Journal of Autonomous Intelligence (2023) Volume 6 Issue 3
doi: 10.24294/jai.v6i3.592

ORIGINAL RESEARCH ARTICLE

A Blockchain-based secure Internet of Medical Things framework for smart healthcare

Surjeet Dalal[1], Umesh Kumar Lilhore[2], Sarita Simaiya[2], Ashish Sharma[3], Vivek Jaglan[4], Manish Kumar[5], Monika Jangra[6], Nitin Goyal[7,*], Arun Kumar Rana[8]

[1] *Department of Computer Science and Engineering, Amity University Haryana, Gurugram 122413, India*
[2] *Department of Computer Science and Engineering, Chandigarh University, Mohali 140413, India*
[3] *Department of Computer Engineering and Applications, GLA University, Mathura 281406, India*
[4] *Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior 474020, India*
[5] *Department of Computer Science and Engineering, Punjab Engineering College, Chandigarh 160012, India*
[6] *Skill Department of Computer Science and Engineering, Skill Faculty of Engineering and Technology, Shri Vishwakarma Skill University, Palwal 121102, India*
[7] *Department of Computer Science and Engineering, School of Engineering and Technology, Central University of Haryana, Mahendragarh 123031, India*
[8] *Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida 201306, India*

*** Corresponding author:** Nitin Goyal, dr.nitingoyal30@gmail.com

ABSTRACT

The Internet of Medical Things (IoMT) industry has grown lightning during the estimated time frame. Privacy and security are essential concerns given the scale and widespread use of IoMT networks. Blending healthcare data in one place storage device to prepare an effective predictive model, on the other hand, increases more severe security and privacy issues, ownership, and regulation. An advanced system is required to enhance information utilization while restricting privacy issues. This research presents a new architecture to address security and privacy challenges in e-healthcare services in Healthcare 5.0. This paper integrates the distributed ledger technology (DLT) with IoMT. This integration has become necessary due to the growing demand for e-health-related technologies and services. The proposed solution in this research is based on a Blockchain framework to enhance medical data privacy and integrity. This research evidence found that Blockchain can overcome IoMT privacy and data protection. The proposed framework has far-reaching consequences for the medical field. The proposed method has reduced Commit time by up to 10 seconds, and Commutative probability has been gained to 88%. It has advantages, including faster data exchange, less duplication of effort, and more secure patient information.

Keywords: Blockchain; Internet of Medical Things; security; privacy; Internet of Things; Health 5.0

ARTICLE INFO

Received: 12 April 2023
Accepted: 10 July 2023
Available online: 15 September 2023

1. Introduction

Health 5.0 describes an environment where humans and intelligent machines coexist. Robots improve human productivity using cutting-edge tools like the Internet of Things (IoT) and big data. Integrating this human element with the core tenets of automation and efficiency is a critical component of Industry 4.0. Robots have traditionally been used to undertake risky, monotonous, or physically demanding tasks in manufacturing environments, like welding and painting automobiles and lifting large warehouse objects[1]. Health 5.0 seeks to integrate cognitive computing capabilities with human intellect and resourcefulness in joint operations as machines in the

workplace become more intelligent and interconnected. The world needs fast payment networks to overcome these and other challenges[2].

These trust-building mechanisms do not require special hardware, monthly refunds or fees, and transparent and reliable scrapbooking solutions. Industrialized countries spend a large portion of the gross domestic product (GDP) on healthcare; however, hospital costs continue to rise due to ineffective practices and the loss of health data. This is a place wherein Blockchain generation can enhance this situation. You can do many things, from securely encrypting affected person statistics to handling outbreaks[3]. Estonia is a pioneer on this subject and commenced to apply the strength of Blockchain within side the healthcare area in 2020. Currently, 94% of clinical facts and 98% of prescription statistics in the complete healthcare billing system are digitally saved through Blockchain. Sensor nodes have been used globally to enhance transport services, medical care, bioengineering, portable devices, augmented and virtual reality, and Intelligent systems in Health 5.0. Ever since they were developed, IoT technologies have greatly enhanced healthcare[4]. Extensive use of sensor nodes has been made to transform health data into detectable neural activity. As a worldwide distributed ledger, Blockchain makes it easier to keep track of assets and record financial transactions throughout an organization's network. Real estate, vehicles, funds, undeveloped land, and intellectual property rights like patents and trademarks are all examples of tangible and intangible assets. For Blockchain, this is the best possible development. Think of a powerful yet inexpensive programming environment to learn more about Blockchain. Financial transactions require a safe and dependable system for their execution and documentation[5].

The word "Blockchain" is shorthand for a distributed ledger in which each transaction is recorded in its own immutable "block", and the entire catalogue is encrypted and stored using a single key (a "hash"). These signatures or keys are stored in a standard register that tracks activity on the node grid or the method used to connect the nodes[6]. A copy of the whole chain is kept in sync and updated at each node. According to the National Institute of Standards and Technology (NIST), many advantages are resistance to hacking, the absence of a centralized authority responsible for maintaining the ledger, and the impossibility of modifying past transactions involving the network of users with access to the catalogue. DLT is another name for this era[7].

The most critical challenges for Blockchain applications in the healthcare sector include the following:

- Security of network infrastructure at all levels;
- Identity verification and identity verification of all participants;
- Unified authorization template for accessing electronic health information.

DLT may be used in many regions of fitness care; however, all fitness care sports aren't transactional; however, because the general public chain information is broadly distributed, it can't be used to shop for personal statistics and fitness information identification. Providers remember privateers' troubles to assist guard fitness statistics. Second, the Blockchain era is at risk of positive varieties of attacks, even though it provides integrated safety towards different attacks. Therefore, we must connect outstanding significance to statistics security, mainly with the subject of scientific care[8].

Figure 1 depicts the historical prevalence of centralized data management, storage, and sharing infrastructures in business networks. Databases and patient records were kept privately by healthcare facilities such as hospitals, clinics, and pharmacies. Due to incompatible systems, data silos, and privacy issues, interoperability and data interchange between institutions were typically tricky. After the Blockchain, these records are digitally signed, and all documents have a replica of the ledgers[9].

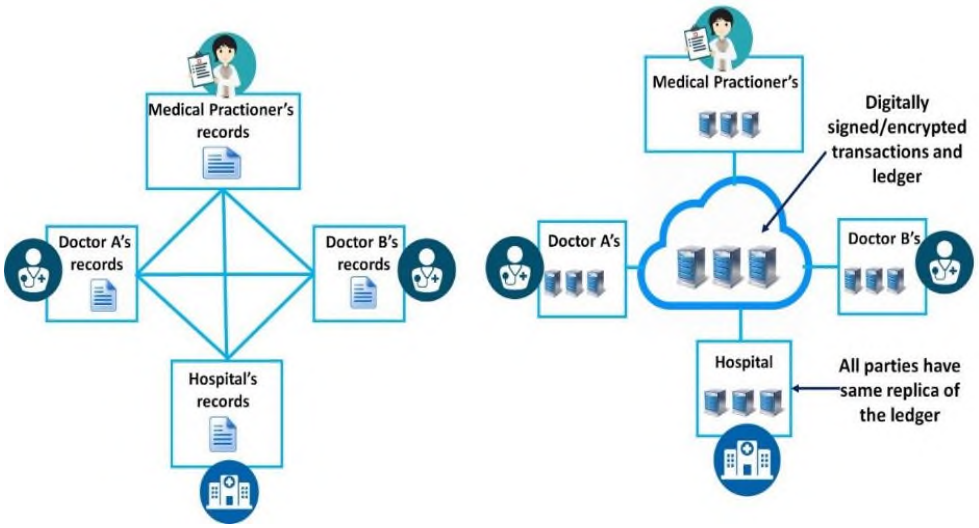

Figure 1. Commercial network before and after the Blockchain.

Figure 2 shows the application of Blockchain for medical records. Electronic health records (EHRs) were the usual repository for patient information inside healthcare facilities. There were sometimes delays in getting life-saving patient data because of the need for manual authorization and coordination among healthcare practitioners. Safe and private personal health record (PHR) is made possible by identity management solutions built on the Blockchain. Patients may protect themselves from identity theft and other forms of data breach by limiting the information shared with healthcare providers. Centralized systems pose severe threats to data security and privacy due to the ease with which they might be breached or tampered with. The era behind the crypto foreign money boom is now being considered for greater personal purposes: your scientific and fitness records. A big part of your scientific documents is already within the cloud of scientific practices and hospitals-you could shop information control costs, reap brief entry to, or even shop lives. However, it reveals your private records to hackers and protection threats. Traditional security features aren't sufficient. It isn't clear whether or not that is beneficial and legally feasible[10].

Although such economic and web-based systems and equipment may change reactive care for preventive care, the privacy of patient information and safety concerns of these web-based sites are often ignored. Gadgets and associated correspondences must be exceptionally secured to protect the patient's privacy, as the clinical gadgets capture and cycle individual health-related information. These IoMT devices are only limited in capacity and limited in security features. Hence the general use of IoMT devices makes it challenging to manage and guarantee the security of IoMT frameworks. This proves to be a significant problem in implementing IoMT for medical purposes. Our paper recommends a new e-medical IoMT design that addresses safety and protection challenges[11]. The critical contribution of the article includes.

- This work highlights security and privacy issues faced in IoMT designed in Health 5.0.
- This work proposes a Blockchain-based security framework for maintaining privacy and improving security levels from Health 5.0 perspective.
- This work gains minimum commit time and maximum Commutative probability.
- This work demonstrates the real-life application of the proposed framework in IoMT devices.
- This paper justifies that this proposed system gains more security in the IoMT domain.

The complete article is organized as follows: section 2 covers the related work in Blockchain-based healthcare research, section 3 covers the problem formulation, section 4 covers the proposed solution, section 5 covers the results and discussion, and Section 6 covers the conclusion and future scope.

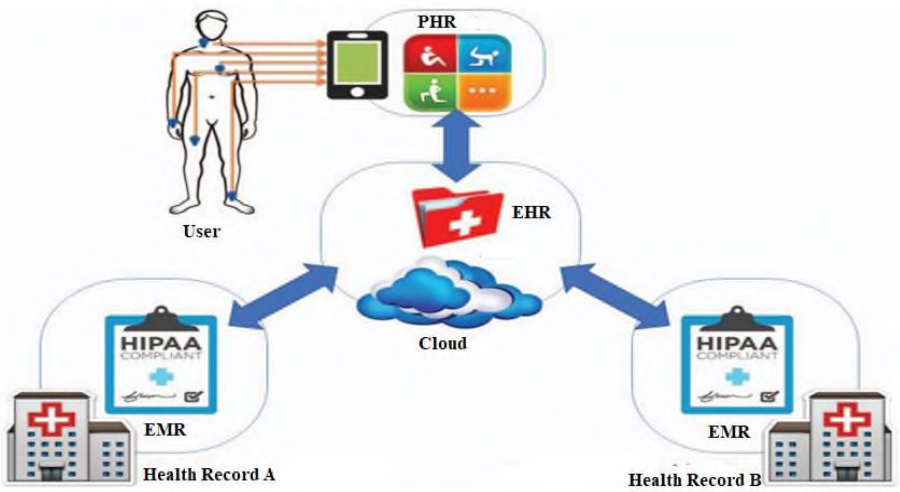

Figure 2. Blockchain for medical records.

2. Related work

In recent decades, specialists in intelligent healthcare have accepted the concept of "Blockchain technology," and many scientific studies have examined how cryptographic protocols might be implemented in the domain. This section covers the latest research work and comparative analysis of Blockchain based healthcare research. Islam et al.[11] aimed to find the actors involved in the Blockchain network and explain their contribution to Bitcoin splits. The study found that non-human and human actors comprise heterogeneous actor networks. This paper successfully explained the influence of Blockchain splits after merging homogenous groups with actors. While describing the involvement process in and fusion with other macro and micro actors, their consequences are also elaborated.

Bao et al.[12] provided a solution to the challenges in Blockchain (e.g., scalability, privacy, and security issues). They focused on Intel software guard extensions (SGX) technology to improve the performance of the Blockchain system. The research presented the advantages, disadvantages, and applications of pre-existing works according to the six-layered hierarchical organization of Blockchain. The authors then analyzed the pros and cons of SGX technology. They found the solutions based on SGX according to different layers. To incorporate the Blockchain in financial sectors, Walsh et al.[13] aimed to provide a model of resistance to Blockchain system usage by the managers of economic organizations. Sequential and quantitative approaches were executed to develop new assumptions, refine the conceptual model, test the mentioned assumptions using surveys, and develop the resistance model. Various factors were analyzed, such as switching costs, self-efficacy, environmental and organizational support, individual resistance, etc. These factors decreased the resistance to introducing a Blockchain system in the organization. Fernández-Caramès and Fraga-Lamas[14] examined the possible quantum attacks on Blockchain cryptographic systems. They thus studied the current scenario of post-quantum cryptosystems to execute them on Blockchain. The paper provided a complete analysis of various post-quantum encryption and digital signatures characteristics to be applied to the Blockchain systems. This study made a detailed comparison of the most effective post-quantum Blockchain cryptosystems.

Commercializing ads using vehicles are used by advertisers for the growth of their business. But some issues in executing it are represented in Li et al.[15]. The "free-riding" attack is handled efficiently, with contracts having time-locked deposit fair protocol and other efficient algorithms. The Merkle hash tree was adopted to counter the attacks on Ad, which is to be received by the Vehicle without any changes. Using zero-knowledge proof techniques, the problems related to privacy, such as anonymity, got resolved by developing an efficient scheme. Treiblmaier and Sillaber[16] point out the various high-level questions related to the potential influence of Blockchain on respective areas of the e-commerce field. Academia can be

benefitted from the questions revolving around four domains such as technical, legal, quality, and organizational issues and the problems related to consumers. Nalin et al.[17] highlighted the issues (ethical, regulatory, and administrative) in exchanging health data across European Union Member states. The research discussed the KONFIDO toolset using OpenNCP and eIDAS European Frameworks. With this implementation, data vulnerability was handled by never exposing the simple test of gathered data in any non-secure region.

Abu-elezz et al.[18] presented a review of research on the threats and benefits of Blockchain usage in healthcare organizations. Out of 84 relevant searches of studies, 37 were highlighted in this paper, which focuses on eight benefits of Blockchain related to patient health and other organizational benefits. The authors categorized threats associated with using Blockchain into three categories such as corporate, social, and technological. To understand the security threats related to Blockchain, Homoliak et al.[19] focused on developing a security reference architecture (SRA) based on a stacked model with different layers than the ISO/OSI model. This paper introduced a threat risk model based on ISO/IEC 15408 to capture threats effectively. Samples of Blockchain incidents were collected and analyzed. The incidents were relatively less than the number of threats. The authors then organized security threats in various layers of the model, found their origin, and provided the countermeasures to handle them. Inkinen et al.[20] studied digitalization in Finnish ports by gathering data from two group interviews. The authors identified the main drivers and technology required as an essential element of executing digitalization. These drivers were discussed based on the scenarios, which were classified with frameworks of SWOT and PESTEL. The systematic review of systematic literature discussing the progress of technical aspects in EHR and PHR maintenance was presented in the paper by Negro-Calduch et al.[21]. This research selected a few documents, and based on them, the information extraction tools and NLP technology have been focused on. The authors successfully presented the opportunities, challenges, and technical solutions of EHR technological advancements identified in the literature review.

Sai et al.[22] presented a comprehensive overview of centralization in decentralized Blockchains by reviewing the literature published between 2009 and 2019 and was then followed by expert interviews to evaluate the findings. The authors highlighted the security threats as the impact of centralization. They also reported the platform-specific results for Bitcoin and Ethereum. The taxonomy of centralization was developed with six architectural layers, which referred to 13 aspects of centralization. To generate verified and reliable information, Jaquet-Chiffelle et al.[23] generated a tamperproof time-stamped provenance ledger using an already existing Blockchain system. The catalogue developed many advantages comprising scalable capability, automation, interoperability, and standardization. To maintain the data integrity, the original data's three hash values, MD5, SHA1, and SHA256d, were computed and then sent to the server. Schniederjans et al.[24] gathered textual data from 2010 to 2018 and analyzed it to research the digitization of the supply chain. Significant disparities in the frequency and growth of supply chain digitization industry/field applications, technology, and subjects in scholarly and practitioner-oriented literature were determined using statistical analysis. Radoglou-Grammatikis et al.[25] developed SPEAR (Secure and PrivatEsmArtgRid) SIEM (Security Information and Event Management) system to handle the issues of Smart Grid (SG). They could be organized to address the monitoring, detection, and prevention measure. The four components, so SPEAR SIEM, helped monitor infrastructure, integrated a set of machine learning/deep learning based intrusion and other anomaly detection models, supported in parallel detection and correlation, and finally correlated the various security events and computed the reputation value of each SG asset.

Leal et al.[26] aimed to provide quality of a large amount of data produced by the computerized pharmaceutical system. The explained EU-funded SPuMoNI project and, using Blockchain end-to-end verification achieved authenticity, transparency, and immutability of data using smart contracts, identified behavioural data patterns based on the implementation of models of data quality assessment, and used intelligent agents to gather and change data. The decentralized mechanism of smart contracts poses many

security threats, as presented by Huang et al.[27]. The authors provided an approach of focusing on smart contracts from the viewpoint of the software lifecycle. They found the cause of security issues in smart contracts in Ethereum and Fabrics by reviewing the key features of Blockchain and concluded.

Koshy et al.[28] focused on developing an IoT Architecture decentralized by involving Blockchain components. But as the original Blockchain has high complexity and significantly less scalability, thus the authors proposed a modified sliding window Blockchain (SWBC) architecture to develop IoT applications. The subsequent hash blocks could be generated from previous blocks with less complexity in proof-of-work (PoW) but at the cost of increased time with each addition. The resultant memory and computational overhead were found to be reduced. The security issue in IoT was efficiently handled as the next hash block was generated from n blocks in a sliding window. For selective imaging on live Windows, Faust et al.[29] developed a framework called SIT using the framework DFIR ORC to create a single portable pre-configured binary implemented as a command-line tool. The primary goal of the SIT implementation was to collect forensic artefacts on a file system level, along with crucial metadata, validate the results to detect unexpected results and external interferences, integrate the results into an AFF4 forensic image, and then verify the artefacts using hash codes, all while adhering to the new live forensic soundness rules. To remove the data storage problem in Blockchain without compromising its decentralized architecture and security, Xu and Huang[30] focused on developing a segment of Blockchain that can be used for bulky applications. The research comprised a PoW membership threshold, which allowed the adversary to take a new node. The authors allowed only n/2 nodes of the total n nodes to be stored by an adversary. In case all copies were held in the adversary. It would cause a complete system failure leading to permanent segment loss. The system provided the failure probability of (AD/n)m if the adversary consisted of at most AD nodes and m number of nodes stored in each segment.

Yousefnezhad et al.[31] presented extensive research on product lifecycle security in IoT. The authors provided security solutions for various lifecycle phases and found new challenges in the lifecycle stages. Paavolainen and Carr[32] rejected many assumptions associated with light client security in Ethereum. The authors found that the success probability of an adversary subverting an existing mining pool increased substantially. The model developed in this research confirmed that assurance of security in the eclipsed light client was reduced to a great extent. Identifying mitigation strategies was done appropriately while providing many other research areas for future use. The research by Wang et al.[33] proposed the basic requirements of CPC-2.0-L3 on the Blockchain. It provided enforcement proposals for the Blockchain's P2P networks, consensus mechanisms, distributed ledgers, and contract layers. Data non-repudiation, ledger data synchronization, and ledger data idempotence were added as evaluation items to evaluate distributed ledgers. Based on 28 evaluation items, Bitcoin, Ethereum, and Hyper ledger Blockchain systems were assessed. It concluded that Hyper Ledger was better than the rest.

Li et al.[34] investigated the drawbacks of joint relay and jammer selection, average optimal relay selection, and standard maximum relay selection techniques. They created an ideal relay and jammer selection strategy after assessing the results. The model developed in this research produced reduced complexity and proved that the proposed approach worked efficiently compared to JRJS, TMRS, and AORS schemes. Chaturvedi et al.[35] aimed to provide security in Spatial Data Infrastructure (SDI) by securing distributed intelligent city applications and services to allow users to perform single sign-on. OAuth 2.0 access tokens, OpenID Connect, and SAML were used to facilitate user authentication in the SSO environment. The authors implemented the proposed model for a specific scenario within London's Queen Elizabeth Olympic Park district. Dai et al.[36] used Ethereum and Intel's Software Guard Extensions to develop a secure data trading platform (SDTP) based on the Blockchain to handle the limitations of the existing data trading market. The model traced the unauthorized transactional modifications and protected the source data and the analysis result with the execution of SGX-based secure contracts.

Krzywiecki et al.[37] introduced the highly secured model resistant to the subliminal setting of ephemeral secrets by analyzing the Schnorr Identification Scheme (IS). This IS scheming helped handle the impersonation issue done by the adversary by denying its role from a verifier to a proverb. After analyzing Schnorr IS, the authors concluded that the immunity of this model against malicious activities, such as the generation of random numbers for ephemeral secrets. The main limitation of Blockchain is scalability which is handled quite efficiently by Rožman et al.[38] by developing a framework for Blockchain-based Shared Manufacturing, which is entirely scalable; provides transparency and immutability characteristics of transaction records. For service execution, the author defined a protocol based on Blockchain following shared economy principles. The pre-existing papers were analyzed, and then the cross-chain solution was proposed to be integrated with the Blockchain system. The authors implemented cross-chain tree topology to analyze the usage of various cross-chain technologies in sync with the requirements of Shared Mfg. They compared the Ethereum public network and the Xdai sidechain network base on the parameters of cost and time. They concluded that by the implementation of side chain technology, the cost and execution time was reduced.

The Blockchain solution for various security issues associated with product serialization in multi-party perishable goods supply chains is presented in Thakur and Breslin[39]. To control the authenticity of the serial number, the authors have proposed a serialization protocol that is immensely secure and implemented Blockchain offline channels. The two primary techniques, clustering heuristics and attribution tags in cryptocurrency investigation forensic tools, are discussed by Fröwis et al.[40] to develop a technical data-sharing framework to foster compliance with law enforcement and follow technical standards. The research found the potential sources of misinterpretation by empirically analyzing CoinJoin transactions. Akyildirim et al.[41] presented the expressions of interest in utilizing cryptocurrency and Blockchain systems by publicly traded companies. The research found that based on the type of cryptocurrency announcements, there exists stock price premium, increase in both unconditional and conditional share price volatility, changes in dynamic correlations between cryptocurrency markets and companies, substantial change in the determination of price discovery and information flow and decoupling of companies with domestic peers.

Lisi et al.[42] developed a Blockchain-based decentralized rating framework to remunerate the users depending on their participation using a token-based reward mechanism for making the Recommender Systems (RSS) application more efficient. In the proposed mechanism, the Blockchain stores the item's ratings, reputations, users' tokens, and respective algorithms to calculate the item's scores. Ropsten Ethereum test network was used to evaluate the framework's performance and cost. The research by Benedetti and Nikbakht[43] provided an empirical analysis of returns, activities related to trading, and the behaviour of the network around cross-listings in an ecosystem of tokens. The results displayed a significant increase in returns, volume of trading, market availability, and user growth on the network. The cumulative abnormal returns are 27.9% and 15.5%, respectively, after adjusting the Bitcoin and MVIS index returns-the research improved information production to reduce financial misconduct in the digital marketplace. Huang et al.[44] proposed a reputation-based secure, fast Blockchain system via sharding, known as RepChain, to provide heterogeneity among the validators and found a high incentive-generating solution. An efficient Raft-based synchronous consensus was provided for the transaction chain. Shrestha and Nam[45] analyzed the regional Blockchain's design for VANET to manage the problem of secure message dissemination in vehicular networks. The authors developed a condition based on the number of excellent and malicious vehicles, average puzzle computing time, and block message delivery delay to limit the success probability of immutability assaults, roughly 51%. Park et al.[46] propose a three-factor authentication method, Neighbor Assisted Healthcare Authentication Protocol, based on physically unclonable functions. The suggested framework has a high dependability (100%) and a low computing time (6 ms) overhead (only 193 bytes). Formal analysis, Burrows, Abadi, Needham logic, and informal analysis all attest to the validity of the suggested work.

Using a physical unclonable function (PUF) and ML, Onyema et al.[47] propose multidevice authentication for the hospital setting. With the suggested technique, only one message is required to verify the authenticity of many devices. In contrast to most protocols, the proposed system does not need central server storage of PUF keys. Additionally, authentication and data are transmitted to the server in the same message, reducing the time it takes to process. Further, a single ML model may validate a batch of devices simultaneously. The suggested technique successfully classifies the gadgets with a 99.54 per cent precision. In addition, the proposed method requires just 2.6 milliseconds and 104 bytes to finish the authentication of a single device and less time as more widgets are added to the cluster[48].

The status of IoMT's outstanding issues is now displayed in **Table 1**.

Table 1. Open issue in IoMT.

Research papers	**Open issues**									
	Security	**Privacy**	**Single-sign-on**	**SAML+OAuth**	**Sensors and IoT**	**Scalability**	**Authentication**	**Storage**	**Data Integrity**	**Decentralization**
[12], [15]	✔	✔				✔	✔	✔	✔	
[17]	✔	✔					✔	✔	✔	
[19]	✔	✔				✔	✔	✔	✔	✔
[21]	✔	✔				✔		✔	✔	
[22]	✔					✔		✔		✔
[23]	✔	✔							✔	
[27]	✔						✔			
[28]	✔	✔			✔					✔
[30]								✔		
[31]	✔	✔			✔	✔	✔	✔	✔	
[33]	✔						✔	✔		
[34]	✔									
[35]	✔	✔	✔	✔	✔					
[36]	✔								✔	
[38]						✔				
[39]	✔					✔		✔		
[42]		✔						✔	✔	✔
[44]	✔					✔				
[45]	✔					✔				

3. Problem formulation

Using Blockchain in conjunction with IoMT can overcome security and privacy concerns. This is referred to as Blockchain-enabled IoMT. The architecture of Blockchain-enabled IoMT is shown in **Figure 3**. The Blockchain system is implemented through the interconnection of computers and all participants[49]. The Blockchain-based health system is described in **Figure 3**. The doctor is displayed graphically in some distant location to observe the patient's activity and provide advice via the Blockchain system. In the health clinic, the doctor also analyses the reports produced. The diagnostic clinic doctor uploads electronic medical records (EMR) that are finally added to the patient's history.

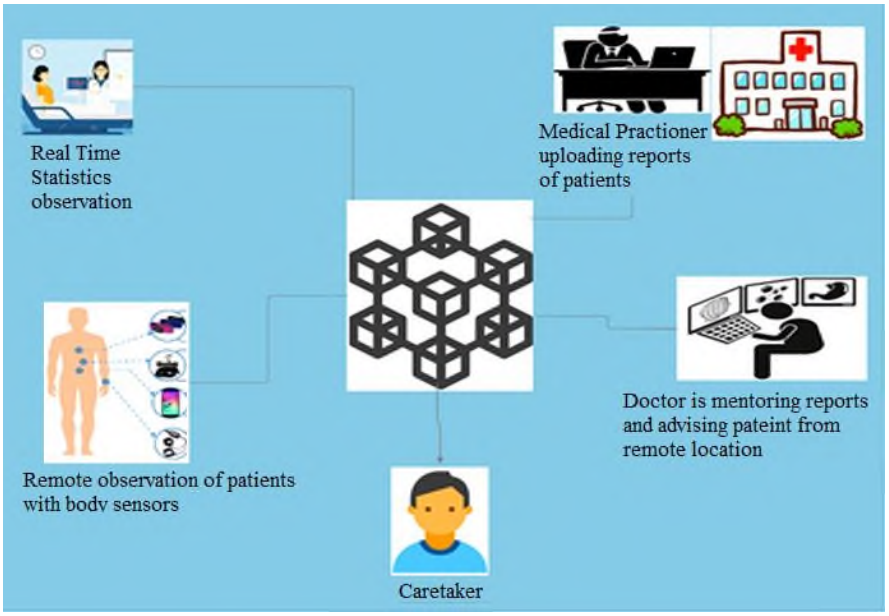

Figure 3. Blockchain-enabled IOMT architecture.

The privacy and security of patients might be jeopardized if an attacker gains unauthorized access to IoMT devices, networks, or data. The result might be the theft, disclosure, or loss of private medical records. In the IoMT, devices and systems gather and send personal information about patients. Data breaches and the loss or abuse of individual health information may occur if inadequate security measures are in place to protect it[50].

Intruders might compromise the security or functionality of IoMT devices. Wrong diagnoses, inappropriate prescriptions, or bodily injury to patients might result from illegal changes to device settings, firmware, or software.

3.1. Opportunities of Blockchain-enabled IoMT

IoMT is affected by concerns of safety and confidentiality. The Blockchain-enabled IoMT has opened up possibilities for entertaining such problems. Our paper highlights the benefits of Blockchain-enabled IoMT in under mentioned areas.

3.1.1. Security improvement of IoMT

The incorporation of Blockchain into IoMT can expand IoMT security fundamentally. First, Blockchain's implicit security features, like asymmetric encryption/decryption schemes and computerized signature, may support protecting IoMT data. Secondly, joining Blockchain with different security mechanisms, such as authentications and access controls, may upgrade framework security. Thirdly, brilliant contracts in IoT gadgets can consequently initiate auto-upgradation algorithms for updating IoT gadget firmware, improving the system's security. Furthermore, the decentralization of Blockchain may bring down the danger of framework

failure brought about by single-point failure or additional malicious assaults like; "distributed denial-of-service attacks."

3.1.2. Privacy preservation of IoMT data

All the Blockchain is public, so hashing encryption has been used to provide the privacy remedy. Compared with conventional systems, Blockchain can bring increased security and certain advantages. We need to know the contents of the block to understand hash encryption. A block is nothing but a container that handles the transaction's details. For cryptography, Blockchain uses the hash function. Blockchain may offer protection against privacy by Blockchain account address masking and Blockchain transaction data encryption. Users can get better privacy protection by integrating Blockchain-enabled IoMT with other security safeguarding strategies like homomorphic obfuscations and cryptographic algorithms. This allows protection-sensitive IoMT info to be stowed and handled locally before moving too far off the cloud[51].

3.1.3. Traceability of IoMT data

Furthermore, in Blockchain-enabled IoMT, using digital signs and access control mechanisms may improve the traceability of "off-chain IoMT data." For example, putting "off-chain IoMT data" hash values in the Blockchain helps ensure IoMT data traceability while lowering Blockchain storage costs. The distribution chain is used for sequence following and deciding the item's starting point. Traceability is a block layout in the Blockchain where every block uses the hash key to connect the two blocks next to each other[52].

In Blockchain-enabled IoMT, info may be classified as "on-chain data" or "off-chain data," depending on whether the info is stowed on Blockchain. The data stored on the Blockchain is traceable virtually across the framework. The traceability and non-repudiation of "on-chain data" may be guaranteed through means of Blockchain's decentralized consensus algorithms and asymmetric cryptographic methods (For example, computerized sign)[53]. Nonetheless, considering the gigantic sizes of IoMT data, predominantly clinical photographs and video recordings, putting away all IoMT data in Blockchain is unrealistic. Thus, IoMT information like photographs and motion pictures should be put away off-chain, with Blockchain simply holding meta-data or hash values of "off-chain IoMT data".

Additionally, in Blockchain-enabled IoMT, using computerized signs and access control instruments may enhance the traceability of off-chain IoMT data[50]. For instance, putting off-chain IoMT data hash values in Blockchain supports guaranteeing IoMT info tracing while bringing down Blockchain storage expenses. This has become important in managing and maintaining the security of intelligent health devices[51–53]. ECC offers robust protection with significantly lower key lengths than more conventional cryptographic methods like RSA. This factor makes it computationally efficient and well-suited for devices with limited resources, such as mobile phones and IoT gadgets. However, ECC algorithms and their implementations are more involved compared to more standard encryption techniques[54–57]. This intricacy makes it challenging to comprehend and implement appropriately, leaving systems vulnerable if they aren't. Secure device authentication using PUFs ensures only authorized devices can access restricted areas or data. However, UFs can be affected by external factors like temperature and voltage changes, making them less consistent and reliable. The integrity of the produced cryptographic keys may be compromised due to this vulnerability[58].

4. Proposed methodology

Blockchain technologies have several indisputable qualities that make them ideal for IoMT applications. Blockchain, for example, can bring advancements to data storage, security, and privacy protection in the IoMT due to its immutability and traceability. It improves the efficiency of medical incident tracing and tracking while preventing data loss and tampering.

4.1. Proposed architecture

In this part, we present a proposed architecture for introducing Blockchain into IoMT systems and the benefits and limitations of the proposed architecture. The convergence of Blockchain with IoMT can increase IoMT system interoperability, considerably improve IoMT security, and improve IoMT privacy protection. The proposed architecture (Blockchain-IoMT system) architecture is depicted in **Figure 4**.

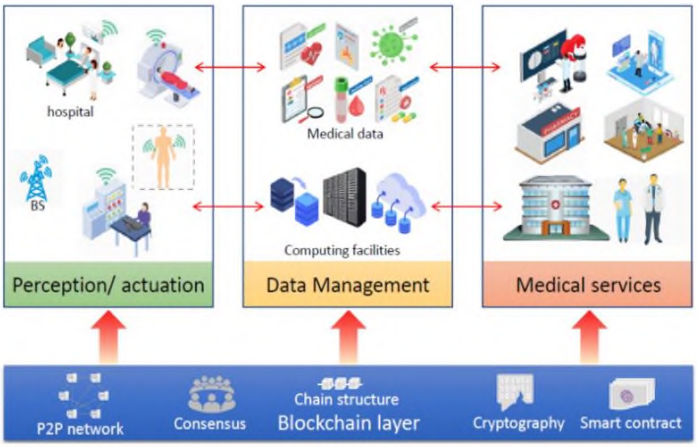

Figure 4. System architecture of the proposed Blockchain-IoMT system.

Figure 4 presents the overview of medical system architecture based on the IoMT. It focuses on perception/actuation, data management, and medical services layers.

4.1.1. Data accumulation and pre-processing layer

This layer gathers the patient's physiological data under standard conditions using wearable biosensors/actuator devices, which then are transmitted to the edge server, base stations, network gateways, or personal internet-enabled devices. Here, the raw physiological data is pre-processed at this stage by reducing data redundancy, compressing it, encrypting the patient's data as it also contains the patient's personal information, and finally transmitting the processed data to the next layer, i.e., Data Management Layer via WiFi or other internet services.

4.1.2. Data Management Layer

The processed data sent by edge servers to this layer is managed efficiently by analyzing and classifying the patient's physiological data based on the priority and timeliness of the task. This layer mainly deals with efficiently storing the gathered data and providing secured access control and authentication mechanisms to protect the patients' personal information.

4.1.3. Medical services layer

This layer acts as an interface between the user and the system, providing the results of the analyzed patients' data in visual data analysis reports. Based on these reports, the healthcare professionals such as doctors can view and analyze the resultant reports of the patients and help them by providing the relevant medical services. These real-time based reports of the patients can generate alarms if the physiological parameters are abnormal, which will immediately notify the Health care persons (such as Doctors and Nursing staff). Based on these alarms, the healthcare staff can initiate necessary and timely action to mitigate the patient's health risks.

4.2. DLT integration with IoMT

In this part, we present the proposed architecture for introducing Blockchain into IoMT systems and the proposed architecture's benefits and limitations. As a promising invention in information technology, DLT

holds great promise for transforming how organizations and teams collaborate across sectors such as the economy, society, and industry. It showcases the most potent DLT breakthroughs since the Blockchain idea was first introduced. The technical principles of DLT are explained in detail to provide the reader with a clear picture. Because Bitcoin's Blockchain was the first genuinely decentralized cryptocurrency without a trusted authority, it illustrates how DLT works (i.e., banks). An explanation of smart contracts and decentralized applications follow this. Following that, we'll look at some specific applications of distributed ledger technology. The convergence of Blockchain with IoMT can increase IoMT system interoperability, considerably improve IoMT security, and improve IoMT privacy protection.

Several advantages for the healthcare sector may result from combining DLT and the IoMT. DLT, like Blockchain, offers a secure and unchangeable database to save patient records. By incorporating DLT into the IoMT, hospitals and clinics may protect their patients' information. It is challenging for bad actors to tamper with or modify the data since each transaction or data entry is cryptographically connected to prior transactions. As a result, patients may have more faith in their medical records and have peace of mind that they won't be tampered with.

DLT allows for safe and open healthcare data exchange amongst all parties involved. Patients, doctors, researchers, and health insurers may safely share and receive medical records because of DLT's incorporation into the IoMT ecosystem. Data sharing may be governed by predetermined norms and consent, which can be enforced using smart contracts. DLT gives people more say over their health records. Patients may control who has access to their information using decentralized identification systems and smart contracts. Patients may control who has access to their medical records and under what circumstances. DLT guarantees that all data access and usage is done in a way that respects the patient's right to privacy.

The proposed architecture's system architecture is depicted in **Figure 5**. As a result, the Blockchain can provide IoMT with security. Adding authentication, homomorphic obfuscation, and group signature to Blockchain can help to secure IoMT data privacy even more. Furthermore, Blockchain systems' overlaid P2P networks can connect diverse sectors in the IoMT to increase interoperability across the board.

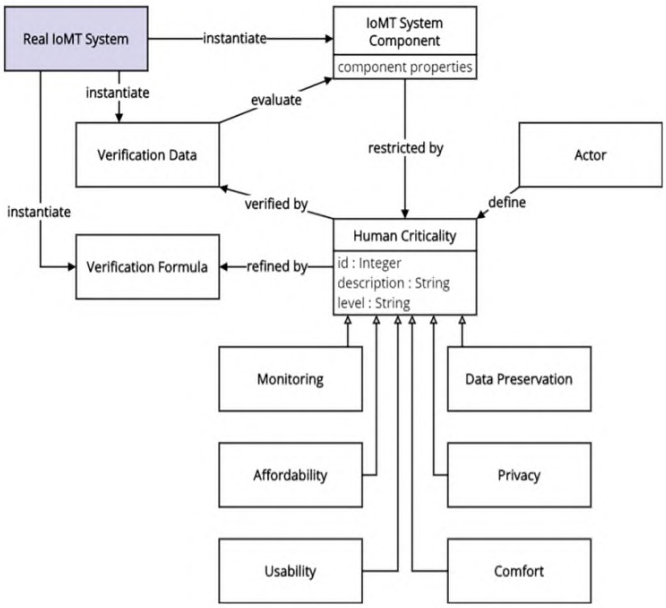

Figure 5. Basic IoMT system design concepts.

5. Results and discussion

The architecture should, we believe, fulfil three primary requirements: the Confidentiality Integrity Authentication (CIA) need for secrecy, integrity, and availability. Confidentiality ensures that authorized users

can only see the message; integrity ensures that the messages received and sent are unaltered; and accessibility guarantees that all services and data are provided. **Table 2** shows that the management hub is an intermediary for data transmission. Other verification methods have been designed to secure the architecture, except for the strict hierarchy.

Table 2. Access control list.

Subject \ Object	l_1	l_2
L_1	"*w,r,c.*"	"*r,c*"
L_2	*Ø*	"*w,r,c.*"

This area considers the combination perfect the architecture of the Bell-La Padula models with the Biba models[28], suitable for the demands of the CIA. We are simplifying these two models and introducing specific attributes.

$$S = (s_1, s_2, s_3, \dots \dots s_n) \quad (1)$$

$$O = (o_1, o_2, o_3 \dots \dots o_n) \quad (2)$$

$$\mu = (M_1, M_2, M_3 \dots \dots, M_n) \quad (3)$$

$$A = (w, r, c) \quad (4)$$

$$L = (l_1, l_2) \quad (5)$$

Where *S* is defined as a subject, *O*'s a set of objects. μ is a set of access matrices that display the access privileges object by object. *A* is the number of access functions that store *w*, *r*, and *c*. *L* focuses on various levels of privilege wherein ($l_1 < l_2$). Safety and integrity can easily be combined within the architecture proposed to achieve complete privileges for the various topics or subjects. We build an access control list founded on the above definition, as demonstrated in **Table 2**. It can be concluded that, in high-ranking matters, the same degree of subjects with every object permission provides equal read and control access. On the contrary, data of the highest level should not be interrupted from the lowest to the highest. Insufficient data must be confined to low to high fluxes. CIA maintains both these rules. Architecture has three entities: device nodes, user nodes, and management hubs. The control nodes are l_2, and the user nodes are l_1. Only data from device and management nodes can be transferred to user nodes. Unable to write or edit information on user nodes. However, all knots of equipment and management hubs can interact efficiently with data. However, we explain an equation too for determining whether the existing situation is safe.

A safe state can be guaranteed once all components are secure and confident. Because the architecture is divided into different levels and specific definitions have been made, *S X O X A* and *L* has been constrained and adhered to strictly; μ is the last element that needs to be seen. Therefore, as shown in **Table 2**, we have designed specific defensive mechanisms to support control of the access matrix. In addition to providing efficient methods with Blockchain technology to govern all forms of access that prevent malicious attacks, they can also improve privacy and security.

$$P(X \geq x) = 1 - e^{(-\lambda x)}$$

where, $P(X \geq x)$ is the cumulative probability of *X* being greater than or equal to *x*. λ is the average rate of block production (λ = 1/commit time). *x* is the number of blocks added to the chain.

Table 3 highlights the performance of the proposed system with existing systems.

Table 3. Performance comparison.

S. No.	Models	Commit time (s)	Commutative probability
1	Bao Z et al.[12], Li M et al.[15]	14	66%
2	Nalin M et al.[17], Homoliak I et al.[19]	19	78%
3	Negro-Calduch E et al.[21],Sai AR et al.[22], Jaquet-Chiffelle DO et al.[23]	20	54%
4	Radoglou-Grammatikis P et al.[25], Paavolainen S and Carr C[32]	12	85%
5	Leal F et al.[26], Huang Y et al.[27]	15	69%
6	Koshy P et al.[28], Faust F et al.[29], Wang D et al.[33]	17	78%
7	Proposed method	10	88%

The proposed architecture can help IoMT overcome its obstacles by providing the following benefits.

- The Elliptic curve cryptography (ECC) function is used in this platform to achieve patient pseudonymity.
- Patients' privacy can be protected using attribute-based signature procedures and access restriction schemes. This technique incorporated numerous authorities to assure patient confidentiality and data immutability in EHRs.

5.1. CASE STUDY: Remote patient monitoring with the IoMT

We show how the proposed methodology can be applied to design a Blockchain-enabled IoMT-based system where elderly patients reside and may use medical equipment in their homes. This particular research centres on fall detection and involves researching and documenting the posture and position of elderly patients (such as sitting, lying, etc.) in case the patient falls. The system sends alerts to remote healthcare providers in case the patient falls.

In the example of the Home situation, an elderly patient with heart failure can lead a self-sufficient lifestyle at home while carefully monitoring his sitting and standing posture and falling. An Azure Fast Healthcare Interoperability Resources (FHIR) Connector was created to implement these goals. Microsoft Azure is a cloud computing platform that offers a wide range of services we may use without buying and arranging our hardware. In an on-premises environment, executing tasks as quickly or efficiently as in the cloud may be impossible. Users can focus on producing excellent products instead of worrying about the infrastructure using Azure Services, such as computation and storage resources, network connectivity, and application services. At home, patients use the following components in the system: a fall detection sensor and a data aggregator, both used to collect sensor-generated data and transfer it to a remote healthcare facility, such as a hospital. Remote healthcare services are now available to the patient after acquiring these devices.

As shown in **Figure 6**, it consists of the following steps as given below:

Step 1. Defining system structure and human criticalities: By specifying the structural properties of a system component in advance, the IoMT designer establishes a basic system structure from which values can be later assigned. IoMTs may be implemented with various medical sensor devices that measure properties such as size, battery consumption, etc. Composite components can comprise other elements that form the system's overall structure. As the patient prescribes, human criticalities may be included in the system. In contrast, patients may have "affordability" as critical when utilizing an IoMT system. Furthermore, the designer lays out design requirements, described as formulas that can be used to validate criticality verification.

These requirements are then connected to the IoMT system component properties, and the system component properties can be validated later in Step 5.

Step 2. Configuring the system: The designer offers estimated value ranges for all IoMT system component properties to help further advance the design process. The alternative configurations of the entire IoMT system represent these values. Different system configurations exist; other matters are used to identify each structure. Each composition is tested in the step where formats are specified.

Step 3. Implementing a simple system: To set up the actual procedure, the system model, as predicted, serves as a reliable starting point. The natural system's fundamental components can, if needed, be manufactured or purchased.

Step 4. Testing system implementation: The validation of the implemented system's hardware devices and software applications is achieved by testing on both hardware and software. The list of values created in the configuration step (Step 2) is explicitly utilized during system testing. Real-world scenarios evaluate multiple combinations of value values for each component, resulting in different performance outcomes (e.g., real-time execution requires minimal processing time). Candidates for further criticality verification, with the metrics yielding the best results, are identified as having the most significant value (see final step).

Step 5. Instantiating system model and criticality verification data: A specific set of values has been selected during system testing and applied to the system components. The formulas for criticality verification are first used to evaluate the component properties, which are used as input to criticality verification formulas. Once these formulas have been completed, the accurate criticality level of human concerns is computed. Criticality verification data elements store the group that has been calculated but also allow users to compare the added level against the desired level and thus determine the criticality verification outcome.

Step 6. Verifying human criticalities: To ensure that human endpoints are indeed human criticalities, desired levels are compared to compute levels. The system cannot meet the patient concern unless the corresponding criticality is verified. Once the system's structure has been set up, implementing the plan and verifying that it addresses the patient's problems can be repeated based on the designer's personal preferences. Thus, the designer can revisit the system structure or its associated criticalities, reconfigure the system if they are not verified, perform another test run and evaluate multiple design alternatives with the patient. The patient's purchase of the IoMT system will enable the customer to start the following healthcare process.

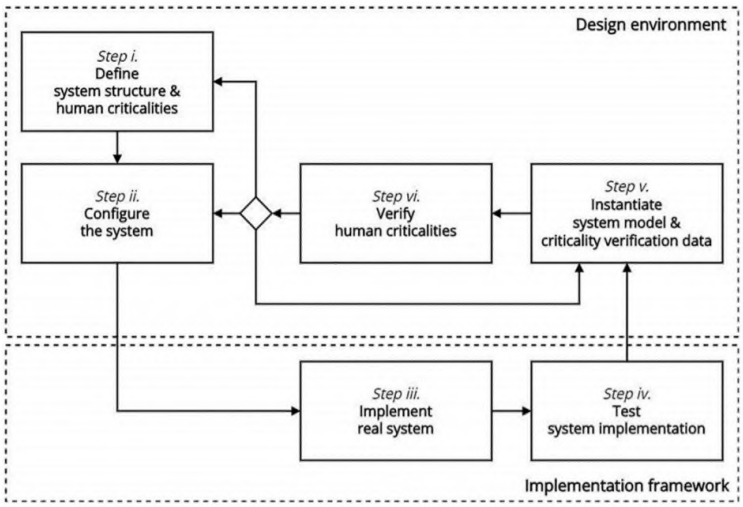

Figure 6. A model-based design methodology for IoMT systems.

5.2. Case research of an eye hospital that stores the details of eye donators

Step 1. An interested candidate visits the eye hospital to register for an eye donation.

Step 2. The assigned doctor diagnoses him to detect any disease or medical problem he suffers from.

Step 3. The registration begins if the candidate is healthy and fit for the eye donation.

Step 4. After filling out the registration form, the candidate's details, like name, age, medical history, eyes, fitness, etc., will be stored in the IPFS. IPFS is a file system that holds records in digital form on the cloud. To provide security, each paper will be stored in encrypted form using any encryption algorithm like AES, DSA, etc.

Step 5. Now store the hash to the location of this record as a block in the Blockchain so that no tempering can be made in the existing history.

If a candidate's details need to be fetched at any time, the hash stored as a block in the Blockchain can be used to get the location of the record kept in the IPFS. Now, the key is needed for the record's decryption shown in **Figure 7**.

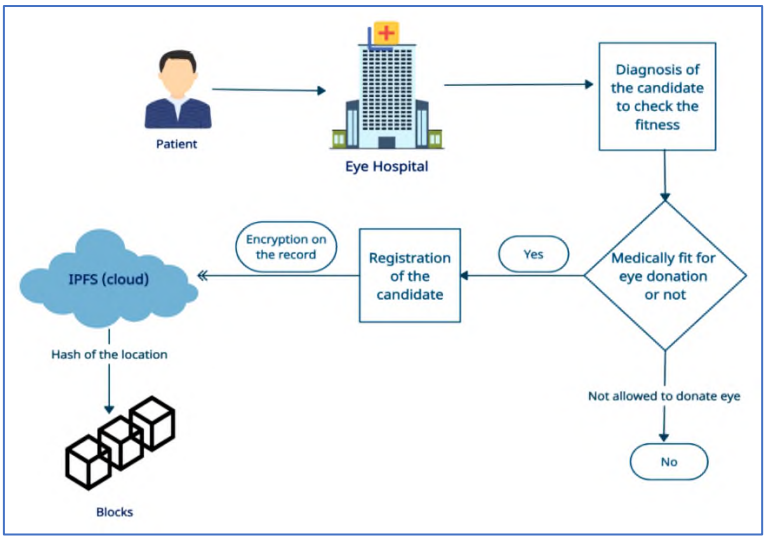

Figure 7. An eye hospital that stores the details of eye donators.

5.3. IoMT FHIR Connector for Azure

IoMT devices connect to an IoMT FHIR (Fast Healthcare Interoperability Resources) connector for Azure. Data from these devices is then persisted in an FHIR server. This Microsoft Healthcare project aims to make it simple for developers to deploy a service for capturing high-frequency IoMT data and dumping it into an FHIR server. Device data can be written to the IoMT FHIR Connector for Azure or in addition to other Azure IoT solutions and remain flexible (IoT Hub and IoT Central). As explained above, the connector does not provide device security or management. Those Azure IoT solutions (such as Azure Device Registration, Azure IoT Edge, and Azure IoT Central) handle these aspects for you. With the help of extensibility, the IoMT FHIR Connector for Azure was designed to make it simple for developers to incorporate new device mapping template types and FHIR resources. The various stages of development include:

- Standardization: Device data is processed into a unified format.
- FHIR Conversion: The data is normalized and grouped before being mapped to FHIR. Templates define and order observations and include references to the device and patient.

The IoMT FHIR Connector for Azure empowers developers, allowing them to customize their own IoMT FHIR Connector service to save time when they need to integrate IoMT data into their applications. The FHIR

developer community will continue to improve this project since it is open-source. PHI's privacy and security requirements are at the forefront, and this IoMT FHIR Connector for Azure was built following those needs (PHI). The Protected Health Information (PHI) compliance requirements for all Azure services utilized in the FHIR Connector for Azure are met. The Microsoft Healthcare team backs this open-source project. However, we know that your feedback and contributions will only improve it. We are heavily involved in creating this code base, and our daily testing of build and deployment artefacts occurs.

5.3.1. Setup and requirements

- An R4 FHIR Server with Device, Patient, and Observation resources that also supports a server with the corresponding resource set.
- A credentials-configured OAuth 2.0 identity provider is given access to the FHIR server.
- Both a patient and device resource on the FHIR server already exists. It should be connected to the patient. Due to the internal id potentially being the same as the device identifier, the users must note that the identity extracted for the device during the normalization step is not the internal ID.
- An item was added to the template storage container with a device content template.
- An FHIR mapping template has been uploaded to the template storage container.

5.3.2. Architecture

To send messages to the connector, use an Azure IoT solution and export messages to the FHIR Connector.

As shown in **Figure 8**, there are following components of this architecture as given below:

- Ingest: Event Hub is the point of ingestion for device data. The throughput of your Event Hub is proportional to the volume of your messages.
- Normalize: Device data is processed and compared to templates in the devicecontent.json configuration file. Important information is extracted, including types, values, and other information. A second Event Hub receives the final product.
- Group: The Normalized group is normalized data grouped according to the identity of the device, measurement type, and the period that has been selected.
- Transform: Latency (delay) is controlled by the period in which the data is written to FHIR. Buffering and output group stages' results are combined. Template definitions are matched against grouped normalized data to produce observations.
- Persist: Once this has happened, the device and patient are retrieved from the FHIR server.

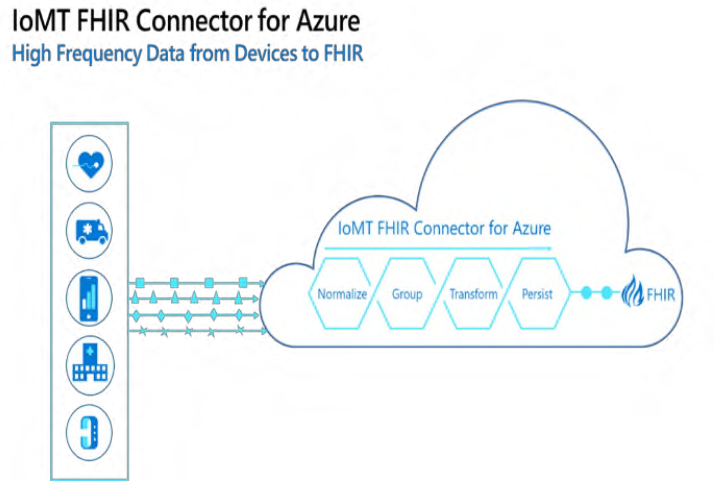

Figure 8. IoMT FHIR connection.

5.4. Discussion

Several advantages and crucial considerations are presented by installing an optimized Blockchain architecture for safe and intelligent healthcare in the context of IoMT devices. The optimized framework offers a reliable method of protecting private medical information produced by IoMT gadgets using Blockchain technology. Blockchain's distributed structure makes it such that information is kept in several different places, each less likely to be breached. In addition, cryptographic techniques may be used to secure data privacy, limiting access to sensitive patient information to only those who need it. Blockchain's verifiable and unalterable characteristics inspire confidence among healthcare ecosystem participants. The optimized architecture makes a shared, immutable ledger of healthcare data available to providers, patients, and other authorized parties. This level of openness greatly enhances accountability, data integrity, and audibility, all essential in healthcare settings.

The Blockchain-based infrastructure allows for the safe and efficient exchange of information between the many players in the healthcare system. Data sharing with the proper authority and compliance with privacy requirements may be ensured through smart contracts, which can set predetermined norms and consent processes. Through the use of defined data formats and protocols, IoMT devices and systems can communicate with one another and share data without disruptions. The system provides a foundation for creating Blockchain-based, immutable, auditable medical records. A patient's medical history can be recorded this way, from initial diagnosis through therapy to the final result. Better continuity of treatment, medical research, and information sharing between providers can all benefit from immutable medical data.

The improved framework can make IoMT devices easier to maintain and safer to use. Thanks to Blockchain-based device identity and authentication protocols, only approved and certified devices will be able to connect to the network. When data and maintenance records for a device are saved on the Blockchain, its performance, maintenance history, and firmware changes can be easily tracked, traced, and verified. The discussion topic must include how the enhanced Blockchain infrastructure conforms to healthcare sector regulations. The General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) are two examples of data protection laws that must be followed. To handle the massive amounts of data produced by IoMT devices, the framework should also consider scalability and performance needs. The debate should consider the difficulties and restrictions of adopting a Blockchain framework for intelligent and secure healthcare in the IoMT setting. Scalability, energy efficiency, compatibility with current healthcare systems, and widespread acceptance are all potential obstacles. Research and development recommendations might look at ways to improve the framework by tackling these issues.

6. Conclusion and future work

In this paper, the authors integrate DLT with IoMT devices. This framework has a significant impact on the commit time and commutative probability. The proposed method has reduced commit time by up to 10 seconds, and Commutative probability has been gained to 88%. This framework can help move healthcare systems toward becoming more cost-effective, secure, and patient-centric by addressing the stated components and considering the obstacles. Adoption and acceptance by healthcare organizations and regulatory authorities depend on investigating governance structures and frameworks compatible with existing regulatory standards.

For Blockchain-based healthcare solutions to be widely adopted, they must provide a positive user experience. User input and participation throughout development can produce more efficient and pleasant final products. Scalability, interoperability, privacy, AI/ML integration, practical implementation, legal concerns, and user-centric design are all aspects of the Blockchain architecture for safe and intelligent healthcare in IoMT devices that need to be addressed in the future. Improvements in these spheres are necessary for the framework

to achieve its full potential in reshaping healthcare delivery and enhancing patient outcomes. They will help bring about its widespread acceptance.

Ethical approval and consent to participate

No ethical approval is required, and authors consent to participate in the paper.

Consent for publication

Authors provide support for publication.

Availability of supporting data

The corresponding author may provide the supporting data on request.

Author contributions

Conceptualization, SD and UKL; methodology, SS; software, AS; validation, VJ, MJ and SS; formal analysis, AS; investigation, VJ; resources, NG; data curation, SD; writing—original draft preparation, SD; writing—review & editing, MK; visualization, MJ; supervision, NG; project administration, AKR; funding acquisition, NG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Manzoor A, Braeken A, Kanhere SS, et al. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on Blockchain. *Journal of Network and Computer Applications* 2021; 176: 102917. doi: 10.1016/j.jnca.2020.102917
2. Belhadi A, Djenouri Y, Srivastava G, et al. Privacy reinforcement learning for faults detection in the smart grid. *Ad Hoc Networks* 2021; 119: 102541. doi: 10.1016/j.adhoc.2021.102541
3. Li G, Dong M, Yang LT, et al. Preserving edge knowledge sharing among iot services: A Blockchain-based approach. *IEEE Transactions on Emerging Topics in Computational Intelligence* 2020; 4(5): 653–665. doi: 10.1109/TETCI.2019.2952587
4. Dalal S, Poongodi M, Lilhore UK, et al. Optimized LightGBM model for security and privacy issues in cyber‐physical systems. *Transactions on Emerging Telecommunications Technologies* 2023; 34(6): e4771. doi: 10.1002/ett.4771
5. Baniata H, Anaqreh A, Kertesz A. PF-BTS: A privacy-aware fog-enhanced Blockchain-assisted task scheduling. *Information Processing and Management* 2021; 58(1): 102393. doi: 10.1016/j.ipm.2020.102393
6. Meenakshi M, Rainu N, Surjeet D, et al. An efficient driver behavioral pattern analysis based on fuzzy logical feature selection and classification in big data analysis. *Journal of Intelligent and Fuzzy Systems Preprint* 2022; 43(3): 3283–3292. doi: 10.3233/JIFS-212007
7. Jindal U, Surjeet D, Rajesh G, et al. An integrated approach on verification of signatures using multiple classifiers (SVM and Decision Tree): A multi-classification approach. *Institute of Advanced Science Extension* 2023; 9(1): 99–109. doi: 10.21833/ijaas.2022.01.021
8. Reyna A, Martín C, Chen J, et al. On Blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems* 2018; 88: 173–190. doi: 10.1016/j.future.2018.05.046
9. Guo Z, Shi L, Xu M, Yin H. MRCC: A practical covert channel over monero with provable security. *IEEE Access* 2021; 9: 31816–31825. doi: 10.1109/ACCESS.2021.3060285
10. Dalal S, Bijeta S, Radulescu M, et al. Optimized deep learning with learning without forgetting (LwF) for weather classification for sustainable transportation and traffic safety. *Sustainability* 2023; 15(7): 6070. doi: 10.3390/su15076070
11. Islam AKMN, Mäntymäki M, Turunen M. Why do Blockchains split? An actor-network perspective on Bitcoin splits. *Technological Forecasting and Social Change* 2019; 148: 119743. doi: 10.1016/j.techfore.2019.119743
12. Bao Z, Wang Q, Shi W, et al. When Blockchain meets SGX: An overview, challenges, and open issues. *IEEE Access* 2020; 8: 170404–170420. doi: 10.1109/ACCESS.2020.3024254

13. Walsh C, O'Reilly P, Gleasure R, et al. Understanding manager resistance to Blockchain systems. *European Management Journal* 2021; 3(39): 353–365. doi: 10.1016/j.emj.2020.10.001
14. Fernández-Caramès TM, Fraga-Lamas P. Towards post-quantum Blockchain: A review on Blockchain cryptography resistant to quantum computing attacks. *IEEE Access* 2020; 8: 21091–21116. doi: 10.1109/ACCESS.2020.2968985
15. Li M, Weng J, Yang A, et al. Toward Blockchain-based fair and anonymous ad dissemination in vehicular networks. *IEEE Transaction on Vehicular Technology* 2019; 68(11): 11248–11259. doi: 10.1109/TVT.2019.2940148
16. Treiblmaier H, Sillaber C. The impact of Blockchain on e-commerce: A framework for salient research topics. *Electronic Commerce Research and Applications* 2021; 48: 101054. doi: 10.1016/j.elerap.2021.101054
17. Nalin M, Baroni I, Faiella G, et al. The European cross-border health data exchange roadmap: Caseresearch in the Italian setting. *Journal of Biomedical Informatics* 2019; 94: 103183. doi: 10.1016/j.jbi.2019.103183
18. Abu-elezz I, Hassan A, Nazeemudeen A, et al. The benefits and threats of Blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics* 2020; 142: 104246. doi: 10.1016/j.ijmedinf.2020.104246
19. Homoliak I, Venugopalan S, Reijsbergen D, et al. The security reference architecture for Blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys and Tutorials* 2021; 23(1): 341–390. doi: 10.1109/COMST.2020.3033665
20. Inkinen T, Helminen R, Saarikoski J. Technological trajectories and scenarios in seaport digitalization. *Research in Transportation Business and Management* 2020; 41: 100633. doi: 10.1016/j.rtbm.2021.100633
21. Negro-Calduch E, Azzopardi-Muscat N, Krishnamurthy RS, Novillo-Ortiz D. Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. *International Journal of Medical Informatics* 2021; 152: 104507. doi: 10.1016/j.ijmedinf.2021.104507
22. Sai AR, Buckley J, Fitzgerald B, Gear AL. Taxonomy of centralization in public Blockchain systems: A systematic literature review. *Information Processing Management* 2021; 58: 102584. doi: 10.1016/j.ipm.2021.102584
23. Jaquet-Chiffelle DO, Casey E, Bourquenoud J. Tamperproof time-stamped provenance ledger using Blockchain technology. *Forensic Science International: Digital Investigation* 2020; 33: 300977. doi: 10.1016/j.fsidi.2020.300977
24. Schniederjans D, Curado C, Hedayati MK. Supply chain digitization trends: An integration of knowledge management. *International Journal of Production Economics* 2020; 220: 107439. doi: 10.1016/j.ijpe.2019.07.012
25. Radoglou-Grammatikis P, Sarigiannidis P, Iturbe E, et al. SPEAR SIEM: A security information and event management system for the smart grid. *Computer Networks* 2021; 193: 108008. doi: 10.1016/j.comnet.2021.108008
26. Leal F, Chis AE, Caton S, et al. Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. *Big Data Research* 2021; 24: 100172. doi: 10.1016/j.bdr.2020.100172
27. Huang Y, Bian Y, Li R, et al. Smart contract security: A software lifecycle perspective. *IEEE Access* 2019; 7: 150184–150202. doi: 10.1109/ACCESS.2019.2946988
28. Koshy P, Babu S, Manoj BS. Sliding window Blockchain architecture for Internet of Things. *IEEE Internet of Things Journal* 2020; 7(4): 3338–3348. doi: 10.1109/JIOT.2020.2967119
29. Faust F, Thierry A, Müller T, Freiling F. Selective imaging of file system data on live systems. *Forensic Science International: Digital Investigation* 2021; 36: 301115. doi: 10.1016/j.fsidi.2021.301115
30. Xu Y, Huang Y. Segment Blockchain: A size reduced storage mechanism for Blockchain. *IEEE Access* 2020; 8: 17434–17441. doi: 10.1109/ACCESS.2020.2966464
31. Yousefnezhad N, Malhi A, Främling K. Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications* 2020; 171: 102779–102779. doi: 10.1016/j.jnca.2020.102779
32. Paavolainen S, Carr C. Security properties of light clients on the ethereum Blockchain. *IEEE Access* 2020; 8: 124339–124358. doi: 10.1109/ACCESS.2020.3006113
33. Wang D, Zhu Y, Zhang Y, Liu G. Security assessment of Blockchain in Chinese classified protection of cybersecurity. *IEEE Access* 2020; 8: 203440–203456. doi: 10.1109/ACCESS.2020.3036004
34. Li G, Sheng X, Wu J, Yu H. Securing transmissions by friendly jamming scheme in wireless networks. *Journal of Parallel and Distributed Computing* 2020; 144(3): 260–267. doi: 10.1016/j.jpdc.2020.04.013
35. Chaturvedi K, Matheus A, Nguyen SH, Kolbe TH. Securing spatial data infrastructures for distributed smart city applications and services. *Future Generation Computer Systems* 2019; 101: 723–736. doi: 10.1016/j.future.2019.07.002
36. Dai W, Dai C, Choo KKR, et al. SDTE: A secure Blockchain-based data trading ecosystem. *IEEE Transactions on Information Forensics and Security* 2019; 15: 725–737. doi: 10.1109/TIFS.2019.2928256
37. Krzywiecki L, Bobowski A, Słowik M, et al. Schnorr-like identification scheme resistant to malicious subliminal setting of ephemeral secret. *Compututer Networks* 2020; 179: 107346. doi: 10.1016/j.comnet.2020.107346
38. Rožman N, Diaci J, Corn M. Scalable framework for Blockchain-based shared manufacturing. *Robotics and Computer-Integrated Manufacturing* 2021; 71: 102139. doi: 10.1016/j.rcim.2021.102139

39. Thakur S, Breslin JG. Scalable and secure product serialization for multi-party perishable good supply chains using Blockchain. *Internet of Things* 2020; 11: 100253. doi: 10.1016/j.iot.2020.100253
40. Fröwis M, Gottschalk T, Haslhofer B, et al. Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation* 2020; 33: 200902. doi: 10.1016/j.fsidi.2019.200902
41. Akyildirim E, Corbet S, Cumming D, et al. Riding the wave of crypto-exuberance: The potential misusage of corporate Blockchain announcements. *Technological Forecasting and Social Change* 2020; 159: 120191. doi: 10.1016/j.techfore.2020.120191
42. Lisi A, Salve AD, Mori P, et al. Rewarding reviews with tokens: An Ethereum-based approach. *Future Generation Computer Systems* 2021; 120: 36–54. doi: 10.1016/j.future.2021.02.003
43. Benedetti H, Nikbakht E. Returns and network growth of digital tokens after cross-listings. *Journal of Corporate Finance* 2021; 66(2): 101853. doi: 10.1016/j.jcorpfin.2020.101853
44. Huang C, Wang Z, Chen H, et al. Repchain: A reputation-based secure, fast, and high incentive Blockchain system via sharding. *IEEE Internet Things Journal* 2020; 8(6): 4291–4304. doi: 10.1109/JIOT.2020.3028449
45. Shrestha R, Nam SY. Regional Blockchain for vehicular networks to prevent 51% attacks. *IEEE Access* 2019; 7: 95033–95045. doi: 10.1109/ACCESS.2019.2928753
46. Park SK, Kwon O, Kim Y, et al. Mind control attack: Undermining deep learning with GPU memory exploitation. *Computer and Security* 2021; 102: 102115. doi: 10.1016/j.cose.2020.102115
47. Onyema EM, Umesh KL, Praneet S, et al. Evaluation of IoT-Enabled hybrid model for genome sequence analysis of patients in healthcare 4.0. *Measurement: Sensors* 2023; 26: 100679. doi: 10.1016/j.measen.2023.100679
48. Arora S, Surjeet D. Trust evaluation factors in cloud computing with open stack. *Journal of Computational and Theoretical Nanoscience* 2019; 16(12): 5073–5077. doi: 10.1166/jctn.2019.8566
49. Le DN, Bijeta S, Surjeet D. A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: A revolutionary approach. *Journal of Cyber Security and Mobility* 2018; 7(4): 379–408. doi: 10.13052/2245-1439.742
50. Jazaeri SS, Jabbehdari S, Asghari P, Javadi HHS. An efficient edge caching approach for SDN-based IoT environments utilizing the moth flame clustering algorithm. *Cluster Computing* 2023. doi: 10.1007/s10586-023-04023-9
51. Dalal S, Poongodi M, Umesh KL, et al. Extremely boosted neural network for more accurate multi-stage cyber attack prediction in cloud computing environment. *Journal of Cloud Computing* 2023; 12(1): 1–22. doi: 10.1186/s13677-022-00356-9
52. Wang Z, Hu J, Min G, et al. Spatial-temporal cellular traffic prediction for 5 G and beyond: A graph neural networks-based approach. *IEEE Transactions on Industrial Informatics* 2022; 19(4): 1–10. doi: 10.1109/tii.2022.3182768
53. Jazaeri SS, Parvaneh A, Sam J, Javadi HHS. Toward caching techniques in edge computing over SDN-IoT architecture: A review of challenges, solutions, and open issues. *Multimedia Tools and Applications* 2023. doi: 10.1007/s11042-023-15657-7
54. Sadhu PK, Yanambaka VP, Ahmed A. Internet of Things: Security and solutions survey. *Sensors* 2022; 22(19): 7433. doi: 10.3390/s22197433
55. Sadhu PK, Yanambaka VP, Ahmed A, Kumar Y. Prospect of Internet of Medical Things: A review on security requirements and solutions. *Sensors* 2022; 22(15): 5517. doi: 10.3390/s22155517
56. Sadhu PK, Jesse E, Yanambaka VP, Ahmed A. Supervised machine learning tools and PUF based internet of vehicles authentication framework. *Electronics* 2022; 11(23): 3845. doi: 10.3390/electronics11233845
57. Sadhu PK, Yanambaka VP, Ahmed A, Kumar Y. NAHAP: PUF-based three factor authentication system for Internet of Medical Things. *IEEE Consumer Electronics Magazine* 2022; 12(3): 107–115. doi: 10.1109/MCE.2022.3176420
58. Sadhu PK, Yanambaka VP, Ahmed A. Physical unclonable function and machine learning based group authentication and data masking for in-hospital segments. *Electronics* 2022; 11(24): 4155. doi: 10.3390/electronics11244155