Health Services and Outcomes Research Methodology (2024) 24:112–139
https://doi.org/10.1007/s10742-023-00306-1

Privacy preservation of the internet of medical things using blockchain

Anu Raj[1] · Shiva Prakash[1]

Received: 10 October 2022 / Accepted: 11 March 2023 / Published online: 28 March 2023

Abstract

Nowadays, the Internet of Things (IoT) is used in every domain, especially in the healthcare system it plays a very important role in our life and made our life easier by providing various facilities in every area. On the Internet of Medical Things (IoMT), IoT devices collect real-time data from patients and send it to the cloud through the Internet. These gathered data are extorted to centralized processing and computational power. Centralization can lead to a single point of failure, data modification, snooping, security, and privacy evasion. Blockchain can resolve such issues by providing decentralized computational power and better storage capacity for IoT data. Therefore, integrating IoT and blockchain technologies can be an intelligent way to implement a decentralized IoT-based smart healthcare system. We find that integration of the blockchain and IoT is persuasive and can cause remarkable transformations across the healthcare system. We discussed blockchain and its applicability in the healthcare industry. The paper explores blockchain's dimensions, making the innovative healthcare system more secure and stable. We provide a comparative analysis of well-known recent research on IoT-based smart healthcare system security using blockchain based on different parameters such as architecture, data integrity, medical information sharing, distributed electronic health records, patient encryption key, access control, hardware implementation, etc. The paper focuses on the current security issues in IoT-based smart healthcare systems, architectures, taxonomy, and research gap and their possible solutions we point out various research challenges that should be considered before the deployment of a blockchain network in an IoT setting. This paper will be helpful to new researchers to get an overview of IoT-based healthcare system security.

Keywords Internet of medical things · Blockchain · Decentralization · Electronic medical record · E-healthcare system

✉ Anu Raj
anu.raj10@yahoo.com

Shiva Prakash
shiva.plko@gmail.com

[1] Department of Information Technology and Computer Application, Madan Mohan Malaviya University of Technology, Gorakhpur, India

1 Introduction

Nowadays, the Internet of Things (IoT) plays a vital role in every aspect of human life. IoT devices gather data from patients and send it to the hospital for other medication; meanwhile, these collected data are extorted to centralized processing and computational power. Because centralization can lead to a single point of failure, data modification, snooping, security evasion, etc. (Leible et al. 2016) can resolve such issues by providing decentralized computational power and better storage capacity. It is a technology with a public ledger for storing data, tracking assets, etc. It has many applications in healthcare and as well other fields. It strengthens e-health applications security, security monitoring devices security, recording and exchanging e-media records, medical trial data, remote health monitoring records, etc. Therefore, integrating IoT and blockchain technologies can be an intelligent way to implement a decentralized IoT-based smart healthcare system (Reyna et al. 2018). Combining IoT and Blockchain drives a high impact on the healthcare industry. Blockchain additionally provides security, durability, and a trustless foundation. The Healthcare system is another area that impacts human lives. Technological development has always been a critical issue that needs to be uplifted in each viable way. Blockchain is a technology in which a ledger is used for storing vast amounts of data. The details of every accomplished transaction are recorded in a distributed block that shares all the blockchain network's dynamic systems. It efficiently records every transaction on the distributed peer-to-peer network, having saved information co-owned by all participating systems within the network. Blockchain offers an immutable, relied upon, and impervious platform for a couple of entities to alternate data/assets, collaborate, and operate transactions. All the dynamic systems have to reach a consensus by applying a consensus algorithm before accepting a block into the chain. Various consensus algorithms are Delegated Proof-of-Stake (DPoS), Proof- Stake (PoS), Proof-of-Work (PoW), and Practical-Byzantine-Fault-Tolerance (PBFT) (https://www.section.io/engineering-education/blockchain-consensus-protocols/). The Healthcare system has always been a critical issue that needs to be uplifted in each viable way with technological development.

The Industrial Internet of Things (IIoT) is one of the most significant applications of IoT in industries that interconnect the automation system with various kinds of enterprises, planning, and product lifecycle at a broad scale in IoT applications. Industry 4.0 transforms industrial processes using multiple technologies such as smart devices, communication, computational processing, etc. (Lampropoulos et al. 2019). Cyber-Physical Systems (Gupta et al. 2020), Cloud Computing, IoT, Machine Learning (Tanwar et al. 2020), Data Analytics, etc., are various technologies that use different drivers necessary for industrial transformation. The concept of industry 4.0 is used in healthcare 4.0, which utilizes numerous industrial IoT concepts to implement secure and reliable smart healthcare systems (Bhattacharya et al. 2020). It incorporates the IoT, cloud computing, IIoT, deep learning, virtual reality healthcare system, augmented reality, fog computing, artificial intelligence, etc. IoT is a group of various electronic things or devices connected over the Internet in a small geographic area such as in the healthcare system. A medical specialist can deal with numerous patient records, medical clinic hospital records, etc. At the same time, IIoT assists with interconnecting these things or devices at a significant scale (For instance, the association of hospitals and emergency clinics across urban areas). IoT devices collect real-time data over the Internet (Raj and Prakash 2019). With cognitive computing and artificial intelligence, data collected over the cloud is analyzed and processed for e-healthcare systems (https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence).

The continuous developments in IoT have drastically extended the scope of the network between connected devices for real-time data access and sharing. Thus, IoT changed the industrial sector worldwide, from the education sector to the healthcare system; everything has changed from mechanical work to device-based work. The healthcare system has exhibited a fantastic performance by facilitating diagnostics strategies and effectively monitoring the action of the patients. With the advancement of blockchain, total access control, storage management, transaction, etc., all these services are provided by this technology. It shows tremendous hold and potential across numerous sectors like healthcare, supply chain, retail, finance, etc. The main problem that consistently arises in this sector is the security of information. A lot of stakeholders regularly use it for seeking different activities. In effect, IoT and blockchain innovations are intensely taken advantage of and utilized in many spaces, particularly for e-medical care frameworks. Integrating IoT and blockchain technologies in the healthcare system is useful in every aspect of healthcare.

2 Research contributions of this paper

i A detailed taxonomy of the smart healthcare system is described.
ii The advantages and disadvantages of the current security solutions regarding the smart healthcare system are discussed.
iii Finally, the open issues and challenges in IoT-based healthcare systems are presented.

The remaining paper is arranged as follows: Section II explores the taxonomy of smart healthcare system and their category and subcategory based on various parameters. Section III describes the literature review and comparative study of blockchain technology in it. Section VI explores the basic architecture of blockchain technology as well as Blockchain architecture for IoT-based smart healthcare systems using a different network. Section V describes IoMT deployment, considering possible blockchain solutions and analysis. Section VI describes the open challenges and issues in the IoMT. Section VII is about the conclusion and future direction.

3 Taxonomy of internet of medical things

The section illustrates the classification and subclassification of the research related to the smart healthcare system. Figure 1 explores the taxonomy of the smart healthcare system, which depends on the accompanying parameters: services, requirements, applications, and security.

3.1 IoT health-care services

3.1.1 Ambient assisted living (AAL)

This is a kind of service or product that empowers the advancements and the social surroundings to improve the life standard. It provides the privilege to older people in their living place. AAL provides independence and instant remote assistance whenever needed (Islam et al. 2020).

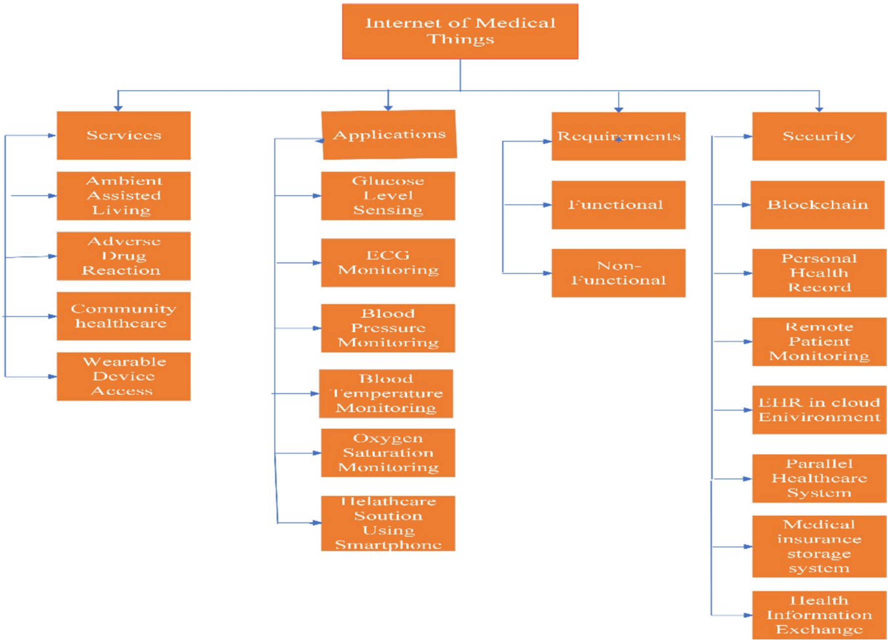

Internet of Medical Things
Services
Ambient Assisted Living
Adverse Drug Reaction
Community healthcare
Wearable Device Access
Applications
Glucose Level Sensing
ECG Monitoring
Blood Pressure Monitoring
Blood Temperature Monitoring
Oxygen Saturation Monitoring
Helathcare Soution Using Smartphone
Requirements
Functional
Non-Functional
Security
Blockchain
Personal Health Record
Remote Patient Monitoring
EHR in cloud Enivironment
Parallel Healthcare System
Medical insurance storage system
Health Information Exchange

Fig. 1 Taxonomy of the internet of medical things

3.1.2 Adverse drug reaction (ADR)

This reaction happened because of using the medicine recommended by the medical specialist. Thus, ADR is the consequence of utilizing an unusual quantity of medication or maybe the impact of blending two or more prescriptions.

3.1.3 Community healthcare (CH)

It is a service that makes its local network dependent on the Internet of things all across the all-healthcare centers in rural and urban areas.

3.1.4 Wearable device access (WDA)

In this service, several sorts of sensors trespassing to health are produced for various clinical usage (Rohokale et al. 2011), available for benefits of smart healthcare reliant upon remote sensor organization. They are additionally enough for the arrangement of similar services on IoT.

3.1.5 Embedded gateway configuration (EGC)

It is a combinational service that provides liability to the framework that is associated (explicitly linked with patients) in the network.

3.2 Healthcare applications

There are many applications of the e-healthcare system as we know that it provides a lot of smart healthcare services so customers and patients can accurately utilize the applications (Mosa et al. 2012). Blood glucose monitoring finds the difference in blood glucose levels and helps maintain a proper diet, proactive tasks, and medication time. ECG detects electrical movement in the human heart and incorporates the approximate of the straight-forward pulse and the revelation of imperative rhythm alongside the assurance of perplexing arrhythmias (Liu et al. 2019).

3.3 Smart healthcare requirements

Those requirements are needed while implanting the e-healthcare system. It can be considerably organized into functional and non-functional requirements, as shown in Fig. 1. The technical specifications manage the specific requirements of the medical services plan. The temperature monitoring system monitors body temperature, and the activity range of the thermometer, action frequency, and data collection methods may be unique.

3.4 Smart health-care security

In this part, several technologies are used for security purposes in the smart healthcare system, such as fog computing, edge computing, machine learning, blockchain, etc. Blockchain is one of the most secure technologies as it provides irreversible and unmodifiable records after completing the transaction. Electronic health record (EHR) Yanamadala et al. (2016) is a cloud data storage beneficial for good and suitable health record sharing in EHR with different medical healthcare suppliers. The personal health record is the medical health records management in which patients are regularly incapable of checking their information stored in the EHR database. Healthcare information exchange (HIE) consists of EHR data records and sharing of these records. Thus, significant personal health information is dismissed into cloud storage using a complicated validation system to stop undesirable information dissemination. Remote patient monitoring (RPM) provides a wide variety of services without human contribution, like RPM. Parallel healthcare systems (Wang et al. 2018) provide patient disease information in which diseases need cross-line clinical specialists from different backgrounds to work together utilizing technology. Multi-site clinical trials (Mutlicentre trial et al. 2021) are the patients' multiple medical trials. Telecare medication data framework gives patients and doctors to get medical benefits or information from a remote location. Therefore, the security of patients' data should be mainly concerned.

4 Literature review

This section is a detailed survey about the latest blockchain network and the Internet of Medical Things and its functionalities in the digital world. There is also a brief comparative analysis of pre-existing research papers on the blockchain.

Gross and Miller (2019) proposed a specific blockchain technology with an inbuilt healthcare system. This system enables patients to share their information securely, which resolves various research problems like authentication, data security, authorization, confidentiality, integrity, privacy, optimizing or data modification, etc. The optimization learning technique is a fundamental process in blockchain technology for data security. It instructed the healthcare management on data and made it suitable to share in protected surroundings that consider all legal aspects. The framework has mainly focused on information privacy and security, authentication, and developing patient trust in the system. Hameed et al. (2021) proposed a cloud-based medical decision support framework for the prediction as well as monitoring of disease with its seriousness level that has a combination of 5G administrations and blockchain advancements. This architecture assembles the information of patients using the wearable devices connected to the patient, and this information is recorded in a cloud server with all relevant clinical records. The collaboration of blockchain and 5G innovation empowers patients to send their data to cloud servers safely at a quick transmission rate with proficient response time. Chakraborty et al. (2020) explained a healthcare setup design infrastructure using blockchain. This work has developed a high abundance regarding the proficient method of serving and directing clinical medical services to the patients to keep up with the protection of the patient's information and the most common way of spreading out constant precise and confided-in information to the clinical experts. Hussien et al. (2019) analyzed various research papers related to Blockchain, and IoT explored from three databases IEEE, ScienceDirect, and Web of Science. Various medical terminologies are necessary to understand the efficacy of the blockchain-based IoMT. Koo et al. (2015) clarified that the frameworks inside the blockchain need to concur upon a consistent arrangement of systematic exchanges to extract the block and update the blockchain after some time interval. If a transaction is locked and stored in a block, reversing the completed transaction is impossible. The asymmetric key combination is used to validate the transactions in the blockchain; after this, no one can refuse their role in the transactions. Budida et al. (2017) proposed an intelligent framework that incorporates the healthcare sector and IoT technology. The proposed design fundamentally lies in generating and processing real-time data from intelligent devices or biosensors and following up on some appropriate feedback and suitable solution for the patients. Sivagami et al. (2016) presented an e-healthcare framework that coordinates the sensor's effectiveness and proposes human reaction for quick and convenient exhortation to the patients. The framework avails the use of WSN, RFID, and smart wearable devices that works with one another over a solitary stage to perform a specific task; like smart monitoring of the patient's environment, allotment of the patient to a specific ward, checking the patient's activities and report examination. It is dependent on the information given by the framework, then post the shared information. Viriyasitavat et al. (2019) discussed various emerging research challenges during the collaboration of one technology integrated with blockchain to implement new solutions using the blockchain. Towards industry 4.0 patterns, incorporation of blockchain advancement with cyber-physical systems, IoT, and other industrial advances are the base of digital economy-based applications, making a significant arrangement in the coming future. The study has investigated that many publications are expanding dramatically, incorporating different industry 4.0 points of view with adaptability, flexibility, security, and independence into innovative design and development of business work. Liang et al. (2017a) introduced an improvised blockchain system for data exchanging and combining with IoT in their proposed framework. It describes the work done by collaborating several elements like the patient, specialist, medical care suppliers, and healthcare coverage organizations on the sharing and coordinated effort in the healthcare system. A tremendous amount of information is generated every second, and a cloud server is utilized for the storage of efficient data processing as well as data integrity management. The proposed framework benefits medical healthcare research and storing personal health records, where data privacy and security are significant issues. Giungato et al. (2017) explained how blockchain is in very high demand for data security purposes where implementation and deployment are at the highest possible level. It is working in every domain on its applicability in multiple fields because of its enormous advantages. Most authors trust the traditional centralized framework because of its applicability and storage capacity. But the decentralized blockchain technology has overcome the centralized architecture. Sharma et al. (2020) discussed the concept of blockchain and their collaboration with the IoT to implement a secured smart healthcare system. The author described the blockchain dimensions, which have a decentralized network and smart contracts that will make the IoT-based smart healthcare system more secure and authentic.

Ehab Zaghloul et al. (2020) explained the relationship between bitcoin and the Internet of Things. The author discussed various applicability of blockchain in different research regions, including real-time trace data and reducing its duplicity in IoT applications, the medical services industry, etc. The author investigated the complete foundation of Bitcoin and its essential security. The author also depicted the hidden Bitcoin distributed organization security risks and Bitcoin data recording security.

Gatteschi et al. (2018) examined whether the acquisition of blockchain technology in various domains could work on their efficiency as well as quality or not. They described how blockchains had been utilized in different IoT applications. As shown in Fig. 2 there are three hospitals connected over the Internet to exchange medical data and

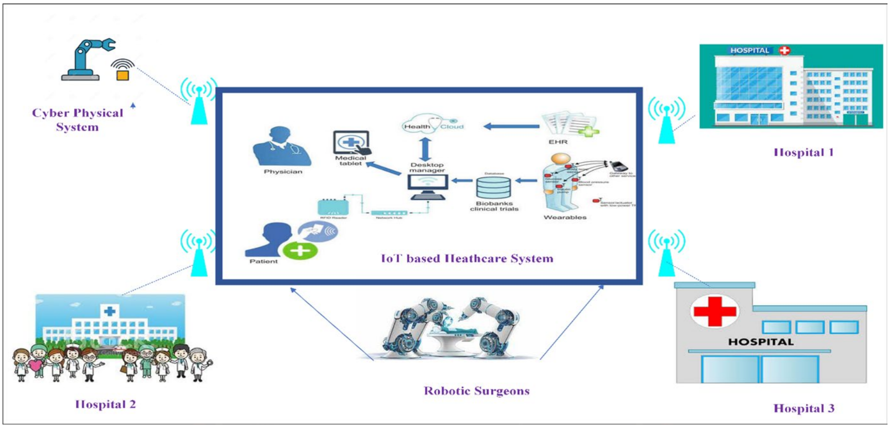


Fig. 2 IoT based on smart healthcare services

Table 1 Comparative study of research on IoT security using blockchain

Author	Year	Goal	Pros	1	2	3	4	5	6	7
Mettler et al. (2016)	2016	To discuss the Healthcare system security with blockchain	To feigned drugs in the pharmaceutical industry Database ownership are available	x	✓	✓	x	✓	x	x
Yli-Huumo et al. (2016)	2016	To summarise the latest research on blockchain technology	Given proper research gaps on the blockchain security in healthcare, Uses of decentralized environment for transactions;	x	✓	x	✓	✓	x	✓
Ahram et al. (2017)	2017	To propose the new revolution in blockchain technology	Proposed secured health information for patients with proper access rights and enhance robustness and validity of PHI	✓	✓	x	✓	✓	x	x
Weiss et al. (2017)	2017	To explain about a PHI using Blockchain technology	Decentralization and elimination of single point of failure; Timestamped as well as unmodifiable transactions	✓	✓	x	✓	x	✓	x
Zhang et al. (2017)	2017	To implement the advanced blockchain framework for healthcare system	Estimate metrics relevant to the blockchain concerning healthcare	✓	✓	x	✓	x	✓	x
Krieger et al. (2017)	2017	To elaborate the advanced blockchain architecture for smart healthcare system	Distributed databases and irreversible storage records and better computation power	✓	✓	x	✓	✓	✓	✓
Duan et al. (2017)	2017	To describe the blockchain applicability in educational sector	Use of auto evaluation software and design the framework Through digital signatures timestamps, Merkle tree	✓	x	x	✓	x	x	x
Radanovic et al. (2018)	2018	To describe the blockchain applicability in healthcare	Cost-effective, optimized, secured, and personal health records	x	✓	✓	✓	✓	✓	x

Table 1 (continued)

Author	Year	Goal	Pros	1	2	3	4	5	6	7
Zhang et al. (2018)	2018	To explore How Blockchain Are applicability indifferent field	Elimination of duplicity and manipulation in the land registry	x	x	x	✓	✓	x	x
Konstantinidis et al. (2018)	2018	To describe the Blockchain application-based Business in Industry 4.0	Explore blockchain applicability in various sector	x	✓	x	✓	x	x	x
Dave et al. (2019)	2019	Explain Blockchain applications in different sectors in Industry 4.0	The investigation is done from blockchain viewpoint using IoT applications	x	✓	x	✓	x	x	x
Monrut et al. (2019)	2019	Explore Blockchain applications in various fields	Blockchain applications and Issues are clarified exhaustively	✓	x	✓	✓	✓	x	✓
Hathaliya et al. (2020)	2020	security and privacy Issues in healthcare	Security and privacy research challenges are described	x	✓	x	✓	x	✓	x
Bodkhe1 et al. (2020)	2020	Taxonomy of blockchain based Industry 4.0 applications are discussed	The advantages and disadvantages of the recent security management using Industry 4.0 and Blockchain is mentioned	✓	x	✓	✓	✓	x	✓
Adarsh Kumar (2020)	2020	To implement a blockchain-based healthcare Framework	Enhance the working of blockchain-based decentralized applications for the framework of medical services	✓	✓	✓	✓	✓	✓	✓
Eman M Abou-Nassar et al. (2020)	2020	To introduce a Blockchain-based Trust System for IoMT	Trust architecture is used for Internet of things networks where a smart contract ensures verification of financial as well as Indirect Trust Inference Framework	✓	✓	x	✓	x	✓	x

Table 1 (continued)

Author	Year	Goal	Pros	1	2	3	4	5	6	7
Veeramakali et al. (2021)	2021	to diagnose the diseases through the optimal deep neural network model	This framework includes the orthogonal particle swarm optimization methodology for the private sharing of clinical records	✓	✓	x	✓	x	✓	x
Hussien et al. (2021)	2021	To introduce blockchain in the healthcare system	Reviews and evolutions are done regarding privacy and security, Case studies of telecare medicine information system	x	✓	✓	✓	x	x	✓
Xu et al. (2021)	2021	To review IoT security dependent on the blockchain	Worked on blockchain-embedded IoT security, approaches as well as recent issues	x	x	✓	✓	✓	✓	✓
Pradhan et al. (2021)	2021	to present a systematic overview of IoT-based healthcare systems and advancement applications, services, and enabling technologies	A comprehensive source of information regarding the different fields of application of HIoT	x	✓	x	x	✓	✓	✓
Srivastava et. al. (2022)	2022	To compare d different data collection algorithms graphically based on their accuracy and error rate	Provides a comprehensive study for maintaining the energy efficiency of an AI-based IoMT framework	✓	✓	✓	x	x	✓	x
Kelly et. al. (2020)	2020	To resolve potential issues that IoT-based health care generates, standardization and remuneration	Improve the efficiency of the health system	x	✓	x	x	x	✓	✓
Yuehong YIN (2016)	2016	Develop methodologies, IoT-based smart devices, and systems	The advancement of IoT in the healthcare system	✓	✓	✓	x	x	✓	x
Analysis of existing Works based on different parameter*	2022	Privacy Preservation of the Internet of Medical Things using blockchain	Comparative analysis of IoMT security using blockchain based on different parameters such as patient encryption key, hardware implementation, etc	✓	✓	✓	✓	✓	✓	✓

*(Comparison on the basis of this paper) 1. architecture, 2. healthcare, 3. comparison analysis, 4. security, 5. taxonomy, 6. IoMT protocols 7. research challenges. From Table 1, most of the researchers do not consider the data security of the smart healthcare system. From above table, we find that a lot of researchers did not mention comparative analysis, taxonomy, and healthcare issues what's why there is significantly less concern about the security of the smart healthcare system

perform certain medical operations. It also depicts the framework where a certain number of hospitals are connected and share medical information with secure boundaries, and explore regions for better outcomes.

4.1 Comparison and analysis

The comparison of existing surveys on IoMT security using blockchain with the proposed survey is given in Table 1. Based on specific criteria, which are as follows:

Architecture, healthcare, comparison analysis, security, taxonomy, the study of IoMT protocols research challenges. Table 1 shows that most researchers mainly focus on the implementation of the smart healthcare system and its functionalities. The security status of the IoMT protocols in medical devices is less concerning. From this table, we find that a lot of authors did not mention comparative analysis, taxonomy, and healthcare issues what's why there is significantly less concern about the security of the smart healthcare system.

On the basis of Table 1, a visualization is done of different research work on the basis of the journal/conference articles over year of publication. Figure 3. shows the highest rates of published articles over time. It has been shown that most of the journals/conferences are published in IEEE.

5 Blockchain architecture for the internet of medical things

In this section, the fundamental architecture of blockchain and IoT is discussed in such a manner that covers all basic units, transactions, block networks, and their functions. There are two parts to this section which first part covers the basic Blockchain architecture, and the second one covers blockchain architecture for IoT, which are as follows:

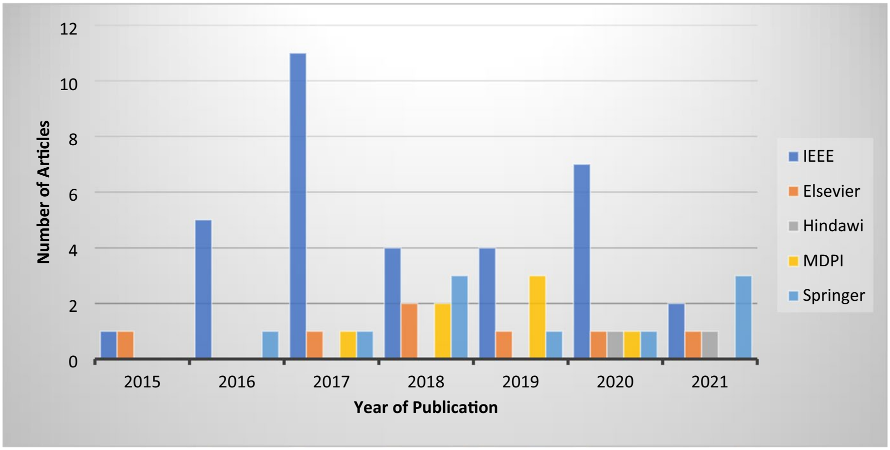


Fig. 3 The distribution of reputed journal/conference articles over time

5.1 Basic blockchain architecture

It is a technique in which a ledger is used for storing massive data. The details of every accomplished transaction are stored in a public ledger shared throughout all engaged systems of the blockchain network. It is proficiently recording transactions between two or on an appropriated shared (P2P) organization, with the saved information co-operated by utilizing all organization's people, and permanently.

- *Adding a new transaction in the block:* Adding a recent transaction has specific steps. First, it is to add a user request for a new transaction; then, it is stored in the blocks in the network.
- *Transmission to available systems:* In this part, a block is comprised of the transactions transmitted to every method available across the network.
- *Transactions Validation:* The network utilizes the SHA-256 algorithm to make a unique cryptographic hash value. Every block is related to the hash function of the previous block which creates an unbeatable transaction network. Suppose somebody attempts to add on a new transaction, it should be approved by the organization framework or smart contract and consensus protocol.
- *Addition of block in the chain:* After verifying a new transaction by the other system nodes, a new block is joined within the chain. The current blockchain is extended by joining another block that is irreplaceable and unmodifiable for the third party.

This is the fundamental framework of blockchain in which every single transaction requires verification, and these transactions cannot be modified, as shown in Fig. 4.

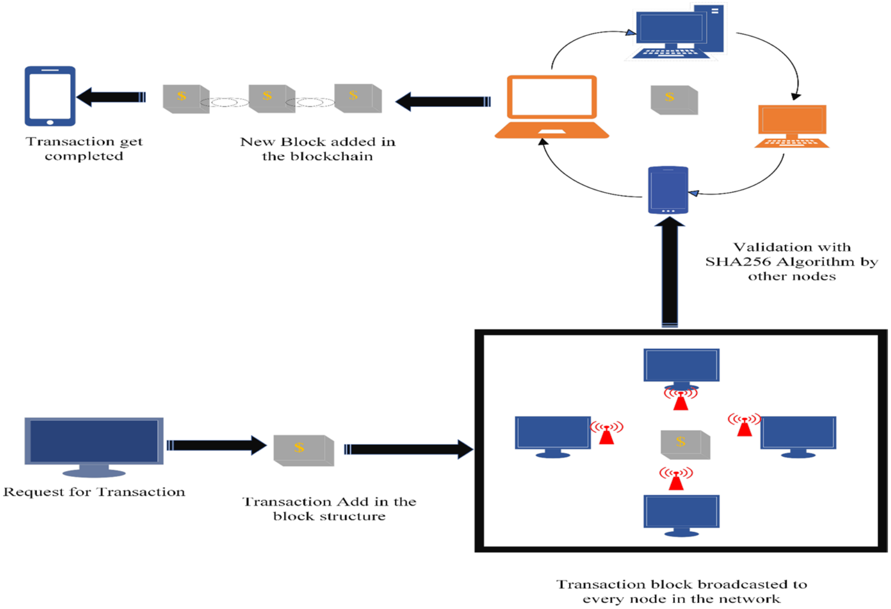
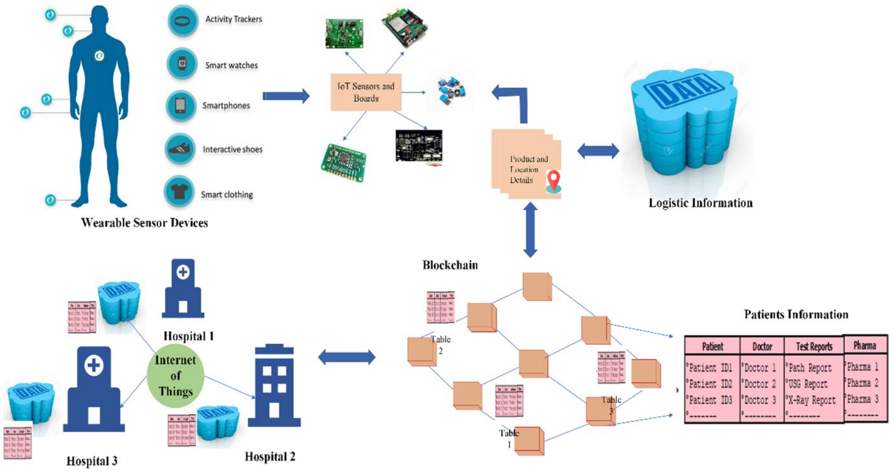

Transaction get completed
New Block added in the blockchain
Validation with SHA256 Algorithm by other nodes
Request for Transaction
Transaction Add in the block structure
Transaction block broadcasted to every node in the network

Fig. 4 A blockchain architecture



Patient	Doctor	Test Reports	Pharma
°Patient ID1 °Patient ID2 °Patient ID3 °-------	°Doctor 1 °Doctor 2 °Doctor 3 °--------	°Path Report °USG Report °X-Ray Report °--------	°Pharma 1 °Pharma 2 °Pharma 3 °--------

Fig. 5 Blockchain architecture for IoMT

5.2 Blockchain architecture for the internet of medical things

This part covers the basic architecture of IoT-based medical healthcare Systems using blockchain, which has two modules as given below:

5.2.1 The IoT module

This module gathered and detected information from the wearable devices worn by the patients or deployed within surroundings where patients are observed. If a patient is following some medical treatment or undergoing serious surgery, then at that point, wearable devices detect the information every single second, which is generated continuously by the patient (Chakraborty et al. 2020). The information gathered by the wearable devices from the patient such are Breath Strengthening, Calorie Release, Heart Rate, and Sleep Stage Monitoring; additionally, if pulse estimating devices are utilized or then again assuming pacemakers are implanted within the patient, this information can likewise be remotely monitored using the IoMT devices.

5.2.2 Access and transaction management using blockchain

Every second, millions of tons of information are produced; however, do we deal with this information? Fundamentally a lot of information continuously made by the patient is needed to be overseen and handled by setting up some consensus algorithm. Besides, whenever there are multiple partners related to the information being produced, an access management framework is also inscribed by the Blockchain Network (Chakraborty et al. 2020; Hussein et al. 2019).

The IoMT framework supports the medical services area and is named smart healthcare. Smart contracts are utilized in the sector of IoT-based healthcare systems where the number of procedures is expanding progressively (Laplante and Amaba 2018), and the need to observe and implement the smart agreement is turning out to be progressively troublesome. Blockchain is utilized to facilitate this work by eliminating intermediaries in the smart healthcare system. The Intermediaries available in the blockchain network for data validation and decision-making, consume an enormous number of devices, for example, computation power and period, etc.

It resolves the problem by eliminating the usage of these mediators by setting up the taking part frameworks itself to work through on their behalf (Dobrovnik et al. 2018). Resource management is the primary utilization of this technology which is implanted with smart contracts that characterize who claims which issue at what point in time. In this process, every transaction works on a set of input variables, which is characterized according to the prerequisites. The connected devices in the IoMT can work as an autonomous unit and generate results adequately, as shown in Fig. 5. Smart contracts are implanted in devices with a unique address inside the blockchain system. In the network, the same code is executed on the other system and the chain is connected. All the completed transactions are irreversible with the goal that the chain becomes sealed and unavoidable (Betti et al. 2019). For reversing any transaction, a counter transaction must be performed, which cannot be possible. Smart contracts are used in Blockchain excel in applications where a tremendous amount of data is available. It will be useful in the healthcare system because a huge amount of information is being produced, and its processing is still deficient (Wang et al. 2018).

5.3 Security in IoMT communication protocols

In this subsection, we describe the security characteristics of the IoT communication protocols that are specifically used in IoMT devices.

5.3.1 Infrared

There are no embedded security protections in infrared (IR) communications. Data transferred between the transmitter and receiver can be read by anyone who can block the IR beam. Security concerns were seen as outside the purview of their threat model since IR technologies are directed beams that only function in close proximity; for example, an attacker must be present extremely close to the IR device and have the necessary materials.

5.3.2 RFID- (radio-frequency identification)

The embedded data in RFID communications are read-only and unsecured. RFID does not by default apply any security measures to prevent tag scanning, either for the tag or the scanner. This opens the door for attackers on tag data integrity, unauthorized tag cloning, and attacks on the device, equipment, or medical data confidentiality.

5.3.3 Bluetooth/BLE

Prior to connection formation, Bluetooth device authentication is carried out, and stream cipher encryption is used to minimize the risk of Man-In-The-Middle (MITM) attacks. Its encryption mechanism establishes symmetric encryption between devices by using the address of the master device, clock time, and a key.

5.3.4 Z-wave

Encryption, behavior detection, and proximity security methods are used by Z-Wave. Through the "Security" command class, the protocol additionally safeguards the privacy, source integrity, and data integrity of its data. Through the use of three shared keys and AES encryption, frames and payloads are both encrypted and integrity-protected.

5.3.5 WiFi

The IEEE 802.1X Standard authentication processes are carefully adhered to by wireless security (WiFi) devices seeking to join wireless networks. The WiFi Protected Access 2 (WPA2) standard, which is currently used to secure WiFi networks, encrypts data delivered over wireless networks with a 256-bit key. Although many security precautions are typically implemented by wireless technologies, they are not always enforced by default in all networks.

5.3.6 ISA 100.11a

To provide message authentication, and data privacy against replay attacks, ISA 100.11a supports several security measures. A linchpin is used for device authentication to stop a fake device from connecting to a network.

5.3.7 LoRaWAN

Two layers of cryptography are used in the LoRaWAN design. The network server and the end nodes share a special network session key which is the first thing that is applied. For packets transmitted across the LoRaWAN network, the AES encryption technology is utilized to support authentication and data integrity.

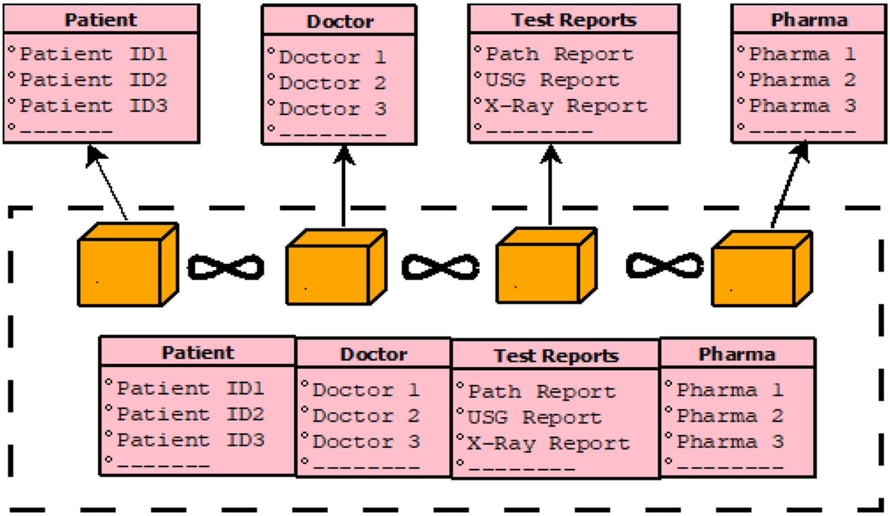


Fig. 6 Blockchain using smart contracts for IoMT

The decentralised blockchain-based smart contracts for IoMT establish all the data identified with every patient transaction with its records, for example, specialist medical information, medicine details, and diagnostic test reports. Every record keeper works as a single block where information moves, starting with one block and then constructing a chain onto the next block. It also assists with mechanizing this interaction quickly and compelling information execution, handling, and storage capacity, as shown in Fig. 6. etc.

6 Blockchain deployment in IoMT

Nowadays, After the covid pandemic, healthcare facility is the topmost priority of every country. In a conventional healthcare system, all information related to the patient is recorded in a centralized database, but it does not give access to information to any unauthorized person. The security of patient data is vulnerable to network attacks (Vora et al. 2018). Thus, we found that the centralization framework can't satisfy these prerequisites completely. Hence, the e-healthcare system is introduced to the world to deal with the various challenges and issues in traditional healthcare setups. Due to privacy and security issues, it is hard to share and communicate data. It influences significant decisions like implementing new services and analysing the symptoms of various sicknesses or medical problems. Table 2. provides a comparative study of healthcare security standards used for the intelligent healthcare system using multiple parameters such as the research goal, merit, demerit, etc. A comparison of specific healthcare security standards is made, which are as follows: Architecture, Data integrity, medical information sharing, access control, distributed electronic health records (EMR), patient encryption key, simulations, algorithms, benefits, and drawbacks of the existing approaches.

1. Architecture, 2. Data integrity 3. Medical information sharing, 4. Access control, 5. Distributed electronic health records (EMR), 6. patient encryption key, 7. Simulations, 8. Algorithms.

7 Open issues and research challenges

Blockchain gives a reliable solution for explicit medical services application challenges, like security, protection, interoperability, availability, and ongoing updates of clinical information, mainly when applied effectively. Nonetheless, blockchain has some limitations and constraints. Figure 7 presents the classification of these challenges.

7.1 Privacy and security

The current secure correspondence designs of EHR dismiss clients' or patients' privacy, for example, the trading framework uncovering all information beyond proprietors' consent in the information solicitor summary (Srivastava and Prakash 2020a). Although, if current EHR applications depend upon blockchain, the solicitor requires exact patient information to offer customized types of assistance. The critical problem in information security is to propose an architecture that utilizes cryptographic components for information security using blockchain-based EHR. This framework perceives a specific patient as troublesome through his present record number. In any comparative system, inadequacies ought to be tended to keep up with patients' private information.

Table 2 Blockchain-based techniques to secure healthcare system

Name of Author	Year	Goal	1	2	3	4	5	6	7	8	Merit	Demerit
Yue et al. (2016)	2016	To secure the healthcare system using blockchain									Data controlled by patients	It does not have access control management
Azaria et al. (2016)	2016	To spasm healthcare information and permission management With Blockchain	x							x	Availability of healthcare data via a distributed Ledger as well as sharing of patient data	Very Big policy and bureaucratic incompleteness
Shae et al. (1980)	2017	To design the framework using blockchain for medical examination								x	It has distributed framework and shares healthcare information	Computationally Limited things or devices, no developed schemes
Zhang et al. (2016)	2017	To protect substantial social network based healthcare system									Distributed databases, allow sharing of health data	Computationally limited devices,
Dubovitskaya et al. (2017)	2017	To empower e-smart healthcare Health								x	Shared, immutable—transparent ledger	Latency in data connectivity
Xia et al. (2017)	2017	To design a trust-based healthcare system in which information-sharing services utilizing cloud computing with blockchain									Surreptitious transactions, access control protocol to find out data as well as permissions	Lack of reliability, data interoperability, key management
Rifi et al. (2017)	2017	To explore blockchain for smart Health data accessibility							X	x	Data exchange is more secure, in this decentralized network	Huge amount of data exchange
Liang et al. (2017b)	2017	To implement blockchain in the organization for secure data transmission and collaboration With mobile healthcare							X	x	A Secured Merkle root tree for transactions	Limited interactivity

Table 2 (continued)

Name of Author	Year	Goal	1	2	3	4	5	6	7	8	Merit	Demerit
Magyar et al. (2017)	2017	To resolve security issues and accessibility of Electronic health records utilizing blockchain technology	x						X	x	This framework is reliable, removes intermediatory, distributed EHR	Exchangeability, Security issues, compact user information
Alhadhrami et al. (2017)	2017	To describe the feasibility of blockchain in the e-healthcare system							x	x	Organized data, consent management	Sybil attacks
Jiang et al. (2018)	2018	To design blockchain in the smart healthcare system for data sharing system									It is useful in Combining off-chain records and on-chain rectification	Depleted system throughput, complicated authentication
Theodouli et al. (2018)	2018	To implement a framework for simple healthcare data exchange								x	Proper Patient information management, Inspection and data availability	Counterfeit, source of the problem
Zhang et al. (2018)	2018	To design flexible queries with the access control systems to EMRs									Enhanced Access control management without reveling unauthorized users	Secure control management is not mentioned
Li et al. (2018)	2018	To explain data privacy and security solutions in smart healthcare									Fortified cryptographic solutions	Huge amount of record destruction; shortage of storage space
Fan et al. (2018)	2018	To set up an effective and secure smart healthcare system using blockchain									Data transmission from EMR;	High computational power
Wang et al. (2018)	2018	To provide security to Electronic Health Record systems								x	Identity-based encryption for data records; assured integrity and identifiability	Implementation is not available

Table 2 (continued)

Name of Author	Year	Goal	1	2	3	4	5	6	7	8	Merit	Demerit
Khezr et al. (2019)	2019	Explain current blockchain techniques implemented in healthcare				x					QTUM	Security issues
Bhattacharya et al. (2019)	2019	Collaboration of deep learning and Blockchain to provide security to the EHR system			x						Cord AD App	Health-related data sharing issues

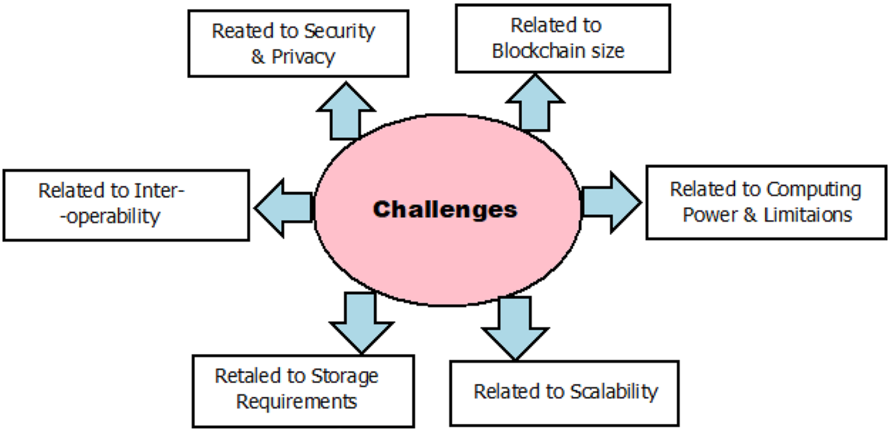

Reated to Security & Privacy
Related to Blockchain size
Related to Inter- -operability
Challenges
Related to Computing Power & Limitaions
Retaled to Storage Requirements
Related to Scalability

Fig. 7 Research challenges in smart healthcare

7.2 Computing power limitations

The data collected by IoMT using blockchain are frequently computationally restricted, with the end goal that cryptographic techniques might not be utilized (Dwivedi et al. 2019). There are numerous health-related applications in which cryptosystems have asset imperative things that handle sensor and actuator security. They are stood up to with current situation and secure public-key cryptography plans. Blockchain uses public-key cryptosystems-based ECC with productivity and security issues, subsequently determining the proper cryptography issues.

7.3 Latency and throughput restrictions

Blockchain innovations will set aside effort for agreement to meet some specific criteria and confirmed transactions, which can be an issue in incorporating blockchains with medical healthcare applications requiring information gathered execution progressively. A blockchain sets aside effort for handling these transactions (Srivastava and Prakash 2020b).

7.4 Scalability

The blockchain framework presents one more issue in adaptability and expanding computational assets in IoT-based healthcare devices to expand the number of framework systems. Such issues can be immediate computational prerequisites for the whole blockchain technology.

7.5 Interoperability and standardization

Interoperability and standardization are critical research challenges in IoMT that need to be addressed to fully realize the potential of this rapidly growing field (Schmeelk et al. 2022). One of the biggest challenges in interoperability is the lack of common data exchange formats. Different devices and systems often use different data formats, which can make it difficult to exchange data between them. Research is needed to develop common data exchange formats that can be used by all devices and systems in IoMT. The current EHR frameworks work over the centralized database and disconnected framework, while cloud-based blockchain innovation is decentralized (Verma and Prakash 2020a). Appropriately, moving medical care frameworks towards this implementing blockchain will first and foremost require a proficient EHR framework equipped for working with joint effort and interoperability among clinical and established researchers. By overcoming these challenges, IoMT has the potential to transform healthcare and improve patient outcomes.

7.6 Storage requirements

Blockchain technology requires a vast capacity to store the entire transaction sequence in the network, which may be an issue for prohibitive systems that send data. The technology ensures that collected and shared EHR data is not modified, irreversible, and confidential. Yet, it can adequately experience storage-related issues and prerequisites of large-scale appropriated EHR information (Sharma and Prakash 2020).

Table 3 provides a correlation between issues and research issues in the medical healthcare sector and their suitable solutions using blockchain.

a) *Master patient indices*

Consistently vast amounts of health-related information increments, and frequently, records become manipulated when managing medical care information. Additionally, unique electronic healthcare records frameworks have their information format and informational index to execute the information, increasing the requirement for a normalized data format design.

b) *Patient information management*

The Health Insurance Portability and Accountability Act controls patients' information privacy. The patients must provide their clinical information to other parties like drug specialists, pathologies, doctors, etc., which securely store the information. A cryptographic value for every patient's data is produced in the blocks consisting of all patient identities using blockchain technology.

c) *Data integrity*

Patients' health records, EHR, and information gathered from wearable devices (Raj and Prakash 2018) are stored in the decentralized database, which requires data privacy and integrity while sharing this information with other parties. The blockchain is more valuable in such situations due to its capacity to give information respectability. The blockchain methodology is to store and exchange information on transactions securely.

d) *Clinical trials*

Table 3 Comparative analysis of smart healthcare system solution using blockchain

Aspect	Issues	Implications	Solutions using blockchain
Master patient indices	Instability in medical records, various EHR schemas in the different research domains	Data surfeit, complications in patient data identification	More than one address and keys are linked to a single patient ID
Patient information management	Exchanging patients' information with third parties	Unauthorized personal data access	Access blocks controlling health record
Data integrity	A huge amount of data management; complexity in information processing	Security challenges	Immutable medical audits
Clinical trials	Companies utilize their information management system	Data standardization for clinical data	Data access restrictions
Drug traceability	Drug duplicity, false medicine	Less number of clients satisfied with drugs	Irreversible time-sampled transactions to find out fraudulent drug dealers
Data enrichment	Accuracy, privacy, data understandability, data duplicity	The incompatible and inefficient treatment procedure	Substitution of patient's identity using a public hash value

Specialists employed in different areas consistently need their confidential data stored securely and safely so that no unauthorized individual can modify or alter the information. Data alteration is inconceivable using the SHA256 algorithm, which makes a specific hash value associated with the chain (Verma and Prakash 2021). The medical services sector requires storing and sharing information identified with medical preliminaries safely, which must be imparted to approved gatherings, such as research supports or administrative advisory groups. The information can be overseen or followed with assent inside numerous destinations, conventions, and frameworks with the blockchains. Patients with legitimate access advantages can likewise get this data regarding their medical problems and related examination.

e) *Drug traceability*

As of now, the primary obstacle in pharmacology is medication duplicity. The detrimental impact of this is the severe loss in the business, which can prompt serious harm to an individual's health. The utilization of blockchain across medical healthcare can identify cheats from the medication dealer (Verma and Prakash 2019, 2020b). All the task providers are composed in the blockchain network that empowers them to follow the entire course of medications.

f) *Data enrichment*

Gathering raw data can prompt changeability, time utilization, and the absence of sustainability (Sharma et al. 2020). Information enhancement is an activity to add qualities to expand quality. Healthcare information should be organized, accurate, secured, time-stepped, and simple to peruse.

8 Conclusion and future direction

The paper presents a comprehensive study of the Internet of medical things. The paper describes how IoT- Blockchain integration can be leveraged to develop improved smart Healthcare frameworks. This survey is categorized into six sections; the first section describes the introduction of the paper and the second section emphasizes on taxonomy of the smart healthcare system. The third section includes the literature review of the blockchains-IoT system in smart healthcare. The fourth section explores the basic architecture of blockchain and IoMT architecture. The fifth section accentuates the real-time implementation of the blockchain in smart healthcare, which explains current solutions using Blockchain for IoT applications. The sixth section explores research challenges and open issues in the smart healthcare system. Compromising private data to unauthorized parties in medical services applications reduces the patient's trust in the EHR framework. Hence, it is difficult to maintain public trust if the privacy of real-time healthcare data is leaked. Blockchain permits easy identification of a particular system and easily enables patient private data gathering, such as names, diseases, and present addresses in the network. Comparative analysis of well-known recent research on IoT-based smart healthcare system security using blockchain is done based on different parameters such as architecture, data integrity, access control, medical information exchange, EMR, patient encryption key, hardware implementation, etc.

Many systems are designed to give users more control over their data, but the challenge of building a fully decentralized user-centric system for health data still exists. There are situations when the use of permission solutions controlled by healthcare organizations is unclear, potentially allowing users to manage their data but ultimately forcing them to follow consortium guidelines about data management. Even if user data is stored in a decentralized manner, solutions cannot guarantee a user-centric system if the Blockchain runs the danger of being hacked by participants. An innovative model can be designed where each user physically owns their data, possibly on a smartphone or a small device they have at home. If these devices serve as secure, decentralized data storage, then any unknown party might simply access the information stored there while abiding by the regulations imposed by the users who own the content they share. Additionally, proper data collection methods and determining connections across the blockchain network will be addressed to manage confidential and private transactions. In the near future, we will design a model based on a cryptographic scheme for private transactions and attempt to verify the performance of the enhanced blockchain version on the decentralized healthcare system. We hope that this paper will provide a background related to working on future blockchain systems that will be secured and scalable in the real world.

Authors contributions Anu Raj was responsible for system designing, mediating any data screening and extraction discrepancies, interpreting the results, and writing the initial manuscript. Dr. Shiva Prakash contributed to the study design and provided feedback on the initial review protocol and the manuscript.

Funding This research did not receive any specific grand from funding agencies in the public, commercial, or not-for-profit sectors.

Declarations

Conflict of interest The authors did not receive support from any organization for the submitted work.

References

Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.-Y., Bashir, A.K., Abd El-Latif, A.A.: Distrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access **4**, 111223–1111238 (2020)

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: “Blockchain technology innovations,” In Technology and Engineering Management Conference (TEMSCON), pp. 137–141, IEEE, (2017)

Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J.A., Shuaib, K.: “Introducing blockchains for healthcare.” In: International Conference on Electrical and Computing Technologies and Applications, pp. 1–4. (2017)

An Overview of Consensus Protocols in Blockchain, https://www.section.io/engineering-education/blockchain-consensus-protocols/ accessed-17.-9.2019

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: “Medrec: Using blockchain for medical data access and permission management.” In: 2nd International Conference on Open and Big Data (OBD), pp. 25–30. (2016)

Betti, Q., Khoury, R., Hallé, S., Montreuil, B.: Improving hyperconnected logistics with blockchains and smart contracts. IT Prof. **21**, 25–32 (2019)

Bhattacharya, P., Tanwar, S., Bodke, U., Tyagi, S., Kumar, N.: Bindaas: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Transact. Netw. Sci. Eng. **8**(2), 1242–1255 (2019)

Bhattacharya, P., Tanwar, S., Bodke, U., Tyagi, S., Kumar, N.: BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Trans. Netw. Sci. Eng. **8**(2), 1242–1255 (2020)

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab, M.: Blockchain for industry 4.0: a comprehensive review. IEEE Access **8**, 76764–79800 (2020)

Budida, D.A.M., Mangrulkar, R.S.: "Design and implementation of smart HealthCare system using IoT", Innovations in Information, Embedded and Communication Systems, International Conference on pp. 1–7. IEEE, (2017)

Chakraborty, S., S, Aich., Hee-Cheol K.: "A secure healthcare system design framework using blockchain technology." International Conference on Advanced Communications Technology. (2020)

Dave, D., Parikh, S., Patel, R., Doshi, N.: A survey on blockchain technology and its proposed solutions. Proced. Comput. Sci. **160**, 740–745 (2019)

Dobrovnik, M., Herold, D., Fürst, E., Kummer, S.: Blockchain for and in logistics: what to adopt and where to start. Logistics **2**(3), 18 (2018). https://doi.org/10.3390/logistics2030018

Duan, B., Zhong, Y., Liu, D.: "Education application of blockchain Technology: learning outcome and meta-diploma." In Parallel and Distributed Systems, IEEE 23rd International Conference on, pp. 814–817. (2017)

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: "How Blockchain Could Empower eHealth: An Application for Radiation Oncology". pp. 3–6. (2017)

Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (switzerland) **19**(2), 1–17 (2019)

Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: Medblock: Efficient and secure medical data sharing via blockchain. J. Med. Syst. **42**, 1–11 (2018)

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaría, V.: To blockchain or not to blockchain: that is the question. IT Prof. **20**(2), 62–74 (2018)

Giungato, P., Rana, R., Tarabella, A., Tricase, C.: Current trends in sustainability of bitcoins and related blockchain technology. Sustainability **9**, 2214 (2017)

Gross, M.S., Miller, R.C., Jr.: Ethical implementation of the learning healthcare system with blockchain technology. Blockchain Healthcare Today **2**, 2019 (2019)

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., Kim, W.: Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE Access **8**, 24746–24772 (2020)

Hameed, K., Bajwa, I.S., Sarwar, N., Anwar, W., Mushtaq, Z., Rashid, T.: Integration of 5G and Blockchain technologies in smart telemedicine using IoT. J. Healthcare Eng. **2021**, 1–18 (2021). https://doi.org/10.1155/2021/8814364

Hathaliya, J.J., Tanwar, S.: An exhaustive survey on security and privacy issues in healthcare 4.0. Comput. Commun. **153**, 311–335 (2020)

https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence, Accessed date- 15–09–2021

Hussein, H.M., Yasin, S.M., Udzir, S.N.I., Zaidan, A.A., Zaidan, B.B.: A systematic review for enabling of developing a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations, and future direction. J. Med. Syst. **43**(10), 320 (2019)

Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I.H., Salman, S.: Blockchain technology in the healthcare industry: Trends and opportunities. J. Ind. Inform. Integr. **22**, 100217 (2021). https://doi.org/10.1016/j.jii.2021.100217

Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The internet of things for health care: a comprehensive we agree with this comment, all spelling and grammatical errors pointed out by the reviewers have been corrected in the revised manuscript the survey. IEEE Access **3**, 678–708 (2020)

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: "Blochie: A blockchain-based platform for healthcare information exchange," In: IEEE International Conference on Smart Computing (SMARTCOMP), pp. 49–56. (2018)

Kelly, J.T., Campbell, K.L., Gong, E., Scuffham, P.: The internet of things: impact and implications for health care delivery. J. Med. Internet Res. **22**(11), e20135 (2020). https://doi.org/10.2196/20135.PMID:33170132;PMCID:PMC7685921

Khezr, S., Moniruzzaman, M., Yassine, A., Benlamri, R.: Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl. Sci. **9**(9), 1736 (2019)

Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., Decker, S.: "Blockchain for business applications: a systematic literature review," International Conference on Business Information Systems, pp. 384–399, Springer, (2018)

Koo, D., Piratla, K., Matthews, C.J.: Towards sustainable water supply: schematic development of big data collection using internet of things (IoT). Procedia Eng. **118**, 489–497 (2015)

Krieger, U., Liu, W., Zhu, S., Mundie, T.: "Advanced block-chain architecture for e-health systems, (2017)

Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., Hossain, E.: A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access **8**, 118433–118471 (2020)

Lampropoulos, G., Siakas, K., Anastasiadis, T.: Internet of things in the context of industry 4.0: an overview. Int. J. Entrep. Knowl. (2019). https://doi.org/10.37335/ijek.v7i1.84

Laplante, P.A., Amaba, B.: Blockchain and the internet of things in the industrial sector. IT Prof. **20**, 15–18 (2018)

Leible, S., Schlager, S., Schubotz, M., Gipp, B.: "A review on blockchain technology and blockchain" projects fostering open science. Front. Blockchain. (2016)

Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., Liu, S.: Blockchain-based data preservation system for medical data. J. Med. Syst. **42**, 1–13 (2018)

Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," In: 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5. (2017b)

Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: (2017a) "Integrating blockchain for data sharing and collaboration in mobile healthcare applications". In personal, indoor, and mobile radio

Liu, S.H., Lin, C.B., Chen, Y., Chen, W., Huang, T.S., Hsu, C.Y.: An EMG patch for the real-time monitoring of muscle-fatigue conditions during exercise. Sensors **19**, 3108 (2019)

Magyar, G.: Blockchain: Solving the privacy and research availability trade-off for EHR data: A new disruptive technology in health data management. In: IEEE 30th Neumann Colloquium (NC), pp. 000135–000140. (2017)

Mettler, M.: "Blockchain technology in healthcare: The revolution starts here in e-Health Networking, Applications, and Services (Healthcom)", IEEE 18th International Conference on, pp. 1–3. (2016)

Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)

Mosa, A.S., Yoo, I., Sheets, L.: A systematic review of healthcare applications for smartphones. BMC med informatics. Decis. Mak **12**, 67 (2012)

Mutlicentre trial, https://en.wikipedia.org/wiki/Multicenter_trial, accessd- 17–09–2021

Pradhan, B., Bhattacharyya, S., Pal, K.: IoT-Based applications in healthcare devices. J. Healthcare Eng. **2021**, 1–18 (2021). https://doi.org/10.1155/2021/6632599

Radanovi´c, Liki´c, R.: Opportunities for the use of blockchain technology in medicine. Appl. Health Econ. Health Polic **16**(5), 583–590 (2018)

Raj, A., Prakash, S.: Mobile data gathering approaches in wireless sensor networks: a survey. In: 2019 6th International Conference on Computing for Sustainable Global Development, pp. 758–762. (2019)

Raj, A., Prakash, S.: Internet of everything: a survey based on architecture, issues, and challenges. In: 6th IEEE UPCON-(2018)

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/j.future.2018.05.046

Rifi, N., Rachkidi, E., Agoulmine, N., Taher, N.C.: "Towards using blockchain technology for e-health data access management." In: 4th International Conference on Advances in Biomedical Engineering, pp. 1–4. (2017)

Rohokale, V.M., Prasad, N.R., Prasad, R.: "A cooperative internet of things (IoT) for rural healthcare monitoring and control." In: 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory, and Aerospace and Electronic Systems Technology, Chennai, India, pp. 1–6. (2011)

Schmeelk, S., Kanabar, M., Peterson, K., Pathak, J.: Electronic health records and blockchain interoperability requirements: a scoping review. JAMIA Open **5**(3), ooac068 (2022)

Shae, Z., Tsai, J.J.P.: "On the design of a blockchain platform for clinical trial and precision medicine," In: IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 1972– 1980. (2017)

Sharma, R., Prakash, S.: An adaptive ensemble localization approach for sensor nodes in WSN-IoT. EAI End. Transact. Energy Web **7**(29), e5 (2020)

Sharma, A., Sarishma, R.T., Chilamkurti, N., Kim, B.-G.: Blockchain based smart contracts for internet of medical things in e-healthcare. Electronics **9**(10), 1609 (2020). https://doi.org/10.3390/electronics9101609

Sharma, R., Prakash, S., Roy, P.: "Methodology, Applications, and Challenges of WSN-IoT", International Conference on Electrical and Electronics Engineering, India, pp. 502–507. (2020)

Sivagami, S., Revathy, D., Nithyabharathi, L.: Smart health care system implemented using IoT. Int. J. Contemp. Res. Comput. Sci. Technol. **2**(3), 641–646 (2016)

Srivastava, S., Prakash, S.: Security Enhancement of IoT Based Smart Home Using Hybrid Technique, Network Security and Data Sciences. MIND, Communications in Computer and Information Science, vol. 1241, p. 2020. Springer, Singapore (2020b)

Srivastava, J., Routray, S., Ahmad, S., Waris, M.M.: Internet of medical things (IoMT)-based smart healthcare system: trends and progress. Comput. Intell. Neurosci. **2022**, 1–17 (2022). https://doi.org/10.1155/2022/7218113

Srivastava, S., Prakash, S.: An analysis of various iot security techniques: a review. In: 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 355–362. (2020a)

Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P.K., Hong, W.-C.: Machine learning adoption in blockchain-based smart applications: the challenges, and a way forward. IEEE Access **8**, 474–488 (2020)

Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., Tzovaras, D.: On the design of a blockchain-based system to facilitate healthcare data sharing, pp. 1374–1379 (2018)

Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P.C., Krishnaraj, N.: An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. J. Supercomput. **77**(9), 9576–9596 (2021). https://doi.org/10.1007/s11227-021-03637-3

Verma, G., Prakash, S.: Emerging Security Threats, Countermeasures, Issues, and Future Aspects on the Internet of Things (IoT): A Systematic Literature Review Advances Interdisciplinary Engineering. Lecture Notes in Mechanical Engineering Springer, Singapore (2020a)

Verma, G., Prakash, S.: Design and implementation of modified unicode strategy for data security in IoT. Int. J. Adv. Sci. Technol. (IJAST) **29**, 6271–6294 (2020b)

Verma, G., Prakash, S.: Internet of Things for Healthcare: Research Challenges and Future Prospects: Advances Communication and Computational Technology. Springer Nature, Singapore (2021)

Verma, G., Prakash, S.: A study towards current trends, issues and challenges in internet of things (IoT) based System for intelligent energy management. In: 2019 4th International Conference on Information Systems and Computer Networks (ISCON). IEEE, (2019)

Viriyasitavat, W., Xu, L.D., BiPungpapong, Z.V.: Blockchain and internet of things for modern business process in digital economy—the state of the art. IEEE Trans. Comput. Soc. Syst. **6**(6), 1420–1432 (2019)

Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S., Hsiao, K.: Ensuring privacy and security in e-health records. In: International Conference on Computer, Information and Telecommunication Systems, pp. 1–5. (2018)

Wang, S., et al.: Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Transact. Comput. Soc. Syst. **5**(4), 942–950 (2018)

Wang, H., Song, Y.: Secure cloud-based system using attribute-based cryptosystem and blockchain. J. Med. Syst. **42**(8), 152 (2018)

Wang, B., Sun, J., He, Y., Pang, D., Lu, N.: Large-scale election based on blockchain. Procedia Comput. Sci. **129**, 234–237 (2018)

Weiss, M., Botha, A., Herselman, M., Loots, G.: Blockchain as an enabler for public health solutions in South Africa. In IST-Africa Week Conference (IST-Africa), 2017, pp. 1–8, IEEE, (2017)

Xia, Q., Sifah, E., Omono Asamoah, K., Gao, J., Du, X., Guizani, M.: Medshare: trustless medical data sharing among cloud service providers via blockchain. IEEE Access **5**, 1–1 (2017)

Xu, L.D., Lu, Y., Li, L.: Embedding blockchain technology into IoT for security: a survey. IEEE Internet Things J. **8**(13), 10452–10473 (2021)

Yanamadala, S., Morrison, D., Curtin, C., McDonald, K., Hernandez-Boussard, T.: Electronic health records and quality of care: an observational study modeling impact on mortality, readmissions, and complications. Medicine **95**(19), e3332 (2016). https://doi.org/10.1097/MD.0000000000003332

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology? —a systematic review. PLoS ONE **11**(10), e0163477 (2016)

Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. (2016). https://doi.org/10.1007/s10916-016-0574-6

Yuehong, Y., Zeng, Y., Chen, X., Fan, Y.: The internet of things in healthcare: an overview. J. Ind. Inform. Integr. **1**, 3–13 (2016). https://doi.org/10.1016/j.jii.2016.03.004

Zaghloul, E., Li, T., Mutka, M.W., Ren, J.: Bitcoin and blockchain: security and privacy. IEEE Internet Things J. **7**(10), 10288–10313 (2020). https://doi.org/10.1109/JIOT.2020.3004273

Zhang, N., Voas, J.: Blockchain in developing countries. IT Professional **20**, 11–14 (2018)

Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. IEEE Access **4**, 9239–9250 (2016)

Zhang, X., Poslad, S.: Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6, (2018) Zhang, P., Walker, M.A., White, J., Schmidt, D.C., Lenz, G.: Metrics for assessing blockchain-based healthcare decentralized apps. In e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on, pp. 1–4, (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.