Annals of Emerging Technologies in Computing (AETiC)
Vol. 9, No. 2, 2025

Research Article

Blockchain Aided Smart Consensus Model for IoMT Architecture

Md. Iftekharul Alam Efat[1,*], Tasnim Rahman[1], Md. Jane Alam[1] and Shah Mostafa Khaled[2]

[1]Noakhali Science and Technology University, Noakhali, Bangladesh
iftekhar.iit@nstu.edu.bd; tasnim.iit@nstu.edu.bd; janealam1112@student.nstu.edu.bd
[2]University of Dhaka, Dhaka, Bangladesh
khaled@du.ac.bd
*Correspondence: iftekhar.efat@gmail.com

Received: 17th March, 2024; Accepted: 27th December 2024; Published: 1st April 2025

Abstract: The rapid evolution of technology in healthcare underscores its pivotal role in shaping human lives, particularly with the widespread adoption of wearable Internet of Things (IoT) sensors. This surge has led to the interconnection of a vast array of devices, sensors, and real-time trackers over the internet, driving research interest in the development of a Remote Patient Monitoring system for treatment and consultation. Concurrently, the integration of Artificial Intelligence (AI) into decision support systems has become prevalent, paving the way for the creation of a smart consensus system that enhances efficiency through live remote sensor data. Nevertheless, the adoption of such advanced technologies is not without challenges, particularly in the realms of privacy, security, and standardization for data transmission and transaction cataloguing. To address these concerns, blockchain has emerged as a compelling solution, seamlessly integrating with existing solutions and providing heightened security and privacy assurances, especially in collaboration with third-party entities. In response to these challenges, a proposed blockchain-enabled Internet of Medical Things (IoMT) architecture takes centre stage. This innovative framework leverages real-time wearable sensor data from patients as the primary source for diagnosis, ensuring secure storage and transmission through the application of blockchain technology. Furthermore, the proposed IoMT architecture extends its reach by integrating stakeholders from the healthcare domain. This collaboration enhances the system's effectiveness, with an AI-based decision support system aiding consultants in remotely monitoring patients with ease. However, the simulated experiment demonstrates improved access control, authentication, scalability (150 TPS), low energy consumption (50kWh/year), and reduced transaction latency (200ms) compared to PoW, PoS, and PoA. In summary, the fusion of wearable IoT sensors, AI, and blockchain in this IoMT architecture not only addresses the challenges of privacy and security but also establishes a robust foundation for advancing electronic healthcare systems.

Keywords: ***Blockchain; Consensus System; Decision Support System; Internet of Medical Things; Smart Healthcare System***

1. Introduction

The creation of the Internet of Medical Things (IoMT) is a significant milestone in the field of healthcare, which has witnessed a revolutionary phase brought about by the Internet of Things (IoT). IoMT holds immense importance in the medical sector by revolutionizing patient care through the integration of smart devices capable of collecting, transmitting, and analyzing health-related data. It represents the healthcare-centric adaptation of IoT, enabling healthcare professionals to remotely and instantly monitor diverse health parameters, including heart rate, body temperature, and oxygen levels, through various sensors positioned on or within the patient's body [1-3].

The Internet of Medical Things (IoMT) consists of applications such as physical wellness programs, remote health monitoring, elderly care and the management of chronic health conditions. It has notable implications for home medication management and the enforcement of treatment adherence protocols [4].

Md. Iftekharul Alam Efat, Tasnim Rahman, Md. Jane Alam and Shah Mostafa Khaled "Blockchain Aided Smart Consensus Model for IoMT Architecture", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 31-52, Vol. 9, No. 2, 1st April 2025, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2025.02.003, Available: http://aetic.theiaer.org/archive/v9/v9n2/3.html.

This transformative technology not only enhances the quality of patient care but also facilitates remote monitoring, diagnosis, and treatment, thereby addressing the evolving needs of the healthcare landscape.

However, one of the significant difficulties is to maximize data transfer from these sensors by developing an Internet of Things platform with a central structure [5]. The dynamic nature of medical data such as including textual, video, and continuous data exchange and the interconnectedness of devices raise concerns about data protection and privacy. The sheer amount of sensitive health information being transferred within IoMT architectures necessitates robust mechanisms to ensure confidentiality and prevent unauthorized access.

Additionally, interoperability issues pose a hurdle, as seamless communication between diverse IoMT devices and healthcare systems becomes paramount for optimal functionality [6]. The increasing popularity of this technology is driven by the growing expenses of analytic data platforms, the increasing number of internet devices, and the establishment of standardized protocols for collecting data from IoT devices. Also, managing extensive data at exceptionally high speeds and fortifying the fundamental infrastructure essential to this process. This underlines the need to automate the processing of substantial data gathered from sensors, all while ensuring the confidentiality and privacy of the collected data [7].

In present healthcare systems, wireless-enabled devices like sensors and wearables communicate via a central device, commonly referred to as a gateway. In general, this gateway sends the collected data to the cloud [8]. Features like peer authentication, scalability, availability, control over access, and data transparency are essential to an IoMT system because of its cloud-based design [9-11].

However, the downsides of a cloud based IoMT system include challenges in service availability, user privacy, security, interoperability, and potential data manipulation [9, 12]. A significant concern is the vulnerability of the system to cloud server failures, leading to unavailability for patients, doctors, and medical staff in case of downtime.

Currently, the digital healthcare industry is undergoing a substantial rise in the integration of blockchain technology which seeks to address challenges related to storage, sharing, data security, and privacy. The utilization of blockchain technology, characterized by its distributed ledger, holds promising advantages for IoMT applications [13]. With its decentralized nature, these challenges are managed by creating multiple replicas in different servers, ensuring the authenticity and security of electronically signed transactions. The distributed architecture stands out as a key benefit, addressing a significant issue – the drawbacks of the cloud in IoMT applications.

Besides, blockchain technology provides further merits such as smart contracts, reliable recording, trust less consensus, protection through data access control, clarity, and an open architecture that makes decentralized data exchange between hospitals and patients convenient [14]. The worldwide distribution of devices empowered by the Internet of Medical Things (IoMT) seamlessly aligns with patients' medical history through the integration of blockchain and IoT. Utilizing a secure smart contract mechanism for sending IoMT data to the blockchain significantly reduces data forgery and information mutation [15].

In essence, blockchain security policies enhance trust among stakeholders, simplifying the streamline for data gathering, sharing, storing, and maintenance system through decentralized storage. This approach ensures proper control of patient privacy policies. In this article, our work lies in addressing the challenges faced by existing IoMT systems, particularly concerning data security, privacy, and interoperability issues inherent in cloud-based architectures. In addition, we have explored the integration of blockchain technology to enhance the storage, sharing, and protection of sensitive health data while facilitating decentralized data exchange among healthcare stakeholders.

In this article, we have introduced a cutting-edge architectural design that incorporates blockchain into the Internet of Medical Things (IoMT). The focal point of this architecture revolves around leveraging real-time wearable sensor data from patients as the primary source for diagnostic purposes. The utilization of blockchain technology ensures the reliability of storage and transmission of this critical data. Furthermore, our approach integrates key stakeholders within the healthcare domain, fostering a comprehensive system that promotes widespread adoption. Notably, the inclusion of an AI-based decision support system enhances the capabilities of consultants, enabling seamless remote monitoring of patients with heightened ease and efficiency.

The innovative aspect of our proposed IoMT architecture is its establishment of a decentralized, distributed, and reliable ecosystem that addresses the shortcomings of conventional IoT-based healthcare systems, which primarily focus on challenges related to data transfer, storage, and privacy.

However, a thorough examination employing the latest electronic healthcare systems to substantiate the security requirements of the proposed architecture reveals a notable improvement in the performance of this Internet of Medical Things (IoMT) framework. This comprehensive study highlights the benefits and improvements provided by the proposed IoMT architecture in the realm of electronic healthcare systems. Finally, this research aims to optimize patient care through secure and efficient management of IoMT data.

The rest of this article is organized in the following manner: Section 2 Analysing the related literature on blockchain enable healthcare systems using IoT. Section 3 proposed consensus architectural model. Following that, Section 4 will showcase the experimental results that were consequently obtained, and this will be succeeded by concluding statements and prospective work in Section 5.

2. Literature Review

The integration of blockchain technology into the Internet of Medical Things (IoMT) architecture offers a transformative approach to enhancing security, transparency, and efficiency in healthcare data management through a Smart Consensus Model. This literature review examines the current research on blockchain-aided consensus mechanisms, focusing on their effectiveness in tackling challenges such as scalability, data security, and regulatory compliance.

Nayyar *et al.* [3] explored the transformative impact of the Internet of Medical things (IoMT) in healthcare. Their research addressed connectivity challenges through IoMT-PLM integration, tackled battery efficiency using innovative algorithms, and introduced the BioSenHealth 1.0 framework for medical applications. The effectiveness of the proposed system was substantiated through successful testing on over 50 live patients, showcasing notable improvements in cost-effectiveness, accuracy, portability, and real-time response.

Correspondingly, Almalki *et al.* [5] explored the transformative impact of the Internet of Medical Things (IoMT) in healthcare evolution. Their research proposed a prototype integrating blockchain for secure patient data analysis, featuring a three-layered decision-making structure and AI, with demonstrated efficacy in a testing network involving two peer nodes. The study explored IoT's disruptive potential as a business opportunity, emphasizing wireless communication standards, envisioning a future with billions of connected sensors, and discussing applications such as home automation and social communication. Furthermore, another research addressed emerging social and governance issues associated with IoT [6]. Considering IoT in the healthcare context, the authors presented a platform for patient health monitoring utilizing IoMT and Blockchain for data security. They employed smart sensors and an embedded Raspberry PI 4, showcasing the system's effectiveness as a low-cost, secure Electronic Health Record (EHR) solution [7].

Moreover, Mutlag *et al.* [11] introduced a geographically distributed fog computing architecture designed to connect diverse devices at the network's edge, providing adaptable communication, computation, and storage services. Their study investigated the integration of the Internet of Medical Things (IoMT) with cloud computing for the processing and analysis of healthcare data, with a particular emphasis on security challenges inherent in conventional cloud platforms. The systematic review conducted by the authors evaluated ten blockchain-based solutions, categorizing them into decentralization and security aspects. This categorization aimed to address issues such as centralization, overhead, trust evidence, adaptability, and inaccuracy in cloud-based trust management [14].

On the other hand, Irving and Holden [16] introduced clinical experiment through applying blockchain to specify evidence of pre-specified termination. There they conducted experimental trials for a healthcare-based trial protocol, which had previously been associated with reported outcome switching. Also, they determined the reliability of the scientific approach of blockchain, which provides independently verifiable and low cost. To enhance this security later digital lightweight signature model was proposed [17].

Comparably, Xia *et al.* [18] emphasized privacy risks in the dissemination of medical records and criticized existing protection methods. They introduced MeDShare, A system based on blockchain that tackles challenges related to sharing medical data by employing smart contracts and access controls to

ensure secure monitoring and establish data provenance. Additionally, Roehrs *et al.* [19] identified challenges in creating a unified view of patients' health records across organizations and proposed OmniPHR, a distributed model, which addressed Personal Health Record (PHR) challenges through a unified view and secure access for healthcare providers, validated in a feasibility evaluation. Another proposal by Ren *et al.* [20] focused on enhancing data security in Wireless Body Area Networks (WBANs) using blockchain. They introduced a sequential aggregate signature scheme (DVSSA) to protect user privacy and reduce blockchain storage space.

Table 1. State-of-art Blockchain based Applications for Healthcare Systems

Authors	Year	Blockchain Technologies/ Methodologies	Merits	Demerits
Zhang *et al.* [21]	2016	Blockchain-based method for PSN nodes	Forward secrecy of master key, confidentiality of secret keys	It may bring heavy storage load to PSN nodes
Dimitrov *et al.* [22]	2016	Ethereum, Proof of Concept, Public blockchain	Using WBAN smart contracts runs exactly without third-party interference and automatically monitor the patient's health along with high authenticity	Insufficient ingestion of data
Zheng *et al.* [23]	2017	Separate blockchain	A public ledger and all dedicated contacts are accumulated in a catalogue of blocks	Difficulties using algorithm
Srivastava *et al.* [24]	2018	Proof-of-work	Ensure the security of data exchanges among connected edges	Security vulnerability for health monitoring
Rahman *et al.* [25]	2018	Private blockchain	Calculating dyslexic symptoms data possible to shared safely with mobile multimedia medical practitioners	Delay average test module uploading time
Hang *et al.* [26]	2019	Hyperledger Fabric Platform	Hardy against network failures like distribution Node down	Denial-of-Service (DoS) attack is not considered and smart contracts take long time to execute
Alqaralleh *et al.* [27]	2021	GO-FFO, ECC, NIS-BWT, and DBN	Secure IoT, efficient image transmission, accurate disease diagnosis.	Limited Resources & inadequate training data
Bhattacharjya *et al.* [28]	2022	Separate blockchain	Enhances security, decentralization, tamper-proof, versatile IoT application, incentivizing participation.	Potential ECDSA backdoor risks, limited PoW incentives, reliance on experimental implementations.
Sahar *et al.* [29]	2023	Private blockchain	Ensures secure and trustworthy services, decentralized IoMT with optimal performance.	Complexities with hardware accelerators integration.

Similarly, Blockchain showed a digital ledger that affords end-to-end communication without non-trusting members exclusive of each intermediary. Blockchain security technology is providing to protect data from any security attack during data transmission. In this research, authors examine various blockchain technologies and the operation of blockchain within the IoMT security architecture to guarantee the security of data transmission among interconnected pathways [22].

Implementing the platform for blockchain technology, Hang *et al.* [26] describes Hyperledger Fabric architecture, the explanation back different design arrangements, and its several pre-eminent implementations feature, the programming pattern of its distributed applications is implemented by Fabric, achieving throughput exceeding 3500 transactions per second in a broad configuration.

However, Bhattacharjya *et al.* [28] underscored the significance of securing Internet of Medical Things (IoMT) systems, highlighted the increasing use of Blockchain for real-time communication and data integrity. They proposed a Blockchain-based technique, emphasizing the CIA triad (Confidentiality, Integrity, and Availability) for ensuring secure and trusted real-time communication in IoMT applications, with a specific focus on a cloud-based hospital scenario.

Additionally, Badri *et al.* [29] highlighted vulnerabilities in existing cloud based IoMT architectures and introduces a private and scalable blockchain framework, ensuring security and trust in medical data

sharing. Their suggested framework has good performance with an average throughput of 857 TPS and 151 TPS for read and write operations, along with minimal latency. It uses attribute-based encryption and an IoT-friendly consensus mechanism.

Existing blockchain-based IoMT applications in the healthcare sector face significant limitations, particularly in scalability, which hinders the management of large volumes of real-time patient data. IoMT devices typically lack the necessary computational power and energy to support the resource-intensive consensus mechanisms of blockchain. Also, challenges related to data privacy compliance, regulatory adherence, and integration with legacy healthcare systems hold up widespread adoption and practical implementation. State-of-the-art models also struggle to integrate with existing stakeholder systems due to diverse legacy technologies and a lack of standardized data formats, alongside regulatory and privacy concerns that conflict with the transparency of blockchain.

Nevertheless, the main driving factor for conducting this research is the adoption of Artificial Intelligence to manage IoMT data for blockchain consensus model, which is one of the most challenging and underexplored research areas. The complexity arises mainly from the high computational demands of AI algorithms, which often surpass the capabilities of many IoT devices, complicating effective implementation in practical scenarios.

3. Proposed method

The complete structure of the anticipated model is based on the integration of all healthcare stakeholders with the system, where each stakeholder will connect to the proposed architecture individually with their existing systems. In this regard, we have considered Doctors, Hospitals, Diagnostic Centers, Ambulances, Pharmacy, Patients and their relatives.

Through this system, patient and doctor can communicate with each other as well as observe all previous treatment record by that or other consultants for those particular patients can be accessed. Also, the diagnosis report and other regular patient data like blood pressure, temperature, blood sugar, pulse rate, movement or calorie burn etc. data are integrated that will give the consultant a precise overview about the patient for treatment.

Correspondingly, the other stakeholders like ambulance or hospital will be connected in same way, however there is another intelligent decision support system which will trigger the system based on patient risk status based on their continuous data. Again, through this secured system, patient can purchase medicines from pharmacy with prescription, which also leads to ethical usage of medicines. Moreover, for any emergency patient or accident case, hospital or emergency doctor can start treatment procedure with less diagnosis test and using the patient's previous records.

3.1. IoMT Architecture

The proposed IoMT architecture has 3 (three) layers: Figure 1 displays the Storage, Business, and Application layers. The activities of each layer are connected through the Blockchain application exists in the Business Layer, which is described in the next sub-sections:

3.1.1. Storage Layer

The storage layer is consisting of three parts: data sensing and generating, data processing and data storing. This data sensing part is the core feature of IoMT, where the data come from the patient end through some wearable sensors and devices. Due to precise measurement of the wearable devices, now-a-days medical consultant can rely on these kinds of sensor data for diagnosis and treatment purpose [30].

However, in this proposed IoMT architecture, patient's Blood Pressure (BP), Body Temperature, Pulse and Oxygen in Blood Sensor (SPO_2) [2], Continuous Glucose Monitoring [31] data named Blood Sugar Level, Positioning Sensor (Accelerometer) etc. can sense the data and through Bluetooth, RFID or WiFi medium send to the Local Storage or Mobile Device. There, an existing system or Local storage will process those data to desired format and transmit to the Data Storing portion via Cloud network.

In this Data storing portion of this Storage Layer, an integration of off-chain and blockchain based storage system is deployed which is connected through the cloud network. The sensitive patient data that is encrypted in the blockchain are observable to every node in the network [32]. Also, the off-chain storage used here, is actually acted like isolated database; while the Blockchain maintains meta information

prerequisite for authenticating the integrity of the data with a timestamp, which is shown in Figure 2. However, this data storing association ensures the immutability requirement of the storing system.

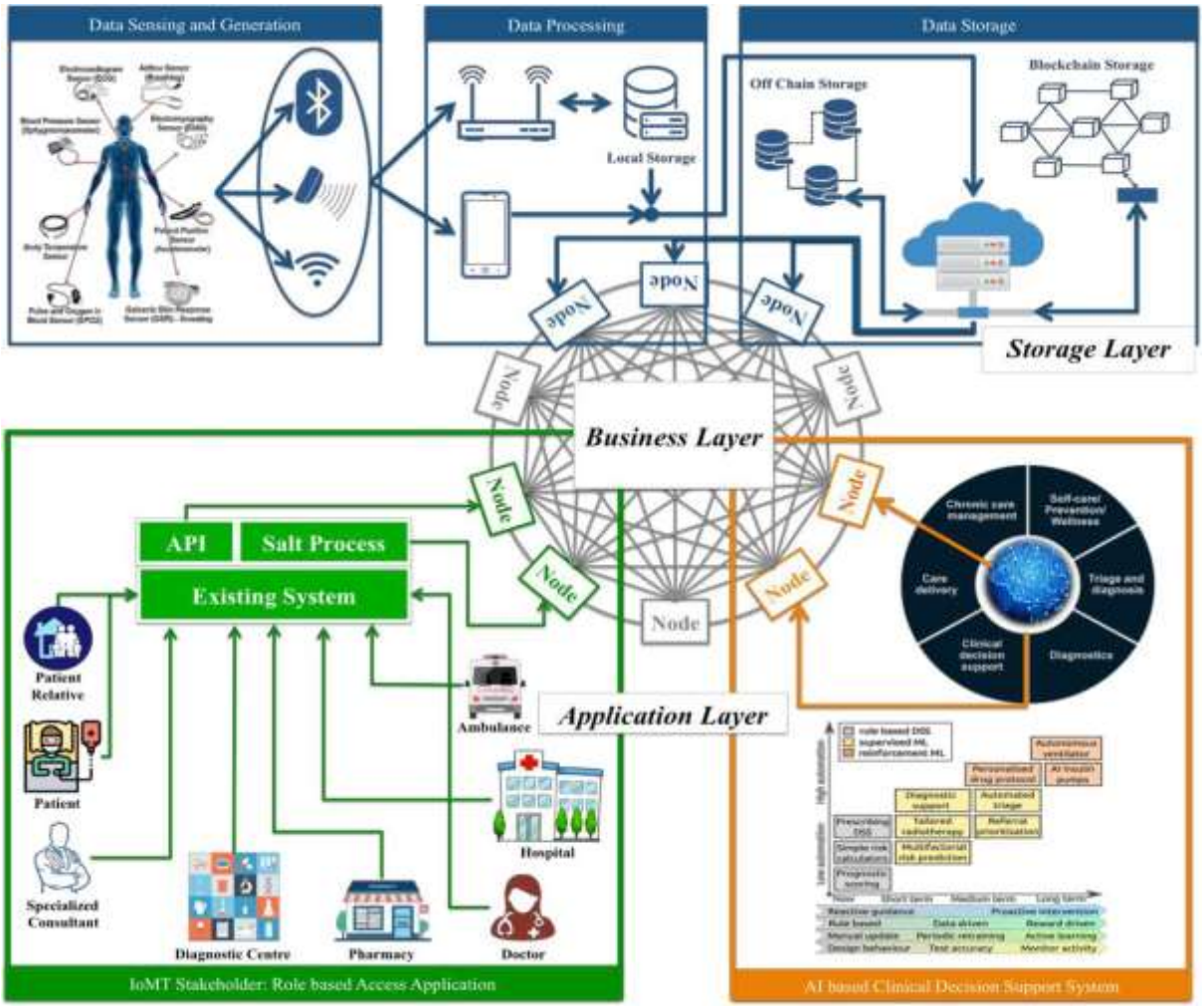

Figure 1. The proposed IoMT Architecture with interaction of the Stakeholders

In addition, expensive medical particulars like prescriptions; MRI images, CT scan, X-ray or other similar kinds of diagnosis report could be store in off-chain storage in any size or format. On the other hand, summary data in text format will be kept in Blockchain, which is instantly visible and ingestible to all the stakeholders of this framework in a trustworthy manner.

Moreover, this storage procedure is fault-tolerant, therefore bottleneck or single point points of failure can be avoided. Also, handling the big medical sensor data in blocks is much expensive, which is resolved using this off-chain storage integration. However, in the Business layer, there exists secured digital signature-based authenticity mechanism to access the off-chain database access.

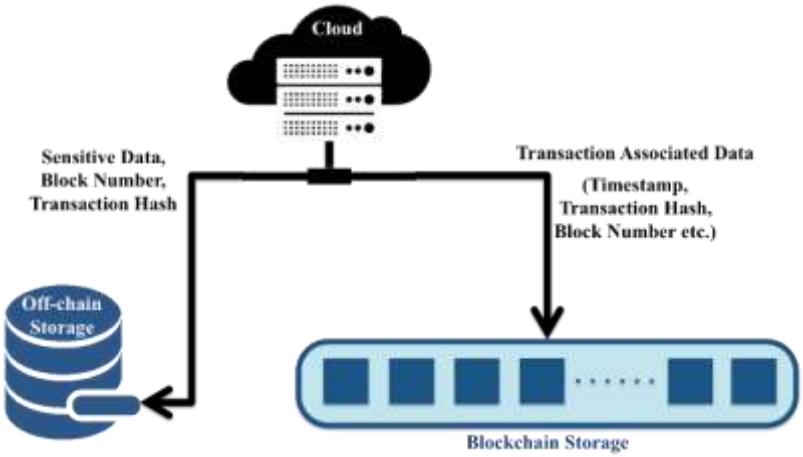

Figure 2. Off-chain and Blockchain Data Storage Association

3.1.2. Business Layer

The core of the architecture lays on this Business layer, which acts as an abstraction between Blockchain and Application layer. To illustrate, the main Blockchain protocols is overlaid in this layer that is reusable and the components are according to the applications specific. However, this layer also functions as the service layer, encompassing elements such as Smart Contracts, Role-based Authentication, Digital Signature, User Validation, Access Control, and more.

Here, the blocks contain batches of legitimate transactions that have been hashed and programmed into a Merkle tree [23]. Each block contains two links the cryptographic hash of the prior block in the chain. Linked blocks are created of a particular chain. This iterative process guarantees the integrity of the preceding block in every aspect of the newly created block [33]. The block body consists of a transaction counter and the transactions. However, each block is composed of a block header and block body, as depicted in Figure 3. In particular, the blocks used in this layer will have some properties that are described in Table 2.

Table 2. Block Properties of the Blockchain in Business Layer

Indicators	Description	Size
Magic Number	Unique identifier for the blockchain network with a fixed value of 0xD9B4BEF9.	4 bytes
Block Size	Maximum limit a block can be filled up with transactions	1 MB
Header: Next 80 bytes		
Version of the Block	Denotes the authentication rule for the respective block to be trailed	4 bytes
Ancestor Block Hash	A hashed value indicating the preceding block.	32 bytes
Root of Merkle Tree	Encrypt all the transaction to a hash value of the respective block	32 bytes
Time Data	The current time, measured in seconds since January 1, 1970, in Coordinated Universal Time (UTC).	4 bytes
Difficulty Target	Threshold value for authorized block	4 bytes
Nonce	Starts with 0 and increases in each hash	4 bytes
Body of the Block		
Transaction Counter	Number of transactions that are part of the block	1-9 bytes
Transaction List	Holds the digital fingerprint of every transaction within that block.	< 1 MB

Again, the highest number of transactions relies on the block size and the size of each individual transaction. Asymmetric cryptography technique is used to verify the legitimacy of a transaction in Blockchain [23]. Digital signature used an untrustworthy environment based on asymmetric cryptography. Also, a new node, which wants to add transaction to the Blockchain, needs the consent of the networked nodes where the transaction should appear. This contract occurs when nodes are allowed to be connected a chain in the next block of a transaction.

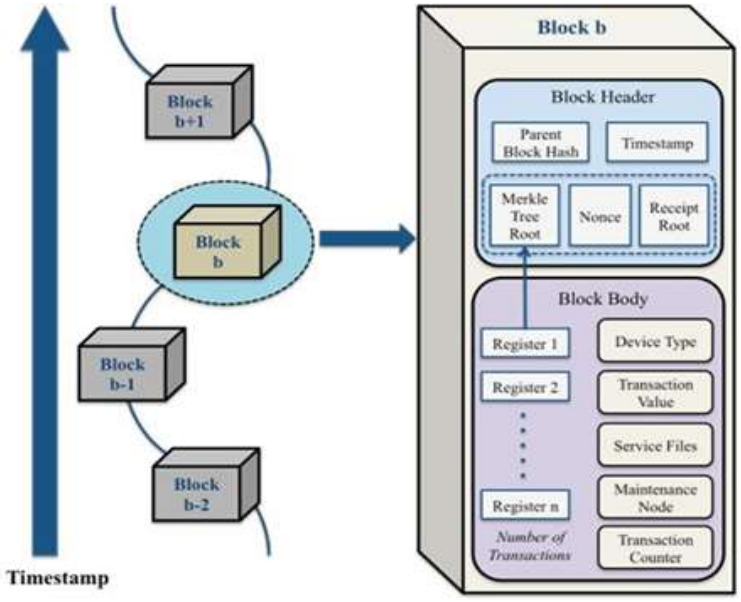

Figure 3. An Abstraction of the Block in Blockchain

3.1.3. Application Layer

This layer is basically acts as an interface with all the stakeholders through existing systems using Application Program Interface (API) encrypted with salt value to access the data [34]. Therefore, unwanted application or unauthorized access can be prevented and a secured transmission channel will be established between the system and the stakeholder. Also, an AI based clinical decision support system is integrated in this layer, which basically works on the patient's sensor data and takes decision accordingly like informing nearest hospital based on critical condition of the patient or informing patient's relative etc. [30].

However, this layer is inconsistent with both rules based [35] as well as supervised and reinforcement machine-learning [36] approaches to provide impulsive decisions based on patient health condition and prescribe treatment correspondingly. To illustrate, using rule based DSS prognostic scoring, risk calculator, prescribing etc. applications are considered for implementation [30]. Similarly, diagnostic support, tailored radiotherapy, referral prioritization, multifactorial risk prediction etc. types of short and mid-term automation could be applied using supervised machine-learning approaches. Furthermore, considering the reward driven periodic retraining commonly known as reinforcement approach can produce autonomous ventilator, personalized drug protocol, AI insulin pumps etc. schemes that implies to a patient-centric system [37].

3.2. Assimilation of Blockchain in Business Layer

The business layer of the IoMT architecture is integrated with blockchain technologies. Here, Authentic, secure, transparent, and unshakable transactions across a distribution platform are made possible by the decentralized data storage provided by blockchain [38]. Also, the sensitive data transmission challenges could be potentially solved using this technology. Here, using public-key cryptography, all other nodes in the network verify transactions; then store in a block that is connected to the previous blocks [23]. However, the nodes are referred to as miners in this verification process, and the process is called mining, where each node stores the transaction data to the block.

Nevertheless, this consent technique in blockchain is essential for it to perform precisely, which guarantees peer-to-peer node synchronization before confirming block-level transactions. Also, the privacy, authenticity, and other security issues of IoT based applications can be potentially resolved through this blockchain technology [39]. Moreover, such integration facility of different types of application reveals higher degree of opportunities to implement decentralized system. However, the distributed and independent behaviour of the blockchain suited best to incorporate with IoT networks, which leads to ensure the security requirements [40], which is displayed on Table 3:

Table 3. Security Requirements for Integrating Applications in Blockchain

Requirement	Description
Autonomy	Interaction of the IoT devices must be ensured with all other devices/nodes independently without central control
Decentralization	Avoiding single point of failure of centralized system to decentralized peer-to-peer architecture must be inveterate
Identity	Individual identification, authorization and authentication of each connected IoT device will be ensured
Reliability	Legitimacy and distributed nature must be guaranteed with substantial data reliability acquired from the IoT devices
Scalability	Ascendable enough to integrate decentralized applications must be accomplished considering fault tolerance
Security	Data communication, storing, validating should be processed using a secured channel and process

3.2.1. Accessing Patient's Longitudinal Healthcare Data

The total data storage and access of this IoMT architecture is designed using blockchain, which provides a secret key that is matched with the supplier's security key, through which patient can get access to their longitudinal healthcare records.

However, no private medical data will be retained as a result of adherence to Blockchain or smart contract compliance. Here, it merely records the events that took place and use blockchain technology as a record. It has been found that, maintaining the interoperability of the healthcare data blockchain is a potentially convenient technology [41], which can be accomplished through:

- Storing patient agreement
- Creating trusted and tenable health related data
- Coupling patient historic data with other transactional data providing anonymity

This proposed healthcare record is designed using Blockchain node technology that is integrated with the central record management system. Here the fundamental elements consist of a Backend Library, an Ethereum Client, a database interface called Database Gatekeeper, and the supporting interface for the Electronic Healthcare Record (EHR Manager). These components deployed on servers; thus, a consistent distributed system is combined that is displayed on Figure 4.

This process starts with sending the record to EHR Manager that generally store and update the record to off-chain database as well as using the backend library point to the database interface for further query. Now, while establishing any patient-provider relationship like smart contract, the record is sent from Provide node to the Blockchain, where the blocks will store all these relationships. After linking with the smart contract and Blockchain the mining process will start, three another node named Miner will execute this mining and bounty from the blocks and gradually updates the smart contract.

However, in the Patient node a notification will be sent about this smart contract, where an acknowledgement from the patient will be ensured, where patient can accept or reject the contract as well as validate. Subsequently, the update status is sent to the Blockchain as well as do some signed query with the provider node to store in the off-chain database therefore it can overcome the network dependency of the Blockchain and can give service simultaneously. Finally, in the patient node, this contract is updated to the off-chain database for quick access.

3.2.2. Interoperability: Storing Enormous Patient Data

It is already mentioned that only the sensitive data are stored in the blocks because of giving protection (especially data integrity) and confidentiality with existing health IT instances, assuring inevitably published identities, creating extreme monitoring streams, and improving healthcare security on behalf of suppliers and patients [41].

Despite of the technical competencies of blockchain architecture, there are numerous technical difficulties as well. However, considering the performance issue, the combination of off-chain and blockchain data storage requires a consortium of professional and healthcare consultants for high volume of transactions. Eventually, a practicable roadmap will be developed based on this blockchain structure for such healthcare system.

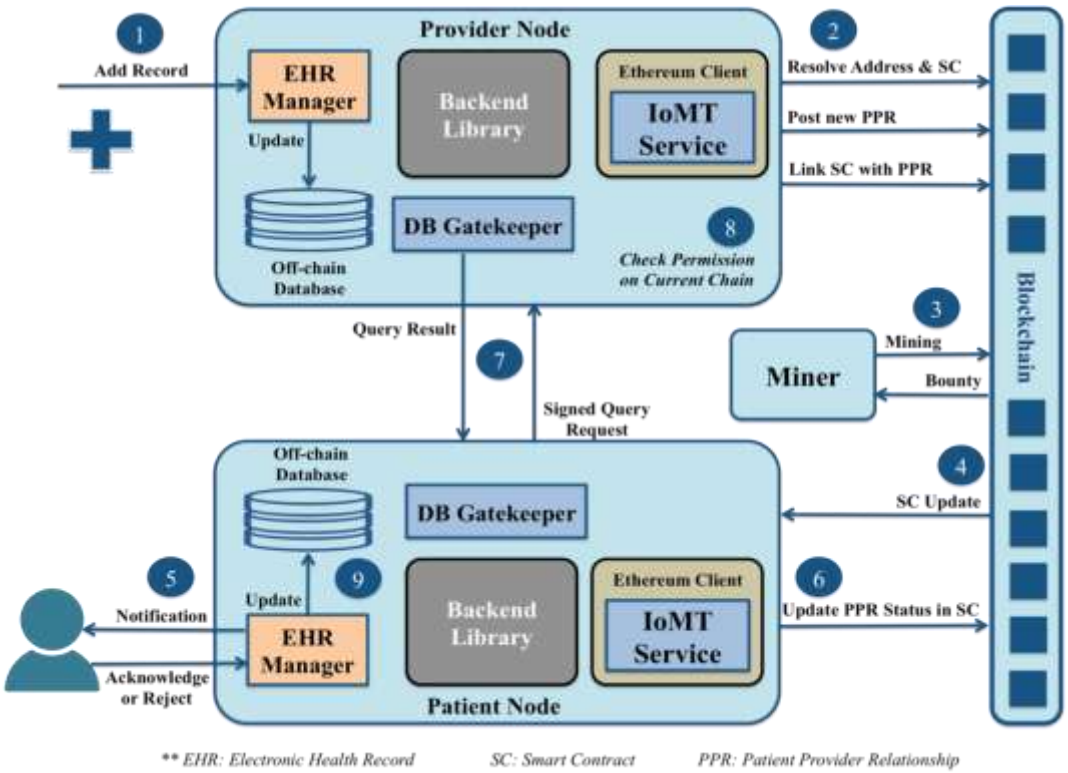

Figure 4. Patient Healthcare Record and Mining Process with Smart Contract

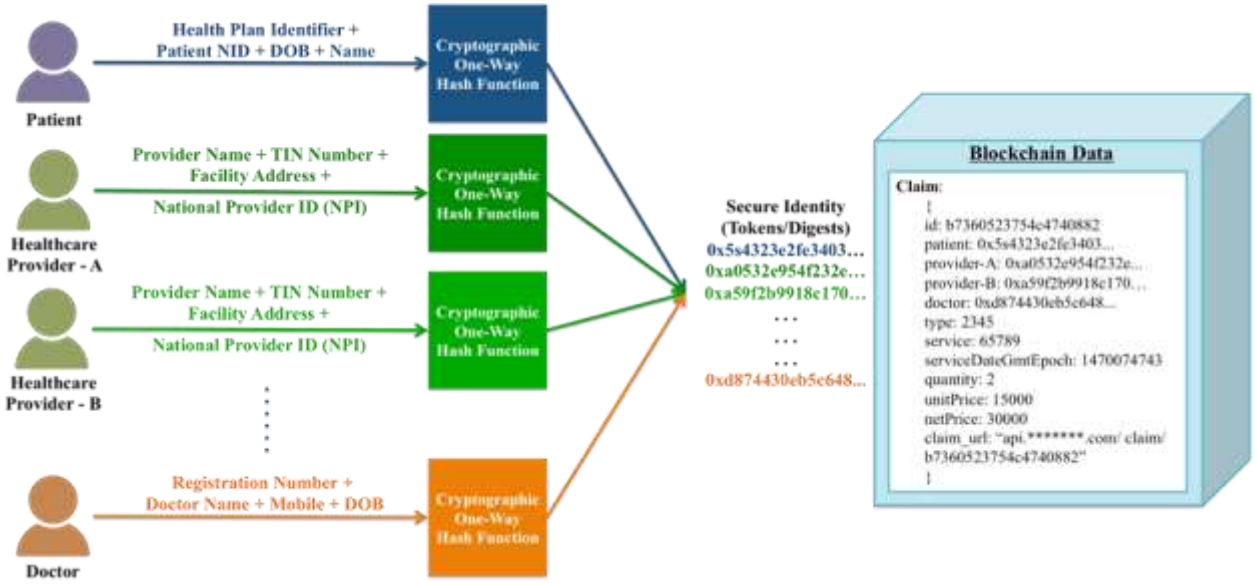

Figure 5. Tokenization Example of Blockchain Cryptographic Security Concept

In this architecture, only the encrypted claim is stored instead of storing confidential data. For example, A cryptographic one-way hash function is used while creating a smart contract or creating a connection that the patient provides. This is creating a hexadecimal number from the patient's name, date of birth, national identity number, and health plan identifier and storing it in the block. Similarly, the National Provider ID (NPI), name, TIN number, address, and healthcare provider (such as a hospital or diagnostic center) do the same and create a new hexadecimal number to be stored in the block.

Ultimately, a claim is present in the block data that solely stores these hexadecimal digits in addition to the necessary block parameters; Figure 5 illustrates this claim visually. However, through this data reliability is ensured as well as cost of Blockchain is minimized, that is also secured in terms of cryptographic security concepts.

3.2.3. Digital Ring Structure

Building a secure transaction as well as anonymity of the stakeholders' digital ring signature is applied, which is created by a member of a group in which each has its own keys, through which anonymity, unforgivably, and collusion resistance is guaranteed [42]. It is not possible to determine the signature of the person in the group. However, one of the groups is able to log in with this suggested framework. Though they are unable to grasp the login person's details, the system administrator can determine who created the signature on the system.

In this proposed architecture, A combination of the ring structure and authentication is employed, ensuring the signer's ambiguity and verifiability, the recipient's identification and ambiguity, verification dependency, and convertibility, as well as semantic security [43]. Here, the identity of the sender depends on his/her willing to expose through which the recipient can verify the sender; however, this contract mixing ring structure is displayed on Figure 6. Also, the authorized signature is accessible, but no opponent can control whether the shared message is the genuine message approved by the real person or node.

To illustrate this ring structure, there are several groups based on the types of external stakeholders of the architecture. In each type of group, the group member has their own public and secret/private key pairs denoted as (PK_{x1}, SK_{x1}), (PK_{x2}, SK_{x2}), …, (PK_{xn}, SK_{xn}), where x represents the group type. If any entity of the group desires to endorse a message (M_i), the own secret key (SK_{x1}), therefore the validity of the signature could be determined but the signer identity will not be exposed.

Conversely, during smart contract, this ring structure is used for signature verification [17]. Here, the sender generates a new key pair and then share the public key through Blockchain to the recipient, then both parties generate a shared random number. This happens for almost each type of groups who are conducting signature verification, where a list of public keys of the senders is mapped with their associate secret key (random numbers). After that the recipient sends a signature to the contract along with a tag, which is matched with the public keys that it has, and then conduct the transaction between them.

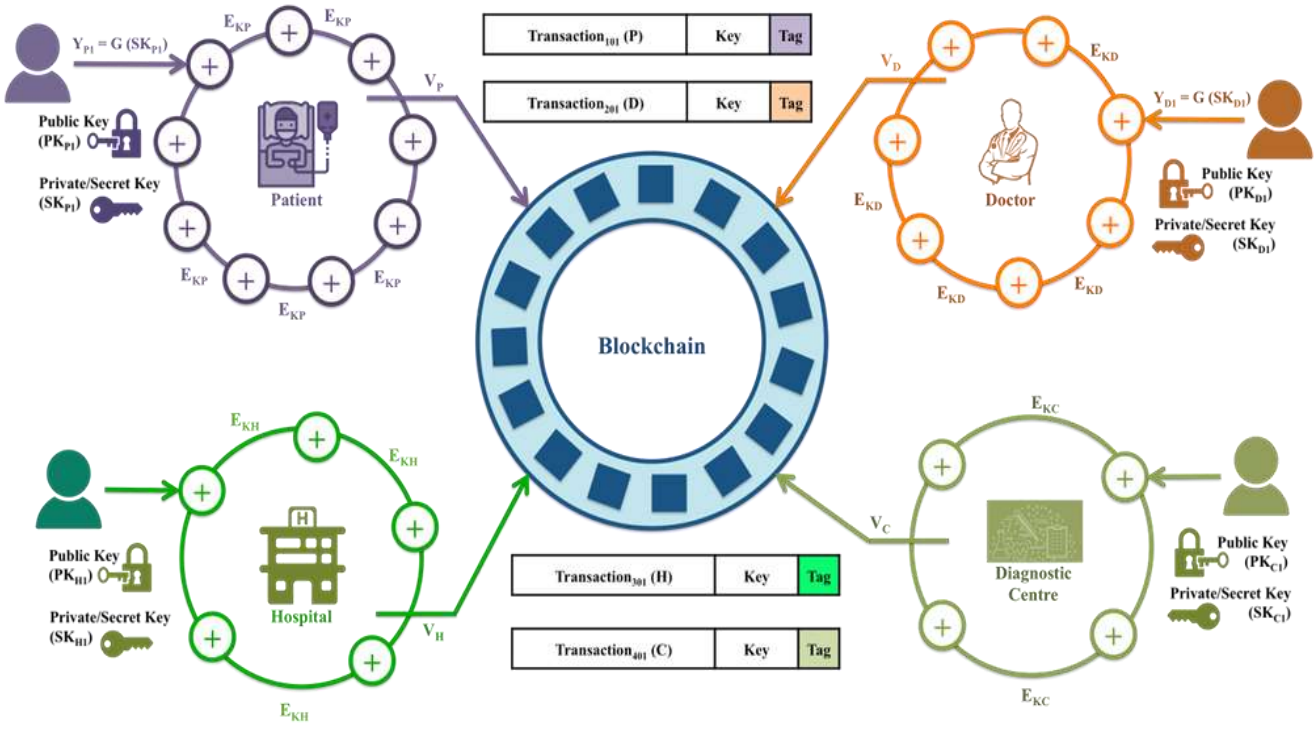

Figure 6. Digital Ring Structure with Mixing Contract

To accomplish this signature, firstly a large prime p is chosen by the sender, which is computationally hard for discrete logarithms GF(p). Then another two numbers q and t are chosen, which is the large prime divisor of (p – 1) and (q – 1) respectively. Here, the base point for GF(p) is noted as g whose order is q. Finally, these three number p, q and g are published; based on which the message (M) is signed using **Algorithm 1**, where S and R is denoted as signer and recipient respectively in the subscript of any notation.

Algorithm 1. Signature Generation

Input: Message: M, Shared Number: p, g_S
Public Keys: PK_S and PK_R
Secret/Private Key: SK_S

Output: Signature: σ

1: Begin
2: computes symmetric key $\lambda \leftarrow Hash(M, g, PK_R)$
3: initialize uniform random value $\delta_S \leftarrow \{0,1\}^R$
4: for each $\mathbf{\Lambda}_i^G \in \mathbf{\Lambda}^G$ do
5: $\delta_i \leftarrow rand\ (\alpha_i, \beta_i)$ where $i \neq S$
6: $PK_i \equiv g_i(\delta_i)\ mod\ p$
7: $\zeta \leftarrow \zeta \cup PK_i$
8: end for
9: Solve using PKs $C_{\lambda,\delta}(\zeta) = \delta_S$
10: Solve $(\alpha_S, B_S) = g_S^{-1}(PK_S)$
11: $\sigma \leftarrow \{M, \Lambda^G, \delta_S, \{(\alpha_1, B_1), (\alpha_2, B_2), \ldots, (\alpha_i, B_i)\}\}$
12: End

Now, if the recipient wants to verify the signature, then the shared numbers will be used through the recipient's secret/private key using the following equation:

$$\alpha_S . SK_R = PK_S\ mod\ p$$
$$SK_R = g^{\beta S} . PK_S\ mod\ p$$

If the secret key satisfies with the above-mentioned equations, then the authentication of the signer will be confirmed.

3.3. Consensus Model for Decision Making

In the proposed IoMT architecture a consensus model is anticipated using machine-learning algorithms using sensor data. Here, a dynamic sense reduction approach is proposed, based on the expert assessment method, and the urgency of the low consent of the group emergency decision-making [44]. The key indicator of this model is based on the opinion of the expert doctors of relative fields. Actually, these doctors will basically work on with the sensor data coming from the patients and classify the risk level and/or critical conditional analysis of the patient that is processed with Artificial Intelligence system to provide run-time decisions [30]. However, in the proposed model, there are three parts: Consistency/Consensus Control Unit, Dynamic Consensus Process unit and Consensus Evaluation Unit that is briefly displayed with their functionalities in Figure 7.

First of all, the consensus control unit where the previous patient sensor data is stored as feature vector, which is processed to numeric values therefore the machine learning algorithms can easily process those. However, before processing a panel of expert doctors will give consent about the individual patient clinical/health condition with their prior knowledge. These data along with the knowledge is then simulated through the machine-learning algorithms, where a part of the data is used for train the system and rest part is used for testing and error calculation. After this the threshold value is set, which is eventually stored in an XML file with the rest of the parameters.

Next, the major portion of the consensus model exists, which works on live patient data. This unit starts with collecting the patients' wearable sensor data that is processed with some cleaning and classifying to fit for the machine-learning algorithm. Later, this data is transmitted to both Human Decision Evaluation Process as well as Machine Learning Algorithms. In the human generated process, an expert panel of the doctors will analysis those patient live data considering each patient prior condition and then take some clinical decision and/or prescription for that individual patient.

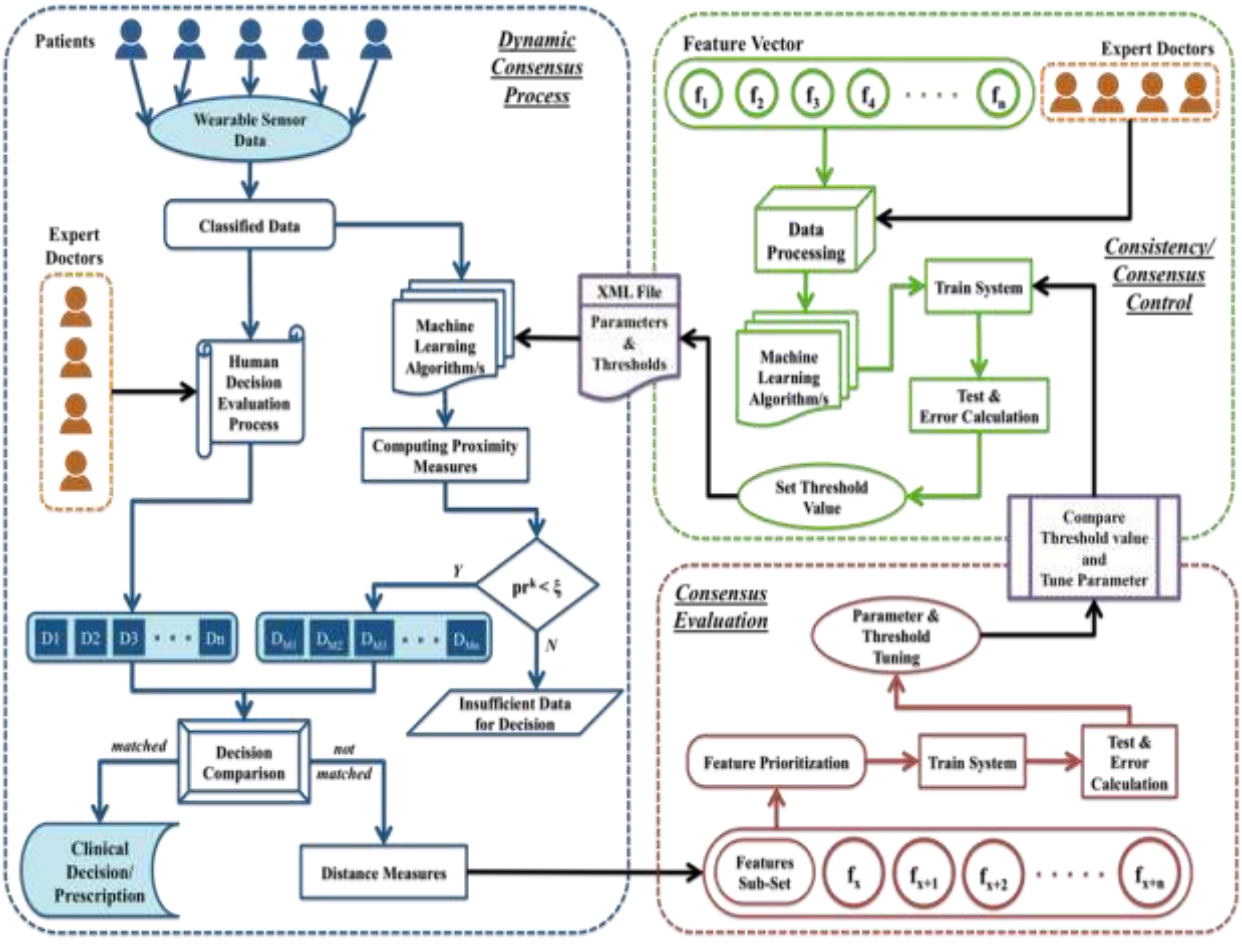

Figure 7. Dynamic Consensus Structure for Decision Support System

Similarly, in machine learning part, the previously developed XML file will give input to tune the parameters of the live data. After processing the data, the proximity measurement is computed that is send

to the next step to compare with the threshold value. If the proximity value is enough to take decision, then the system will automatically prescribe clinical suggestion for each individual patient. On the other hand, if the proximity value can't satisfy the threshold, then no decision will be generated, which means lack of data is there for making decisions.

Now, both the human generated and machine generated decisions are compared based on similarity index, where the similar data is sent to the final step that is the Patient specific Decision. However, the dissimilar data will be sent to another step for calculating distance measurement of the decisions, which is subsequently sent to the Consensus Evaluation unit. The consensus evaluation unit actually works to adjust the human generated decisions to the artificial intelligent system.

Here, the dissimilar data is categorized based on the features that are the reason of mismatched. This sub-set and the other features are prioritized based on their importance and impact on making meaningful decision and then again train and test to adjust the parameters. Afterwards, the previous stored parameters and thresholds from control unit are compared with the evaluation and then again send to the control unit for train the system once again. Eventually, with the earlier process of the control unit, the parameter tuning and threshold setting is done with live data.

The algorithm presented in **Algorithm 2**, integrates with sensor data from patients, expert knowledge, machine learning, and blockchain technology. The process begins with the extraction and normalization of patient sensor data, which is combined with expert doctor feedback. The data is tokenized and hashed for secure storage and processing. A smart contract is used to verify the validity of tokenized patient data, ensuring security. The neural network model then processes the data to generate proximity measures, which are compared against a predefined threshold. Based on this proximity, decisions are made, either autonomously by the system or with human input.

The final consensus decision is securely stored on the blockchain, ensuring immutability and security, with off-chain storage used for managing tokenized data. This ensures that patient data is processed, authenticated, and stored in a decentralized and secure manner.

Algorithm 2. Blockchain-Enabled Consensus for Patient Data

Input: $X_p = \{x_1, x_2 \dots x_n\}$: Live patient sensor data (heart rate, temperature, etc.)
$K_p = \{k_1, k_2 \dots k_m\}$: Knowledge from expert doctors for patient p
$\mathcal{M}$: Smart contract for mining and authentication
$\mathcal{T}_i$ = Tokenized patient data for node i
T = Threshold value from trained XML model
$\mathcal{N}_\mathcal{D}$ = Neural Network Model (trained) and $\boldsymbol{\theta}$ is the model parameters
$\mathcal{B}_c$: Blockchain network with N nodes

Output: $\mathcal{D}_p$: Final consensus decision for patient p
$\mathcal{B}_c^{new}$: Secure blockchain record

Begin
$X'_p = f(X_p)$, where f is a feature extraction function
$E_p = \sum_{i=1}^{m} w_i k_i$, where w_i is the weight of expert knowledge
$X'_p \leftarrow \frac{X_p - \min(X_p)}{\max(X_p) - \min(X_p)}$
$\mathcal{T}_i \leftarrow \mathcal{H}(X'_p) \oplus \text{Token}(X_p)$, where $\mathcal{H}$ is the hash function, and represents token encryption
$\mathcal{M}(\mathcal{T}_i) \rightarrow \begin{cases} MinerVerification, & \mathcal{T}_i \text{ is valid} \\ reVerification, & otherwise \end{cases}$
for each $\Gamma_1^P \in \Gamma^P$
    $M_p = \mathcal{N}_\mathcal{D}(X'_p)$
    $P_p \leftarrow \text{Proximity}(M_p, T) = |M_p - T|$
    $\widehat{\mathcal{D}}_p = \begin{cases} \text{GenerateDecision}(M_p), & P_p \le \varphi, \text{where } \varphi \text{ is the proximity threshold} \\ K_p, & otherwise \end{cases}$
end for
$\mathcal{D}_p \leftarrow Consensus(\widehat{\mathcal{D}}_1, \widehat{\mathcal{D}}_2, \dots, \widehat{\mathcal{D}}_N$
Update Blockchain $\mathcal{B}_c^{new} \leftarrow \mathcal{B}_c^{old} \oplus \mathcal{D}_p$
$\text{Offchain}_i = \text{Store}(\mathcal{T}_i)$
End

4. Result and Discussion

The proposed blockchain model has been experimented with the open source Ethereum platform where the sensor data are integrated using Application Programming Interface (API). Again, a pivotal element in this IoMT architecture is the smart contract, crafted through Solidity in conjunction with web3.py and web3.js. This component essentially facilitates the interactions between the blockchain application and the smart contract. The binary management and Smart contract deployment support the Truffle framework environment. However, automatically testing the smart contract and patient health record management system this environment helps through rapid prototyping.

Similarly, the interactive APIs are designed using Python where the end-to-end communication among heterogeneous nodes (miner and IoT devices) is implemented. However, the patient sensor data, smart contract and dynamic consensus process along with data mining are displayed on Figure 8.

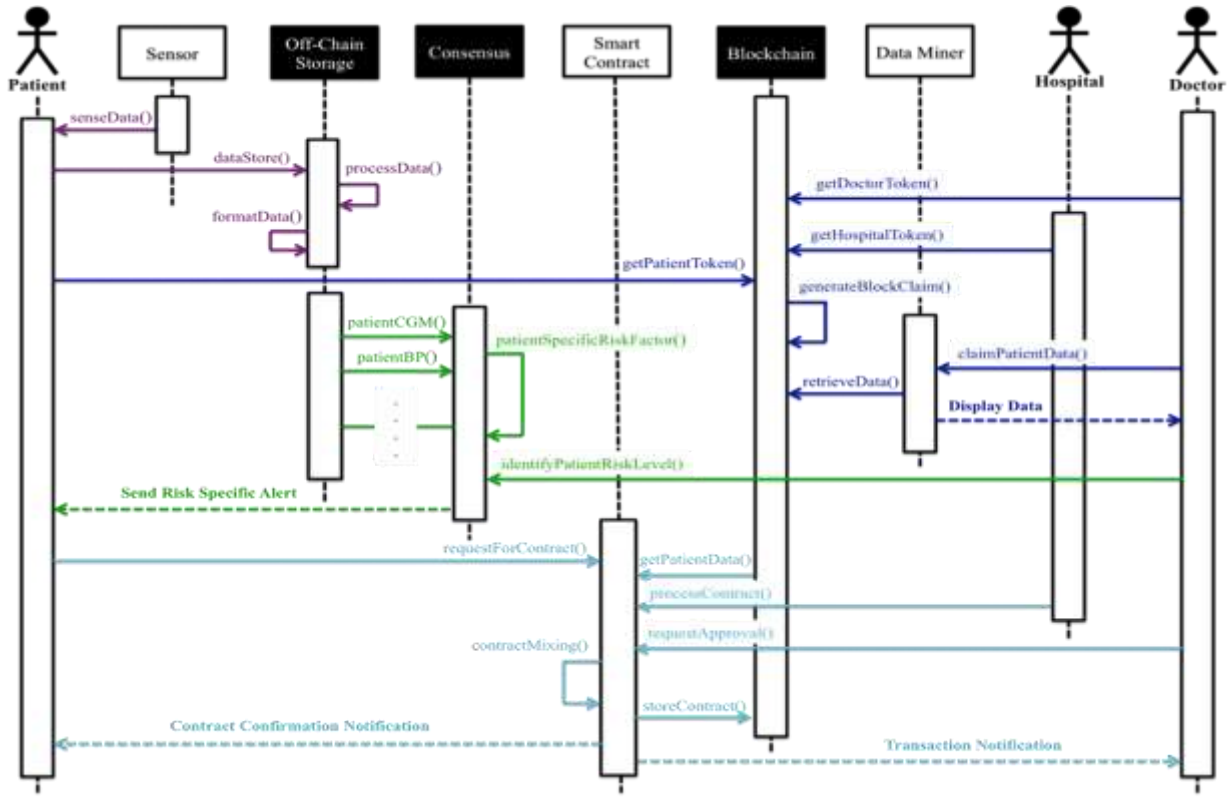

Figure 8. The Logical Execution Flow of the IoMT Architecture

4.1. Simulation Setup and Synthetic Data Generation

4.1.1. Simulation Environment

For simulating the IoMT architecture, a controlled environment was set up using Python 3.8.4, which allowed the generation and processing of synthetic data mimicking real-world sensor readings. The simulation employed the blockchain framework Ethereum 2.3.2, adapted for healthcare data transactions. Machine learning models (e.g., neural networks) were used for decision-making and diagnosis, integrated seamlessly into the blockchain-based IoMT system.

4.1.2. Synthetic Data Generation

Data Type and Structure: The synthetic data was generated to simulate real-time sensor data, which included heart rate, blood pressure, temperature, and other patient vitals [45]. Each data point was timestamped to represent continuous monitoring over a period, mimicking the output of real IoT devices like wearable sensors.

Data Acquisition Simulation: The data acquisition protocol mimicked real-world conditions by simulating different sampling rates (e.g., 1 sample per minute for heart rate, 10 samples per minute for accelerometers). The synthetic data was designed to reflect variability similar to human biological data, including normal ranges, anomalies, and noise to reflect realistic scenarios.

4.1.3. Blockchain Integration

Data Processing for Blockchain: The synthetic data was processed in batches, where each block in the blockchain represented a batch of sensor readings over a given period (e.g., 10-minute intervals). Each data batch was verified, encrypted, and stored using blockchain technology to ensure security and immutability, simulating real-world secure data transmission.

Consensus Algorithm: The custom consensus algorithm processed the sensor data in real-time, allowing efficient handling of transactions and ensuring that data was verified and securely added to the blockchain without delay.

Since real sensors were not employed, synthetic data was designed to closely emulate the nature of IoMT data, the configuration of that is displayed on Table 4. This approach ensures that the consensus algorithm and blockchain performance can be evaluated under realistic conditions without deploying real hardware. However, while synthetic data provides flexibility in testing various scenarios, the behavior of real sensors in dynamic environments (e.g., patient movement, varying network conditions) may introduce additional challenges in real-world applications. Future work could focus on validating the system with real sensor hardware to verify scalability and robustness.

Table 4. Configuration Table for Data Simulation

Parameter	Configuration
Blockchain Framework	Ethereum / Hyperledger Fabric
Consensus Algorithm	Custom Algorithm
Synthetic Data Types	Heart Rate, Temperature, BP
Data Generation Rate	1 sample/minute
Number of Sensors Simulated	10
Simulation Time	24 hours
Network Latency (simulated)	50ms
Blockchain Node Count	10 nodes
Transaction Size	256 KB

4.2. Results and Statistical Comparison

With the simulated environment our proposed blockchain-aided smart consensus model is compared with existing consensus algorithms (PoW, PoS, PoA) based on various key parameters such as access control, authentication, interoperability, mining, off-chain storage, scalability, smart contracts, etc. The statistical metrics for our model show improvements in several areas, which is displayed on Table 5.

4.2.1. Results Analysis

The proposed blockchain-aided smart consensus model demonstrates significant improvements across several key parameters when compared to existing consensus mechanisms like PoW, PoS, and PoA [46]. One of the most notable improvements is in **authentication** and **access control**, where the proposed model achieves 98% effectiveness in multi-factor authentication driven by AI. This surpasses PoW's traditional cryptographic keys, which offer 90% effectiveness, and even PoA's centralized identity validators, which offer 95% effectiveness. The decentralized, role-based access control further enhances security, with a 95% success rate in managing user permissions.

In terms of **scalability**, the proposed model handles 150 transactions per second (TPS), a considerable improvement over PoW's 10 TPS and PoS's 100 TPS. This makes the system more suitable for real-time healthcare applications where large volumes of data from multiple IoT sensors need to be processed and verified quickly. Moreover, the incorporation of **off-chain storage** via IPFS boosts data management, achieving 90% effectiveness in storing and retrieving large medical datasets, compared to PoW's limited capacity at only 30% effectiveness.

Finally, the proposed model's **energy efficiency** is another clear advantage. With an energy consumption of just 50kWh per year, it drastically reduces the carbon footprint, especially when compared to PoW's notoriously high energy demands (1200kWh per year). This low energy requirement, coupled with the AI-assisted lightweight mining, ensures a more sustainable model while maintaining high performance and security.

Table 5. Comparison of the Proposed Blockchain-Enabled Consensus Model with PoW, PoS, and PoA

Parameter	PoW	PoS	PoA	Proposed Model
Access Control	Permissionless (75%)	Permissioned (85%)	Centralized (90%)	Decentralized Role-Based (95% effectiveness)
Authentication	Cryptographic Keys (90%)	Staking Validators (92%)	Identity Validators (95%)	Multi-factor, AI-driven (98%)
Interoperability	Low (50%)	Moderate (70%)	Moderate (75%)	High (90%)
Mining	High Energy (1000kWh)	Low Energy (100kWh)	Low Energy (70kWh)	Lightweight, AI-assisted (Low Energy: 50kWh)
Off-chain Storage	Limited (30%)	Moderate (70%)	Moderate (65%)	Enabled with IPFS (90% effectiveness)
Scalability (TPS)	10 TPS	100 TPS	120 TPS	150 TPS (Tested)
Smart Contracts	Basic (70%)	Basic (75%)	Moderate (80%)	Advanced, automated with AI (95%)
Transaction Latency	10 minutes	1 minute	10 seconds	200 ms
Energy Consumption	High (1200kWh/year)	Medium (150kWh/year)	Low (80kWh/year)	Low (50kWh/year)

The integration of advanced smart contracts that are AI-automated (95% effectiveness) further improves decision-making processes in healthcare, ensuring that the system is both efficient and reliable in providing secure, real-time patient monitoring.

4.3. Evaluation of Security Threats

Evaluating security requirements, a model need to address: Confidentiality, Integrity and Availability. Here, also these three issues have been considered to ensure basic security where the Confidentiality is addressed through giving access to the authorized user as well as with Digital Ring Signature. Similarly, Integrity is ensured through the Tokenization concept of blockchain and Availability is established by storing the data in blockchain cloud storage through which users can easily access the data.

Again, we have analysed the proposed model security margin among different threats, where the adversary might attack in the system or part of the cloud storage or any node. These adversaries have the capability to manipulate events, eavesdrop on conversations, initiate erroneous actions, or manipulate data stored in the system. Our model aims to protect the chain from the adversary. That's why we have focused on the entity's nodes. Likewise, an honest node is certified when that registered node passes the proof of authority by the network. In that case if the network identifies any mischievous activities, then identified node is blocked from the network. However, according to the security constraints of Blockchain application in section 3.2, we have evaluated our proposed IoMT Architecture, which is displayed on Table 6.

Next, we have assessed the security vulnerabilities of this healthcare system using the STRIDE (Spoofing, Tampering, Repudiation, Denial of service, and Elevation of privilege) classification method [47]. Utilizing this framework, we have examined diverse security threats and incorporated marginal security measures accordingly.

4.3.1. Avoidance of DoS Attack

A Denial of Service (DoS) attack occurs when unauthorized users gain access to the network and overwhelm the nodes with excessive activities, often referred to as Eclipse attack and Sybil attack [48]. To illustrate, the adversary keeps the other nodes busy and increase traffic in the network. However, to prevent such incidents, our suggested model prevents the inclusion of random users into the network, which is addressed by binding the NID and mobile number with verification of each type of users. Regardless, False transactions in the network are mitigated through the implementation of Digital Ring Signature.

4.3.2. Altering Node in Dropping Attack

The antagonist would manipulate the cluster heads during an attack. When under the attacker's influence, the cluster heads become incapacitated within the network. They lose the ability to connect to other nodes or clusters and may discard the received blocks. Ultimately, the node designates an alternative node as a cluster head within that chain.

4.3.3. Minimize Storage Attack

Our IoMT architecture permits cloud storage in addition to off-chain storage, opening the door to storage attacks in which a malicious party could remove, alter, or add data to the cloud. In contrast, in our projected architecture, we have used hashing and tokenization of the data block to amass data in cloud storage; therefore, alterations of the data can be identified undoubtedly. Again, public key cryptosystem is mandatory in our model to store or manage data by the users; therefore, any modification made by other nodes will be blocked by the network.

Table 6. Security Requirement Evaluation

Requirement	Traditional System	Proposed Model Solution	Section Reference
Autonomy	Encoded peer-to-peer data communication to a stand-alone database	Off-chain and Blockchain Storage	3.1.1
Decentralization	Cloud Storage or Centralized Database System	Data Blocks to store Record and Smart Contract	3.2.1
Identity	Patients' identity is not secured and/or verified along with lack of association with remote transaction records	Public and Private Key	3.2.2 and 3.2.3
Reliability	Alternation to the health records is not addressed and revealing mechanism is not assured	IoMT Architecture and Tokenization during Smart Contract	3.1 and 3.2.2
Scalability	Existing system integration is challenging due to fault tolerance and easy plug-in issues	Data Blocks Add/Remove	3.1.2 and 3.1.3
Security	Encryption techniques during data transmission may fleece data, but still distinguishable to adversary	Public Key Cryptography and Digital Signature	3.2

4.3.4. Traceability over Mining Attack

Attackers can sometimes take control of other nodes by hacking a few cluster heads in consensus mechanisms and data mining. This is known as a Selfish-Mining attack, Timejack assault, Finney attack, Race attack, etc. [48]. To put it briefly, in a blockchain application, this kind of fraudulent mining is easily conceivable, but it could also be easily identified and tracked. Therefore, in the proposed model, Digital Ring Signature is implemented without that any contract mixing will not happen. Also, A false node alters the ring structure and is immediately eliminated from the network.

4.4. Discussion

The state-of-art blockchain based healthcare systems generally focus on less application and/or integration part; meanwhile the proposed IoMT architecture has come up with easy integration of the IoT devices/sensors and other stakeholder/users through Ethereum based permissioned blockchain technology. Again, the artificial intelligent centric Consensus model has been proposed that make the system more dynamic and useful. However, the security requirements were maintained significantly in such way, therefore any alternation or device malfunction could be easily identified through the network. Also, new concept of Interoperability, and mining is addressed with off-chain and blockchain blended storage. A comparative analysis of the system feature with state-of-art healthcare systems is exhibited on Table 7.

Moreover, the proposed IoMT architecture is designed in such scalable way; therefore, any kind of sensor or IoT device can be integrated easily through API (using slat), where the cost is optimized through the off-chain and blockchain data storage system. Here, only connected data are stored in blockchain, and sensitive and/or less frequent data are accumulated in the off-chain storage, which minimize the operation of data size and escalations the number of operations that can be adapted inside the block. Thus, the complete system become significantly scalable as well as abated the throughput.

On the other hand, smart contract-deployed system with role-based access, where tokenization maintains block integrity. Eventually, the tamperproof nature is guaranteed through the digital ring signature where it is more challenging for an adversary to alter the transaction records on the nodes. Since the enumerated users ensure data confidentiality through access to the off-chain and blockchain storage.

Finally, the novelty of the proposed IoMT architecture lays on designing the decentralized distributed and trustworthy ecosystem where traditional IoT based healthcare system focus on transfer, storage and/or privacy issues. Nevertheless, the proposed model eases the computational process by blending the off-chain storage with cloud when this authentic node is coupled to the Ethereum central network.

Table 7. Comparative Analysis of the Proposed Model with state-of-art Blockchain based Healthcare Systems

Applications	Blockchain Platform	Access Control	Authentication	Authorization	Consensus Model	Interoperability	Mining	Off-Chain Storage	Scalability	Smart Contract
Patient EHR [5]	Hyperledger Fabric	☑	☑	☑	X	☑	X	X	☑	☑
MeDShare [18]	Multiplatform	☑	☑	X	X	X	☑	X	X	☑
OmniPHR [19]	Multiplatform	X	X	☑	X	X	X	☑	☑	X
WBAN_PHM [20]	Multiplatform	☑	☑	☑	X	X	X	X	X	X
PSN [21]	Ethereum	☑	☑	☑	X	☑	X	X	X	X
Sensing Data Integrity [26]	Hyperledger Fabric	☑	☑	X	X	☑	X	X	X	☑
Diagnosis Image Transmission [27]	Multiplatform	X	X	X	X	☑	☑	X	X	☑
Proof of Authentication [46]	Ethereum	☑	☑	☑	☑	☑	X	X	☑	X
Gem Network [49]	Hyperledger	☑	☑	X	X	X	X	X	X	X
MedRec [50]	Ethereum	☑	☑	☑	X	X	☑	X	X	☑
PCA [51]	Ethereum	☑	☑	X	☑	X	X	X	X	X
Proof of Concept [52]	Ethereum	☑	☑	☑	X	X	X	☑	☑	☑
Proposed Method	Ethereum	☑	☑	☑	☑	☑	☑	☑	☑	☑

5. Conclusion and Future Work

Now-a-days healthcare systems are keeping pace with technological advancement, where wearable devices or sensors are getting popular, which motivates researchers to design IoT based healthcare system. On the other hand, addressing security, privacy, scalability, integrity etc. issues are also vital, which could be minimized using blockchain technology. Most importantly, amalgamation of this IoT concept with blockchain technologies Artificial Intelligence is very much essential for dynamic decision-making.

However, considering these mixing challenges, Internet of Medical Things (IoMT) architecture has been proposed along with a dynamic consensus model. Here, the IoT concept is used for collecting and processing sensor data from patient, Blockchain technology is utilized as an intermediary platform to do data management tasks utilizing off-chain and cloud-based storage. Also, the intelligent decision system based on the sensor data has been anticipated as a dynamic consensus model.

Besides, combining these widespread technologies all together in one model the security criteria fulfilment was most challenging. However, the proposed model has come-up with the accomplishment of such security issues with comparatively better solution from state-of-art healthcare system. Here, patient record, mining; node interoperability, tokenization; digital ring structure has been used to strengthen the IoMT architecture. Also, the consensus model is designed with self-learning intelligent process, which enables patient-centric easy prescription system. Eventually, the suggested model's feature enrichment and scalability have been demonstrated through an experimentation-based comparative study with cutting-edge healthcare systems.

Furthermore, it is clear that such IoMT architecture not only creates new research wings for integrating challenges but also very much needful for remote patient monitoring and/or prescription especially in pandemic situation like covid-19. Again, this model could be commercialized due to easy incorporation with the healthcare related stakeholder using their existing system with minimal adoption. Therefore, this research undoubtedly creates new opportunities for both academic and commercials.

Despite of the academic and commercial importance the consensus model could be scale up with better machine-learning techniques as well as it's computational complexity. Also, the sensor performance for data extraction is not considered in this research, which could be later improvised as hardware challenge.

CRediT Author Contribution Statement

Md. Iftekharul Alam Efat: Conceptualization, Methodology, Formal Analysis, Writing – Original Draft, Supervision, Writing – Review & Editing; Tasnim Rahman: Data Curation, Validation, Writing – Review & Editing; Md. Jane Alam: Software Development, Visualization, Structuring the Manuscript; Shah Mostafa Khaled: Ensuring Logical Flow and Coherence, Language Precision, Compliance with Journal Guidelines, Addressing Reviewers' Comments.

Acknowledgement

This research is funded by the Research Cell of Noakhali Science and Technology University, grant no. NSTU-RC-IIT-T-23-162.

References

[1] Ali Hassan Sodhro, Sandeep Pirbhulal and Arun Kumar Sangaiah, "Convergence of IoT and product lifecycle management in medical health care", *Future Generation Computer Systems*, ISSN: 0167-739X, Vol. 86, September 2018, pp. 380-391, Published by Elsevier, DOI: 10.1016/j.future.2018.03.052, Available: https://www.sciencedirect.com/science/article/pii/S0167739X17328509.

[2] Li Haoyu, Li Jianxing, N. Arunkumar, Ahmed F. Hussein and Mustafa M. Jaber, "An IoMT cloud-based real time sleep apnea detection scheme by using the SpO_2 estimation supported by heart rate variability", *Future Generation Computer Systems*, ISSN: 0167-739X, Vol. 98, September 2019, pp. 69-77, DOI: 10.1016/j.future.2018.12.001, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18326980.

[3] Anand Nayyar, Vikram Puri and Nhu Gia Nguyen, "Biosenhealth 1.0: A novel Internet of Medical Things (IoMT)-based patient health monitoring system", in *Lecture Notes in Networks and Systems (LNNS)*, vol. 55, Online ISBN: 978-981-13-2324-9, Print ISBN: 978-981-13-2323-2, DOI: 10.1007/978-981-13-2324-9_16. pp. 155–164. 2019, Published by Springer, Singapore, Available: https://link.springer.com/chapter/10.1007/978-981-13-2324-9_16.

[4] Shiraz Ali Wagan, Jahwan Koo, Isma Farah Siddiqui, Muhammad Attique, Dong Ryeol Shin *et al.*, "Internet of medical things and trending converged technologies: A comprehensive review on real-time applications", *Journal of King Saud University - Computer and Information Sciences*, ISSN: 1319-1578, Vol. 34, No. 10, November 2022, pp. 9228-9251, Published by Elsevier, DOI: 10.1016/j.jksuci.2022.09.005, Available: https://www.sciencedirect.com/science/article/pii/S1319157822003263.

[5] Jameel Almalki, Waleed Al Shehri, Rashid Mehmood, Khalid Alsaif, Saeed M. Alshahrani *et al.*, "Enabling blockchain with IoMT devices for healthcare", *Information*, Vol. 13, No. 10, September 2022, pp. 448-471, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/info13100448, Available: https://www.mdpi.com/2078-2489/13/10/448.

[6] Mohsen Hallaj Asghar, Atul Negi and Nasibeh Mohammadzadeh, "Principle application and vision in Internet of Things (IoT)", *in Proceedings of the 2015 IEEE International Conference on Computing, Communication & Automation*, 15-16 May 2015, Greater Noida, India, ISBN: 978-1-4799-8890-7, pp. 427–431, Published by IEEE, DOI: 10.1109/CCAA.2015.7148413, Available: https://ieeexplore.ieee.org/abstract/document/7148413.

[7] Jalel Ktari, Tarek Frikha, Nader Ben Amor, Leila Louraidh, Hela Elmannai *et al.*, "IoMT-based platform for E-health monitoring based on the blockchain, *Electronics*, Vol. 11, No. 15, 2022, p. 2314, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/electronics11152314, Available: https://www.mdpi.com/2079-9292/11/15/2314.

[8] Darshan K R and Anandakumar K R, "A comprehensive review on usage of Internet of Things (IoT) in healthcare system", in *Proceedings of the 2015 IEEE International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, 17-19 December 2015, Mandya, India, ISBN: 978-1-4673-9563-2, pp. 132–136, Published by IEEE, DOI: 10.1109/ERECT.2015.7499001, Available: https://ieeexplore.ieee.org/abstract/document/7499001/.

[9] Suvini P. Amaraweera and Malka N. Halgamuge, "Internet of things in the healthcare sector: Overview of security and privacy issues", Security, Privacy and Trust in the IoT Environment, Print ISBN: 978-3-030-18074-4, Online ISBN: 978-3-030-18075-1, 31 May 2019, pp. 153–179, Published by Springer, Cham, DOI: 10.1007/978-3-030-18075-1_8, Available: https://link.springer.com/chapter/10.1007/978-3-030-18075-1_8.

[10] Madhura Jayaratne, Dinithi Nallaperuma, Daswin De Silva, Damminda Alahakoon, Brian Devitt *et al.*, "A data integration platform for patient-centered e-healthcare and clinical decision support", *Future Generation Computer Systems*, ISSN: 0167-739X, Vol: 92, 2019, pp. 996-1008, Published by Elsevier, DOI: 10.1016/j.future.2018.07.061, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17308142.

[11] Ammar Awad Mutlag, Mohd Khanapi Abd Ghani, N. Arunkumar, Mazin Abed Mohammed and Othman Mohd, "Enabling technologies for fog computing in healthcare IoT systems", *Future Generation Computer Systems*, ISSN:

0167-739X, Vol: 90, 2019, pp. 62-78, Published by Elsevier, DOI: 10.1016/j.future.2018.07.049, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18314006.

[12] Eduard Marin, Mustafa A. Mustafa, Dave Singelée and Bart Preneel, "A privacy-preserving remote healthcare system offering end-to-end security", in *Lecture Notes in Computer Science (LNCS)*, Print ISBN: 978-3-319-40508-7, Online ISBN: 978-3-319-40509-4, Vol. 9724, 18 June 2016, pp.237–250, Published by Springer, DOI:10.1007/978-3-319-40509-4_17, Available: https://link.springer.com/chapter/10.1007/978-3-319-40509-4_17.

[13] Mohammed Mohammed Sadeeq, Nasiba M. Abdulkareem, Subhi R. M. Zeebaree, Dindar Mikaeel Ahmed, Ahmed Saifullah Sami *et al.*, "IoT and Cloud computing issues, challenges and opportunities: A review", *Qubahan Academic Journal*, ISSN: 2709-8206, Vol. 1, No. 2, 2021, pp. 1-7, DOI: 10.48161/qaj.v1n2a36, Available: https://journal.qubahan.com/index.php/qaj/article/view/36.

[14] Mohammad Khalid Imam Rahmani, Mohammed Shuaib, Shadab Alam, Shams Tabrez Siddiqui, Sadaf Ahmad *et al.*, "Blockchain-based trust management framework for cloud computing-based Internet of Medical Things (IoMT): a systematic review", *Computational Intelligence and Neuroscience*, Vol. 2022, No. 1, 19 May 2022, p. 9766844, Published by Wiley, DOI: 10.1155/2022/9766844, Available: https://onlinelibrary.wiley.com/doi/full/10.1155/2022/9766844.

[15] Aya Hamid Ameen, Mazin Abed Mohammed and Ahmed Noori Rashid, "Enhancing Security in IoMT: A Blockchain-Based Cybersecurity Framework for Machine Learning-Driven ECG Signal Classification", *Fusion: Practice & Applications*, ISSN: 2770-0070, Vol. 14, No. 1, 5 December 2023, pp. 221-251, Published by American Scientific Publishing Group (ASPG), DOI: 10.54216/FPA.140117, Available: https://www.americaspg.com/articleinfo/3/show/2343.

[16] Greg Irving and John Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science", *F1000Research*, Vol. 5, 2017, Published by Faculty of 1000 Ltd., DOI: 10.12688/f1000research.11888.1, Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4866630.

[17] Lukas Malina, Jan Hajny, Petr Dzurenda and Sara Ricci, "Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions", in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018)*, July 26 - 28, 2018, Holiday Inn Porto Gaia, Portugal, ISBN: 978-989-758-319-3, pp. 692-697, DOI: 10.5220/0006890505260531, Available: https://www.scitepress.org/papers/2018/68905/68905.pdf.

[18] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang D *et al.*, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", *IEEE Access*, ISSN: 2169-3536, Vol. 5, 24 July 2017, pp. 14757-14767, Published by IEEE, DOI: 10.1109/ACCESS.2017.2730843, Available: https://ieeexplore.ieee.org/abstract/document/7990130/.

[19] Alex Roehrs, Cristiano André da Costa and Rodrigo da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records", *Journal of Biomedical Informatics*, ISSN: 1532-0464, Vol. 71, 2017, Published by Elsevier, pp. 70-81, DOI: 10.1016/j.jbi.2017.05.012, Available: https://www.sciencedirect.com/science/article/pii/S1532046417301089.

[20] Yongjun Ren, Yan Leng, Fujian Zhu, Jin Wang and Hye-Jin Kim, "Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network", *Sensors*, ISSN: 1424-8220, Vol. 19, No. 10, 2019, p. 2395, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: https://doi.org/10.3390/s19102395, Available: https://www.mdpi.com/1424-8220/19/10/2395.

[21] Jie Zhang, Nian Xue and Xin Huang, "A Secure System for Pervasive Social Network-Based Healthcare", IEEE Access, ISSN: 2169-3536, Vol. 4, 29 December 2016, pp. 9239–9250, DOI: 10.1109/ACCESS.2016.2645904, Available: https://ieeexplore.ieee.org/abstract/document/7801940.

[22] Dimiter V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare", *Healthcare Informatics Research*, Vol. 22, No. 3, 31 July 2016, pp. 156-163, Published by Korean Society of Medical Informatics, DOI: 10.4258/hir.2016.22.3.156, Available: https://synapse.koreamed.org/articles/1075790.

[23] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", in *IEEE international congress on big data (BigData congress)*, 25-30 June 2017, Honolulu, HI, USA, Electronic ISBN: 978-1-5386-1996-4, pp. 557-564, Published by IEEE, DOI: 10.1109/BigDataCongress.2017.85, Available: https://ieeexplore.ieee.org/document/8029379.

[24] Gautam Srivastava, Ashutosh Dhar Dwivedi and Rajani Singh, "PHANTOM Protocol as the New Crypto-Democracy", in *Lecture Notes in Computer Science (LNCS)*, Print ISBN: 978-3-319-99953-1, Online ISBN: 978-3-319-99954-8, Vol. 11127, 05 September 2018, pp. 499–509, Published by Springer, DOI: 10.1007/978-3-319-99954-8_41, Available: https://link.springer.com/chapter/10.1007/978-3-319-99954-8_41.

[25] Md. Abdur Rahman, Elham Hassanain, Md. Mamunur Rashid, Stuart J. Barnes and M. Shamim Hossain "Spatial Blockchain-based Secure Mass Screening Framework for Children with Dyslexia", *IEEE Access*, ISSN: 2169-3536, Vol. 6, October 10 2018, pp. 61876-61885, Published by IEEE, DOI: 10.1109/ACCESS.2018.2875242, Available: https://ieeexplore.ieee.org/abstract/document/8488459.

[26] Lei Hang and Do-Hyeun Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity", *Sensors*, ISSN: 1424-8220, Vol. 19, No. 10, 2019, p. 2228, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/s19102228, Available; https://www.mdpi.com/1424-8220/19/10/2228.

[27] Bassam A. Y. Alqaralleh, Thavavel Vaiyapuri, Velmurugan Subbiah Parvathy, Deepak Gupta, Ashish Khanna *et al.*, "Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment", *Personal and Ubiquitous Computing*, Vol. 28, February 2021, pp. 17-27, Published by Springer, DOI: 10.1007/s00779-021-01543-2, Available: https://link.springer.com/article/10.1007/s00779-021-01543-2.

[28] Aniruddha Bhattacharjya, Kamil Kozdrój, Grzegorz Bazydło and Remigiusz Wisniewski, "Trusted and secure blockchain-based architecture for Internet-of-Medical-Things", *Electronics*, ISSN: 2079-9292, Vol. 11, No. 16, 2022, p. 2560, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/electronics11162560, Available: https://www.mdpi.com/2079-9292/11/16/2560.

[29] Badri Sahar, Ullah Jan, Sana Alghazzawi, Daniyal Aldhaheri Sahar and Pitropakis Nikolaos, "BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the Internet of Medical Things", *Computer Systems Science and Engineering*, Print ISSN: 0267-6192, Vol. 46, No. 3, 2023, pp. 3667-3684, Published by Tech Science Press, DOI: 10.32604/csse.2023.037531, Available: https://napier-repository.worktribe.com/output/3064760.

[30] Md. Iftekharul Alam Efat, Shoaib Rahman and Tasnim Rahman, "IoT Based Smart Health Monitoring System for Diabetes Patients using Neural Network", in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST)*, Print ISBN: 978-3-030-52855-3, Online ISBN: 978-3-030-52856-0, Vol. 325, 30 July 2020, pp. 593-606, Published by Springer, DOI: 10.1007/978-3-030-52856-0_47, Available: https://link.springer.com/chapter/10.1007/978-3-030-52856-0_47.

[31] Tuan Nguyen Gia, Mai Ali, Imed Ben Dhaou, Amir M. Rahmani, Tomi Westerlund *et al.*, "IoT-based continuous glucose monitoring system: A feasibility study", *Procedia Computer Science*, Online ISSN: 1877-0509, Vol. 109, 01 January 2017, pp. 327-334, Published by Elsevier, DOI: 10.1016/j.procs.2017.05.359, Available: https://www.sciencedirect.com/science/article/pii/S1877050917310281.

[32] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen and Charalampos Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts", in *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, 22–26 May 2016, San Jose, CA, USA, ISSN: 2375-1207, pp. 839–858, Published by IEEE, DOI: 10.1109/SP.2016.55, Available: https://ieeexplore.ieee.org/abstract/document/7546538.

[33] Nirupama Devi Bhaskar, Chen Wanfeng, Li Haili and David Lee Kuo Chuen, "Bitcoin Mining Technology", In Handbook of Digital Currency, ch. 3, pp. 41-64, 2nd ed. Amsterdammer, The Netherlands: Elsevier, 2024, Online ISBN: 9780323989732, DOI: 10.1016/B978-0-323-98973-2.00002-2, Available: https://www.sciencedirect.com/science/article/abs/pii/B9780323989732000022.

[34] Saba Khanum and Khurram Mustafa, "A systematic literature review on sensitive data protection in blockchain applications", *Concurrency and Computation: Practice and Experience*, ISSN: 1532-0626, Vol. 35, No.1, p. e7422, Published by Wiley, DOI: 10.1002/cpe.7422, Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.7422.

[35] Priyan M K, Lokesh Selvaraj, R. Varatharajan, Gokulnath Chandra Babu and Parthasarathy Panchatcharam, "Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier", *Future Generation Computer Systems*, ISSN 0167-739X, Vol. 86, 21 April 2018, pp. 527-534, Published by Elsevier, DOI: 10.1016/j.future.2018.04.036, Available: https://www.sciencedirect.com/science/article/pii/S0167739X18303753.

[36] Andre Esteva, Alexandre Robicquet, Bharath Ramsundar, Volodymyr Kuleshov, Mark DePristo *et al.*, "A guide to deep learning in healthcare". *Nature Medicine*, ISSN: 1546-170X, Vol. 25, No. 1, 07 January 2019, pp. 24-29, Published by Nature Medicine, DOI: 10.1038/s41591-018-0316-z, Available: https://www.nature.com/articles/s41591-018-0316-z.

[37] Ji-In Woo, Jung-Gi Yang, Young-Ho Lee and Un-Gu Kang, "Healthcare decision support system for administration of chronic diseases", *Healthcare Informatics Research*, ISSN: 1225- 8903, Vol. 20, No. 3, 31 July 2014, pp. 173-182, Published by Korean Society of Medical Informatics, DOI: 10.4258/hir.2014.20.3.173, Available: https://synapse.koreamed.org/articles/1075697.

[38] Paulo Valente Klaine, Hao Xu, Lei Zhang, Muhammad Imran and Ziming Zhu, "A Privacy-Preserving Blockchain Platform for a Data Marketplace", *Distributed Ledger Technologies: Research and Practice*, Vol. 2, No. 1, 14 March 2023, pp. 1-16, Published by ACM New York, DOI: 10.1145/3573894, Available: https://dl.acm.org/doi/abs/10.1145/3573894.

[39] Rasel Iqbal Emon, Md. Mehedi Hassan Onik, Abdullah Al Hussain, Toufiq Ahmed Tanna, Md. Akhtaruzzaman Emon *et al.*, "Privacy-preserved Secure Medical Data Sharing Using Hierarchical Blockchain in Edge Computing", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, Vol. 6, No. 4, 01 October 2022, pp. 38-48, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/aetic.2022.04.005, Available: https://aetic.theiaer.org/archive/v6/v6n4/p5.html.

[40] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications", *IEEE Communications Surveys & Tutorials*,

ISSN: 1553-877X, Vol. 17, No. 4, 15 June 2015, pp. 2347-2376, Published by IEEE, DOI: 10.1109/COMST.2015.2444095, Available: https://ieeexplore.ieee.org/abstract/document/7123563.

[41] C. Brodersen, B. Kalis, C. Leong, E. Mitchell, E. Pupo *et al.*, "Blockchain: Securing a New Health Interoperability Experience", *Accenture LLP*, August 2016, pp. 1-11, Published by Accenture Chicago, Available: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf.

[42] Ronald L. Rivest, Adi Shamir and Yael Tauman, "How to Leak a Secret", in *Lecture Notes in Computer Science*, Vol. 2248, Print ISBN: 978-3-540-42987-6, Online ISBN: 978-3-540-45682-7, 20 November 2001, pp. 552-565, Published by Springer, DOI: 10.1007/3-540-45682-1_32, Berlin, Heidelberg, Available: https://link.springer.com/chapter/10.1007/3-540-45682-1_32.

[43] Moonmoon Das, Rahat Uddin Azad and Md. Iftekharul Alam Efat, "Blockchain aided vehicle certification (BVC): A secured e-governance framework for transport stakeholders", in *23rd International Conference on Computer and Information Technology (ICCIT)*, 19-21 December 2020, Dhaka, Bangladesh, Print ISBN:978-1-6654-4668-6, Online ISBN:978-1-6654-2244-4, pp. 1-6, Published by IEEE, DOI: 10.1109/ICCIT51783.2020.9392725, Available: https://ieeexplore.ieee.org/abstract/document/9392725.

[44] Xuan-hua Xu, Xiang-yu Zhong, Xiao-hong Chen and Yan-ju Zhou, "A Dynamical Consensus Method Based on Exit-Delegation Mechanism for Large Group Emergency Decision Making", *Knowledge-Based Systems*, ISSN: 0950-7051, Vol. 86, 2015, pp. 237-249, Published by Elsevier, DOI: 10.1016/j.knosys.2015.06.006, Available: https://www.sciencedirect.com/science/article/abs/pii/S0950705115002245.

[45] Bella, "Human Vital Sign Dataset", Kaggle, 2024, Published by Kaggle, DOI: 10.34740/KAGGLE/DSV/8992827, Available: https://www.kaggle.com/dsv/8992827.

[46] Neetu Sharma and Rajesh Rohilla, "Scalable and Cost-Efficient PoA Consensus-Based Blockchain Solution for Vaccination Record Management", *Wireless Personal Communications*, Vol. 135, 07 May 2024, pp. 1177–1207, Published by Springer, DOI:10.1007/s11277-024-11115-1, Available: https://link.springer.com/article/10.1007/s11277-024-11115-1.

[47] Frank Swiderski and Window Snyder, *Threat Modeling*, Microsoft Press, 01 July 2004, ISBN: 0735619913, DOI: 10.5555/983226, Available: https://dl.acm.org/doi/abs/10.5555/983226.

[48] Afsana Begum, Abu Hasnat Tareq, Mahmuda Sultana, M. Khaled Sohel, Tasnim Rahman *et al.*, "Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack", *International Journal of Machine Learning and Computing*, ISSN: 2010-3700, Vol. 10, No. 2, 2020, pp. 352-357, DOI: 10.18178/ijmlc.2020.10.2.942, Available: https://www.ijml.org/vol10/942-M114.pdf.

[49] Giulio Prisco, "The Blockchain for Healthcare: Gem Launches Gem Health Network with Philips Blockchain Lab", *Bitcoin Magazine*, Vol. 26, April 2016, Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938.

[50] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, "Medrec: Using blockchain for medical data access and permission management", in *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, 22-24 August 2016, Vienna, Austria, Print ISBN: ISBN:978-1-5090-4055-1, Online ISBN: 978-1-5090-4054-4, pp. 25–30, Published by IEEE, DOI: 10.1109/OBD.2016.11, Available: https://ieeexplore.ieee.org/abstract/document/7573685.

[51] Md. Ashraf Uddin, Andrew Stranieri, Iqbal Gondal and Venki Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture", *IEEE Access*, ISSN: 2169-3536, Vol. 6, 13 June 2018, pp. 32700-32726, Published by IEEE, DOI: 10.1109/ACCESS.2018.2846779, Available: https://ieeexplore.ieee.org/abstract/document/8383967.

[52] Krishna Prasad Satamraju and B. Malarkodi, "Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare", *Sensors*, Vol. 20, No. 5, 2020, pp. 1389, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/s20051389, Available: https://www.mdpi.com/1424-8220/20/5/1389.