IoT are Confidentiality, Integrity, and Availability (CIA). Based on vulnerabilities, there are four categories of attacks in IoT: "Physical attack," "Software attack," Network attack," and "Encryption attack."

1.1. Physical Attack

(i) Node tempering: the attacker, by altering the compromised node, obtains the encryption key

(ii) Physical damage: this damage results in a Denial of Service (DOS) attack as the attacker physically harms IoT system components

(iii) Malicious code injection: by this attack, the attacker can get full control of the IoT system

(iv) RF Interference on RFID: the attacker sends noise signals over radio frequency signals, and these signals are used for RFID communication

(v) Social Engineering: the attacker obtains sensitive information from the user of an IoT system to achieve his goals

(vi) Sleep Deprivation Attack: shutting down nodes is the main aim of the attacker

(vii) Node Jamming in WSNs: this attack can disturb wireless communication by using a jammer

1.2. Software Attack

(i) Phishing attacks: this is a widespread attack. The attacker uses fake websites to obtain the private information of the user.

(ii) Virus, Worms, Trojan horse, Spyware, and Aware: arrival of these entities can damage the system by spreading the malicious code through e-mail attachments and from the Internet. The worm can replicate itself without the involvement of humans.

(iii) Malicious scripts: this attack is used to access the system.

(iv) DOS: the adversary's main aim is to block the users.

1.3. Network Attack

(i) Traffic analysis attacks: to obtain the network information, the attacker intercepts and examines messages.

(ii) RFID spoofing: an attacker spoofs RFID signals, changes the message, and gives wrong information to the system. The system accepts the wrong information, which is altered by the attacker.

(iii) Sinkhole attack: it is a very common type of attack. The primary purpose of this attack is to send fake information about the route to the neighboring nodes.

(iv) Sybil attack: the attacker inserts the malicious node inside the network, and that one node in the network takes the identity of multiple nodes.

1.4. Encryption Attack. The main aim of this attack is to obtain the private key, which is used by two devices while communicating with each other.

(i) Side–channel: in this attack, when the message is transferred from user to server or vice versa, then the attacker reveals some additional information

(ii) Cryptanalysis attacks: in this attack, attacker decodes the message from the nonreadable format to a readable format without knowing the key

(iii) Man in the middle attack: the attacker keeps on observing the communication between the nodes to steal sensitive information

There exist various security proposals in the literature. However, security is still the topic of concern in IoT networks because of existing challenges like centralization, single point of failure, etc. So, a new and emerging technology known as the Blockchain can be used along with IoT for enhancing the security of IoT. The strength of Blockchain technology can be introduced in IoT to enhance its security and make it a more secure network by removing the challenges and issues of centralization in the existing

security techniques and introducing the concept of decentralization using the Blockchain.

Blockchain is a point-to-point distributed network in which no third party is required for the transaction and communication [4]. All the transactions are independent and isolated from other transactions. The technology behind the popular and revolutionary concept of cryptocurrency is the Blockchain. Cryptocurrency is believed to be highly secure and unhackable. This very same concept of Blockchain can be used in other networks for security enhancement. In the Blockchain, a public distributed ledger system is opened to everyone. Blockchain is a list of records that store data publicly and in a chronological order. Block is a container that holds transaction details. Each block contains data, the hash of the previous block, and the hash of the concerned block. It has two parts: Header and Transaction details. The header contains information regarding the block. "Timestamp" keeps a record of the time at which the block was created. "Difficulty level" decides how hard it will be to mine a block. "Merkle Root" represents the fingerprints of all the transactions stored in the block, and "NONCE" is the solution to the mathematical puzzle in the Proof-of-work algorithm.

1.4.1. Motivation. In this article, two emerging technologies, IoT and Blockchain, are integrated, and their possibility and application in the Healthcare sector have been explored. IoT technology in healthcare can be used for applications like remotely monitoring patients' health. The patients who require regular attention can be monitored by the doctors remotely using the IoT Sensors deployed on their bodies and surroundings. Similarly, Blockchain technology in healthcare can handle the issue of drug traceability, medical record management, etc. However, IoT is prone to security attacks like attacks on integrity, privacy, confidentiality, and availability. So, using IoT alone in the Healthcare sector for applications like remote patient monitoring can lead to patient data leakage, data manipulation during its transmission, etc., which, in the worst case, can claim the life of the patient. So, Blockchain technology can be brought into use along with the IoT in healthcare to enhance the capabilities of the Healthcare sector and ensure the security and privacy of the patients' records.

However, the introduction of new and emerging technology in any sector can give rise to some issues as well as challenges. So, it is crucial to identify those issues and challenges, especially in the Healthcare sector, where people's lives are directly associated. In this article, the possibility of deploying Blockchain and IoT in the Healthcare sector is explored, and various new healthcare applications that are possible using these innovative technologies are presented. Various challenges and issues in the deployment of these two emerging technologies in the Healthcare sector are then presented in detail.

1.4.2. Main Contributions of This Article

(1) The possibility and benefits of using Blockchain and IoT technologies for enhancing the Healthcare and Medical sector have been explored

(2) Various areas of application in healthcare where IoT and Blockchain can be applied are presented

(3) Various challenges in the use of IoT and Blockchain technologies in the Healthcare sector have been explored and presented

2. Review Technique and Strategy

This section elaborates on the motivating factors as well as the review strategy used for conducting this study on Blockchain and IoT in the Healthcare sector.

2.1. Review Plan. Stages that were involved in this literature review on the use of Blockchain and IoT technologies in the Healthcare and Medical sector includes building a review strategy, downloading research articles from different online sources, analyzing the quality of articles, interpreting and enumerating observed results of the review, recording the results of the review, and finally presenting various research challenges and future research directions.

2.2. Research Questionnaire. The initial step involved in conducting this survey was to frame the different research questionnaires and the motivating factors, and searching for different online research databases for relevant articles. Table 1 gives the set of research questions along with the motivation required to plan and conduct the survey on the use of Blockchain and IoT in the Medical sector.

2.3. Source of Information. For conducting this review, various possible relevant resources have been consulted for finding the required and related research resources required for this study. Various online sources like Springer (http://www.springer.com), Google Science Direct (http://www.sciencedirect.com), IEEE Explore (http://www.ieeeexplore.ieee.org), Scholar (scholar.google.com), and online tutorials, such as Edureka, National Program on Technology Enhanced Learning (NPTEL) for understanding the concepts, etc., have been consulted in this study.

2.4. Search Keywords. This exhaustive search on understanding the possibility of using Blockchain and IoT technologies in the Medical and Healthcare sector includes qualitative and quantitative research papers from 2008 to 2020. However, it mainly includes the papers after the year 2016. The research on IoT was started long back, but the concept of Blockchain was introduced from 2009 onward. Research papers from journals, conferences, symposiums, college thesis, workshops, etc., were included in this review.

Initially, a total of 79 papers on IoT, Blockchain having their applicability in the Healthcare sector were retrieved using the keywords mentioned in Table 2, which after applying certain inclusion and exclusion criteria as filters based on titles, abstracts, full-texts, publisher value, etc.,

Table 1: Research questionnaire and motivation.

Questions	Motivation
1. What is IoT? 2. What is the current status of research in IoT? 3. What are the challenges and research opportunities in IoT? 4. What are the different applications of IoT?	IoT is an emerging network that allows communication among different objects that surround us. These objects include homes, refrigerators, air-conditioners, traffic lights, etc. IoT is being used in different sectors, including agriculture, healthcare, transportation, smart homes, etc. It is crucial to find the challenges of IoT. Security, privacy risk, and trust are some of the challenges of IoT that require consideration.
1. What is a Blockchain? 2. Can the Blockchain be used use with bitcoin only? 3. What are the areas where Blockchain can be used? 4. How can the Blockchain be integrated with IoT? 5. What are the different challenges in the integration of Blockchain with IoT?	Blockchain is another emerging technology that has various applications and domains for improved security, privacy, and trust, considering the peculiar feature that makes it robust and unhackable. The privacy and security issues of the IoT network can be handled using the Blockchain. However, the possibility of integration and deployment of Blockchain in IoT networks is required to be explored.
1. How Blockchain and IoT can be used in the medical sector? 2. What are the different application areas of healthcare where Blockchain and IoT can be used? 3. What are the challenges in the deployment of IoT and Blockchain in the healthcare sector?	The combination of IoT and Blockchain can be introduced in the Healthcare and Medical sector for improving the current issues in the Healthcare sector like drug traceability issues. This integration of two powerful technologies can enhance the capability as well as the quality of the current Healthcare sector.

Table 2: Search strings.

S. no.	Keyword	Synonyms	Content-type
1	IoT applications	Application of IoT	Journals, conference, symposium, online tutorial, university thesis
2	IoT, Blockchain in healthcare	IoT and Blockchain in Medical sector	
3	Blockchain for patient health	Blockchain for remote monitoring of patients	
4	Blockchain and IoT for Medical supply chain tracking	IoT and Blockchain in medicine tracking	
5	Blockchain applications	Applications of the Blockchain	
6	Features of the Blockchain	Blockchain features	
7	Challenges in Blockchain, IoT	Blockchain ongoing challenges	
8	Blockchain IoT healthcare	Blockchain healthcare framework	

Table 3: Parameters considered for shortlisting and exclusion of articles.

S. no.	Considered parameters	Shortlisting for inclusion criteria	Exclusion criteria
1	Period	Articles published on the use of the Blockchain, IoT for healthcare and medical-related applications between the year 2016 and 2020	Articles published before the year 2016 were excluded
2	Type of articles	Articles with implementation results	Review and survey articles, theoretical papers without implementation results
3	Language	Articles are written in the English language	Articles in languages other than English
4	Title, abstract, citations, and journal/conference value and indexing	Articles with their titles and abstracts that match the use of Blockchain and IoT in the Healthcare domain were selected	Firstly, based on the titles, articles were selected and excluded
		Number of citations, value of journal/conference where the article is published is also considered	Then, abstracts of articles shortlisted based on titles were checked for inclusion and exclusion

got reduced to 22 quality papers. Various search strings like "Blockchain and IoT in Healthcare" have been used for searching papers. Table 3 shows the various parameters that were considered for shortlisting and exclusion of irrelevant articles. The exclusion criteria for shortlisting of quality and relevant articles are shown in Figure 1.

3. Blockchain Technology and Related Concepts

Blockchain is an emerging technology used in numerous different networks to ensure security and reliability in those networks. Blockchain technology is also given preference in various transaction management systems, and it is replacing the current existing transaction management system.

The issues with the current banking system are as follows:

(i) High transactional fees

(ii) Double spending

(iii) Banks have become synonymous with cries

With its decentralization feature, Blockchain has solved the issue associated with centralized banks and is the primary technology behind bitcoin. Blockchain is a public distributed database that holds the encrypted ledger [5]. There is a central coordination system in a centralized architecture, and every node is connected to that central coordination system. All information between the nodes will be shared, passed, and approved through this central coordination system. Under this platform, all of these individual dependent nodes will get disconnected if the central coordination platform fails. Therefore, the switch from the centralized system toward a decentralized system is the need of the hour. In the decentralized system, there will be more than one coordinator. In a decentralized system, each node is treated as a coordinator, i.e., there is no centralized authority. Each node is connected to other nodes, and this system is not dependent on any particular coordinator.

Blockchain consists of a chain of blocks, and each block is a collection of all recent transactions that have taken place and are verified. The detailed and general structure of the Blockchain is shown in Figure 2, where the sequence of blocks is shown, and each block is connected cryptographically. All these transaction details are stored on each block, and a consolidated hash code block-wise is computed and stored into the block. Once the transaction is verified, this block becomes the permanent part of the Blockchain, and the chain keeps growing.

Blockchain is a leading technology, only second to the popular bitcoin. The working of bitcoins using the Blockchain can help to understand Blockchain technology better. Bitcoin is the first decentralized digital currency that was introduced in 2009 by Santoshi Nakamoto [6]. Bitcoin uses various cryptography as well as mathematical concepts that ensure that the creation, as well as the management of bitcoin, is restricted and secured. The algorithms and the cryptography technologies are used to keep on updating regularly. The ledger system that keeps track of how much bitcoin gets transacted is electronic and highly secure, and this ledger is known as the Blockchain.

In the Blockchain, there are various key concepts. One of them is the Previous Hash Code. Every block has to specify the hash code associated with it, which is used as an identifying factor for that block. This hash is created with a very complex hashing algorithm. The hash details of every transaction that has happened have to be completed to be a part of that block. The transaction details of a block are contained in the header in a hex value known as Merkle Root.

Another important concept associated with the Blockchain is the value or proof of work of that block. This is the mathematical solution that is attached to the block to ensure that this is the valid block.

Let us take an example to understand how the Blockchain works. Suppose A wants to send money to B. The transaction is represented as a block, and the block is broadcasted to every node in the network. After that, there is a group of sufficient miners that have the authority to approve the transaction. After getting approval from miners who solve the proof of concept, the transaction is added to the Blockchain, and finally, B gets the money.

A block is the crucial part of a Blockchain that records all of the recent transactions and, once completed, goes into the Blockchain as a permanent database. Blockchain is built from three technologies. First is that the Blockchain uses private key cryptography to secure identities and hash function to make the Blockchain immutable. It uses a P2P, a network, which ensures complete consistency with the Blockchain [7, 8].

Suppose a person tries to make a slight change concerning the transaction or a block that is part of a Blockchain, then the changed block cannot be added or reflected in the Blockchain because most of the people in the network have the original Blockchain, and this changed block cannot be accepted.

The program in which the Blockchain is created has a lot of protocols and security features. Solidity is the most preferred language for writing the Blockchain program. In any Blockchain, every transaction that gets verified and validated in the creation of a new block is logged along with the information about time, date, participants, and the amount that gets transmitted across. Each user who is part of the Blockchain holds the complete Blockchain in itself. The miner verifies each transaction involved in the Blockchain after solving a complex mathematical puzzle, and once it is solved, the transaction is verified and maintained in the ledger.

3.1. Types of Blockchain. Blockchain is of three types Public, Private, and Consortium. A public Blockchain is similar to bitcoin in which anyone in the world can be a part of. Anyone who is part of the Blockchain and is a miner can read as well as write data into this Blockchain.

Private Blockchain is, however, something that is quite restricted. Usually, one central person has the exclusive right to both verify the transaction as well as add a new block to the Blockchain.

A consortium Blockchain is something between public and private Blockchain. Instead of one person, there are a group of people who verify and add transactions.

In conclusion, Blockchain uses mathematics to create a secure, distributed ledger that enables transactions without a third party.

3.2. Decentralized Applications. Decentralized applications are the central part of the Blockchain. It promises to deal with all the problems that come with the centralized

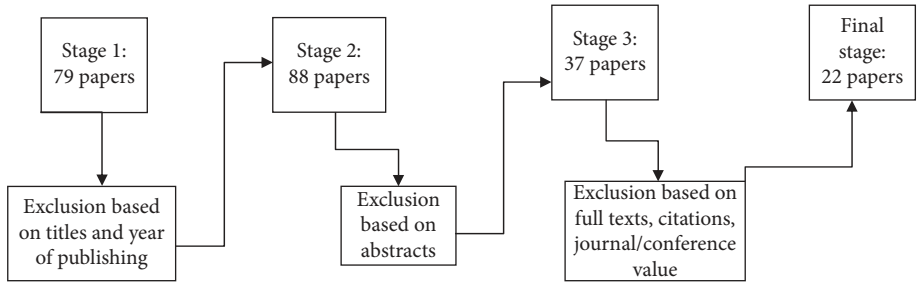

Figure 1: Exclusion criteria for shortlisting of quality and relevant articles.

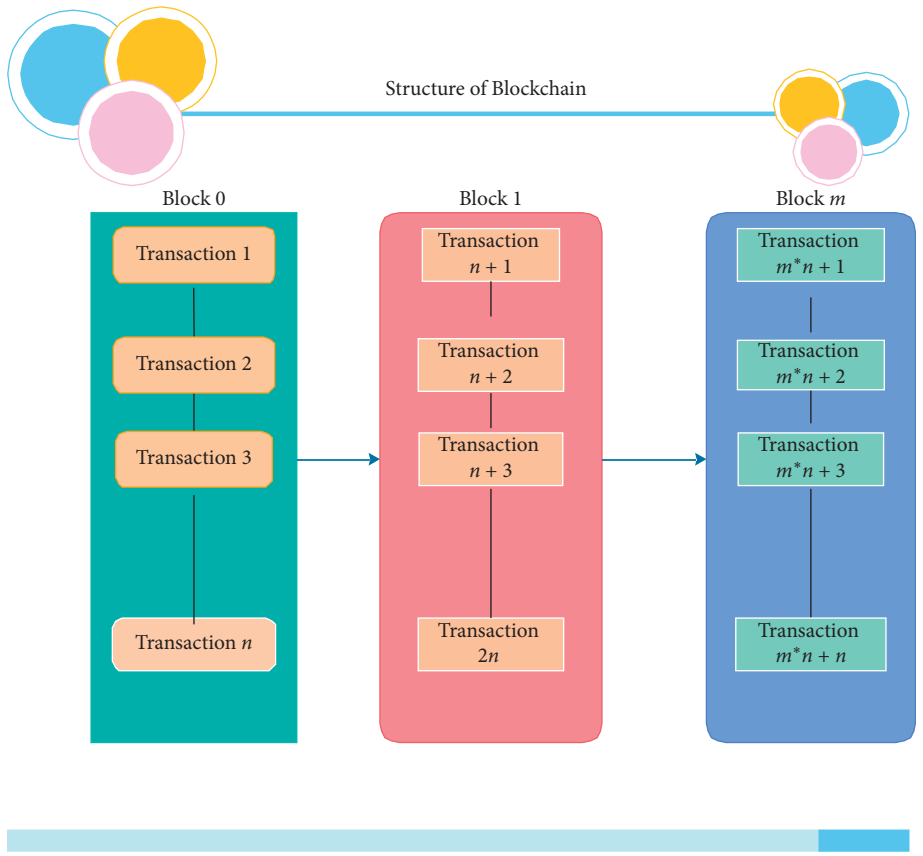

Figure 2: Structure of the Blockchain.

system. The decentralized architecture works as the user invokes the smart contracts. Ethereum is a decentralized platform that runs smart contracts. It was proposed in 2013 and released in 2015. The value token of the Ethereum Blockchain is called Ether, listed under ETH on cryptocurrency exchanges. The smart contract contains all the rules that are pertinent for the service that is provided to contain state information, which contains data for smart contracts [9]. Smart contract is an automated computerized protocol used for digitally facilitating, verifying, or enforcing a legal contract's negotiation or performance by avoiding intermediates and directly validating the contract over a decentralized platform. Nick Szabo, a computer scientist and cryptographer introduced the term in 1996. He claimed that smart contracts could be realized with the help of a public ledger.

The advantages of decentralized applications are the following

(1) *Autonomy*. You are the one agreeing; there is no need for a broker or a lawyer

(2) *Trust*. Entire documents and data in blockchain-based decentralized applications are encrypted using advanced encryption technologies, and all the data are distributed on a decentralized network that is being run by a shared Ledger. If the data are corrupted or altered, then it will be rejected by the members of the Ledger

(3) *Backup*. On the Blockchain, documents are duplicated and stored in many locations

(4) *Accuracy*. Smart contracts are faster and cheaper and avoid errors that arise from tedious manual work

3.3. Some Applications Supported by the Blockchain. A Blockchain wallet is similar to a bank account. It allows us to receive bitcoins, store them, and then send them to others. There are many Blockchain features, for example, security, instantaneous transaction, currency conversion, and accessibility. There are various types of Blockchain wallets:

3.3.1. Based on the Location of Private Key. This is where exactly our private key is being stored. The hot wallet is the Blockchain program where the private key is ultimately stored on a cloud-based server. Cold wallet: All the transaction details are going to get the first hash, and only the transaction hash gets prorogated throughout the network. With regard to the security feature, a cold wallet is more secure than a hot wallet.

3.3.2. Based on Device and Clients. In this category, there are desktop wallets, online wallets, mobile wallets, and physical wallets.

Apart from its use in cryptocurrency, Blockchain technology has its applicability in other domains like banking, payments and transfers, healthcare, law enforcement, voting, IoT, online music, real estate, and many more.

3.4. Peculiar Features of Blockchain. Blockchain has various peculiar and prominent features like decentralization, transparency, open source, autonomy, immutability, and anonymity that make it a unique and powerful technology for ensuring security, as well as reliability, in an IoT-inspired network for healthcare [10]. Many terms are required while studying the concept of Blockchain. Some of the key features supported by Blockchain technology are shown in Figure 3 and are as follows.

3.4.1. Public Distributed Ledger. The data within a Blockchain are accessible to everyone. With this, as long as you are part of the network, you could access the entire history of transactions that have taken place since the Blockchain was created. Any additions to Blockchain have to be approved by the user. A majority of the members within the network have to approve any additions to the Blockchain. This is the "public" part of the ledger [11]. Hyperledger can be thought of as a software that everyone can use to create one's personalized Blockchain service. On the Hyperledger network, only parties directly affiliated with the deal are updated on the ledger and notified.

3.4.2. Hashing Encryption. In the Blockchain, security is ensured by hashing encryption. Blockchain utilizes the hash function to perform cryptography. The transaction details are contained in the header in a hexadecimal value known as

Figure 3: Characteristics of Blockchain.

Merkle Root. To ensure security, Blockchain also includes a digital signature. Users are provided their own private and public keys.

3.4.3. Mining. Miners collect all transactions that people send to each other over the network, and only valid transactions are relayed to other nodes. Each miner takes several collected transactions and put them in a newly formed block.

3.4.4. Decentralization. One of the significant features of Blockchain is decentralization. Decentralization means data are not dependent or stored in the central part. Instead of this, data are stored in each block of the Blockchain. Transactions are not communicated to various nodes by the central authority. Every block acts as the verified digital ledger. Many research areas apply Blockchain to eliminate the concept of centralization and switch to the concept of decentralization, e.g., cloud, IoT, edge computing, and big data [12].

3.4.5. Immutable. Immutable means something which cannot be changed. It is an important feature of Blockchain in which blocks cannot be altered. Immutability is achieved by the concept of proof of work. Proof of work is achieved by mining and the work of miners is to change the nonce. A nonce is a varied value to create a unique Hash address of the block, which is less than the target hash value. The probability of proof of work calculation is very low. Many trials have to be done to acquire valid proof of work. There is only one possibility of changing the block when the attacker takes control of more than 51% of the node simultaneously [13].

3.4.6. Consensus Protocol. The word autonomy is based on Consensus Protocol. Consensus means agreement ensures the latest block has been added to the chain correctly [13]. For ledger consistency and user security purpose, consensus algorithms have been implemented [14]. There are many consensus mechanisms given in Table 4 [15].

3.4.7. Anonymity. Anonymity here means namelessness, and it also comes under the features of the Blockchain. The anonymity set is divided into two parts: First is the sender anonymity set, and the other is the receiver anonymity set. This example works when one user sends the data to other users; it does not reveal the user's real identity. Instead of this, it communicates with the other users by using Blockchain address. By this process, one user never knows the other user's real identity [13, 14].

3.4.8. Enhanced Security. Everything is public in the Blockchain, so the privacy solution is done by hashing encryption. Blockchain can bring increased security and have certain benefits as compared to conventional systems [15, 16]. To understand hashing encryption, we need to know about the contents of the block. A block is a container that controls the transaction detail. The block has two parts: Header and Transaction details. The transaction details of a block are contained in the header in the hexagonal value known as Merkle Root. Blockchain utilizes the hash function to perform cryptography [17].

3.4.9. Persistency. In the Blockchain, there is a major feature called mining. Mining is the concept of validating the transaction, with the invalid transactions being emitted quickly [14]. Miner is the first person who finds the nonce value that falls within the target requirement.

3.4.10. Traceability. Traceability is the distribution chain to find out the origin of the product and follow the sequence. Traceability is an arrangement of blocks in the Blockchain in which each block is connected with adjacent two blocks by means of the hash key [9].

3.4.11. Currency Properties. Blockchain is a point-to-point network. No third party is required for the transaction. All the transactions are independent of the third party. In cryptocurrency Blockchain, the transaction is used, and its circulation is fixed. All the activities of Blockchain 2.0 and 3.0 applications have the property of currency [9].

4. IoT and Related Concepts

4.1. Architecture of IoT. The basic architecture of IoT is the same as the TCP/IP architecture. There are many factors in IoT architecture that need to be focused like Scalability, Interoperability, Reliability, and QoS. The basic architecture of IoT consists of many layers [18], and the general architecture of IoT is described in Figure 4.

Table 4: Various consensus mechanisms.

Consensus mechanism	Examples
Proof-of-work	Bitcoin, Litecoin
Proof-of-stake	NXT
Delegated proof-of-stake	BitShares
Proof-of-activity (PoW/PoS-hybrid)	PeerCoin
Proof-of-burn	Counterparty
Proof-of-validation	Tendermint
Stellar consensus protocol	Stellar
Ripple protocol consensus algorithm	Ripple

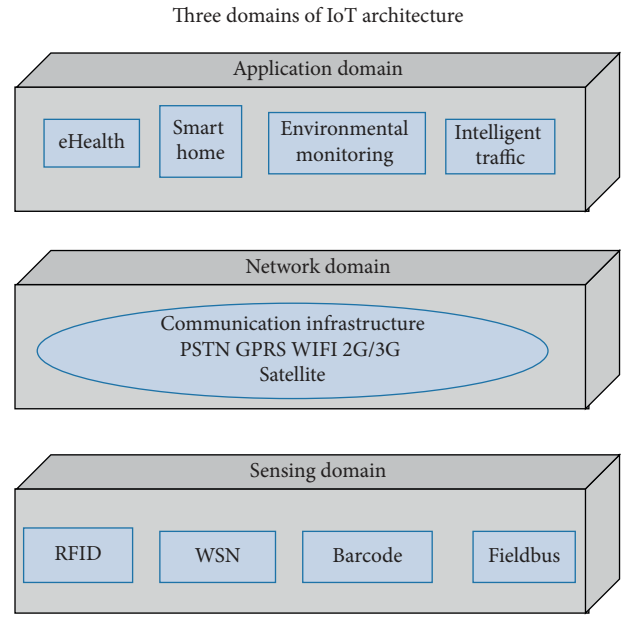

Figure 4: Domains of IoT architecture.

Perception layer: first is the perception layer, also known as the device layer. In this layer, sensors sense and gather information about the environment.

Transport layer: it transfers the sensor's data between different layers through networks such as wireless, 3G, LAN, and RFID.

Processing layer: this layer stores, analyses, and processes huge amounts of data. Modules and concepts like databases, cloud computing, and big data are used in this layer.

Application layer: this layer is responsible for delivering application-specific services to the user.

Business layer: it manages the whole IoT system, including applications, business and profit models, and user privacy. This layer also helps in future actions and business strategies.

Apart from the abovementioned general architecture of IoT, many other architectures are built-in literature by various researchers to fulfill different requirements of the application. The first NDN architecture was proposed by Jacobson et al. [19, 20]. NDN manages many functionalities of IoT at the network layer, e.g., data aggregation, security,

etc. IoT is the collection of heterogeneous applications. There are many requirements of IoT applications that can be fulfilled by NDN, e.g., due to low power operation, the nodes of NDN make data available to a different consumer. NDN helps in improving the energy efficiency of the network. There are many features of NDN that help to fulfill the main requirements of IoT. Energy efficiency in-network caching is also available. Similarly, for reliability, in-network caching and multipath routing feature are used. Data integrity is also a feature of NDN for security purposes in IoT.

In another work [21], the authors have discussed a general architecture of IoT in which the requirement and importance of Quality of Service (QoS) in IoT are focused. This paper discusses the various tasks in IoT, i.e., inquiry task, control task, and monitoring tasks. The monitoring tasks have different service requirements. The main requirements of QoS are service awareness. The architecture of QoS is divided into three layers: Application layer, Network layer, and Perception layer. One factor, which needs to be focused on, is Interoperability. Interoperability is the interconnection between devices. This concept covers the major applications of IoT, and this concept of interconnectivity is required at each of these layers: data model, messages, and network [22]. This is the modified version of architecture because, in existing architecture, there is a concept of end-to-end message delivery, but this architecture achieves the intelligent solution by integrating the web technologies with the existing architecture. The next architecture in the list is Software-Defined Networking Architecture, which is used for a more secure network. SDN-based architecture for IoT is Scalable with multiple SDN domains [23]. It also does the work of interoperability that was also focused on in the previous architecture.

4.2. Communication Technologies in IoT. Aggregation of heterogeneous networks and devices is done in IoT. To make centralization decisions concerning IoT, reliable communication between the gateway and things is essential [24]. The IoT gateway works as a communication between the sensing domain and the network domain. Zigbee, Bluetooth, WiFi are the technologies that are used to connect Smart Things to IoT gateway [25].

IoT gateways are required in two situations: when the connection occurs between different sensing domains like Zigbee, Bluetooth, and the connection between sensing and network domain, e.g., Zigbee and 3G. The commonly used communication standards and technologies used in IoT Communication are given below:

4.2.1. NFC. It is short-distance wireless communication technology. When two NFC-enabled devices are very close to each other, roughly around 4 cm, they can communicate using radio waves. NFC modes of operation are card emulation mode, peer-to-peer mode, and reader/writer mode. Some useful applications of NFC are file sharing, mobile payment, information sharing using smart posters, and business cards. Apart from that, it can be used for home automation, library systems, and healthcare [26]. At home, automatic switching off of lights, closing of doors, and turning off of air-conditioners can be performed using NFC.

4.2.2. RFID. Radiofrequency identification is a technology that works on radio frequency or radio waves. This technology is used to identify objects automatically. Here, the objects can be anything. Objects can be books in the library or any item you are purchasing from the shopping mall, or it can be your car, etc. They can be used not only to track objects but also to track humans, birds, and animals. It is very similar to the technology that is used in a barcode. The difference is that the barcode is a line of sight technology but RFID is not a line of sight technology. RFID system contains two components, namely, RFID reader and RFID tag. There are two RFID tags, namely, Active and Passive tags. Use cases of RFID are people tracking, school bus tracking, parking selection, healthcare, supply chain management, and manufacturing.

4.2.3. V2V. V2V is a wireless protocol similar to WIFI called dedicated short-range communications. When DSRC is combined with GPS, low-cost technology is formed. The V2V communication system provides a 360-degree view of similarly equipped vehicles within the communication range. Transmitted messages common to all vehicles include current GPS position, vehicle speed acceleration, headings, and vehicle control information such as the transmission state brake status and steering wheel angle, and the vehicle's path history and the path prediction. V2V does not include current technologies such as navigation, Internet access, assistant services, rearview cameras, and other advanced technologies. V2V provides crucial information when the driver needs it. V2V provides the driver with 360-degree awareness. This secure system keeps personal information anonymous and does not track your vehicle. The driver sees warning to prevent potential hazards through the display. It gives warnings like stop crash alert, intersection movement assist, do not pass application, blind-spot warning.

4.2.4. Zigbee Technology. Zigbee is a small packet device with low data rates and low power consumption [27]. It comes under the category of Home network. Zigbee is the technological standard created for control and sensor network. It is based on IEEE 802.15.4 created by the Zigbee alliance. The layers architecture of Zigbee is the application layer, stack, and silicon. The stack part consists of three layers, namely, API, security, and network. And in silicon, there are two layers, namely, MAC and a physical layer. The application layer is for the customer, the stack is under the Zigbee alliance, and silicon comes under IEEE 802.15.4.

4.2.5. WiFi. Wifi gives a facility to the computer and other devices to communicate over wireless signals. Wifi stands for Wireless Fidelity. IEEE gives the standard of Wifi, but it is a trademark of Wifi Alliance. It is commonly used for wireless local area networks. Mobile phone, cities, homes, everything is communicating through the wireless signal.

4.2.6. Bluetooth. Bluetooth was a very good communication medium in the early days. It was the open standard for the development of the personal area network. This technology has features such as low power consumption, low cost, and a short-range. A Bluetooth-enabled device can exchange information with other Bluetooth-enabled devices over a radio. Bluetooth helps in creating a small network of devices that is close to one another.

A comparison of Zigbee, Bluetooth, RFID, and NFC concerning a different domain is done in Table 5.

4.3. Benefits/Applications of IoT. IoT devices have the responsibility to ensure that the messages and data sent by the devices have reached their destination. IoT applications enable interactions between the device and device or human and device [28]. Domain description of the key application areas of IoT summaries are provided in Table 6.

IoT equips a multitude of domains and millions of devices with connectivity every day. IoT technology is used in day-to-day life in which various everyday things are connected to the Internet like online shopping, wearable technology, smartphones, vehicles, home lighting home, appliances, etc.

IoT in healthcare: Healthcare sector faces various issues and challenges that can be handled using the IoT [29]. Also, the healthcare capabilities can be enhanced multifold using the IoT. In the Healthcare sector, there is a lack of real-time data, a lack of smart card devices, inaccurate standard analytics, and other enhancements like remote monitoring of patients that can be made possible using IoT. IoT could be the answer to all these problems.

Smart cities, agriculture, industrial automation, and disaster management are a few domains where IoT can be used. Some applications and domains where IoT can be brought into use are shown in Figure 5.

4.4. Challenges in IoT. While going through many papers, it was found that IoT has some prominent challenges that require consideration. The main issues in IoT are security issues, privacy concerns, interoperability issues, IoT standards issues, legal issues, regulatory rights issues, emerging economy issues, developmental issues [5].

4.4.1. Security and Privacy. The security problem for things is created by vulnerabilities produced by a careless program design. Vulnerabilities mean inherent weakness in designing, configuring, implementing, and managing a network or system that renders it susceptible to a threat [30]. There are many security-related challenges in IoT: design practices and no security laws for developing IoT devices, i.e., set of similar appliance that has the same characteristics. Also, not much sufficient information is given to maintain or upgrade the IoT system. Since many devices are in the loop, one device is being attacked by the rest of the devices. As discussed earlier, security design requires three things, namely Confidentiality, Integrity, and Availability, known as CIA [31].

In the case of the Privacy Concern issue, there are no fixed rules against data users, and the data collected by IoT devices are not protected. User data could be vulnerable to theft. You could be tracked/monitored by anyone, as you are connected 24*7 on the Internet. To take advantage of IoT, the less developed regions have to implement the policy requirement and technical skill requirements.

4.4.2. Architecture. One more main challenge is to choose the architecture of IoT. The selection of architecture is very difficult, as different architectures are needed according to the need [32]. Therefore, there is a chance of developing new architecture or modifying the existing one.

4.4.3. Legal and Regulatory Rights Issues. Just like privacy, there are many legal and regulatory questions surrounding the IoT. QoS is achieved through the wireless network, but it needs attention in cloud computing.

4.4.4. Data Extraction and Management. Data extraction from the complex environment cannot be extracted continuously. For example, if there is a hilly area where there is no Internet, then how to extract data. For example, drugs are to be maintained at a particular temperature. There is no surety that drugs are maintained at the same temperature. If the 1-degree temperature is missed, the drugs could be spoiled. There is no surety of getting the exact data.

4.4.5. Power Requirements. A maximum of 90% of IoT devices is powered by a battery. How long is the battery going to live? Does it have recharging ability? Are there are some green methods of charging from sources like the solar wind? Therefore, power requirements are also the main challenge of IoT.

4.4.6. Complexity Involved. In IoT, a study of many techniques is important. It is not easy; many experts and teamwork among them are necessary. Many technologies need to come together, so one cannot say I have built the IoT product. For IoT products, a team is needed and experts are required to work on particular technologies.

4.4.7. Storage Cloud and Heterogeneous Devices. Storing is also the main challenge. Where to store data, either on the local server or on the cloud? Do we use the cloud for particular storage? If yes, then purchase or store the data in free cloud service. All these decisions are very important. A massive amount of data is generated through IoT sensors and devices; how to manage these data and how to deal with the heterogeneous nature of data are the main challenges [28]. In IoT, there exist many different applications, and it is very difficult to handle the heterogeneous applications in one architecture.

Table 5: Comparison of different communications.

Parameters/technology	Zigbee	Bluetooth	RFID	NFC
IEEE standards	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15	ISO/IEC 14443 A&B, JIS X63194
Frequency band	2.4 GHz	2.4GHZ	125khz, 13.56 Mhz, 902–968 MHZ	125khz, 13.56 Mhz, 860 MHZ
Network	WPAN	WPAN	Proximity	P2P network
Topology	Star Mesh cluster	Star Mesh cluster	P2P network	P2P network
Data rate	250 Kbps	1 Mbps	4 Mbps	106212 or 424 kbps

Table 6: Application areas of IoT.

Security	Security system, surveillance system, device security, data preserving
Payment method	Payment gateways, POS (point of sale)
Health	Remote diagnosis, remote monitoring
Metering service	Water, electricity, cab, energy
Remote access	Various sensors
Manufacturing services	M2M, automation, etc.

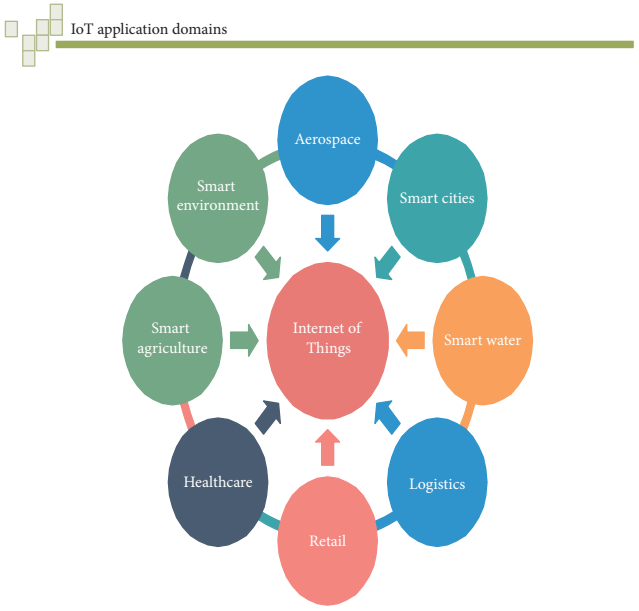

Figure 5: IoT applications.

4.5. Challenges in the Use of Blockchain with IoT. The integration of Blockchain with IoT is very beneficial as the capabilities and application domain of IoT can be increased considerably. However, the integration of different technologies can introduce some challenges in the network considering the different limitations of each network technology [33, 34]. Blockchain is an emerging technology and has various constraints, like massive storage requirements. IoT has its own constraints, like a massive amount of data are involved in this network; all of these constraints can impact technology integration.

Some of the challenges in the use of Blockchain technology along with IoT networks are scalability, storage, lack of skills, legal issues, and smart contracts [35].

Scalability and storage are already a challenge in Blockchain but in the context of IoT, they become a much greater challenge [36]. IoT network contains a large number of nodes and Blockchain scales poorly when there numerous nodes in the network.

IoT devices have low storage capacity but the distributed ledger contains memory as time passes, and with the increased number of nodes, it increases the memory.

Lack of skills is also a main challenge when Blockchain is integrated with IoT, as IoT is used almost in every field. Blockchain technology is new, and very few people know about this technology [9]. Many people think that Blockchain is only used in Bitcoin.

Blockchain is a new territory and connects with different countries without any legal or compliance precedents to follow, which is a serious issue for manufacturers and service providers. This challenge is also a major issue for integrating Blockchain with IoT.

5. Integration of Blockchain and IoT Technologies in Healthcare

The number of patients across the country is increasing day by day and with the increase in the number of patients, it has become difficult to provide full medical care. In the last few years, the quality of medical care has improved with the help of IoT and wearable devices [37]. Remote patient monitoring is the main modality to address healthcare issues. Wearable devices used for collecting and transferring data to hospitals, and IoT devices play an important role in remote patient monitoring [38]. The main aims of these devices are to provide important information such as breathing patterns of a person, blood glucose level, and blood pressure to health providers [39].

Healthcare devices that are used for data collection data can be categorized into four parts: (a) Stationary Medical Devices: these devices are used for specific physical locations, (b) Medical Embedded Devices: these devices are placed inside the human body, (c) Medical Wearable Devices: these devices prescribed by doctors, and (d) Wearable Health Monitoring Devices: these devices are worn on the body. The main motive of RPM is to secure the data that are targeted by hackers. To secure the data, Blockchain

technology is used. Blockchain helps to secure the data from many cyberattacks by using the concept of decentralization. Blockchain also authenticates the data with smart contracts.

Healthcare is an IoT system application that requires unique additional requirements like interoperability and data transfer for securing the patient's information. The term interoperability means the process of sharing data with other sources. The concept of centralization includes the limitation to achieve interoperability. IoT is based on centralization, where the data gets stored in the cloud where the data is not secured. Blockchain integrated with IoT can overcome the security issues faced by healthcare applications [40]. Many experiments are already done in Blockchain regarding healthcare [41].

6. Various Applications of Blockchain and IoT in Healthcare

Blockchain helps to maintain and share the patient's medical record with hospitals and health providers. There are many applications of healthcare:

6.1. Drug Traceability. Drug traceability is usually done in a centralized manner in which some conditions like privacy, authentication of data, and flexibility of the system are not achieved [42]. To overcome issues of drug traceability, many decentralized models have been implemented. For authenticity and privacy of traceability data, a Blockchain-based system is proposed [43] called Drugledger. Drugledger integrates Blockchain with the drug supply chain for drug traceability. Drugledger maintains two flows of drugs: The physical flow of drugs in combination with the supply chain and the information that flow goes to the drug ledger network in the form of a drug chain network. This system changes the previous traditional architecture by separating service providers into three different parts: CSP, certificate service provider; QSP, query service provider; ASP, anti-attack service provider. **Limitations**: the drug traceability scenario, which is shown in this paper, is very simple, but the real-life scenario is more complex. **Future work:** to compare the proposed framework of drug traceability with some existing frameworks and find out which framework is more secure in case of DoS attacks.

IoT when integrated with blockchain makes the system more secure and reliable. In the field of healthcare, many frameworks were proposed regarding the traceability of drugs or patient monitoring systems. Authors in [44] introduce a framework to avoid drug fraud by tracking each drug in the supply chain. The main aim is to reduce counterfeit drugs using Blockchain. The main two technologies that are used to improve the visibility and traceability of drugs are Blockchain and RFID. **Limitations:** Implementation is not done.

For the transparent flow of drugs, the Gcoin Blockchain model (G stands for global governance) is proposed in [45], and this model also changed the drug supply chain system from regulating to surveillance and inspection of drugs, which means the government model combines with DAO (Decentralized autonomous organization). Blockchain is used to build an atmosphere where two parties can trust each other. There are many ways to implement Blockchain but, in this paper, Consortium proof of work is used to implement Gcoin Blockchain. Gcoin Blockchain tracks every drug in the same way as the Blockchain tracks in bitcoin. It builds trust between buyers and sellers. The main aim of Gcoin is to improve the efficiency of data, which is exchanged. **Future work:** analysis of regulatory impact and system simulation test is to be done in the future.

In India every year, many lives are at risk due to the consumption of fake medicines. A framework is proposed [46] to detect fake medicines in the system of the supply chain. This proposed framework is based on Hyperledger fabric architecture, where one PC is serving as the client, and five computers are used for ordering service. This system is purely based on Blockchain technology. The supply chain of medicines from drug manufacturing to wholesale local drug distributors and distributors to hospitals/clinics and retail shops is managed using Blockchain, which helps to track the fake medicines. This system was tested in various scenarios like stolen drugs, audits of drugs in-retailer or distributor, fake drug distribution. The proposed system compares their performance with another existing system in many parameters like resistance against single point of failure, counterfeit medicine detection, diverted medicine detection, medicine shortage detection, ease of operations, involvement of stakeholders, transparency, privacy, security, and immutability. Limitations: the proposed system does not have the ability to find and eliminate out the consumption of unauthorized medicines. Future work: this particular framework can be implemented in many domains like courier consignment tracking and election management.

In the case of drugs, a very common threat is that the drug which is manufactured is not received by the pharmacy and is replaced by a counterfeit in the supply chain method. The supply chain method does not have the ability to trace the culprit who is responsible for the drug replacement because information is deleted in each step. India manufactured most of the counterfeits in 2006, and it is estimated that around 35% of fake drugs were sold all over the world. To overcome these problems, authors [47] introduced a framework using the Blockchain. Blockchain is more transparent because even if a single-user makes a change or does any transaction, it will reflect to all the users. Blockchain is the concept of decentralization and there is no need for the central authority to verify the transaction. Implementation: the authors analyses the result on two platforms: Ethereum and Hyperledger. Blockchain using Ethereum: in Ethereum Blockchain, every operation requires fees. Miner is given money to execute the transaction and to maintain the Ethereum network. There is no need of Know your Customer (KYC) in this process, which results in a blind spot which tells us about the person who is operating the account. It takes a long time. Ethereum can handle 100 transactions per second (TPS), which is not feasible. Blockchain using Hyperledger: this process does not require fees, which makes it feasible for the manufacturer to make the transaction, and is available for KYC. Certificate authority in this process manages the identity. Hyperledger is the private Blockchain and takes care of throughout and transaction per second.

6.2. Patient Monitoring/Electronic Health Record (ERH). According to the International Organisation of Standardization, electronic health records store the patient data in a digital format, and the data are exchanged securely and only accessible by authorized authority [48, 49]. It contains private information regarding a person's health issues, and its main objective is to maintain and provide efficient service to the patient. There are many Blockchain-based EHR systems:

(a) Medrec**:** it is a decentralized record management model. It is a Blockchain model used for authentication, confidentiality, and data sharing [50, 51]. This model uses all the features of Blockchain-like smart contracts and the concept of decentralized data.

(b) Data sharing through Gem health network: Sharing of data is a big problem in the traditional systems, so to overcome such issues and to provide a secure environment while transferring user's data, Gem health network is used [51, 52]. This network is used to remove the concept of centralization of data and include the concept of decentralization. Gem health network framework is fully based on the concept of decentralization, and the main feature of Gem network is that all the record under this network is transparent, and any alteration with the record will be reflected to all the users of this network.

(c) Healthbank: it is a platform that stores and securely manages health information. This is a new start-up that also provides some incentives to patients for their contribution [52].

(d) OmniPHR: public health record (PHR) provides a facility for patients to access their data. This model is developed to update the records and to differentiate between Electronic health records and PHR [40].

A real-time Blockchain-based patient monitoring system is proposed in [53] using smart contracts. This system secures the data and uses the patient's data in a more relevant form. Smart contracts are used for security purposes and to evaluate the information collected by patient's IoT healthcare devices. Private Blockchain is used for fast transactions. Limitations: time is the main aspect, but there is some delay while verifying each block in the Blockchain. Maintaining the security of each node is also a main challenge. Future work: implementation of the proposed system is done on Ethereum Blockchain. In the future, Hyperledger and other Blockchain platforms will be used on this proposed framework.

Blockchain, when integrated with IoT, always gives a more secure network. There are some Blockchain features due to which IoT network becomes more secure, such as the concept of distributed ledger, public-key cryptography, and the consensus algorithms. Transparency of data is achieved by the decentralization concept of the Blockchain. For a remote patient monitoring system, a framework is proposed in [54] using Blockchain technology. Before proposing the framework, this paper discussed the positive and security benefits of the Blockchain when integrated with IoT and also discussed the practical obstacles that are generated when the Blockchain integrates with IoT. The framework works to try to remove the obstacles and gives a more secure network. Future work: to implement this model for testing the performance.

To provide health services, there are many facilities such as hospitals, pharmacies. Dangerous diseases usually claim human lives. To provide the resources to the patient on time, it is compulsory to continuously monitor the patient`s health. For continuously monitoring patient health, there are many frameworks in which patients are required to wear IoT-based monitoring devices. These devices collect their medical data and store it in the cloud. Healthcare now has become very popular, but the main issue is to provide security to the patient's data. There are many cases registered against healthcare data leakage when storing the data in the cloud [55]. Many countries are very particular about the privacy and security of patient's data. In Europe, Health Insurance Portability and Accountability Act (HIPAA) is used to protect the patient data and guarantee transferring of medical data in a secure manner [56]. To monitor the vital signs of the patient, a framework is proposed in [51] to secure the medical data. The purpose of the framework is based on the healthcare devices that read the vital signs of patients and share that information to the authorized doctors and hospitals in a secure Blockchain network. Hyper Caliper, developed by the Linux Foundation, is used to evaluate the performance in terms of transaction per second, transaction latency, and resources that are used. Future work: interoperability is also an important aspect of the healthcare system. Future work will involve checking the performance of the interoperability of the system with different IoT frameworks.

There are many applications where IoT is used. Healthcare monitoring is also an application of IoT where devices are interconnected to each other, and the data sharing and collection should be done in a secure environment. Fabric Hyperledger, a Blockchain framework, is proposed in [57] to secure the healthcare application. Using the Blockchain technology, the proposed framework provides distributed and secured access to all the data collected by the devices. Limitations: it does not cover all the security aspects of IoT. It does not consider the attacks in IoT. Future work: to create a more secure health monitoring framework, the proposed framework has to implement more functionality based on attacks.

IoT helps to monitor the patient's health using different sensors. The information collected from the human body via sensors are then processed and analyzed. The data that are transferred from the sensor to the cloud have threats of privacy, tempering of data, and data manipulation. To solve these issues, the author in [58] has proposed an architecture to combat all these threats by combining Blockchain and IoT. Each block in the Blockchain consists of the patient's private data. This paper simply applies the Blockchain for secure and transparent data transfer between the hospital and patient. Limitation: this paper describes the basic work

of how Blockchain makes the system more efficient but does not provide the exact example for securing the health records.

6.3. Managing Medical Records and Other Data. The traditional method of monitoring medical records needs to be changed. Now, the use of the Internet in the healthcare system makes it more efficient. Internet smart objects make it easy to store and process the data in any format like audio, images, or text. To efficiently use the medical resources and to enhance the patient's health quality, IoT is used in healthcare. Using the healthcare application with IoT addresses many drawbacks like security, privacy issues, and other issues like doctors recommending unnecessary medicines and tests to patients with a profit motive. To prevent these healthcare issues, a framework of IoT for healthcare using the Blockchain is proposed in [59]. In this framework, a hash of each data is generated to prevent the data from alteration. This framework assures the patient that any malpractices regarding the medical records cannot be done. It focuses on the transparency of records and the security of data. Limitation: transaction time is a very important aspect of healthcare applications. This framework does not focus on transaction time. Future work: this framework ensures that no illegal practices or malpractices are done but does not experiment with the cost required during the communication. So, in the future, an experiment on the cost required in communication will be performed.

To secure data that is transferred from IoT devices in the healthcare system is proposed in [60] using Blockchain technology. Blockchain technology helps to identify users who are associated with the transaction. Blockchain technology is used in healthcare for the privacy and security of data and to provide accurate and proper data of patients to doctors. **Limitations:** implementation is not done in this paper. **Future work**: To implement the framework and to check whether the framework is secure or not.

IoT is important in every field where the applications require fast results, collection of data, storage of data, and efficient usage of that data. Now, IoT is also updated by healthcare applications. Various IoT-based wearable devices are used in healthcare applications. But, these devices are not secure, as there is a chance of data leakage or data misuse. To reduce this risk, IoT technology is connected with Blockchain technology to provide a more secure network. To reduce the various attacks, such as DOS, modification of data, mining attacks, and storage attacks in healthcare, a system is proposed [61]. A hybrid structure was implemented to ensure the security and privacy of data. This system is called hybrid because Blockchain is combined with the private key, public key, and advanced cryptographic functions. This system consists of five parts: (1) overlap network: all the nodes in the network should be verified and certified; (2) cloud storage: data of the users are grouped in the form of blocks, and the system does not need any third party for storage; (3) healthcare providers: these companies provide service when they receive an alert of health issues; (4) smart contract: these are the conditions that are set for the particular framework; and (5) healthcare wearable IoT devices: these are the devices that continuously monitor the patient and collect all its information. Limitations: Blockchain technology is resource-constrained so it is not suitable for many IoT devices. There are some more issues in Blockchain-technology-related costs; it requires high bandwidth and more computational power. Future work: To explore more security issues and to provide the implementation of this conceptual framework.

All the nodes in healthcare when integrated results in the healthcare IoT system. It ensures an efficient delivery process of patient data. But, it does not give security to a trustworthy network. A trustworthy framework of IoT healthcare is proposed in [62] where smart contracts authenticate and validate the other nodes. The framework is named as decentralized interoperability trust model for healthcare IoT. This framework is divided into layers: In the first layer, all the data are collected and changes are made in the data sensor, and actuators are used in this layer. The second layer is used to transmit the data through the gateway and network. The third layer is the health edge layer, and this layer is in between the technology and application levels. The last layer is the application layer. Future work: artificial intelligence and deep learning technology are used in training states to authenticate and identify the pattern to enhance the framework.

Table 7 lists out various proposed frameworks in the literature using Blockchain and IoT technologies for strengthening the capabilities of the Healthcare sector.

7. Challenges of Using Blockchain in Healthcare-Derived Industrial IoT

The main challenges in the use of Blockchain Technology, along with IoT in the Healthcare and Medical Sector, are as follows:

7.1. Interoperability. Healthcare interoperability means exchanging information with each other in the Blockchain network. It is the main challenge due to the large and varied providers and due to its large open nature [63]. There can be different players like hospitals, insurance companies, physicians, private doctors, etc. In the Healthcare sector, ensuring proper interoperability among them can be a challenge.

7.2. Security. As the concept of decentralization is more secure, there are also some disadvantages associated with it. As in decentralized Blockchain, the data are distributed in a public ledger, which can cause privacy leakage. Blockchain provides an atmosphere where people know or trust each other and can securely share data. However, in some scenarios, it can fail—for example, if 51% of the consensus nodes become malicious. Many patients can be uncomfortable in sharing their personal medical information due to security reasons [63].

Table 7: Various proposed frameworks for healthcare based on Blockchain and IoT

Reference	Application of Blockchain	Type of Blockchain used	Advantages	Limitations	Simulation parameters used	Future work
[61]	Managing medical records and other data	Private and public Blockchain	To reduce the various attacks, such as DOS, modification of data, mining attack and storage attack, in the healthcare system	Blockchain technology is resource-constrained, so it is not suitable for many IoT devices. There are some more issues in Blockchain technology-related costs; it requires high bandwidth and more computational power	—	To explore more security issues, and implementation is done to provide some real work
[40]	Patient Monitoring/ Electronic Health Record (ERH)		Blockchain integrated with IoT overcomes the security issues that are faced by healthcare applications	Many issues are not considered yet such as mining incentives, and there are some specific Blockchain attacks, which halt the entire system	—	
[43]	Drug traceability		To overcome the issue of privacy and authentication of data, increase the flexibility of the system	The drug traceability scenario, which is shown in this paper, is complex	Traceability data authenticity and privacy	To make the system more prone to DoS attacks while comparing with the traditional system
[44]	Drug traceability	Public Blockchain	The integration of IoT with Blockchain makes the drug supply chain system more secure and reliable and avoids any drug fraud by tracking each drug in the supply chain	Implementation is not done	Privacy, limiting theft and diversion	
[45]	Drug traceability	—	Improves the efficiency of data exchange	—	Information infrastructure breakdown, information delays, and transparency of drug supply chain	Analysis of the regulatory impact and system simulation test is done in the future
[46]	Drug traceability	—	Detects fake medicines in of supply chain	The consumption of unauthorized and Ingenium medicines not to be eliminated in this system	Resistance against single point of failure, counterfeit medicine detection, diverted medicine detection, medicine shortage detection, ease of operations, involvement of stakeholders, transparency, privacy, security, immutability	This particular framework can be implemented in many domains like courier consignment tracking, election management

Table 7: Continued.

Reference	Application of Blockchain	Type of Blockchain used	Advantages	Limitations	Simulation parameters used	Future work
[53]	Patient Monitoring/ Electronic Health Record (ERH)	Private Blockchain	The system secures the data and uses the patient's data in a more relevant form	Time is the main aspect, but there is some delay while verifying each block in the Blockchain. Maintaining the security of each node is also the main challenge	Speed, privacy, transparency, traceability, availability, confidentiality	Implementation is done using the Ethereum Blockchain; to explore more implementation parts use hyperledger
[59]	Managing medical records and other data	Public	It ensures the patient that any illegal activity cannot be done. It focuses on the transparency of records and the security of data	Transaction time is a very important aspect of healthcare applications. This framework does not focus on transaction time	Number of nodes in a CRN, grid facet, transmission range data size or users request, simulation time	This framework experiments with the illegal activities done on IoT devices but does not experiment with the cost required during the communication. So, in the future experiment on the cost required in communication is to be done
[62]	Managing medical records and other data	Public	The interoperability trust model for healthcare IoT	Identification of patterns of symptoms, which are obtained from wearable devices cannot be done	Scalability, data integrity, mutual authentication, trustworthiness, privacy	Artificial intelligence and deep learning technology are used in training states to authenticate and identify the pattern to enhance the framework
[60]	Managing medical records and other data	Variation of the Blockchain is used in personal health care and external Blockchain for record management	An uplifting of society with accurate and efficient healthcare	Implementation is not done	—	To implement the framework and to check whether the framework is secure or not
[54]	Patient Monitoring/ Electronic Health Record (ERH)	Cannot prefer any particular Blockchain	Try to remove the obstacles and give a more secure network	Implementation is not done	—	To test the performance of the framework, implementation is necessary in the future
[57]	Managing medical records and other data	Medical devices Blockchain consultation Blockchain	Paper works on the security issues	It cannot cover all the security aspects of IoT. It cannot consider the attacks in IoT	—	To make a more secure framework of health monitoring, this proposed framework has to implement more functionality based on attacks
[51]	Patient Monitoring/ Electronic Health Record (ERH)	Public Blockchain	Healthcare devices that read the vital signs of patients and share that information with the authorized doctors and hospitals in a secure Blockchain network	Lack of communication between the server and devices	Energy consumption and efficiency	Interoperability is also an essential aspect of the healthcare system to check the interoperability performance of the system with different IoT frameworks

7.3. Scalability and Storage Requirement Handling. It is not practically possible to maintain the data of every individual. The medical record is usually in the form of documents, images, and lab reports. Digital storage of the medical records of numerous patients will require colossal storage capacity. The medical transactions of every individual stored in a distributed manner with the same record stored in more than one location will require huge storage capacity and could affect the healthcare system [64].

7.4. Lack of Standardization. Blockchain is a trending technology and is adopted in many countries. In domains and networks where the concept of security, trust, and trackability is involved, the Blockchain is used. Proper standardization of protocols, technologies, etc., is very important. Aspects like what data, size, and format can be sent to the Blockchain, and what data can be stored in the Blockchain should be clearly defined [65, 66].

7.5. Hesitation among Hospitals and Related Entities in Sharing Information. Many hospitals can be reluctant to share their patient-related and other medical records, such as in for-profit situations, as they will want to charge different fees from different customers. Similarly, hospitals and insurance companies can be reluctant to share their data, as it can be competitively advantageous for the hospitals to keep the fees-related data with themselves. It is essential to build trust between the parties and convince them to share their data for a better healthcare system [67].

7.6. Hesitation and Lack of Trust among the Patients to Share Their Medical History. Trust building among one of the key stakeholders, the patients, is very important for the success of this technology-driven medical and healthcare system. Many patients can be reluctant and hesitant to share and disclose their medical records in the public domain with third-party entities. So, it is very much required to build trust and confidence among the patients regarding the security and privacy aspects of this whole Blockchain and IoT-driven healthcare system.

7.7. Lack of Skills among Doctors and Medical Practitioners. Asking doctors and other medical practitioners to shift from paper to technology can be a big challenge. The use of electronic records and prescriptions instead of paper-based prescriptions can be a challenge for many. For instance, doctors usually do not fill the unnecessary fields in their day-to-day practice while filling some form. However, in the case of electronic records, doctors cannot omit the fields marked as mandatory. Similarly, relying on technologies like Blockchain and IoT for remote monitoring can raise question marks among many doctors regarding their accuracy and efficiency. This technology-driven healthcare's accuracy, efficiency, and performance will depend on doctors' skills and training. So, before bringing these technologies into practice, proper training and required skills need to be imparted to the doctors to build confidence in using these technologies.

Table 8: Summarizes the list of abbreviations used in this survey.

List of abbreviations	
Abbreviations	Full-form
IoT	Internet of things
CIA	Confidentiality, Integrity, and Availability
RFID	Radiofrequency identification
DOS	Denial of Service
ERP	Enterprise Resource Planning
SWAMP	The smart water management platform
EMR	Electronic medical records
POS	Proof of stake
POW	Proof of work
PSN	Pervasive social network
FHIR	Fast health interoperability resources
POA	Proof-of-activity
POB	Proof-of-burn
POV	Proof-of-validation
WSN	Wireless sensor network
IDPS	Intrusion Detection/Prevention System
DDoS	Distributed denial of service
LAN	Local area network
GPS	Global positioning system
NFC	Near Field Communication
WiFi	Wireless fidelity
SDN	Software-Defined Networking
QoS	Quality of Service
PoS	Point of Sale
M2M	Machine to Machine
V2V	Vehicle to Vehicle
NDN	Named data networking

7.8. Data Ownership and Accountability. Data ownership and accountability are other challenges in deploying Blockchain and IoT technologies in the Healthcare sector. Who will hold the data, who will grant permission to share people's private health-related data, and who will have the ownership are the main questions?

8. Conclusion

In Today's world, IoT technology is implemented in every field like agriculture, healthcare, smart cities, etc. In the field of healthcare, IoT is brought into use for applications like monitoring of the patient's health regularly, drug traceability, etc. However, there exist various security issues in IoT, which can be solved by integrating IoT with the Blockchain. The Blockchain is a decentralized technology that can be used to enhance the security of the system. Blockchain technology along with healthcare ensures that patients' sensitive health-related records remain safe from any type of tampering and leakage.

In this article, an attempt was made to enumerate different possible ways with which the IoT technology along with the Blockchain can be integrated into the Healthcare sector to improve the overall performance and to strengthen the current Healthcare sector. Three major application areas

of healthcare, viz. (a) remote monitoring of patient`s health, (b) drug`s traceability, and (c) medical records management, where IoT and Blockchain technologies have their applicability were explored in detail. Also, various possible challenges and issues in the deployment of these two revolutionary technologies, i.e., IoT and Blockchain, in the Healthcare sector were explored and discussed.

Based on this study, it can be clearly said that these two technologies have a huge potential in the Healthcare sector, and once integrated will revolutionize the whole Healthcare sector. Table 8 provides the list of abbreviations used throughout this survey article.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. M. Kizza, "Internet of things (iot): growth, challenges, and security," in *Guide to Computer Network Security*, pp. 517–531, Springer, Berlin, Germany, 2017.

[2] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to IOT," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

[3] M. A. J. Jamali, *IoT Architecture Towards the Internet of Things*, pp. 9–31, Springer, Berlin, Germany, 2020.

[4] J. Wang, W. Chen, L. Wang, Y. Ren, and R. Simon Sherratt, "Blockchain-based data storage mechanism for industrial internet of things," *Intelligent Automation & Soft Computing*, vol. 26, no. 5, pp. 1157–1172, 2020.

[5] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[6] M. B. Hoy, "An introduction to the blockchain and its implications for libraries and medicine," *Medical Reference Services Quarterly*, vol. 36, no. 3, pp. 273–279, 2017.

[7] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[8] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen, and H.-J. Kim, "Blockchain-based trusted electronic records preservation in cloud storage," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[10] Q. Wang, F. Zhu, S. Ji, and Y. Ren, "Secure provenance of electronic records based on blockchain," *Computers, Materials & Continua*, vol. 65, no. 2, pp. 1753–1769, 2020.

[11] J. Cheng, J. Li, N. Xiong, M. Chen, H. Guo, and X. Yao, "Lightweight mobile clients privacy protection using trusted execution environments for blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2247–2262, 2020.

[12] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[13] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[14] Z. Zheng, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, Boston, MA, USA, December 2017.

[15] J. Mattila, *The Blockchain Phenomenon–The Disruptive Potential of Distributed Consensus Architectures*, The Research Institute of the Finnish Economy, Helsinki, Finland, 2016.

[16] J. Wang, W. Chen, L. Wang, R. Simon Sherratt, O. Alfarraj, and A. Tolba, "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.

[17] G.-J. Ra, C.-H. Roh, and I.-Y. Lee, "A key recovery system based on password-protected secret sharing in a permissioned blockchain," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 153–170, 2020.

[18] R. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of the 2012 10th International Conference on Frontiers of Information Technology*, IEEE, Islamabad, Pakistan, December 2012.

[19] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. Braynard, "Networking named content in CoNEXT," 2009.

[20] M. Amadeo, "Named data networking for IoT: an architectural perspective," in *Proceedings of the 2014 European Conference on Networks and Communications (EuCNC)*, IEEE, Bologna, Italy, June 2014.

[21] R. Duan, X. Chen, and T. Xing, "A QoS architecture for IOT," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, IEEE, Liaoning, China, October 2011.

[22] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for iot interoperability," in *Proceedings of the 2015 IEEE International Conference on Mobile Services*, IEEE, New York City, NY, USA, July 2015.

[23] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Procedia Computer Science*, vol. 52, pp. 1028–1033, 2015.

[24] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[25] H. Chen, X. Jia, and H. Li, "A brief introduction to IoT gateway," in *Proceedings of the IET International Conference on Communication Technology and Application (ICCTA 2011)*, Beijing, China, October 2011.

[26] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of things (IoT): a literature review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015.

[27] S. Al-Sarawi, "Internet of things (IoT) communication protocols," in *Proceedings of the 2017 8th International Conference on Information Technology (ICIT)*, IEEE, Amman, Jordan, May 2017.

[28] I. Lee and K. Lee, "The internet of things (IoT): applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[29] M. Shabaz and U. Garg, "Predicting future diseases based on existing health status using link prediction," *World Journal of Engineering*, 2021.

[30] Z.-K. Zhang, "IoT security: ongoing challenges and research opportunities," in *Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, IEEE, Matsue, Japan, November 2014.

[31] A. Dorri, "Blockchain for IoT security and privacy: the case study of a smart home," in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops)*, IEEE, Kona, USA, March 2017.

[32] R. Porkodi and V. Bhuvaneswari, "The Internet of Things (IoT) applications and communication enabling technology standards: an overview," in *Proceedings of the 2014 International Conference on Intelligent Computing Applications*, IEEE, Washington, DC, USA, March 2014.

[33] B. Le Nguyen, E. Laxmi Lydia, M. Elhoseny et al., "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87–107, 2020.

[34] C. Li, G. Xu, Y. Chen, H. Ahmad, and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Computers, Materials & Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[35] H. Chen, W. Wan, J. Xia et al., "Task-attribute-based access control scheme for IoT via blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2441–2453, 2020.

[36] H. F. Atlam, fnm au, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with internet of things: benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018.

[37] S. Parvathavarthini, "An improved crow search based intuitionistic fuzzy clustering algorithm for healthcare applications," *Intelligent Automation and Soft Computing*, vol. 26, no. 2, pp. 253–260, 2020.

[38] V.-S. Naresh, "Internet of things in healthcare: architecture, applications, challenges, and solutions," *Computer Systems Science and Engineering*, vol. 35, no. 6, pp. 411–421, 2020.

[39] P. Yu, Z. Xia, J. Fei, and S. Kumar Jha, "An application review of artificial intelligence in prevention and cure of COVID-19 pandemic," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 743–760, 2020.

[40] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[41] F. Ajaz, "COVID-19: challenges and its technological solutions using IoT," *Current Medical Imaging*, 2021.

[42] J. Li, J. Cheng, N. Xiong, L. Zhan, and Y. Zhang, "A distributed privacy preservation approach for big data in public health emergencies using smart contract and SGX," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 723–741, 2020.

[43] Y. Huang, J. Wu, and C. Long, "Drugledger: a practical blockchain system for drug traceability and regulation," in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, Halifax, NS, Canada, January 2018.

[44] V. Ahmadi, "Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain," in *Proceedings of the 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ)*, IEEE, Miami, FL, USA, February 2020.

[45] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-w. Liao, "Governance on the drug supply chain via gcoin blockchain," *International Journal of Environmental Research and Public Health*, vol. 15, no. 6, p. 1055, 2018.

[46] P. Pandey and R. Litoriya, "Securing E-health networks from counterfeit medicine penetration using Blockchain," *Wireless Personal Communications*, pp. 1–19, 2020.

[47] M. M. Akhtar and D. R. Rizvi, "Traceability and detection of counterfeit medicines in pharmaceutical supply chain using blockchain-based architectures," in *Sustainable and Energy Efficient Computing Paradigms for Society*, pp. 1–31, Springer, Berlin, Germany, 2021.

[48] K. Häyrinen, K. Saranto, and P. Nykänen, "Definition, structure, content, use and impacts of electronic health records: a review of the research literature," *International Journal of Medical Informatics*, vol. 77, no. 5, pp. 291–304, 2008.

[49] Y. Liu, "A mobile cloud-based eHealth scheme," 2020, http://arxiv.org/abs/2004.11842.

[50] A. Azaria, "Medrec: using blockchain for medical data access and permission management," in *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, IEEE, Vienna, Austria, August 2016.

[51] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, 2020.

[52] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," in *Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)*, IEEE, Munich, Germany, September 2016.

[53] K. N. Griggs, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, 2018.

[54] A. D. Dwivedi, "Optimized blockchain model for internet of things based healthcare applications," in *Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, Budapest, Hungary, July 2019.

[55] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[56] J. K. O'herrin, N. Fost, and K. A. Kudsk, "Health Insurance Portability Accountability Act (HIPAA) regulations: effect on medical record research," *Annals of Surgery*, vol. 239, no. 6, p. 772, 2004.

[57] O. Attia, "An Iot-blockchain architecture based on hyperledger framework for healthcare monitoring application," in *Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, Canary Islands, Spain, June 2019.

[58] P. Hemalatha, "Monitoring and securing the healthcare data harnessing IOT and blockchain technology," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2554–2561, 2021.

[59] P. Rathee, "Introduction to blockchain and IoT," *Studies in Big Data*, pp. 1–14, 2019.

[60] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT)*, IEEE, PyeongChang, Korea, February 2019.

[61] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[62] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable

healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[63] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, *Geospatial Blockchain: Promises, Challenges, and Scenarios in Health and Healthcare*, BioMed Central, London, UK, 2018.

[64] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *Proceedings of the ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, MA, USA, September 2016.

[65] C. Stagnaro, *White Paper: Innovative Blockchain Uses in Health Care*, Freed Associates, CA, USA, 2017.

[66] T. Kumar, "Blockchain utilization in healthcare: key requirements and challenges," in *Proceedings of the 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom)*, IEEE, Ostrava, Czech Republic, September 2018.

[67] R. Beck, "Beyond bitcoin: the rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.