Integrating IoMT and Block chain in Smart Healthcare: Challenges and Solutions

[1]Subhra Prosun Paul, [2]Subba Reddy, [3]Helaria Maria, [4]Balaji T, [5]Balamurugan A G and [6]Radha Mothukuri
[1]Department of Computer Science and Engineering, Uttara University, Dhaka, Bangladesh, South Asia.
[2]Department of Computer Science and Engineering, Sai Rajeswari Institute of Technology, Proddatur, Andhra Pradesh, India.
[3]Department of Computer Science, New Horizon College, Bangalore, Karnataka, India.
[4]Department of Computer Science and Engineering (Data Science), Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India.
[5]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sakunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India
[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
[1]subhra.phd.cu2021@gmail.com, [2]y.subbareddy@gmail.com, [3]helariax@gmail.com, [4]baalaji24@gmail.com, [5]agbm366@gmail.com, [6]radha@kluniversity.in

Correspondence should be addressed to Subhra Prosun Paul : subhra.phd.cu2021@gmail.com

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202404108
Received 02 March 2024; Revised from 08 June 2024; Accepted 28 August 2024.
Available online 05 October 2024.

Abstract – For the past couple years, blockchain technique has been growing as a technique for providing innovative services in various commercial applications, including medical sectors like smart healthcare systems. The blockchain technique is effectively implemented in the Internet of Medical Things (IoMT), patient's electronic health record systems, precise disease detection, and so on. It not only provides efficient data management functionalities such as data storage and exchanging of medical data among various parties involved in the healthcare system but also resolves several privacy and security-related issues of doctor's and patients' sensitive medical data meritoriously. With the help of several cryptographic algorithms and data decentralization methods, such as smart contracts, blockchain is used to ensure health data confidentiality without imposing third-party activities. For the privacy and security analysis of blockchain oriented healthcare systems, both asymmetric and symmetric key cryptographic mechanisms are applied in public and private blockchain mechanisms in order to increase the inclusive performance of secured healthcare systems. This paper's problem statement aims to detect the significant issues and challenges of blockchain-based healthcare systems from a general point of view, as well as security and privacy-related points of view. A comprehensive guideline to handle those issues and challenges is also explained in this paper very carefully. Furthermore, a comparative study of blockchain-oriented healthcare systems is discussed in this article to segregate our research involvement and current studies being conducted in this corresponding area.

Keywords – Blockchain Technology, Privacy and Security, Issues and Challenges, Medical Data Management, Healthcare System, Internet of Medical Things (IoMT)

I. INTRODUCTION

The most recent technological advancement in the medical and healthcare domains is the smart healthcare system (SHS). SHS's primary goal is to expedite patient care, lower costs, and simplify the medical treatment process. Applications of SHS include telehealth services, smart home healthcare, and smart hospitals. All of these are internet-based. These SHS applications are configured through the use of flexible technologies such as IoMT, smart medical devices such as implantable and wearable sensors, and remote observation tools [1]. It is a type of healthcare system (HS) where patients, doctors, hospitals, and diagnostic centers are remotely connected and can communicate with each other through internetwork. SHS is nothing but a system where several medical wearable sensor devices can be attached to patients, which collects necessary medical data from the patient's human body and can transfer that information to hospitals and diagnostic centers. These organizations process medical information and generate some results. After that, this processed medical information is again transmitted to doctors so that they can take the necessary treatment steps. Doctors can directly

communicate with patients and advise on required medication through the internet. So, it is observed that the total process can be generated through the network, where privacy and security are important parameters. In this system, because of the sensitive patient medical data as well as the patient's and doctor's personal data, confidentiality, privacy, and security should be maintained [2].

Healthcare institutions that use cutting-edge ideas and modern technology to enhance patient care and operational efficiency are referred to as "Smart/Digital Hospitals". With healthcare companies realizing more and more that they need creative ways to lower costs and enhance patient care quality, the idea of "smart hospitals" has gained traction [3]. We'll look at the benefits of smart hospitals, namely how they can make medical facilities run more efficiently:

Streamlining Procedures

In order to reduce inefficiencies and simplify procedures, smart hospitals employ technology. For instance, by doing away with paper-based systems in favor of digital medical records, medical professionals may communicate more effectively and retain records more quickly and accurately. Furthermore, staff time can be freed up and wait times decreased with automated systems for patient check-in, appointment scheduling, and other duties.

Better Patient Care

Smart hospitals use technology to give more precise and timely diagnoses, more individualized treatment regimens, and enhanced patient-provider communication. For instance, telemedicine technology can help medical professionals watch patients from a distance, cutting down on the number of hospital visits and infection risks. Digital imaging technologies can also assist doctors in diagnosing patients more precisely, which can result in more successful treatment strategies [4].

Enhanced Protection

Technology is used by smart hospitals to improve security and safeguard patient information. In light of the growing risk of cyberattacks in the healthcare sector, Smart Hospitals can protect confidential patient data by using cutting-edge security protocols. For instance, the confidentiality and integrity of medical records can be preserved with the use of blockchain technology.

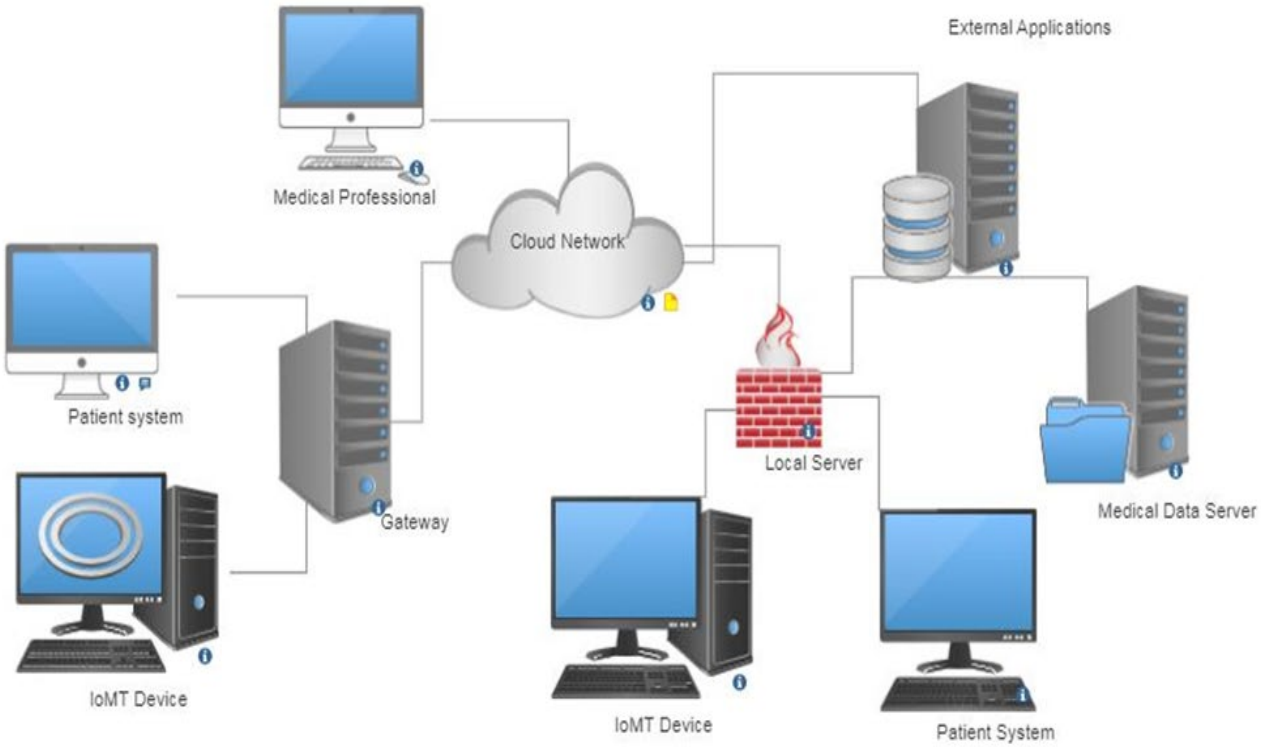

Fig 1. Smart Healthcare System.

Diminished Expenses

By employing technology to enhance operational efficacy, Smart Hospitals can further minimize expenses. Digital technologies have the potential to optimize supply chain management for healthcare enterprises, leading to cost savings and waste reduction. Furthermore, by freeing up employee time for more difficult jobs, automated systems can save labor expenses.

Improved Resource Distribution

Smart hospitals employ technology to more effectively distribute resources, including personnel, supplies, and medical equipment. Digital technologies can assist healthcare businesses, for instance, in monitoring inventory levels and guaranteeing the availability of essential goods at all times. Furthermore, by anticipating patient demands and allocating resources appropriately, predictive analytics can assist healthcare providers in improving patient outcomes [5].

Fig 1 shows the simple operational direction of SHS. There are several prime aspects of SHS, such as remote-level observation, prognostic analytics, telemedicine, online-based health records, medical supply chain management, patient active participation, and overall system data security. Out of these aspects, in telemedicine, patients can consult with doctors or healthcare providers from any remote location in order to improve healthcare service access. In order to digitize a patient's health record, an electronic health record system (eHRS) is required, which makes it easier to access and share with different parties in SHS [6]. Patients can be assisted by accessing various apps. and portals in order to control their own health. This can be achieved by utilizing different services like doctor's appointment fixation, treatment remainder, and health awareness resources from those apps and portals. On the other hand, aided by artificial intelligence and machine learning (ML) methods, SHS can predict disease accurately, detect high-risk patients, and provide private treatment procedures [7].

Blockchain technology is an emerging technique that is commendably implemented in the healthcare system in today's world. It is a type of progressive database technique that allows luminous information exchange within a commercial network. Basically, this technique preserves data in blocks which are linked to each other through a chain. Blockchain assists in the secure storage and sharing of data throughout the system [8]. There are various applications of BC technology in the commercial sector, like money transfers, smart contracts, the internet of things, and personalized identity safes, which are related to the healthcare system. There are four basic steps to creating BC:

I. We have to create the block.
II. We have to add data to each block, which is alienated into two sections: the header and the body.
III. We have made a hash of the block.
IV. We have to create chains to connect the entire block to each other.

Blockchain is a ledger technique that is decentralized and distributed by nature. It reserves all transactional information safely throughout the network. In the healthcare system, this technique has a significant contribution and impact on data management and security-related purposes [9].

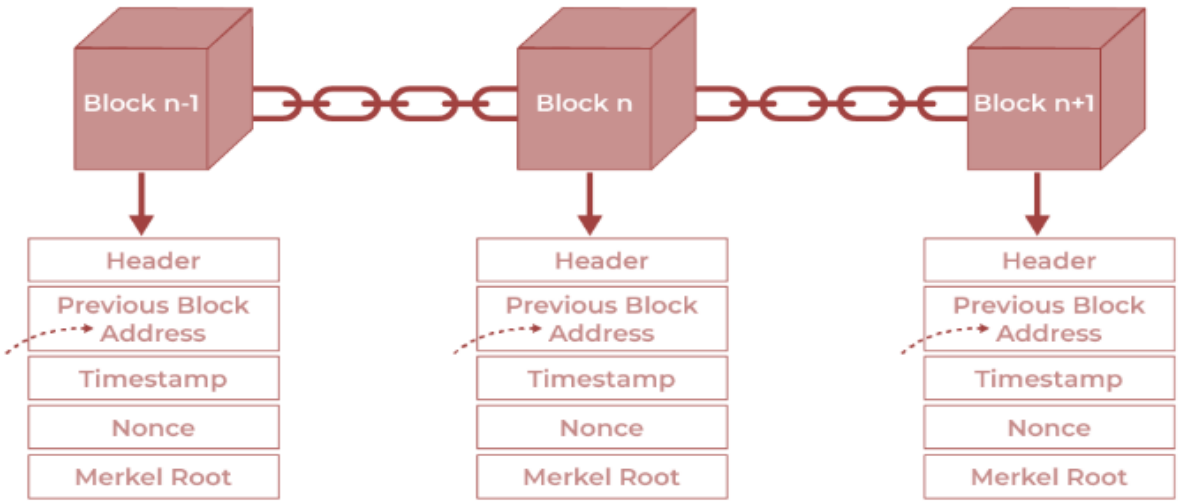

Fig 2. Block Diagram of Blockchain Technology.

Fig 2 illustrates the basic structure of BC technology, where multiple blocks are connected with each other through a chain network. Each block consists of several pieces of information, like the header, address of the previous block, timestamp, nonce, and Markel root values. Blockchain can be applied in the healthcare system in various ways, like medical supply chain supervision activities, online-based identity management, monetary and health insurance recording, medical research, and relevant data access processes. In order to expand the quality of data and diminish healthcare costs, the BC mechanism suggests several data management schemes [10]. In the event that sharing medical data among several parties in SHS, the BC technique develops the data accuracy level and data access method. Drug detection is very secure by using the BC technique in SHS. BC performs a significant role in various medical trial detection schemes safely [11].

Organization of the Paper

The following is the structure of this paper: In the introduction part, the technical concepts of IoMT and SHS are given. How IoMT and BC techniques can be implemented in SHS is discussed in the background study section with reference to some recent research work. Several remarkable outcomes of existing research on this topic are stated in the outcome of the literature genesis overview portion. In the proposed framework part, architecture of secured BC-based SHS is depicted. In Section 5, some noteworthy issues and challenges of IoMT and BC-based SHS are highlighted. Section 6 states some recommended strategies to manage these disputes and challenges effectively. The comparative analysis section reflects the clear differences between the purpose of this work and the state of the field's study. The conclusion section sincerely mentions the overall contribution of this paper in this field.

II. BACKGROUND STUDY

It is already mentioned that IoMT is a leading technology implemented in SHS in the current medical field. IoMT is nothing but an amalgamation of versatile medical hardware and system applications that communicate with the healthcare system via internetwork. It can be used with the help of mobile computing techniques, cloud-computing systems, and various wearable and implantable healthcare sensors in order to observe patient's medical status through real-time medical data analysis [12]. There are various types of IoMT devices used in SHS, like home IoMT, wearable IoMT, mobile IoMT, public IoMT, and hospital IoMT. For example, an infusion pump is a hospital IoMT device, a networked glucometer attached to a smart phone is a mobile IoMT device, a pacemaker is a wearable IoMT device, and so on. This can be done by collecting medical metrics like heart rate, human body temperature, oxygen level, blood pressure, and many more from client patients who are in a remote location. There should be a communication network and secured channel among patients, doctors, and hospitals in SHS. This can be achieved by implementing an efficient cryptographic protocol.

The main goal of using IoMT in the HS is to eliminate the necessity of patients' frequent hospital visits as well as reduce treatment expenditures. By using instance-based health data analysis, healthcare providers can take rapid action, and thus the best healthcare service can be ensured in SHS. It also simplifies the overall medical treatment process for all parties related to SHS. Data availability, an easy and quick patient observation process, and better overall patient medical experiences are the advantages of IoMT-based SHS. But apart from these benefits of using the IoMT technique in SHS, there are still some challenges, like malware attacks and device hijacking. Malevolent software applications can penetrate and restrict the activity of IoMT hardware, which affects their disease diagnosis accuracy and efficacy [13]. Device hijacking can make illegal access to manage medical devices possible through the unapproved manipulation of sensitive medical data, posing grave dangers to patient safety. It can be mentioned here that in the last COVID-19 pandemic, this IoMT technique performed its best functionalities in SHS.

It's understandable why privacy and security are major concerns in the healthcare industry given the sensitive patient data and medical records involved. For hackers and criminal organizations, hospital data and equipment are like gold mines. The introduction of a networked system, such as a smart hospital, makes those goldmines even more accessible. First of all, conventional medical equipment is antiquated and insecure by design [14]. This implies that many would not have been designed to interface with smart appliances or the internet, or evaluated for vulnerabilities. (To be honest, it's a difficult undertaking to predict the fourth industrial revolution.) Attackers may be able to access systems and data illegally thanks to this vulnerability. According to an ENISA investigation, ransomware holds patient data hostage and steals it through malware blitzes and denial of service (DDoS) assaults that take over devices and systems. These types of attacks are the biggest threat to smart hospitals. Attacks on medical facilities and hospitals have sharply escalated since the COVID-19 epidemic, as evidenced by the ransomware-related death that occurred in Germany. Still one of the main risks to patients is human mistake. Consider drug pumps, which allow patients to receive precisely dosed prescriptions from smart hospitals or, more precisely, their staff. These systems contain an override button in case of emergency, but they also prevent over- or under-administration. What happens, though, if the device is incorrectly configured? It is possible for drug distribution to be tampered with, either purposefully or unintentionally, with fatal results. Technologists and healthcare professionals collaborate on projects related to the smart hospital, which goes beyond IT department initiatives alone. To guarantee that smart systems can save more lives, ongoing cooperation is required to defend it against cyber threats [15].

Fig 3 presents the architecture of IoMT and BC-based SHS. Apart from the IoMT technique, blockchain is another leading technique that is now frequently implemented in SHS. Blockchain is primarily used to store the data collected from different locations. After collecting the health data from the patient's body through various sensor devices, it is transmitted through an app to a BC network [16]. Online blockchain contracts facilitate the teamwork scheme of medical sensors and other healthcare devices. Apart from this, the distributive ledger method provides secure transmission of patient medical records. It ensures centralized, secure data storage for SHS. In order to do this effectively, several consensus mechanisms and smart contract techniques are being used. There are many efficient consensus mechanisms, like the POX series: proof of work, proof of stack, and zero knowledge proof algorithms, used in SHS. In order to diminish the incidental error quantity and fraud cases in medical experimental records, blockchain is effective. Additionally, it proves the best-choosy reporting of medical experiments in SHS. BC is an appropriate method for traceability, confidentiality, interoperability, and validity of data for healthcare applications [17].

Strengthening patient privacy is one of the main advantages of integrating blockchain and IoMT together. Blockchain has several uses and capabilities in the healthcare industry. With the ability to manage the medicine supply chain, provide

safe patient medical record transfers, and facilitate genetic code discovery, ledger technology aids in the discovery of genetic codes by healthcare researchers. Sensitive health information is kept safe and unchangeable because to blockchain's decentralized architecture. Only authorized people or companies will be able to access patient records and data that are kept on the blockchain. Healthcare has long placed a high priority on patient privacy. Patients now have sovereignty over their own data thanks to blockchain technology, which solves this problem. Blockchain allows patients to control who has access to their medical records and to transparently and securely record any changes made to their data [18]. Medical blockchain technology is used by healthcare professionals to produce, amend, and store new patient health records in a HIPAA-compliant manner without allowing unauthorized access to the data or record changes. Sturdy patient privacy protection, efficient data transfer, improved communication, and heightened confidence throughout the healthcare system are all benefits of integrating blockchain technology with IoMT devices [19].

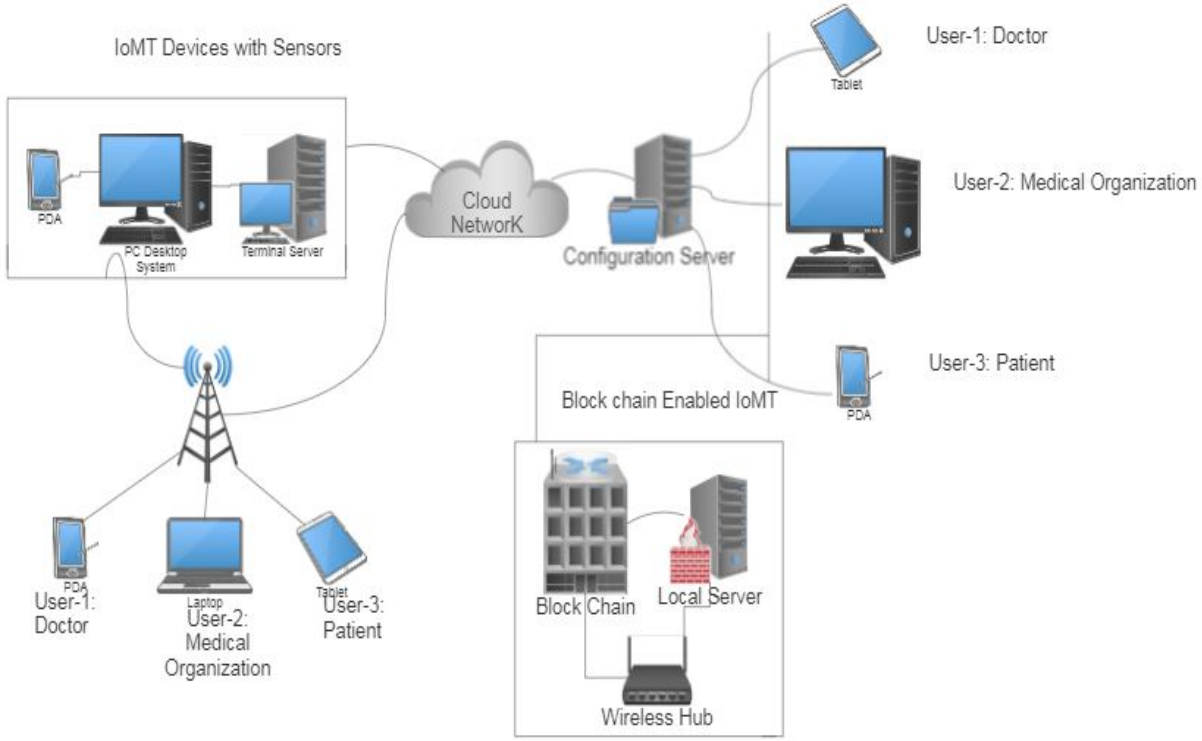

Fig 3. IoMT and Blockchain Oriented SHS.

III. OUTCOME OF THE LITERATURE GENESIS OVERVIEW

This An evaluation of SHS's current research project shows that there has been tremendous development in this area in the last few years. In this case, we have reviewed the last ten (2014–2023) years' research articles, which are considered from some standard research databases like Scopus, Web of Science, etc.

IoMT

Research shows that artificial intelligence (AI) has developed the capacity of IoMT, and point-of-care-based medical hardware is used to detect and treat various lethal diseases like cancer, cardiac arrest, diabetes, and so on. In the modernized biomedical implementation field, AI supports improved robotic surgery, which is the latest development in SHS [20]. The chi-square algorithm helps to construct an automated patient observation process where the last updated health status will be informed to the patient's and patient attendant's email by using a decision support system. BioSenHealth is another significant development of IoMT-based SHS, which is a functional prototype. This prototype analyses real-time patient medical data that is taken from sensors and transferred to the doctorthingspeak.com channel. This mechanism is also used for remote location patient continuous monitoring. It is also noticed that efficient training methods based on deep neural networks serve the same purpose. Apart from these, various machine learning (ML) techniques like KNN, random forest, and decision trees are used for disease prediction, detection, and drug management in IoMT-oriented SHS [21].

Blockchain

BC is another key technology used in SHS, which is basically for privacy and security purposes. Existing research states that BACKM-EHA is an access control mechanism that manages the keys successfully among various parties in SHS for data security purposes. This scheme is' 'real or random' structure based, which is effective in handling many probable attacks in the SHS network. Simultaneously, BC is being used for a digital health record management system. During the

data transmission phase of the SHS network, a hybrid encryption scheme based on a convolutional neural network is used to maintain data privacy. This technique is implemented using the Lion optimization scheme. Additionally, we have observed that BC is widely used for reliability and the sharing of data among different authorities in SHS [22]. Basically, this can be accomplished by implementing consensus mechanisms for the authenticity of health data and the safety of transactions that are operated in SHS. In order to handle restricted data scalability problems, the GHOSTDAG mechanism is introduced, which is designed using Satoshi's BL and blocks of an acyclic graph. The smart contract concept is also used to analyze medical data management in BC-based SHS [23].

IV. PROPOSED FRAMEWORK

The following **Fig 4** depicts a proposed framework for a secured BC-based SHS. In this architecture, there will be a remote user's system and a local network system, both of which can exist. A local network is designed for hospitals and diagnostic centers where multiple systems can be connected. On the other hand, a remote system is for patients and doctors. Both patients and doctors can be connected to the local network through the internet. This means that medical data will be transmitted from patient to hospital and diagnostic center, and then from hospital and diagnostic center to doctor. After analyzing medical data, doctors can share the resulting information with hospitals and diagnostic centers, and they can deliver that doctor's information to patients. For follow-up and future reference, the medical record can be stored in BC. A cryptographic mechanism like the consensus protocol can be implemented during the data sharing phase from the hospital or diagnostic center to BC. Additionally, any homomorphic encryption mechanism can be implemented during the data sharing phase among patients, hospitals, diagnostic centers, and doctors for data security.

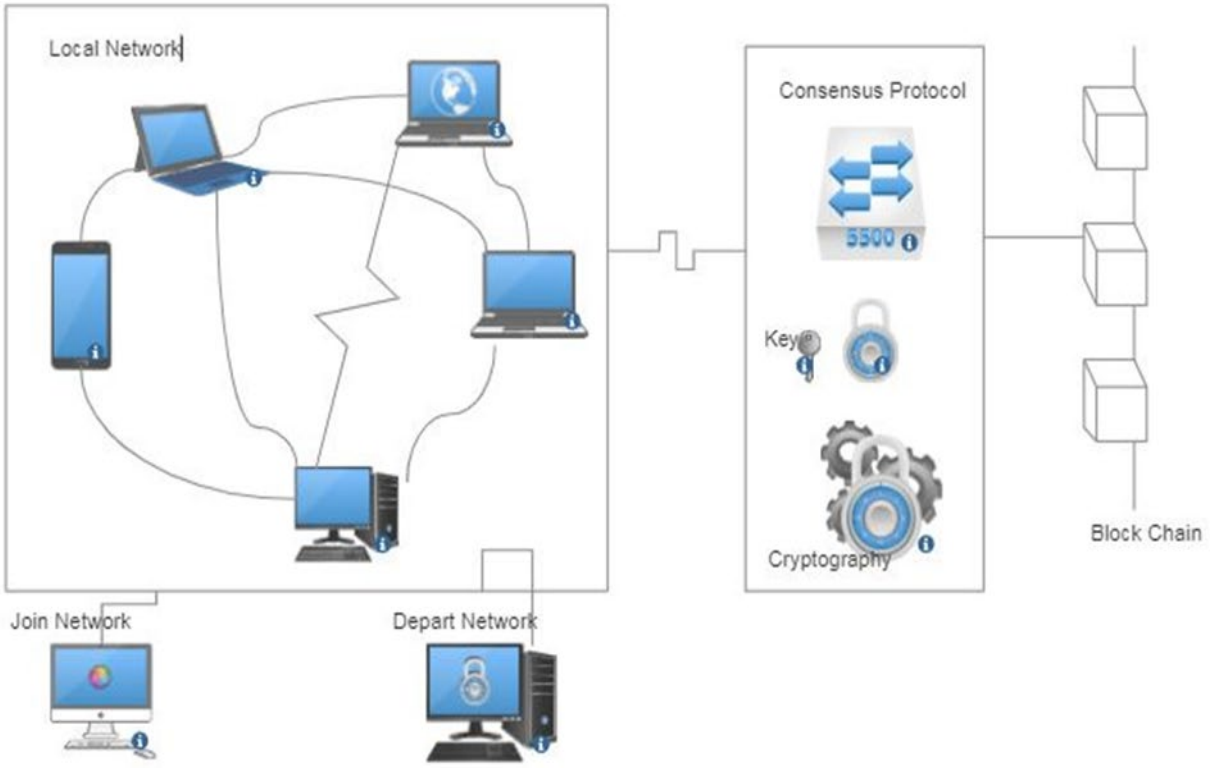

Fig 4. Proposed Framework of Secured Blockchain Oriented SHS.

V. ISSUES AND CHALLENGES OF IOMT AND BLOCKCHAIN BASED SHS

It is already mentioned that there is rapid technological progress in IoMT and BC-oriented SHS day by day, but still, there are some remarkable issues and challenges in this field. Out of these challenges, security and privacy are the key concerns. Although scientists are working on this issue for SHS, until now, data security has not been 100 percent ensured. After a thorough exploration of existing research work in this area, we have identified several prime issues and challenges, which are mentioned in the following:

IoMT-based Issues and Challenges of SHS

IoMT provides so many user-friendly and advantageous features in SHS to perform an overall smooth operation. There are a number of common and security-related issues in IoMT-based SHS. They are:

Health Data Confidentiality
There are several types of attacks, like eavesdropping, traffic analysis, impersonation, and interrogation attacks. In these types of attacks, networks may be vulnerable to threats to data security.

Data Integrity
In this case, MitM, physical, and malware attacks are involved. In this type of attack, data may be altered during the transmission phase between two parties throughout the IoMT network. Even in a physical attack, stored data may be modified, as it is the most harmful attack [24].

Authentication and Authorization
Authentication involved forgery, Sybil, device cloning, and masquerading attacks. In this type of attack, a malevolent user can be treated as an authenticated user. After that, the attacker tries to transfer false data to defraud other real data. On the other hand, authorization involves social engineering and malware attacks. In this case, vulnerabilities can occur in IoMT devices, and as a result, attackers may have access to the health data of medical sensor devices.

Interoperability
The versatile hardware configuration of various devices in IoMT can use different data transmission protocols, which makes the transmission process complex.

Data Organization
IoMT sensors and other hardware generate an abundance of data that may be difficult to maintain and perform relevant processing.

Dependability and Correctness
In order to maintain patient's safety and proper healthcare service delivery, devices of SHS's accuracy and dependability level are a challenging issue as they are network attack-prone.

Cost and Versatility
The hardware and software configuration of medical devices, as well as their maintenance expenditure for small-scale SHS may be challenging.

Moral and Legitimate Issue
Sometimes these types of issues may be recognized in IoMT-based SHS with patient and doctor's consent; their liabilities are involved as SHS deals with sensitive medical data.

Blockchain based Issues and Challenges of SHS
The potential of the BC technique is to transform traditional healthcare systems into SHS. BC has provided various facilities to SHS by developing data safety and patient's secrecy [25]. But there have been some unavoidable issues and challenges in this area till now, which are mentioned here very carefully:

Deficiency of Technical Skill
Since BC is a comparatively new technology in the commercial application field, there is a lack of high-level expertise in this method. So implementing the BC technique in SHS efficiently is still a challenge.

Data Preservation Capability
Stored data in the BC is observable to everyone attached to the chain. This makes data vulnerable, which is unexpected for a decentralized network environment like SHS. Apart from this, since BC's capacity is restricted, a large volume of data may affect BC adversely.

Adaptability
In cases of large quantities of transaction processing, BC's performance may be degraded, which is a significant issue in SHS. Besides, using BC for instance-based data access is complex.

Absence of Global Standard
As this BC technique is still in the primary stage for implementation in various industrial sectors, including healthcare, there is no benchmark constraint for using this technique in SHS.

Smart Contract Issue
Errors in the code of the BC technique may create vulnerability in the smart contract in the SHS network.

Data Quality
This BC technique is fully dependent on the correctness of the data that will be processed in the system. So, data quality can be a remarkable issue in cases of wrong input or any modification of data during the transmission phase due to an attack on the BC-oriented SHS.

VI. PREFERABLE GUIDELINE TO HANDLE ISSUES AND CHALLENGES

In the modern healthcare sector, IoMT and BC techniques have remarkable impact. On the other hand, after a thorough review of the aforementioned issues and challenges of IoMT and BC-oriented SHS, it can be mentioned that a comprehensive methodology is required to manage these issues in a proficient way. The following are some recommended guidelines for doing it carefully:

Energy Issue
Most of the IoMT devices are battery-dependent. When these devices are put on, either they require continuous high-voltage supply or highly charged battery replacement. In this case, renewable energy processes should be implemented in medical sensor-based devices to handle power adaptability issues. For example, there are different types of implantable pacemakers.

Regulatory Acquiescence
It is to be ensured that agreement with related rules and standardized guidelines, like HIPAA, GDPR, and FDA regulations, should be made and followed to guard patient privileges. This can ensure the security and efficacy of IoMT hardware in SHS.

Adaptability
BC adaptability performance can be enhanced by using diversified implementation solution mechanisms such as off-chain, sharding, and sidechains. In this case, a hybrid approach that integrates dissimilar technologies with BC can deliver better performance. For example, BC with ML and IoMT can be a better combination for SHS.

Medical Data Safety
better cryptographic mechanisms like homomorphic encryption techniques can be implemented in the BC network for data storage, uploading, and transmission in order to ensure high-level security. Simultaneously, it is necessary to apply access control and data anonymization methods to secure sensitive medical records.

Smart Contract Issue
A careful code review and testing process should be conducted to detect and minimize issues related to smart contracts in SHS. In this case, a standard verification mechanism can ensure the correctness of the code.

Data Quality Issue
In a BC-oriented network, data integrity and accuracy can be ensured by implementing data validation techniques. In order to put more focus on data quality, a consensus algorithm can be applied in BC-based SHS.

Interoperability Issue
In order to handle this issue effectively, standard data formats and appropriate data transmission protocols should be used in BC-based SHS. In this case, IPFS, WebSocket, MQTT, and CoAP protocols can be used.

Technical Skill
As BC is an emerging technology in the modern commercial sector, proper training and guidelines regarding BC operation and usability should be provided to healthcare employees for better understanding.

VII. COMPARATIVE ANALYSIS

From the above discussion of this paper, it is observed that there are some striking variances among the research publications currently in publication and our work on IoMT and BC-oriented SHS, which will be mentioned in the comparative analysis section. To accomplish this job sincerely, the last fifteen years' (2009–2023) research outcomes in this area. For example, BC-oriented access control and key control mechanisms for digital healthcare processes where IoMT is implemented are discussed in one research article. On the other hand, our paper goes to review the IoMT and BC-based SHS and, at the same time, detects the issues and challenges and recommends some guidelines to handle those challenges of this system.

Let's focus on the subsequent table, in which some fundamental research outcomes on IoMT and BC-based SHS are taken into attention. A comprehensible comparative analysis is tried to be depicted in this precise table, on which our actual contribution in this field will be focused.

Table 1. Comparative Evolution of Our Research Findings with Previous Research

Sr. No.	Year	Authors	Their Work	Our Contribution
1.	**2019**	Vaggelis Malamas and et al.	In this paper, BC oriented authorization scheme for organizing IoMT hardware and health record with the help of distributed chain and data privacy mechanism is explained.	Our paper analyzes how IoMT and BC technique can be implemented in SHS very carefully.
2.	**2023**	Tahir Abbas Khan and et al.	This paper introduces a protected disease prediction mechanism using transfer learning method for IoMT based SHS	In our paper, we have tried to detect important issues and challenges of IoMT and BC oriented SHS.
3.	**2024**	Anichur Rahman and et al.	A framework of remote location based patient observation process using SDN and BC is introduced in this paper.	Our paper delivers some precise guidelines to handle the issues and challenges of IoMT and BC based SHS.
4.	**2021**	Abdullah Shawan Alotaibi	In this paper, author has proposed accurate malware identification technique in IoMT network with the help of deep learning method.	In our paper, BC and IoMT oriented secure SHS framework is proposed.
5.	**2020**	Asma Khaton	In this paper, author has proposed BC based smart contract process for healthcare organization. In order to do this, ethereum tool is used here.	Our paper is a technical review paper based on IoMT and BC used SHS.
6.	**2023**	Anbazhagu U.V and et al.	This paper explains a decentralized observation process for SHS with the help of deep federated learning and RNN.	In our paper, homomorphic encryption and consensus algorithm based SHS framework is provided.

It is perceived from the above **Table 1** that significant differences exist between the findings of our study and the body of current research on IoMT and BC-oriented SHS.

VIII. CONCLUSION AND FUTURE WORK

It is no doubt today that without IoMT and BC, technical, financial, and other related challenges can't be handled efficiently in SHS. Considering the meticulous study throughout this article, it can be revealed faultlessly that in the latest medical technology area, IoMT and BC techniques have a momentous influence on the design and maintenance of SHS effectively. It is also observed from the methodical breakdown of existing research that there is substantial growth in the SHS field using these two revolutionary technologies: IoMT and BC. Regardless of this evolution in IoMT and BC-based SHS, several major challenges exist that are definitely required to be addressed. In this paper, this identification of challenges related to IoMT and BC-based SHS is done very sincerely. At the same time, some unambiguous methods are suggested to manage those issues and challenges commendably. A secured IoMT and BC-oriented SHS using consensus mechanisms and a homomorphic encryption process framework is given in this paper. In the future, this proposed framework can be simulated technically for further development in this field by ensuring maximum level of security and other data management-related operations efficiently. The comparative analysis part of this paper clearly differentiates between our research involvement and existing exertion in this area. A vibrant research scenario in this field is tried to depict in this paper carefully. It is to be believed that by implementing the recommended guidelines of IoMT and BC-based SHS, not only can the identified challenges be addressed successfully, but SHS can also run its total operation very smoothly.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707–8718, Jun. 2021, doi: 10.1109/jiot.2020.3045653.

[2]. M. Wazid and P. Gope, "BACKM-EHA: A Novel Blockchain-enabled Security Solution for IoMT-based E-healthcare Applications," ACM Transactions on Internet Technology, vol. 23, no. 3, pp. 1–28, Aug. 2023, doi: 10.1145/3511898.

[3]. R. Rawat, "A Systematic Review Of Blockchain Technology Use In E-Supply Chain In Internet Of Medical Things (IOMT)," International Journal of Computations, Information and Manufacturing (IJCIM), vol. 2, no. 2, Nov. 2022, doi: 10.54489/ijcim.v2i2.119.

[4]. B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," Sustainability, vol. 15, no. 7, p. 6177, Apr. 2023, doi: 10.3390/su15076177.

[5]. A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 10, Aug. 2021, doi: 10.1002/ett.4333.

[6]. A. Rahman et al., "Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network," Scientific Reports, vol. 14, no. 1, Mar. 2024, doi: 10.1038/s41598-024-55662-w.

[7]. R. Pandey, A. Gupta, and A. Pandey, Eds., The Internet of Medical Things (IoMT) and Telemedicine Frameworks and Applications. IGI Global, 2022. doi: 10.4018/978-1-6684-3533-5.

[8]. V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, "A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain," 2019 IEEE World Congress on Services (SERVICES), Jul. 2019, doi: 10.1109/services.2019.00021.

[9]. K. Kakhi, R. Alizadehsani, H. M. D. Kabir, A. Khosravi, S. Nahavandi, and U. R. Acharya, "The internet of medical things and artificial intelligence: trends, challenges, and opportunities," Biocybernetics and Biomedical Engineering, vol. 42, no. 3, pp. 749–771, Jul. 2022, doi: 10.1016/j.bbe.2022.05.008.

[10]. B. Kim, S. Kim, M. Lee, H. Chang, E. Park, and T. Han, "Application of an Internet of Medical Things (IoMT) to Communications in a Hospital Environment," Applied Sciences, vol. 12, no. 23, p. 12042, Nov. 2022, doi: 10.3390/app122312042.

[11]. V. Sharma and A. Sharma, "IoMT data security approach," An Interdisciplinary Approach to Modern Network Security, pp. 23–34, Mar. 2022, doi: 10.1201/9781003147176-2.

[12]. S. Kaddoura and R. Grati, "Blockchain for Healthcare and Medical Systems," Enabling Blockchain Technology for Secure Networking and Communications, pp. 249–270, 2021, doi: 10.4018/978-1-7998-5839-3.ch011.

[13]. T. A. Khan et al., "Secure IoMT for Disease Prediction Empowered With Transfer Learning in Healthcare 5.0, the Concept and Case Study," IEEE Access, vol. 11, pp. 39418–39430, 2023, doi: 10.1109/access.2023.3266156.

[14]. S. P. Paul and D. Vetrithangam, "A Full-Scale Analysis on Challenges and Issues of Next Generation (5G) Communication in Heterogeneous Wireless Network Based Enterprise Applications," Journal of Theoretical and Applied Information Technology, Vol. 101, no. 11, June 2023.

[15]. "Malware Detection Approaches and Analysis for the Internet of Medical Things Enabled Healthcare Systems," International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 6, pp. 3117–3121, Dec. 2021, doi: 10.30534/ijatcse/2021/061062021.

[16]. S. Ayub, R. Boddu, H. Verma, S. Revathi B, B. K. Saraswat, and A., "Health Index Estimation of Wind Power Plant Using Neurofuzzy Modeling," Computational and Mathematical Methods in Medicine, vol. 2022, pp. 1–8, May 2022, doi: 10.1155/2022/9535254.

[17]. R. Ullah, I. Asghar, and M. G. Griffiths, "An Integrated Methodology for Bibliometric Analysis: A Case Study of Internet of Things in Healthcare Applications," Sensors, vol. 23, no. 1, p. 67, Dec. 2022, doi: 10.3390/s23010067.

[18]. A. K. Ranjan and P. Kumar, "Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission," Multimedia Tools and Applications, Mar. 2024, doi: 10.1007/s11042-023-18043-5.

[19]. A. B. Chaaben, "A Survey of Different IoMT Protocols for Healthcare Applications," ResearchBerg Review of Science and Technology, Vol. 2, no. 1, pp. 41-57, 2022.

[20]. S. Sharma, H. K. Shakya, and A. Mishra, "Medical Data Security Using Blockchain With Soft Computing Techniques: A Review," The Internet of Medical Things (IoMT), pp. 269–288, Feb. 2022, doi: 10.1002/9781119769200.ch14.

[21]. R. ELGawish, M. Abo-Rizka, R. ELGohary, and M. Hashim, "Detecting Ransomware within Real Healthcare Medical Records Adopting Internet of Medical Things using Machine and Deep Learning Techniques," International Journal of Advanced Computer Science and Applications, vol. 13, no. 2, 2022, doi: 10.14569/ijacsa.2022.0130270.

[22]. K. Arthi, B. Chidhambararajan, and A. R. Revathi, "A Deep Investigation of Architectural Elements and Computing Technologies for Internet of Medical Things," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, vol. 38, pp. 556–563, Dec. 2022, doi: 10.1109/iceca55336.2022.10009359.

[23]. A. K. Tyagi, A. Abraham, and A. Kaklauskas, Eds., Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer Singapore, 2022. doi: 10.1007/978-981-16-6542-4.

[24]. M. Uddin, "Three-Tiered Architecture for Access Control in Internet of Medical Things," (Doctoral dissertation, University of Malaya (Malaysia)), 2022.

[25]. A. U. Nwosu, S. B. Goyal, and P. Bedi, "Blockchain Transforming Cyber-Attacks: Healthcare Industry," Innovations in Bio-Inspired Computing and Applications, pp. 258–266, 2021, doi: 10.1007/978-3-030-73603-3_24.