INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS)
ISSN: 2289-8522 e-ISSN: 2180-0650
VOL. 9, ISSUE 2, 119 – 128
DOI: https://doi.org/10.15282/ijsecs.9.2.2023.5.0116

ORIGINAL ARTICLE

Securing IoT Healthcare Applications and Blockchain: Addressing Security Attacks

Muhammad Umar Diginsa[1,*] , Sahnius Binti Usman[2] , Shahnurin Khanam Sanchi[3] ,Muhammad Idris[4] , Sadiq Abubakar Zagga[5]

[1,2,3]Department of Advance Informatics, University Technology Malaysia, 54000 Kuala Lumpur, Malaysia.
[1]Department of Computer Engineering, Binyaminu Usman Polytechnic Hadejia, Jigawa State Nigeria.
[4]Department of Computer Science, Binyaminu Usman Polytechnic Hadejia, Jigawa State Nigeria.
[5]Department of Computer Science, Kebbi State Polytechnic Dakingari, Kebbi State Nigeria.

ABSTRACT – The Internet of Things (IoT) describes the connection of bodily devices as "things" that can communicate with other systems and devices through the Internet and exchange statistics (data or information), facilitating the exchange of data with other systems and devices. These devices have sensors, software, and various components designed to exchange data seamlessly within the IoT network. Securing and protecting the data transmitted over the Internet from unauthorized access is imperative to ensuring the integrity and confidentiality of the information. IoT Smart health monitoring systems, integral components of the IoT landscape, are susceptible to various attacks. These include denial of service (DoS), fingerprint, router, select, forwarding, sensor, and replay attacks, all of which pose significant threats to the security of these systems. As such, there is a pressing need to address and mitigate the vulnerabilities associated with IoT healthcare applications. This paper aims to explore the significant role of IoT devices in healthcare systems and provide an in-depth review of attacks that threaten the security of IoT healthcare applications. The study analyses the existing literature on the vulnerabilities present in smart health monitoring systems and the potential application of blockchain technology as a robust solution to enhance the security of IoT healthcare applications. This research reveals critical vulnerabilities in IoT healthcare applications and highlights blockchain's effectiveness in mitigating them, providing insights for robust security measures and strategic decision-making in secure healthcare systems. This paper provides valuable insight and recommendations for policymakers, researchers, and practitioners involved in the domain of the IoT healthcare system.

ARTICLE HISTORY
Received: 17 May 2023
Revised: 1 November 2023
Accepted: 6 November 2023
Published: 4 December 2023

KEYWORDS
Blockchain
Healthcare System
Security Attacks
Internet of Things
Monitoring System

INTRODUCTION

The Internet of Things has a variety of applications in a wide variety of fields, including "Smart Health," "Smart Transportation," and "Smart Cities.". Through the use of the Internet of Things, it is possible to connect and share information on billions of things simultaneously. It provides various benefits to customers, which will result in a shift in how customers interact with the innovation[1]. The Healthcare Internet of Things (IoT) is an information system that can assist patients with expedited medical care[2]. In the circumstance of medical service applications, the IoT makes it easier for professionals and remote patients to communicate with one another when the patients are armed with wearable sensors[2]. The information on patients is extremely important, and any breach of their privacy could result in serious complications. Payers and providers in the healthcare industry are turning to blockchain technology to manage the data associated with clinical trials and electronic medical records while ensuring continued compliance with applicable regulations[3]. However, according to Chauhan et al. 2022 the decentralized architecture of the blockchain will be able to prepare billions of transactions between Internet of Things (IoT) devices. This will fulfill the computation and storage needs across the billions of devices that make up IoT systems and drastically lower the expenses related to setting up and running big unified server farms. The Internet of Things has done an excellent job in the healthcare industry by improving patient access to timely and cost-effective services. In addition, the primary factor that we have centered around for IoT is the fact that it enables the surveillance of patients in any circumstances, even throughout the non-active hours of the patient, which was exceptionally difficult to achieve using the conventional frameworks. It is practical to administer patient care remotely[2],[4]. The term "Internet of Things" (IoT) describes an interconnected system of physical "elements" that are equipped with sensors, software, and other technologies that allow them to link to other devices and systems to share information, data, and other materials among themselves through an internet connection. IoT- healthcare allows for the collection, storage, and analysis of massive amounts of data in a variety of different forms as well as the activation of context-based alarms by aggregating, processing, and communicating real-time medical information to the cloud through a variety of distributed devices[5]. With the introduction of medical gadgets into the total connectivity offered by the Internet of Things (IoT), which improves the quality of life for patients by enabling them to monitor patient electrical signals and share the data with healthcare professionals, the IoT has opened up a brand-new world for the healthcare system.

*CORRESPONDING AUTHOR | Muhammad Umar Diginsa | ✉ muhammaddiginsa@graduate.utm.my

The ongoing developments in the area of the Internet of Things (IoT) have led to an exponential expansion in the breadth of connectivity between remote objects that are connected to the Internet for the purpose of data and access transmission. As a result, the Internet of Things has changed and disrupted virtually every sector on the face of the earth, beginning with the education sector and working its way up to the management of supply chains. The Internet of Things has also demonstrated outstanding performance in the field of healthcare, where it has simplified diagnostic processes and improved the accuracy of patient activity monitoring. In addition, the primary aspect of the Internet of Things that we are concentrating on is that it enables the monitoring of patients even during their nonactive hours of the patient, which is frequently very difficult to accomplish with the traditional system. Accessing the data remotely and doing continuous analysis of it also reveals a wide range of options that could lead to a quicker diagnosis and more effective therapy[6]. Blockchain technology is utilized as the primary technology to ensure the transmission of data in a secure and intelligent manner[4]. Data regarding a patient's medical history that has been kept in an electronic health record can be very helpful in providing information about that patient. The reputation of the healthcare facility in the eyes of the community is at risk from disclosure without consent. The most important thing is to safeguard the dissemination of patients' medical records to steer clear of embarrassing or immoral circumstances[7]. IoT devices collect data that is measurable and able to be analyzed in the field of healthcare to make the work of healthcare apps easier. As a result, it is essential for healthcare systems to ensure the safety of applications related to the (IoT). IoT components are susceptible to attack due to many security flaws[8].

The primary aim of this paper is to contribute to the existing body of knowledge by exploring the significance of IoT in healthcare applications and providing a review of attacks that are associated with IoT healthcare systems. Moreover, the remaining portion of the paper is broken up into the following sections: The most recent related works in IoT healthcare applications and specific attacks to that domain are discussed in Section III of this paper, Section IV presents security threats relating to IoT healthcare applications, followed by Section V which explain the IoT healthcare architectural layers. Section VI present IoT Application capability, while section VII presents blockchain solution to IoT healthcare application. Section VIII concludes the paper. Therefore, the paper will provide valuable insight and recommendations for policymakers, researchers, and practitioners who are involved in the domain of IoT healthcare systems.

RELATED WORK

The vast majority of smart health monitoring gadgets are linked together through wireless networks, which are commonly vulnerable to security flaws. On the other hand, a lot of attacks have been observed, putting these health monitoring systems and applications in danger. There are several different kinds of attacks that can happen, including Denial of Service (DoS) assaults, Fingerprint and Timing-based snooping, Router attacks, Select and Forwarding attacks, Sensor attacks, and Replay attacks.

This section provides recent works in IoT Healthcare applications and reviews Denial of Services attacks facing the IoT healthcare application domain.

Butt et al. 2019 present a review of threats in IoT Smart health care, he describes many dangers posed by attackers to these systems, attacks in this area include denial-of-service attacks, fingerprint- and timing-based eavesdropping, router attacks, select and forwarding attacks, sensor attacks, and replay attacks. The impact of security risks on the system includes things like the denial of system services, data theft, data updates, changing the data route, and data drop. As a result, the design and development of a safe health monitoring system need the implementation of certain security best practices[9]. Such as Early Intrusion detection.

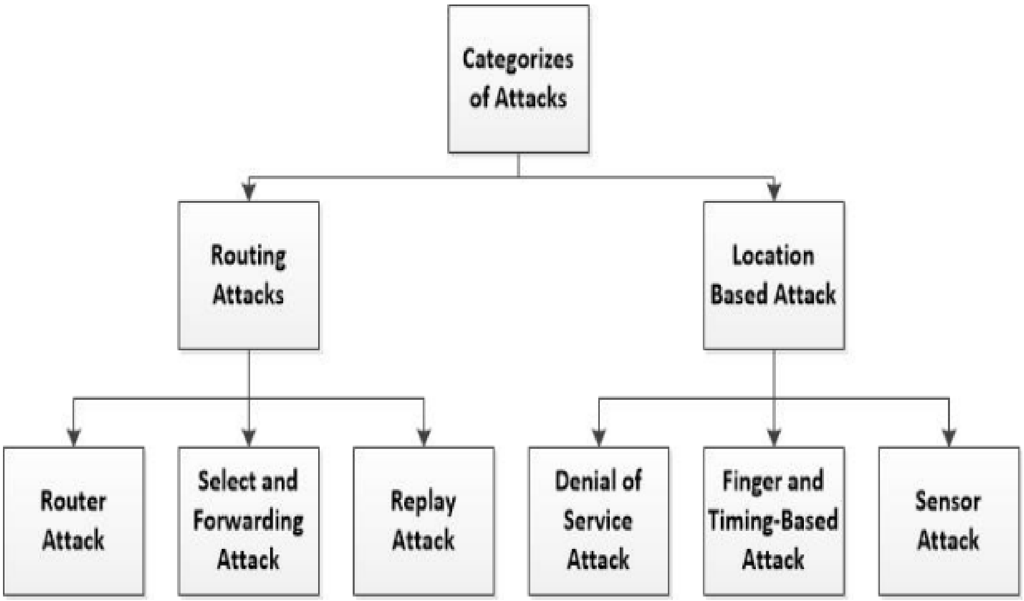


Figure 1. Categories of Attack in Smart Health Systems [9].

As shown in Figure 1 above, there are different categories of attack in smart healthcare systems which are further subdivided into two classes which are routing attacks and location-based attacks. Health monitoring systems are primarily affected by attacks such as unauthorized access, data tampering, denial of continuous monitoring, altered data destination paths, and data drops.

Jamal et al. describe how a DoS attack can be launched if Network Allocation Vector is updated at an unauthorized time, first by abusing the duration field of the Clear To Send (CTS) frame and then, in the second scenario, by misusing the Receiver Address field of the Clear To Send (CTS) frame. Both of these exploits can be found in the Clear To Send (CTS) frame. In Denial of services, the attacker fills up the available bandwidth on the network with unexpected traffic, which prevents other nodes from being able to send their data after detecting that the medium is already in use. This action renders resources unavailable for use by other nodes. In a typical DoS attack, the attacker will modify a few of the control frame flags in order to take advantage of the Network Allocation Vector behavior [10]. It is difficult to identify this kind of assault because, according to the IEEE 802.11 standard, the nodes do not do a counter-check on all of the flags that are contained in the control frames. The primary objective of the attacker is to generate a large amount of traffic and then divert that flow toward the victim's system. [10] suggest that a means of mitigating the effects of a distributed denial of service attack (DDoS), effective configuration of an incident response plan prior to the onset of the attack in the network, as well as routine inspection of traffic format and pattern, will be of great assistance.

In order to ensure that the IoT network can continue to function normally even in the event of an attack, Kalam et al. 2022 propose a model of an epidemic that is being built in conjunction with the network's quarantine area. Whereby, it can lessen the severity of infections by regulating the spread of harmful attacks throughout the Internet of Things network. In order to determine the conditions necessary for stability, the constructed model is analyzed both at attack-free equilibrium points and endemic equilibrium points. In order to solve the system of ordinary differential equations, numerical methods are used, and simulation tools are used to simulate the problem to validate the viability of the newly developed mode. Finally, [11]the fundamental reproduction number, which determines the isolation and spread of the malicious object, determines whether the malicious attack succeeds or fails. It is achieved that the system is stable at the attack-free and endemic equilibrium point and that all equilibrium points are positive and confined by the user-defined area.

Prajakta et al. 2019 give a thorough analysis of machine learning and developments in reinforcement learning algorithms that aid in the creation of improved security measures for IoT devices. The proposed system uses LoRaWAN to connect to the Internet and wearable sensors to gather user data. These check the patient's body temperature, pulse rate, and other vital signs. a standalone local server that can display health information, process raw sensor readings, and send out alerts when an emergency is discovered. IoT cloud server implementation offers features like mobile applications and web monitoring. The architecture uses key management services and data categorization functions for security services. We used reinforcement learning with a security and privacy focus on IoT and took into account authentication, DDoS detection and mitigation, Man-in-the-Middle attacks, intrusion detection, and malware analysis. Encryption was utilized to ensure safe communication and entity authentication. Finally, [12] Prajakta et al. draw the conclusion that the system can avoid both host-based and network-based intrusion assaults and that the suggested prevention technique can also automatically recover trash data from an outside attacker.

Moreover, due to problems with the delivery of pharmaceuticals in healthcare systems (such as the complexity/invisibility of data sharing for many parties, patient privacy leaks, etc.), Ying et al. 2019 propose an architecture that might offer a reliable method of authentication between untrusted parties to keep a criminal agent from learning private drug transactions. whereby, dynamic identification is used to safeguard users' privacy and anonymity. Additionally, using blockchain, secure medicine transactions that are intended to ensure the confidentiality, integrity, and non-repudiation of shared data. According to a security analysis, [13]protocol successfully performs mutual authentication and is immune to attacks such as user impersonation, smart card loss, denial of service assaults, and database compromise. Moreover, Ying et al. protocol can deliver dependable service while preserving patient privacy.

A promising cellular network is the fifth-generation (5G), which offers users excellent service quality across a range of applications, including banking, education, and health. The most important challenge to this technology's dependence is security. The most crucial techniques in any mobile network are registration, authentication, and key agreement procedures with the subscriber and the network has a symmetric key in common and trusts one another. Researchers examined these protocols and found that there are still security issues; they proposed ways for key agreement and authentication. Contrarily, blockchain is one of the emerging technologies that, in the near future, is expected to have a big impact on how we live our lives. Various applications, such as Bitcoin and smart contracts, are granted blockchain security attributes, including authenticity and integrity. Therefore, in 2020 Haddad et al. introduced an innovative, safe, and efficient authentication and key agreement mechanism for 5G networks. Security research indicates that the suggested method is secure and resistant to all known threats, including denial of service, DDoS, man-in-the-middle, hijacking, and compromising. Moreover, [14] evaluation of performance reveals that the suggested method is more efficient than the existing scheme because it protects the small battery features of the user component and the network bandwidth.

Akkaoui 2021 suggests that patients' lives are increasingly in danger because of the recent rise of the smart healthcare age and patients' increased reliance on individualized health monitoring based on Internet of Medical Things (IoMT) devices[15]. Therefore, it is necessary to confirm the validity and dependability of these body sensors in a way that is unquestionable, believable, and auditable without the use of centralized administration. In an IoMT environment, data manipulation and hijacking are also of extreme importance. driven by the aforementioned difficulties. In 2021, Akkaoui [15] proposed a scalable authentication method based on smart contracts that are intended for the Internet of Things devices. The method addresses the weaknesses of conventional centralized systems, which are prone to distributed denial of service attacks, by utilizing blockchain technology's decentralization and security features. The consortium blockchain structure of the proposed method guarantees confidentiality, anonymity, and privacy, and provides secure firmware updates to ensure integrity. The implementation of the authentication process on Ethereum has been evaluated in terms of its computational and communication costs, and its security has been confirmed through a formal analysis using ProVerif. Additionally, the method protects patients from counterfeit devices by utilizing the physically unclonable function[15].

IOT HEALTHCARE ARCHITECTURAL LAYER

The IoT healthcare system has several obstacles and several security issues that vary from one area in terms of approach, motivation, development, and sometimes the complexity of the environment and the nature of the devices that are deployed. There is a requirement for an adaptable architecture that has some degree of flexibility built into it. This kind of architecture is made up of three different layers:

Perception Layer

This IoT architectural layer is responsible for perceiving and collecting all related data, such as patient medical information and physician ID information, it also provides location information of infrastructure, information on healthcare facilities, etc[16]. The devices can interact with the environment in which they have to work. The perception layer is in charge of figuring out what things are and gathering information about them[17].

Network Layer

This is one of the most important layers in an IoT healthcare application. It facilitates access to the IoT infrastructure and makes it easier for all medical data to be sent and received, especially when services are moved to an IaaS Cloud. This layer helps and gives a platform for most services that involve the patient, the medical staff, and other actors[16]. According to Karie et al. 2020 described perception layer and the application layer are connected through the network layer and it oversees ensuring that IoT devices are connected to one another and translated over a network[17].

Application Layer

This layer is in charge of configuring and installing applications that are in charge of the processing and computerization of all healthcare concern management, including radiography, physical therapy, diagnostics, and other related fields[16]. It’s the most important and best layer, the applications layer, which is in charge of delivering various applications to various IoT clients[1].

IOT ABILITIES

In terms of various domains, Dewangan et al. described the IoT capability as[18]:

i. Remote electronic health monitoring: The Internet of Things can be used to help with remote healthcare monitoring by utilizing the patient's real-time information.

ii. Secure communication: The architecture of the Internet of Things has been established and built to give appropriate security and privacy elements for the protection and confidentiality of personal information.

iii. Monitoring the Environment: The Internet of Things can help create a smarter environment by assisting with pollution control and disaster prediction, as well as by sounding an alarm in an emergency so that necessary action can be taken.

iv. Traffic Monitoring: This is utilized for the construction of smart city infrastructure, in which the Internet of Things (IoT) offers efficient control and administration of a city's traffic through the application of various technologies, devices, and networks.

v. Location Sensing: The use of RFID tags to track a person's whereabouts is an example of what is referred to as location sensing.

vi. Ad-hoc network: Ad-hoc networking allows for the network to be dynamically reorganized, resulting in constant connectivity.

Table 1 provides a concise overview of different attacks, how they are detected, and the countermeasures implemented to mitigate the associated risks in each case.

Table 1. Summarized Attacks on IoT Healthcare.

Ref.	Attacks	Detection Approach	Counter-Measure
[9]	Fingerprint, DoS assaults, Timing-based snooping, Router, Forwarding, Sensor, and Replay attacks	Early Intrusion Detection	Implementation of security best practices
[10]	Denial of Services	NAV time is updated illegally which exploits the duration field of the Clear To Send (CTS) frame.	Routine inspection of traffic format and pattern.
[12]	DDoS detection mitigation, malware analysis, man-in-the-middle attacks, intrusion detection.	Host-based and network-based intrusion assaults	Encryption was utilized to ensure safe communication and entity authentication.
[13]	Impersonation smart card loss Denial of service assaults Database compromise	An architecture that could prevent criminals from learning private drug transactions by authenticating untrusted parties.	Proposed a reliable, patient-privacy-preserving protocol.
[15]	DDoS (data manipulation and hijacking)	Smart contract-based scalable authentication	The proposed solution uses a blockchain structure that ensures confidentiality, anonymity, and integrity with secure firmware updates.

SECURITY ATTACKS RELATING TO IOT HEALTHCARE APPLICATIONS

Denial-Of-Service Attacks (DoS)

The purpose of denial-of-service attacks (DoS) is to stop Internet-of-Things (IoT) devices and apps from providing service. IoT components connect to networks to exchange data and communicate with each other. Applications for the IoT need to connect to networks in order to get data from the devices. Eken et al. described DoS assaults, also known as denial-of-service attacks, are potentially harmful to the Internet of Things applications because they target computer or network resources. Usually, the memory capacity of IoT devices is poor, and they also have a restricted bandwidth, battery life, and disc space [8]. As a result, they are susceptible to denial-of-service assaults (DoS) with relative ease.

Privacy

Privacy is any data or information relating to an identifiable individual. The data collected by IoT devices (sensors) are usually transmitted to the data storage on a cloud over the internet, and these devices can communicate with one another over the same internet. this means the patient’s data collected and transmitted by such devices is very vulnerable and must be kept secret [19]. In addition, data pertaining to healthcare are compiled from a variety of health institutions. Multiple health units collaborate to share patient information. Every unit is required to maintain the confidentiality of the data. because healthcare data contains information that is both vital and significant. All the cybercriminals in the world are working toward the goal of stealing sensitive health information. As a result, the confidentiality of the data must be maintained [8].

Data Manipulation

An attack can usually happen against data and privacy, those attackers can intend to attack the IoT healthcare devices trying to steal some sensitive information, or make some alteration or manipulate the data which causes the data to be damaged. The data attack can be on IoT devices during the transmission of the data over the Internet [20]. IoT healthcare applications rely heavily on data. Data is used across the healthcare system. As a result, attacks are directed at data security and privacy [21]. Data theft, data manipulation, and data damage are examples of attacks. Because it contains personally identifiable information, health data is vital and sensitive data for all countries throughout the world [8].

Power Optimization

Sensor devices are usually very small IoT devices, they are responsible for measuring and analyzing healthcare data from a patient’s body. But power consumption is one of the problems facing IoT healthcare devices due to being small in design and constantly collecting and transmitting patient data over the internet. This causes a serious problem for IoT healthcare devices [8]. Sometimes an intruder can easily find a way to drain such a tiny IoT healthcare device's battery. By doing so, an attacker can reduce the battery power of resource-constrained IoT devices [22].

Physical Attacks

IoT devices are often very small and can be integrated into a variety of products, including televisions, automobiles, air conditioners, ovens, and so on. Because of this, these gadgets are susceptible to being stolen or having their settings altered. Insecure Internet of Things (IoT) devices leave themselves vulnerable to cyberattacks because hackers can alter the data they send. IoT devices are vulnerable to a wide variety of physical attacks, including the theft of secrets, the manipulation of software, and the tampering of hardware[8].

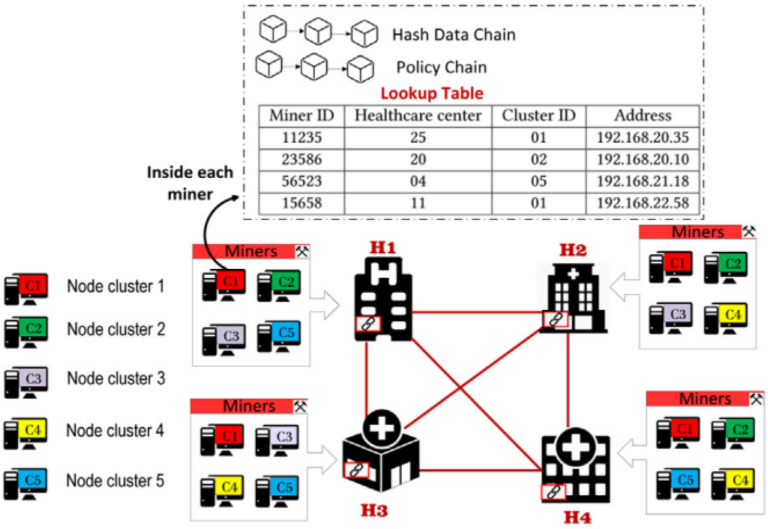
APPLICATION OF BLOCKCHAIN IN IOT HEALTHCARE SYSTEM

In 2021, Bodeis et al. described a blockchain as a distributed, decentralized database that stores records of digital events (transactions) that have taken place and have been shared among the people involved. Each transaction recorded in the public ledger is validated after receiving the unanimous approval of the vast majority of users who are logged into the system[23].

Blockchain Architecture in IoT Healthcare System

To address the trade-off issue between transparency and access control, Mohammad Hossein et al. present a novel architecture (BCHealth) based on blockchain that preserves privacy for IoT healthcare applications in 2021. This architecture allows data owners to specify their preferred access policies for their privacy-sensitive healthcare data. By using a clustering strategy to handle the real-world development difficulties of BC, such as scalability, latency, and overhead, BCHealth is made up of two distinct chains for storing access controls and data transactions. The effectiveness of BCHealth (in terms of computing and processing time) and its resistance to several security assaults are demonstrated through experimental analysis[24].

Figure 2 shows a blockchain health architecture made up of five separate clusters and four healthcare facilities. Each cluster's nodes might be affiliated with various healthcare facilities. The blockchain Health architecture specifically performs the following duties: Miners manage user access permissions, control decentralized patient and medical staff communication, monitor user IHM addresses, and identify changes in data in the IHM, alerting authorities about the alteration of original data through a new hash.



Lookup Table

Miner ID	Healthcare center	Cluster ID	Address
11235	25	01	192.168.20.35
23586	20	02	192.168.20.10
56523	04	05	192.168.21.18
15658	11	01	192.168.22.58

Figure 2. Blochchain Architecture in IoT Healthcare System

Figure 3 below shows a general healthcare blockchain application system, patient records are submitted as digital files. The blockchain encrypts the files, which are then maintained in a secure database or cloud storage and can only be viewed by persons with the proper authorization.

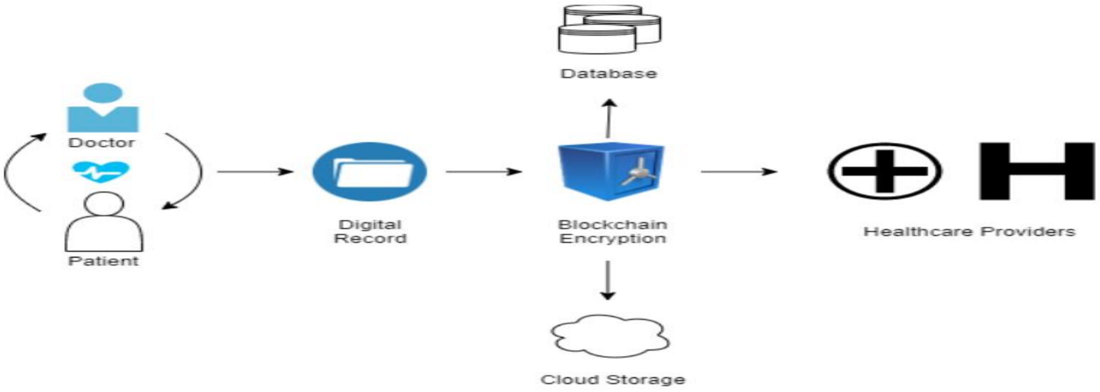
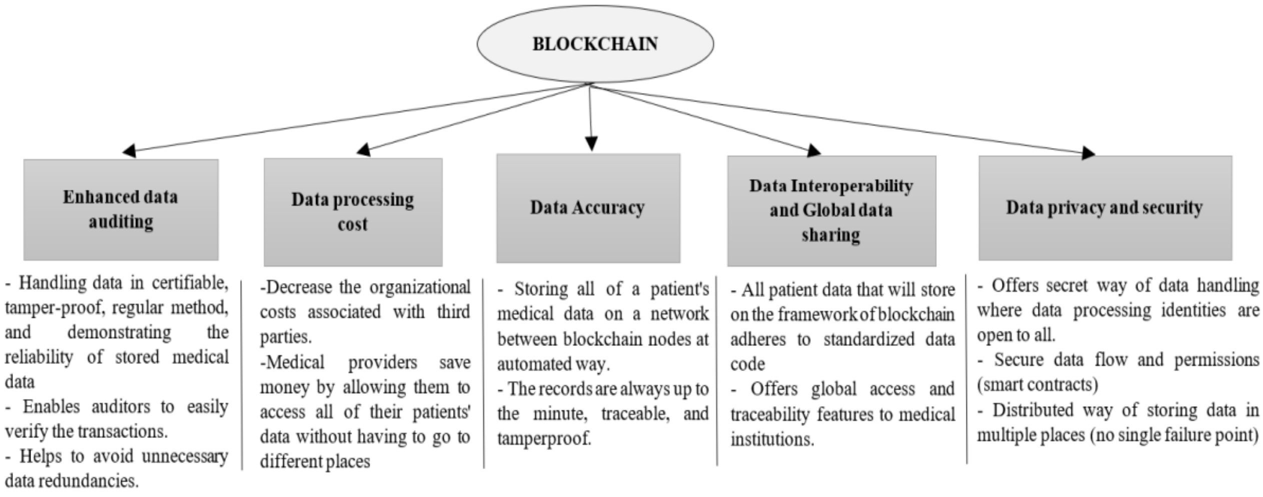


Figure 3. Healthcare Blockchain Application[23].

As seen in Figure 4 below, blockchain has a wide range of applications, including improving data audits to reduce the need for duplicate data and cutting costs related to third parties. Additionally, it is essential for data accuracy since it offers worldwide data sharing and access in a secure data flow while storing data in many locations and making sure that the records are tamperproof and traceable.


BLOCKCHAIN
Enhanced data auditing
Data processing cost
Data Accuracy
Data Interoperability and Global data sharing
Data privacy and security

- Handling data in certifiable, tamper-proof, regular method, and demonstrating the reliability of stored medical data
- Enables auditors to easily verify the transactions.
- Helps to avoid unnecessary data redundancies.

-Decrease the organizational costs associated with third parties.
-Medical providers save money by allowing them to access all of their patients' data without having to go to different places

- Storing all of a patient's medical data on a network between blockchain nodes at automated way.
- The records are always up to the minute, traceable, and tamperproof.

- All patient data that will store on the framework of blockchain adheres to standardized data code
- Offers global access and traceability features to medical institutions.

- Offers secret way of data handling where data processing identities are open to all.
- Secure data flow and permissions (smart contracts)
- Distributed way of storing data in multiple places (no single failure point)

Figure 4. Healthcare Blockchain Data Handling[23]

Table 2. Blockchain Solution To Healthcare's Biggest Problems [23]

Health Area	The main issue in the current healthcare industry	Blockchain solutions
Patient Record Management (PRM)	• Absent being granted access to all health records in whole • Extra costs and time • Patients cannot claim full ownership of their medical records	• Having access to full and longitudinal medical records • Prevent duplicate medical tests. • Increasing patient's records of their health data
Drug supply chain	• Fake drugs • Drug supply chain security • Safety of the drug supply chain • Connecting various drug dealers	• Eliminate the risk of fake medicines. • Ensure data is transparent and security
Research and Development	• Reporting incorrect clinical trial data • Lack of transparency	• Increases the trustworthiness of data. • Improves the accuracy of data analytics. • Improve the integrity of data in a trail.
Ensuring permissions consistency	• Irregular permissions • Access to data requires more time.	• Provides patient's data at moment's notice. • Offer seamless and secure permission management. • Reduces patient data collection
Telehealthcare system	• Virtual connection is vulnerable to security attacks. • Threats of patient's private and sensitive information leakage	• Eliminate the need for intermediaries. • Permits transactions across the network that are anonymous, safe, and unchangeable.
Healthcare insurance	• Involvement of multiple third parties • Time-consuming process • Riddle with inefficiencies	• Overcomes data interoperability problems. • Improved administrative process. • Help to detect fake insurance claims. • Assist in simplifying the insurance process
Healthcare billing system	• Consume more resources and time. • Lack of transparency and security features	• Makes the payment process much easier and more secure

The challenges in the existing healthcare sector from several domain areas are compiled in Table 2 above, along with a blockchain solution that improves the healthcare system. In 2021 Bodeis et al. presented an issue with classification in the sphere of blockchain applications in healthcare, it is possible for researchers to concentrate their study on understudied research areas in order to get the most out of their efforts. Researchers need to check in with themselves at regular intervals and ask themselves what topics have been adequately researched and what topics have not [23].

When it comes to healthcare analytics solutions, the data about patients should be the primary focus of attention. Protecting the privacy of data demands using the most effective design technique, since this leads to the data being secured with a high level of care [25]. In the current climate, many organizations have failed to offer adequate protection for data that is stored on a server and can be accessed by a third party [26]. In order to enhance data security and privacy, hence lowering bandwidth requirements and increasing operational effectiveness, for an Internet of Things (IoT)-based healthcare monitoring system, a consortium technique for reaching consensus known as Enhanced Proof of Work (E-PoW) blockchain has been proposed [27].

DISCUSSION

The velocity of technical advancement in an Internet-enabled global society, the emergence of social concerns, and increasing competitiveness for limited resources are all accelerating the transition to a data-driven world. Blockchain in this environment can provide IoT with a platform for sharing reliable data that defies non-collaborative organizations. Therefore, the integration of blockchain technology with Internet of Things (IoT) devices for remote patient monitoring brings both opportunities and problems that need to be solved. The application of blockchain in healthcare confronts difficulties, such as choosing cryptographic systems that are compatible with the needs and limits of IoT devices while taking into account resource restrictions and effective cryptographic algorithms for security and performance. Additionally, big data management concerns such as data ownership, transparency, security, confidentiality, verification, immutability, and inconsistencies from many sources may be addressed by applications in the healthcare sector. However, choosing cryptographic solutions suited to IoT requirements would help patients and providers while addressing practical issues.

The majority of IoT in healthcare depends on remote and real-time monitoring. The data collecting layer, network layer, computing layer, and analysis layer are the minimal number of layers that the IoT health system must have in order to adhere to the fundamental IoT architecture. The data-collecting layer may gather patient information from a variety of sensors for various medical purposes. IoT has completely changed the way healthcare apps are used by facilitating the real-time data gathering, analysis, and sharing of data from wearable sensors, medical devices, and other equipment.

There are a number of current solutions in IoT healthcare applications, such as patient care, diagnosis, treatment, and monitoring. The benefits of smart wearables have provided expansion of wearable technology, reduced the size of electronic sensors and devices, and progressions of low-power mobile networks at a fast speed. According to Verma et al. (2022), wearable technology can be used to detect issues related to healthcare, including illness detection, monitoring, and treatment. The advantages of smart wearables have accelerated the development of low-power mobile networks, the tiny size of electronic sensors and gadgets, and expanded wearable technology. The study in [28]suggested the use of wearable devices in detecting concerns in healthcare, such as curing, monitoring, and illness detection, with a focus on the use of IoT architecture and its wearable devices.

IoT healthcare apps have a lot to offer, but for their implementation to be safe and successful, several weaknesses and challenges need to be addressed. The current IoT healthcare application solutions have several major flaws and challenges, including concerns about security and privacy, interoperability, data accuracy and reliability, and ethics[29]. From the perspective of security and privacy issues, Venu et al. 2022 highlighted that IoT healthcare applications have weaknesses and challenges due to vulnerabilities in IoT devices and sensors, making the transmitted data susceptible to cyber-attacks. The primary challenge lies in implementing robust security measures such as authentication, access control, and strong encryption techniques to ensure privacy and data integrity[30]. In addition, given the accuracy and reliability of the IoT healthcare system, IoT sensors and devices maintain massive amounts of data, but sometimes they deliver incorrect or unreliable data, which causes treatment decisions to be made incorrectly[30]. As a result, quality control procedures must be put in place, and IoT healthcare apps must guarantee the reliability and accuracy of the data they provide. It might be quite challenging to manage and operate various multiple IoT devices from different platforms. To ensure that services are available to all users of the healthcare system, agreement between the IoT designer and application developer is necessary, regardless of the hardware platform. The most popular examples are the several platforms that mobile communication technologies like GSM and Wi-Fi use to guarantee interoperability[31]. Rayan et al., 2021 [32] suggested that the acquisition of a large volume of patient data presents ethical issues regarding data ownership, consent, and the possibility of discrimination, which is another flaw and difficulty in the IoT healthcare application. Transparency in data collection and ethical rules should be implemented to mitigate such concerns.

At last, IoT healthcare applications and systems must be safe, efficient, and easily accessible while protecting patient privacy and data security. Therefore, a multidisciplinary approach involving healthcare professionals, technology experts, policymakers, and regulatory bodies should be engaged to overcome the challenges and weaknesses in IoT healthcare applications, which highlights the need for this approach.

CONCLUSION

In conclusion, this paper has explored the integration of IoT in healthcare applications, highlighting data collection and transmission capabilities and addressing security attacks like DoS attacks and privacy breaches. This paper highlights the need for continuous innovation to address challenges and complexities, while also highlighting the potential of emerging technologies like blockchain. This paper also discussed the application of blockchain in IoT healthcare systems and how this technology will improve the sector since patient data is collected via IoT devices, and networks to perform an analysis. This paper discussed the existing conversation and encouraged additional investigation of solutions that might raise the standard for security, privacy, and effectiveness in IoT-based healthcare applications. Future work could investigate the challenges of data processing in Blockchain Internet of Healthcare applications (BIoH).

ACKNOWLEDGMENT

We would like to express our gratitude to Universiti Teknologi Malaysia for the support of this research.

REFERENCES

[1] A. Devibala, "A Survey on Security Issues in IoT for Blockchain Healthcare," in *Proceedings of 2019 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2019*, Coimbatore, India: IEEE, 2019, pp. 1–7. doi: 10.1109/ICECCT.2019.8869253.

[2] N. Chauhan and R. K. Dwivedi, "A Secure Design of the Healthcare IoT System using Blockchain Technology," in *Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development, INDIACom 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 704–709. doi: 10.23919/INDIACom54597.2022.9763187.

[3] "What Is Blockchain and How Does It Work? | Synopsys." Accessed: Jan. 25, 2023. [Online]. Available: https://www.synopsys.com/glossary/what-is-blockchain.html

[4] G. S. Gunanidhi and R. Krishnaveni, "Improved Security Blockchain for IoT based Healthcare monitoring system," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1244–1247. doi: 10.1109/ICAIS53314.2022.9742777.

[5] R. K. Kodali, G. Swamy, and B. Lakshmi, "An implementation of IoT for healthcare," in *2015 IEEE Recent Advances in Intelligent Computational Systems, RAICS 2015*, Institute of Electrical and Electronics Engineers Inc., Jun. 2016, pp. 411–416. doi: 10.1109/RAICS.2015.7488451.

[6] S. Chakraborty, S. Aich, and H. C. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," in *International Conference on Advanced Communication Technology, ICACT*, Institute of Electrical and Electronics Engineers Inc., Apr. 2019, pp. 260–264. doi: 10.23919/ICACT.2019.8701983.

[7] A. Yogeshwar and S. Kamalakkannan, "Healthcare domain in IoT with blockchain-based security- A researcher's perspectives," in *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, Institute of Electrical and Electronics Engineers Inc., May 2021, pp. 440–448. doi: 10.1109/ICICCS51141.2021.9432198.

[8] C. Eken and H. Eken, "Security Threats and Recommendation in IoT Healthcare," in *Proceedings of The 9th EUROSIM Congress on Modelling and Simulation, EUROSIM 2016, The 57th SIMS Conference on Simulation and Modelling SIMS 2016*, Linköping University Electronic Press, Dec. 2018, pp. 369–374. doi: 10.3384/ecp17142369.

[9] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT Smart Health Security Threats," in *Proceedings - 2019 19th International Conference on Computational Science and Its Applications, ICCSA 2019*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 26–31. doi: 10.1109/ICCSA.2019.000-8.

[10] S. A. Butt, T. Jamal, P. Amaral, and A. Butt, "Denial of Service Attack in Wireless LAN," in *12th International Conference on Digital Society and eGovernments (ICDS 2018), Proceedings*, Rome, Italy: IARIA, 2018, pp. 42–47. [Online]. Available: https://thinkmind.org/index.php?view=article&articleid=icds_2018_3_10_10051

[11] S. Kalam and A. K. Keshri, "Epidemic model on Denial of Service attack in IoT network," in *2022 International Conference on IoT and Blockchain Technology, ICIBT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICIBT52874.2022.9807815.

[12] K. Prajakta and A. Gawade, "Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks," in *2019 International Conference on Contemporary Computing and Informatics (IC3I)*, Singapore: IEEE Amity Global Institute, 2019, pp. 69–73. doi: 10.1109/IC3I46837.2019.9055531.

[13] B. Ying, W. Sun, N. R. Mohsen, and A. Nayak, "A Secure Blockchain-based Prescription Drug Supply in Health-care Systems," in *The 2019 International Conference on Smart Applications, Communications and Networking (SmartNets 2019) : December 17-19, 2019, Sharm El-Sheikh, Egypt*, Sharm El-Sheikh, Egypt: Institute of Electrical and Electronics Engineers IEEE Communications Society, 2019, pp. 17–19.

[14] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based Authentication for 5G Networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, Doha, Qatar.: Institute of Electrical and Electronics Engineers. Qatar Section., 2020, pp. 189–194. doi: 10.1109/ICIoT48696.2020.9089507.

[15] R. Akkaoui, "Blockchain for the Management of Internet of Things Devices in the Medical Industry," *IEEE Trans Eng Manag*, vol. 70, no. 8, pp. 2707–2718, 2021, doi: 10.1109/TEM.2021.3097117.

[16] A. Djenna and D. Eddine Saïdouni, “CSNet’18 : 2018 2nd Cyber Security in Networking Conference (CSNet) : Paris, France, October 24 - 26, 2018,” in *2018 2nd Cyber Security in Networking Conference (CSNet)*, Paris, France: IEEE, 2018, pp. 1–4. doi: 10.1109/CSNET.2018.8602974.

[17] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, “IoT Threat Detection Advances, Challenges and Future Directions,” in *Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 22–29. doi: 10.1109/ETSecIoT50046.2020.00009.

[18] K. Dewangan and M. Mishra, “Internet of Things for Healthcare: A Review,” *International Journal of Advanced in Management, Technology and Engineering Sciences*, vol. 8, no. 3, pp. 526–534, 2018.

[19] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 32979–33001, May 30, 2018. doi: 10.1109/ACCESS.2018.2842685.

[20] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security,” *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, Jul. 2022, doi: 10.1016/j.eij.2022.02.004.

[21] “IoT in Healthcare: Benefits, Challenges and Applications In February 2023.” Accessed: Feb. 03, 2023. [Online]. Available: https://www.valuecoders.com/blog/technology-and-apps/iot-in-healthcare-benefits-challenges-and-applications/

[22] M. Rana, Q. Mamun, and R. Islam, “Lightweight cryptography in IoT networks: A survey,” *Future Generation Computer Systems*, vol. 129. Elsevier B.V., pp. 77–89, Apr. 01, 2022. doi: 10.1016/j.future.2021.11.011.

[23] W. Bodeis and G. P. Corser, “Blockchain adoption, implementation and integration in healthcare application systems,” in *Conference Proceedings - IEEE SOUTHEASTCON*, Atlanta, GA, USA: Institute of Electrical and Electronics Engineers Inc., 2021, pp. 1–3. doi: 10.1109/SoutheastCon45413.2021.9401885.

[24] K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, “BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications,” *Comput Commun*, vol. 180, no. December 2020, pp. 31–47, 2021, doi: 10.1016/j.comcom.2021.08.011.

[25] G. S. Gunanidhi and R. Krishnaveni, “Improved Security Blockchain for IoT based Healthcare monitoring system,” in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1244–1247. doi: 10.1109/ICAIS53314.2022.9742777.

[26] M. A. Bazel, F. Mohammed, and M. Ahmed, “Blockchain technology in healthcare big data management: Benefits, applications and challenges,” in *2021 1st International Conference on Emerging Smart Technologies and Applications, eSmarTA*, Sana’a, Yemen: Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 1–8. doi: 10.1109/eSmarTA52612.2021.9515747.

[27] G. Srivastava, J. Crichigno, and S. Dhar, “A Light and Secure Healthcare Blockchain for IoT Medical Devices,” in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, Edmonton, AB, Canada: IEEE, 2019, pp. 1–5. doi: 10.1109/CCECE.2019.8861593.

[28] D. Verma *et al.*, “Internet of things (IoT) in nano-integrated wearable biosensor devices for healthcare applications,” *Biosens Bioelectron X*, vol. 11, p. 100153, 2022, doi: https://doi.org/10.1016/j.biosx.2022.100153.

[29] V. K. Quy, N. Van Hau, D. Van Anh, and L. A. Ngoc, “Smart healthcare IoT applications based on fog computing: architecture, applications and challenges,” *Complex and Intelligent Systems*, vol. 8, no. 5, pp. 3805–3815, 2021, doi: 10.1007/s40747-021-00582-9.

[30] D. Venu, D. ArunKumar, and K. V.-I. J. Of, “Investigation on Internet of Things (IoT): Technologies, Challenges and Applications in Healthcare,” *International Journal of Research*, vol. 11, no. 3, pp. 143–153, 2022.

[31] M. S. Al-kahtani, F. Khan, and W. Taekeun, “Application of Internet of Things and Sensors in Healthcare,” *Sensors (Basel) 2022*, vol. 22, no. 15, pp. 1–20, doi: https://doi.org/10.3390/s22155738.

[32] R. A. Rayan, C. Tsagkaris, and R. B. Iryna, “The Internet of Things for Healthcare: Applications, Selected Cases and Challenges,” in *Studies in Computational Intelligence*, vol. 933, Singapore: Springer, Singapore, 2021, pp. 1–15. doi: 10.1007/978-981-15-9897-5_1.