Journal of Theoretical and Applied Information Technology
31st May 2024. Vol.102. No. 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REAL TIME OF CYBERSECURITY RISKS DETECTION APPROACH FOR BLOCKCHAIN BASED PERSONAL MEDICAL DEVICES

TAYSEER ALKHDOUR[1], MOHAMMED AMIN ALMAIAH[2, 3], AITIZAZ ALI[4], ROMEL AL-ALI, ABDALWALI LUTFI[6, 7], MOHAMMAD MANSOUR AL-KHASAWNEH[8], MAHMAOD ALRAWAD[5], TING TIN TIN[9]

[1] Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[3]Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[4] school of technology, Asia Pacific University, Malaysia
[5]Associate Professor, The National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia
[6] College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia
[7]MEU Research Unit, Middle East University, Amman, Jordan
[8]The World Islamic Sciences and Education University (WISE)
[9] Faculty of Data Science and Information Technology, INTI International University, Malaysia

E-mail: Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

Recent methods for storing and disseminating medical data limit user access to electronic health records (EHR). It lowers care providers' access to vital information and ultimately creates a barrier to transitioning from traditional healthcare to a digital healthcare system. Numerous cloud-based systems are used for digital healthcare data allocation, but such an approach relies on third-party software such as the cloud. With the advent of industry 4.0 technologies, blockchain enables a decentralized and trustless environment by removing centralized authority. Existing models mainly utilize blockchain as a data storage tool rather than a security platform. Biomedical and monitoring devices generate massive amounts of data, and the existing approach overloads the blockchain with IoT data. This research proposes blockchain as a unique method for securing patient-related data access and integrating homomorphic encryption with an end-to- end privacy-protecting system. In this research, we propose a blockchain-based architecture for identifying security threats in personal medical devices to address the existing issues related to healthcare devices. The proposed framework uses certificate authority to assign an access control token in order to access a particular session. A certificate authority is the nodes based on the reputation within the blockchain network elected through consensus protocol. Proposed framework uses dual certificate authorities, which leads to more reliability and security if one certificate authority is down. Moreover, the existing algorithm overburden the medical devices which are resource constraint such as power oriented and such approaches leads to storage and communication cost overhead. By minimizing latency, security, and data ownership, the proposed framework outperforms the existing centralized system, by comparing the framework and evaluating its performance with the benchmark models.

Keywords: *Cybersecurity, Cyber-Risk Assessment, Authentication, Blockchain, Smart contracts, Latency, Optimization, Security, Health-care.*

1. INTRODUCTION

Blockchain is one of the technologies that has received the most attention over the past five years due to the rapid development of technology associated with industry 4.0. There have been a number of successful implementations of use cases involving Bitcoin, Ethereum, and other blockchain technology. On the other hand, none of these use cases addressed critical infrastructure, which typically has sensitive systems and data as assets. In spite of the fact that blockchains, like Ethereum, provide key anonymity, integrity, and suitability characteristics for their users, there are significant

privacy and security dangers associated with their use in critical contexts such as IoT environments. These dangers were investigated and presented in this study. Blockchains like Ethereum provide users with key anonymity, integrity, and suitability characteristics. One of the primary design ideas of other blockchains is ledger dispersion, which results in privacy problems for those blockchains. The current roadmap for Ethereum 2.0 contains upcoming updates that will address the issues about users' privacy that are high- lighted in this thesis. Before using a blockchain platform in an environment where latency is a concern, it is essential to do exhaustive tests and study on the platform's performance. This is because blockchains have many additional security and privacy features. We used blockchain technology to develop a novel privacy-preserving homomorphic encryption approach in the digital healthcare system, which provides a secure keyword search facility at the user's end [1]. Furthermore, the suggested framework for the first supports a cross-domain system, which allows a patient to access his or her personal health record (PHR) from a local to a global domain. Our study method promotes immutable, tamper-resistant, and secure data, which lowers healthcare data security breaches [2]. Additionally, our unique approach enables blockchain users to encrypt data locally and upload it to the distributed ledger for record-keeping purposes. Using homomorphic SSE, users can securely search for desired health-related data without decryption. Due to the flexible policy revocation, it also enables resistance against active cooperation and repeated assaults [3].

For digital systems, blockchain technology also supports distributed data, redundancy, and fault tolerance [4]. Current concerns and problems in the literature facing the digital healthcare business will be addressed in this suggested research. We present a frame- work and algorithm that allows users to set access control policies for patient health data in the PHR system, ensuring privacy and security. Users will have more independence with the proposed method, which also offers flexibility and fine-grained keyword search. We used simulations using the hyper-ledger fabric tool to justify our proposed research techniques and rules [5]. In the second stage, we used blockchain technology and DL to implement a novel comprehensive approach of homomorphic encryption in a digital healthcare system, which allows secure keyword search at the user's end [6]. Our suggested approach allows immutable, tamper- resistant, and secure data delivery, resulting in fewer health- care data security breaches. Deep learning has been used to train a model that can detect and monitor assaults, including DoS, DDoS, collusion resistance, Phishing attacks, and replay attacks. We separated our dataset into two categories for training and classification: training and testing data-sets [7]. For cross-validation, 70% of the dataset was utilized for training and 30% was used for testing [8].

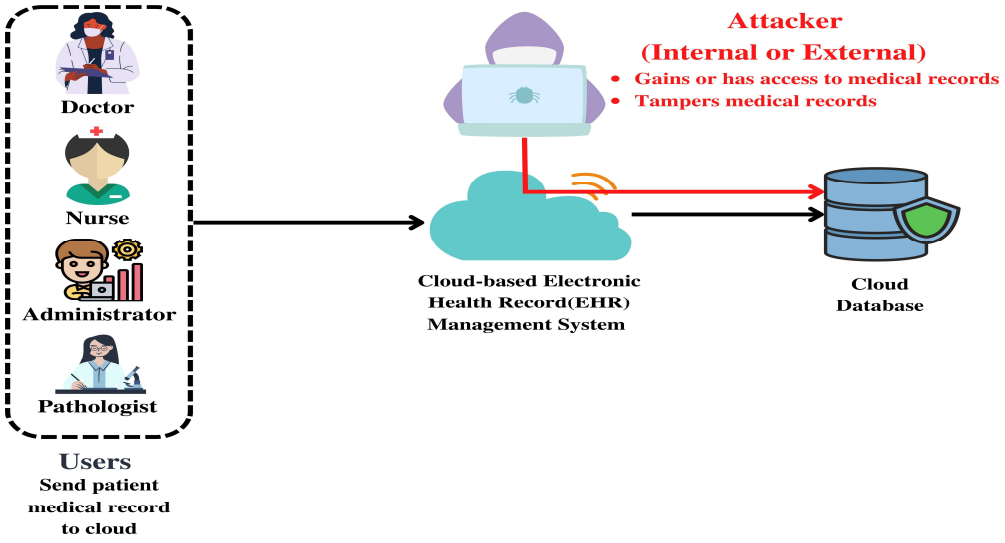


Figure 1. Schematic Representation Of The Centralized Healthcare System.

Additionally, our unique approach enables blockchain users to encrypt data locally before uploading it to the distributed ledger for record-keeping purposes. Using homomorphic SSE, users can securely search for desired health-related data without decryption. We have compared it to benchmark models like [9], among others. Because of the flexible policy revocation, our suggested approach is resistant to active collusion and replay attacks [10]. For digital systems, blockchain technology also supports distributed data, redundancy, and fault tolerance. Current obstacles and problems in the literature faced by the digital healthcare business were overcome due to the proposed research [11]. More and more, we proposed a framework and algorithms that enable users to set access control policies for patient health data in the PHR system, ensuring privacy and security. Users will have more independence with the proposed method, which also offers flexibility and fine-grained keyword search [12]. We used simulations on the hyper ledger fabric tool to justify our proposed research techniques and policies. The proposed model was tested against security threats and was shown to be resistant to external threats using a threat model [13]. Compared to benchmark models such as Medrec, Medchain, and Medbichain, we have increased the security and anonymity using our proposed method as the most up-to-date methodology applied first on healthcare and blockchain technology [14]. Different deep learning approaches, such as classification algorithms, can be used to improve the proposed model in the future [15]. Figure. 1 represent the traditional centralized healthcare system which is more prone to security breaches and very easy for attackers to breach the system. The most common attack associated with such models are DoS, DDoS and Collusion attack which are recovered in our proposed approach. Moreover, Figure. 2 represent the schematic of the proposed framework and the sub-module which are integrated with the framework are explained.

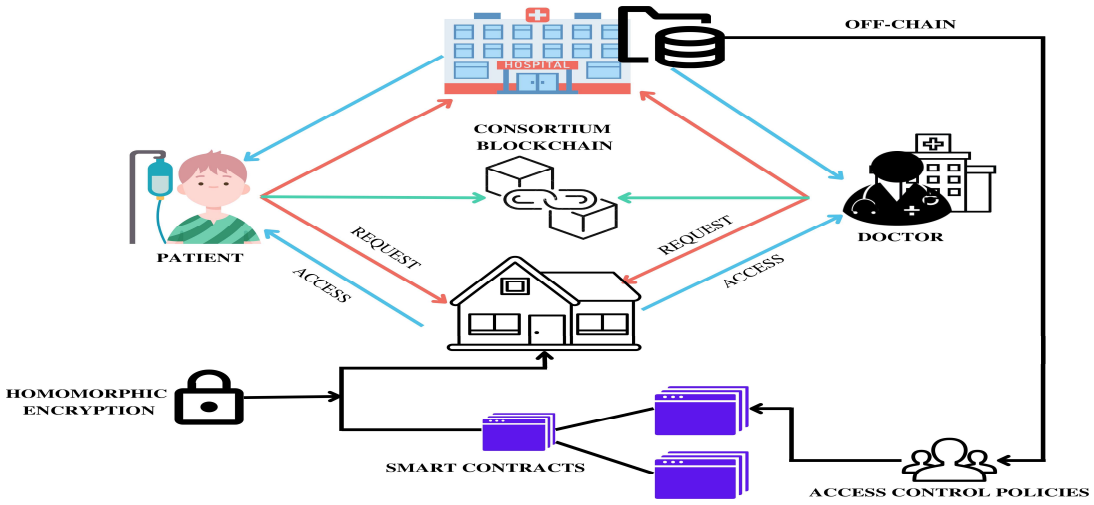


Figure 2. Schematic Representation Of The Proposed Framework Using Cross-Domain Approach.

2. RELATED WORKS

Incorporating smart health systems and PMDs into health- care is a welcome step forward, but it also introduces new security threats for healthcare organizations and people they serve. There have been multiple recent reports that smart health systems are at risk, especially PMDs. In order to carry out harmful operations on PMDs, these threats take advantage of implementation defects in communication protocols or device-specific vulnerabilities [16]. For the purpose of gathering network traffic from PMDs, a system was suggested by Wood et al. [17] that recognized plain text packet payload transmissions that might reveal sensitive medical information. Reverse engineering the Fitbit's communication protocol was accomplished by Classen et al. [18], who examined the whole Fitbit ecosystem and using a variety of techniques, including protocol analysis, software de-compilation, static and dynamic embedded code analysis. All recent fitness data may be obtained, malicious software can be injected, and the linked smartphone app can be modified to disable supported security features (i.e., authentication and encryption) [19]. Additionally, a team of researchers the attacker

could conceivably intercept and manipulate a user's communications Pre-cloud storage of medical and patient data. Li et al [20] carried out both passive and active listening. Assaults (the use of a false identity and the manipulation of medical equipment) diabetes treatment systems by altering the intended therapy information in the public domain and readily available commercially It's hardware [21]. We must raise awareness at the foundational levels in the educational system as these researchers found that it is urgent to educate students in their early years and integrate cybersecurity issues. As pupils become more proficient with information technology, educators' capacity to guarantee the development of good online behaviour patterns is put into question. On the other side, the teacher supplying the security information lacks knowledge and current information regarding Cyber awareness issues, particularly in terms of security. Teachers must receive technological training in order to increase their knowledge and skills. Consequently, improved training and awareness for teachers aid in the development of good awareness in students .This is a high correlation between teachers' expertise and knowledge and their students' evaluations [22]. Several studies have offered a paradigm based on human situational awareness for under- standing how an organization's policies are implemented and controlled. To promote human awareness in human–agent partnerships, the Situation Awareness-based Agent Transparency (SAT) idea was developed by Renaud and Colhoff, (2021). Humans must be able to understand and trust their agent counterparts to collaborate effectively. When agents move from tools to artificial colleagues, the architecture must be broadened to accommodate collaborative paradigms that require bidirectional transparency. With more advanced colleagues, they suggested that an upgraded model could better guide human–agent interaction. For the first time, they presented a study based on the principle of situational awareness to determine why small and medium-sized businesses fail to implement industry-standard cybersecurity measures. To comprehend employees that don't adhere to the policy, they used the pest model.

There is a significant gap in the level of cybersecurity knowledge in the school sector, according to the three writers. As a result, the research shows the researcher how real it is that students aren't taught about cybersecurity Aphane and Mofokeng. According to the World Bank, there are an estimated 85 million teachers in the world's education system. Since they make up the majority of government workers, the vast majority of the workforce is made up of members of this group. It is undeniable that assessing cybersecurity awareness in the education sector for this segment is critical in order to better understand its effects. There is an alternative framework for IoT that uses an SDN network and Fog nodes to deliver remarkable consistency for latency-sensitive IoT devices. They put in place a system. A trustful technique of devolution can be achieved using blockchain technology. The edge layer data is processed and used in all of these methods. Through the IoT architecture's fog layer, data is sent to the cloud of the use of the internet's services. The Internet and the cloud database are sensor (edge layer) or storage (edge layer) data is vulnerable to security threats in the cloud layer. In addition, traditional data storage and security methods are not reliable. To address the issue of data and performance protection, the authors proposed a model for trust translation, introduced an access control for fog nodes, and came up with a service for managing changes in users and their positions in [23] described an AI system that aims to reduce response times and network traffic by distributing diverse activities between cloud and fog-based servers. Comparing this method to other existing ways, the time it takes to respond was shown to be greatly reduced.

In recent years, there have been several reports of cyberattacks and system intrusions. It's no secret that online attacks are getting more frequent and sophisticated, as the media has reported. A growing number of internet criminals are committing an ever-widening variety of cybercrimes, making the human element of cybersecurity appear to be the weakest link. A Stanford University professor and the security firm Tessian collaborated on a study that found that eighty- eight percent of data breaches were caused by user mistake. Human error is to blame for 95% of all cyber security breaches, according to a recent IBM study (2014, 2021). The average cost of a human error-related cyber security breach is 3.33 million. As the first line of defense in ensuring that employees have the knowledge and skills they need to con- duct themselves properly when interacting online, cybersecurity awareness programmers are unquestionably important. Because cybersecurity awareness (CSA) initiatives are the first line of defense in teaching employees and stakeholders how to conduct themselves online safely, their importance cannot be debated. Data leakage in security management was addressed by the authors of using a blockchain-based method [24]. There were a number of nodes and power terminals in their model, which helped them collect data. The authors of [25] suggested a blockchain-based security

management architecture that intelligently generates, releases, receives, and stores data on the blockchain. It was proposed in that blockchain may be used to secure the privacy of surveillance cameras. Its primary function is to protect the privacy of those under surveillance by blurring their images while yet keeping an eye on them.

Finally, like with any IoT-based system, there will always be associated risks. Generally speaking, risk signifies the latent potential for some event, whether positive or bad, to occur. Researchers from [26] developed and implemented a quality estimate framework for commercial cyber insurance in relation to IoT cyber risk. The authors of this paper, in contrast to ours, modelled a projected electronic intrusion with a steady state that ignored time considerations and data retrieval mechanisms in favor of providing an efficient technique for retrieving large amounts of data and managing key generation [27].

3. PROBLEM STATMENT

Existing Access control model doesn't provide an efficient cross-domain authorization in cloud computing while dealing with personal medical devices. Mostly recent schemes rely on centralized system such as cloud and centralized server, and these system use blockchain for data storage which leads to communication and storage overhead. Moreover, the existing model doesn't provided fine-grained access control or consider any security factors such as collusion and phishing attacks [27]. The usage of complex algorithm for consensus approval using IoT and healthcare devices need quite improvement while dealing with millions of healthcare sensors attached with the blockchain. The computational overhead of such framework are too much high and mostly the access control model relies on encryption and storage not on authorization. Due to untrustworthiness these frame- work require very complex management and authorization credentials [25]. Such framework are using Blockchain as a data storage which make such approaches expensive and its computational overhead are too much high in case of PHR Furthermore in order to mitigate security breaches related to the healthcare sector, the existing access control approach don't provide collusion resistance and anonymity using Blockchain Based digital healthcare framework. The security performance of the existing access control based system are low and the computational overhead are too high [28].

3.1 Preliminary data

Our present understanding of blockchain, trust, and e-health records is summarised in the following section. This section also contains information about the study's findings and methods. emph Traditional methods can be used to build consensus in a distributed context. Traditional distributed consensus mechanisms use state machine replication to cre- ate distributed consensus in distributed networks. Moreover, in reference [29] introduced the Byzantine General problem and explored how non-fault nodes gained agreement on specific data in the context of probable failure nodes or ma- licious attacks, which provided the basis for the research on consensus mechanism [30]. A Paxos algorithm was presented by to solve the problem of Byzantine generals. A distributed system value can still be agreed upon even if certain nodes on the network are unavailable, thanks to this approach [26]. In order to resolve the issue of Byzantine generals, just a third of the total number of nodes in his book Practical Byzantine Fault Tolerance were opponents (PBFT). Some researchers have come up with the idea of a novel algorithm known as "Mixed Byzantine Fault Tolerance" (MBFT). It is possible to increase scalability and efficiency while maintain- ing consensus security with MBFT's functional partitioning. Additionally, the MBFT's random node selection and credit method enhances security and fault tolerance [22]. Byzantine fault tolerance dynamic reputation has been put into practice [24]. Dynamic reputation method that relies on agreement to pick candidates for the byzantine fault-tolerant algorithm the monitoring node splits the remainder of the nodes into two groups: consensus nodes and auxiliary nodes in order to keep the consensus nodes up to date [31].

3.2 Blockchain based fog computing

A fog-enabled blockchain ledger was also created to store the sensed data, while a copy of the stored blockchain data was processed on the cloud database as numerous fogs. Moreover, this performance is all about establishing and ensuring that user data is secure and overcoming latency issues around the fog layers. A decentralized and distributed blockchain record management system paradigm was also used in this research, which could mitigate all of the system's scaling and centralization difficulties, thus offering transparency and protecting patient records from intruders. On the other hand, authorized medical personnel can access the data stored on this distributed Blockchain, which

are scattered across the fog. In general, ECC digital signature-based blockchain technology was tested regarding transaction latency (the certification time, data retrieval time, and certificate size measured in milliseconds). In milliseconds, a data-minimization rate of roughly 180 milliseconds was determined by comparing the data retrieval size to the digital certificate efficiency. Also tested and provided were data retrieval latency, storage size, and certificate (critical generating time). As a consequence of this trial, it can be concluded that the proposed method generated keys faster [32]. Special decentralized software could be developed to read and view health documents with- out providing private keys. This could be done in the future. Instead, the software will prompt the user for the sender's public key, which it will use to look up the corresponding private key on the machine. Thus, a crypto hash cipher text that generates the private key can be used to safeguard and prevent the exploitation of patient medical privacy data from a compromised user.

3.3 Distributed ledger

Blockchain provide decentralized as well distributed database which is called distributed ledger. The proposed approach provides two methods to store data i.e. one is off- chain and On-chain data storage method. The proposed ap- proach keep only metadata over blockchain which is termed as On-chain data storage. The secondary is stored using off-chain data storage. Each node's data is stored in a Distributed Ledger (DL). Nevertheless, distributed ledgers keep track of the current BC condition. During transactions, the BC keeps copies of the data. The blockchain structure relies heavily on DL. A merkle root tree is used to store the hash values of each record. [30].

3.4 Symmetric cryptography

Symmetric cryptography is used when the private and public keys are identical. Asymmetric cryptography, on the other hand, is used when both keys are unique and different. Asym- metric cryptography, which is more secure than symmetric cryptography, is applied in our suggested system. [33].

3.5 Asymmetric cryptography

An encryption key and a decryption key, designated as public key and private key, respectively, are used in this encryption technique. The key pair produced by this algorithm is made up of a private key and a distinctive public key that are also produced by the algorithm.

3.6 Consensus mechanism

A consensus algorithm is a process by which at least 51% of the peers agree to authorise a certain transaction. In the blockchain, this is known as the 51 percent approach.

3.7 P2P network

At least 51% of the peers must agree for a transaction to be authorized by the algorithm. The 51 percent strategy is what it's called in the blockchain world. A peer-to-peer (P2P) network is a collection of computers or other electronic devices that are linked together, either physically or virtually, but do not have a single point of control. The BC system uses a consensus algorithm since it lacks a central authority. An agreement reached by 51% of the network's nodes is approved by this consensus procedure. Blockchain-related research has gotten a lot of attention lately, thanks to the rise of crypto technologies like Ethereum and Bitcoin. The immutability and trustworthiness of blockchain make it ideal for decentralized data storage and sharing. BC avoids intermediaries and does not require any central authority to verify the transactions. The blockchain is viewed as a less sophisticated technique of distributing PHR in order to establish trust within a network and among peers. It is better suitable for high computational power and speed since it integrates various computing powers from numerous network nodes. Consensus Protocol, Hashing, P2P topology, the Immutable Ledger, and mining are just a few of the tools available on the blockchain. Smart contracts refer to the mechanisms that control the blockchain network.

3.8 Hyper ledger fabric

In a Linux-based network, hyper ledger Fabric is a blockchain technology for use across several organizations. It has modules for encryption, identity management, consensus protocol, and membership services, all of which can be customized. A consortium blockchain network is another name for the hyper-ledger. A smart contractor chain code, a ledger with a state database and a log of transactions are some of the nodes in this network. A node in an mbox network can be maintained and managed by a single participant or a group of participants. Nodes can be categorized based on the functions they perform. The main contributions of our paper are as following:

1) Design of a novel algorithm for the cross domain blockchain framework for accessing healthcare records.

2) Smart contract design for storage optimization in the existing blockchain based healthcare frameworks.

3) Integration of Homomorphic encryption by allowing users to encrypt their medical data at user layer and outsource to the cloud.

4) End to End privacy preservation by leveraging attribute based access control approach with personal medical devices.

5) Validating and evaluation of the proposed approach with the benchmark model using performance indicators.

4. BLOCKCHAIN IN THE HEALTHCARE SYSTEM USING THE HYPERLEDGER SYSTEM

Tandon et al. claim that patient safety and privacy can be improved with the use of blockchain technology, among other advantages. Farouk and colleagues studied the use of blockchain in an IoT-enabled healthcare system. According to Turjman et al., the integration of healthcare systems with blockchain addresses issues such as securing health data as well as ensuring its integrity, ownership, privacy, and control of its access. Smart contracts, according to Ali et al. [13], perform better in terms of privacy than standard blockchain implementations. In a few studies, it has been found to be useful. The latency, throughput, and efficiency of blockchain networks have all improved. However, the blockchain-based system is expected to be more efficient and secure than traditional client-server EHR systems. It is a requirement of distributed computing (DC) to transfer data when it is required. Blockchain-based security and privacy schemes use the ePoW protocol to authenticate data transfers, according to the proposed smart contract-based protocol. In addition to IPFS, the blockchain contains: The distributed ledger framework explains how a hash of each transaction is recorded in the ledger. It's important to note that these are all examples of blockchain applications: distributed ledger technology. Figure 3 depicts the data flow and structure.

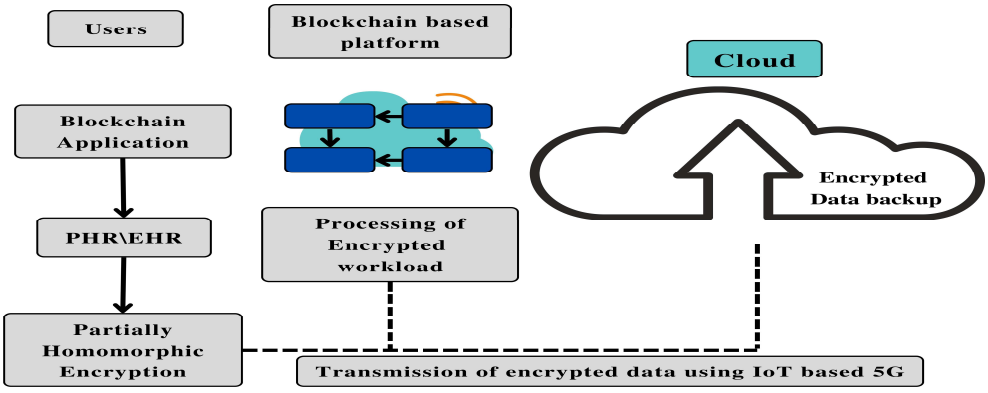


Figure 3. Applications Of Blockchain In Various Domains.

4.1 Blockchain Technology and Proof of Work (PoW)

Real-time communication with others is now possible thanks to the decentralized blockchain technology. Centralized nodes are no longer required with the implementation of blockchain technology. Consensus is the process by which at least 51% of the network's nodes approve transactions. Because the blockchain is a transparent and immutable technology, data and transactions stored on it are protected from tampering. The blockchain network depicted in Figure 2 can, for example, benefit healthcare, IoT, smart cities, and smart power grids. a transactional database that is accessible to everyone Using blockchain technology, edge nodes and cloud nodes of the IoT could be protected (IoT). A hash of the previous block, a time stamp, and any other relevant information are all included in the block of each transaction. You can't change the blockchain once a block has been added. This is ensured by submitting a copy of your work (PoW). Proof of Stake (PoS) is used to verify the legitimacy of a transaction, while Proof of Work is used to add new blocks to the blockchain (PoW). More than 51

percent of the computing power or stake can be used by a malicious miner to affect both methods across the Internet of Things network. Adding nodes and peers to the blockchain network is depicted in Figure 3. Various tracking systems make use of a variety of different approaches. Using RFID, for example, a traceability task was performed for selected elements scattered in different locations within a small area by the suggested system in In addition, a variety of different methods are employed to assist in the tracking of items, such as the QR code method. This technology has more storage capacity and responds more quickly than any of its competitors. There are many ways in which tracking systems can benefit from QR codes. As a result, QR codes can be utilized with the Internet of Things (IoT) to reply in real time. QR codes have been used in a broad variety of smart applications, including tracking systems. Using a QR-based tracking system, one example is given in which a production process is traced through multiple stages. It is possible to cut down on computing time and complexity by employing this method, as stated. BAKMP-key EHR and PHR administration allows secure communication between implanted medical devices and a personal server. On the Internet of Things, P. Gope and his colleagues [34] have faced anti-machine PUF attacks. A method devised by Salem et al. [22] can keep MitMs from interfering with the remote health surveillance system. CNNs and short-term memory networks are two of the most advanced learning models in the field (STLRM). Z. Ning et al. [27] describe the Nash equilibrium. Estimating the number of MECs can also be done by counting the number of patients and looking at the complexity of the algorithm. As a result of their investigation, Liang and his co-authors [11] created an innovative mobile healthcare paradigm. In order to maintain user privacy and restrict unprivileged users' access, this record sharing framework employs user-centric security and channel-formation strategies. This strategy is computationally intensive because of the complexity of the encryption mechanism. Figure. 3 shows the actors involved in the proposed framework as well as the function of smart contract and the data storage optimization approach. In Figure. 3 it's very obvious that the proposed framework uses two approaches for data-storage i.e. on chain and Off-chain data storage. On chain data is the only meta data stored in the distributed ledger, whereas the off-chain data is stored over the cloud in encrypted form using homomorphic encryption. The proposed approach provides data storage optimization and fault tolerance capability as compared to the benchmark models. Our suggested blockchain-based healthcare systems with intelligent smart contracts are depicted in Figure. 4

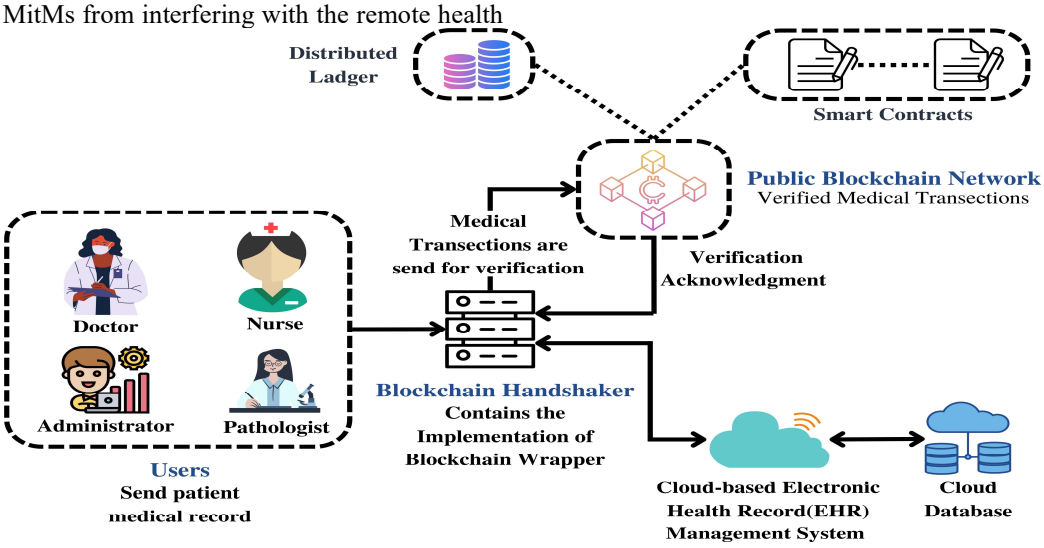


Figure 4. Schematic Representation Of The Proposed Blockchain Handshake Algorithm And The Transaction Flow.

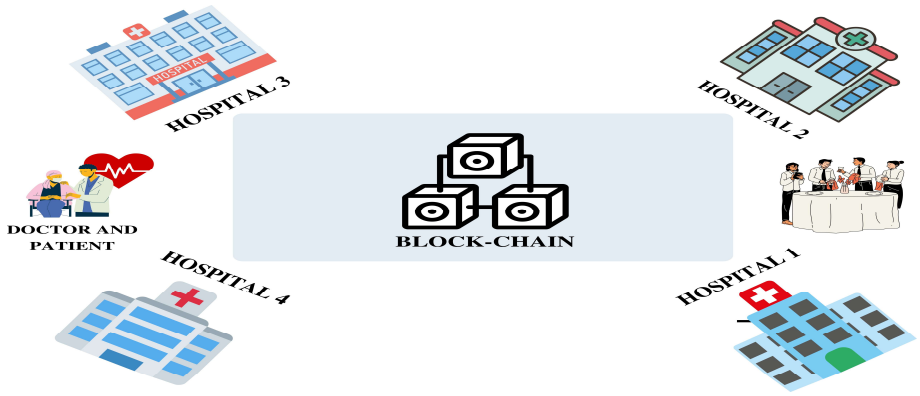


Figure 5. Cross-Domain Blockchain-Based Healthcare System.

Table 1. List Of Parameters For Our Proposed Algorithms

S.No	Parameters	Details
1	BN	Blockchain Network
2	CID	Clinician ID
3	LID	Lab ID
4	PHR	Patient Health Record
5	R^s	Ring Signature
6	U^{Name}	Username
7	P^K	Private Key
8	r	Integer
9	N	Number of Nodes
10	G	Bi-linear order group
11	P^1	Generator of Additive Group 1
12	P^2	Generator of Additive Group 2
13	id	Bi linear identifier
14	H	Homomorphic Encryption
15	k	degree of signature

4.2 Proposed blockchain-based model IoT integration

The Internet of Things (IoT) is a vast network of interconnected electronic devices and sensors. Peers and a central server, known as a "server," share the data from sensors. Denial-of-service (DoS) attacks and IoT network security flaws are the biggest dangers. Using blockchain technology, it is possible to keep the IoT network secure by removing the network's central node [35]. Working of the proposed blockchain based healthcare sys- tem is explained as below:

1) Verification Phase: Node and users request are verified through the account smart contracts. The account smart contracts verify the integrity and eligibility of each authorized user. If the users or the node attributes matches the requirement then the request is accepted otherwise it's denied.

2) Phases of item validation and block creation: If the data is successfully registered, the blockchain process is joined. The following are the stages involved in creating and validating blocks: Please edit if there is any missing information.

3) The first step is to establish a key value pair (P Bkj, P Rkj), where P Bkj is the public key and P Rkj is the private key of the jth light node.

4) In addition, the registration process has begun.

5) The creates a signature and sends it to the appropriate nodes for verification.

6) The signature is validated by the access control policies. When the signatures match correctly, the client sends a joining network request using the credential P Bkj.

7) For validation of the user's location, security smart contracts send validation requests to peer nodes (N-p).

8) Peer nodes (N-p) use smart contracts to validate the location of nodes using timestamps recorded by smart contracts in blockchain according to latitude and longitude.

9) After it has been confirmed, the appropriate node receives a True/False acknowledgment.

10) A new block (Bj) is constructed and attached to the blockchain network with the credential P B-k-j for True status.

11) Creating data and updating blocks: The data generating process is described in this step. The generated data through personal medical devices are referred to as transaction data (Tj). Below is a description of the data creation and block updating procedure.

5. PROPOSED METHODOLOGY

In this section we discuss the proposed methodology and steps carried out during the experiments. Figure. 6 represent the proposed experimental methodologies and the installation required to run the proposed methodology. In order to run the experiment we design a blockchain network using hyper-ledger fabric based on the virtual nodes and interface for the doctor and patient login. Figure. 2 illustrates the suggested medical data security at the fog layer of the IoT-based cloud computing model employing public permissioned blockchain technology with an ECC digital signature as a security solution in the model. In first step we carried out the software installation, then in second step we run our experiment and count the number of rounds and number of transaction. The elliptical curve cryptography digital signature technique (ECDSA) uses the secure hashing algorithm 256 (SHA-256) for certificate hashing. This is the primary foundation for bitcoin security and is widely utilized to secure messaging apps. Since the WSN-IoT had a security countermeasure that lacked computational complexity, memory inconvenience, processor power consumption, and latency, along with other concerns that social attackers may exploit, blockchain technology was adopted. The ECDSA strategy incorporated a hash algorithm into the blockchain for security, immutability, and transparency. Ellipse cryptography hashing is faster, more efficient, and 10,000 times more secure than traditional RSA, with keys of 256 bits (equal to 2048 and 3072 bits in traditional RSA). Hashing's random number generation suffers from the avalanche phenomenon. Fog-enabled blockchain ledgers are used to store the collected data, with a copy being transferred to the cloud via numerous fogs. The decentralized records at the fog layers in this paradigm help safeguard the data (immutability) and overcome latency difficulties. Blockchain technology using an elliptic curve cryptography hash method alleviates the problems of scalability and centralized storage [36].

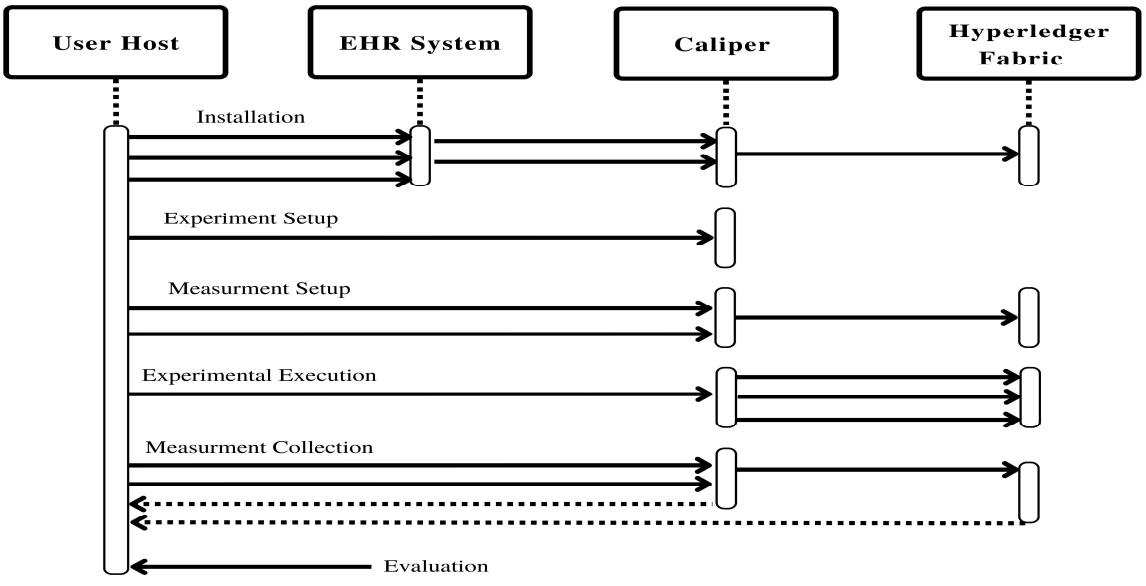


Figure 6. Flow Of The Proposed Experiment.

5.1 Mathematical Modeling

In this section we have carried out mathematical modeling in order to proof my proposed model encryption and decryption process. Moreover, we have also carried out the mathematical modeling for the number of rounds as explained below:

$$y^2 \bmod q = (x^3 + ax + b) \bmod q \quad (1)$$

$$G_q = (x, y) : a, b, x, y \text{ belong to } F_q, (x, y) \text{ belong to } F_q, (a, b) \quad (2)$$

$$k_P = P + P + \ldots + P (k \text{ belong to } Z_q), \quad (3)$$

where k denotes the key and Zq is the random integer chosen by the users in order to create a key.

$$((ui + vi) * G), \text{ if } i = S \quad (4)$$

where *ui* is the value 1 for the signature, *vi* is the second value for the signature creation, *G* is group of bi-linear pairs, and *S* represent the length of signature.

$$(u_i G + (v_i + w_i)) * p k_i, \text{ if } i = !S \quad (5)$$

where w_i is the weight assigned to each and k_i.

$$R_i = \sum (u_i + w_i) * H_0(p * k_i), \text{ if } i = s \quad (6)$$

where R_i represent the real number and s is the signature length.

$$R_I = \sum u_i * H_0(p * k_i) + (v_i + w_i) * I_s \text{ if } i = s \quad (7)$$

where R_I denoted ith real number selected by the users, and I_s is the index value of the signature.

$$H = h(m||r), \quad (8)$$

where *h* represents the homomorphic encryption, *H*2 is the Homomorphic encryption, *m* is the modulus of r value, and*r* is the integer value.

6. PROPOSED CERTIFICATE AUTHORITY AND ITS FORMULATION

In order to understand the working of the proposed model and the integration with CA here we explain the working of dual CA. The Proposed approach provide the interoperability with different certificate authorities relies on our proposed certificate authority.

6.1 Function of our proposed CA

From the literature, it is very clear that Fabric CA performs the following functions on a blockchain network:

• Users Identity Registration: In first step user is registered through certificate membership.

• Issuance of Enrolment Certificates (ECerts): EC is issued only to the authorized users.

• The proposed CA approach support flexible member- ship to the users.

6.2 Setup of certificate authority (CA)

A limited number of CAs dependent on the size and scope of the blockchain-based network. The proposed approach supports dual CAs in each domain which provide more flexibility to the user's enrolment in case one CA is down or busy with the users' registration. The main objective of the dual CA is to provide robustness and reduce latency in the communication. Moreover, the proposed dual CAs can be categorized as an Organization CAs and TLS CAs. The function of the organization CA is to manage the flow of transaction inside the organization such as users' enrolment, key assignment and attribute updates whereas TLS CA works on the encryption of communications between peers in the domain on the network. TLS, on the other hand, support each peer with a certificate to ensure secure communication. Organization and node identities have been generated by combining multiple CAs on the opposite side.

7. SIMULATIONS SETUP

In addition to the Ethereum remix IDE, we use the Hyperledger Fabric tool for blockchain design and transaction processing to carry out the proposed method. We use the mat- lablib library for statistical data analysis. Importing pandas, a tool for data analysis and processing, was made possible thanks to the matlablib package. The graphs were plotted using a python programming tool for evaluation reasons. The Wireshark utility captured network data, which was then saved to a pcap file. TCP files, transmission and receiving times, and source and

destination ports are all included in a Pcap file. Data can be seen to its fullest potential using the caliper transaction and blockchain analysis tool. Transaction rate, throughput, latency, the number of peers, CPU use, and storage utilization are all analyzed during this review process.

7.1 Events on Consortium Blockchain

Blockchain smart contracts can send events and logs to the blockchain, which the front-end can subsequently process, when a transaction is mined. An application front-end or other subscribed applications can then utilise these events to communicate with a smart contract. Due to the fact that events on Blockchain are not regarded to be a state change, they use much less gas than transactions that are. The experimental and simulations process are shown through the following attached screenshot which show the Hyperledger Fabric CLI interface.

8. SIMULATIONS RESULTS

In this section we have discussed and evaluated the proposed results. The simulations results are carried out using hyperldeger fabric and for test purpose we used etherum testnet. Our proposed framework relies on patient health records as the primary source of data (PHR). PHR privacy characteristics, explicit id, and quasi-id all fall under the PHR category. A patient's age, date of birth, and home or office address are all suggested by Q-ID. The sensitive qualities of a patient, such as the type of sickness and the patient's income or resources, are included in the term "privacy-related information." In order to publish and retain patient health data, it is vital to ensure that the new dataset's specific attributes are processed effectively. Anonymity is not provided by most of the current approaches. Uncovering a new technology strategy that encompasses anonymity, variety and trust is at the heart of what we're proposing in this framework. Because it was so extensively used, traditional -anonymity imposes no restrictions on sensitive data. If the attackers cannot get their hands on sensitive data and personal contact, they will have difficulty getting the information they need.

8.1 Scenario 1: Basic Experiment

With the help of PHR, researchers will examine and assess the Hyperledger Platform for Blockchain Technology (PHR). All of the transactions will be written to the ledger in ten sequences of 1200 transactions each, with a ratio of 100, 150, 250, and 300 transactions per second for the whole network.

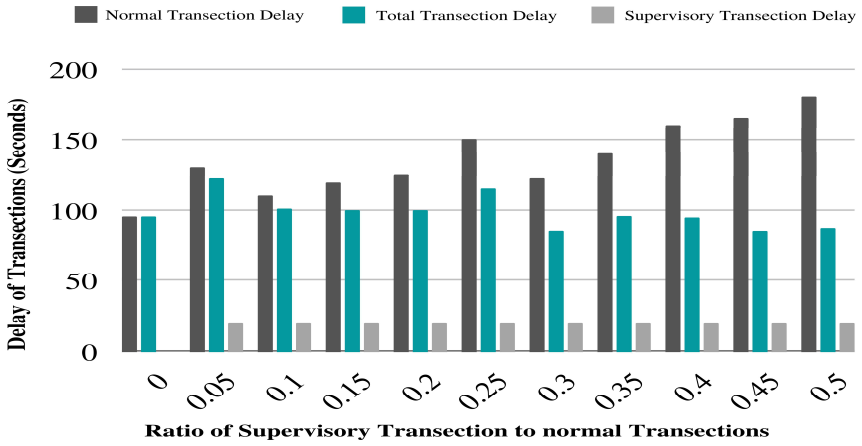


Figure 7. Simulations Results For Proposed Method-Confirmation Time Vs. No. Transactions.

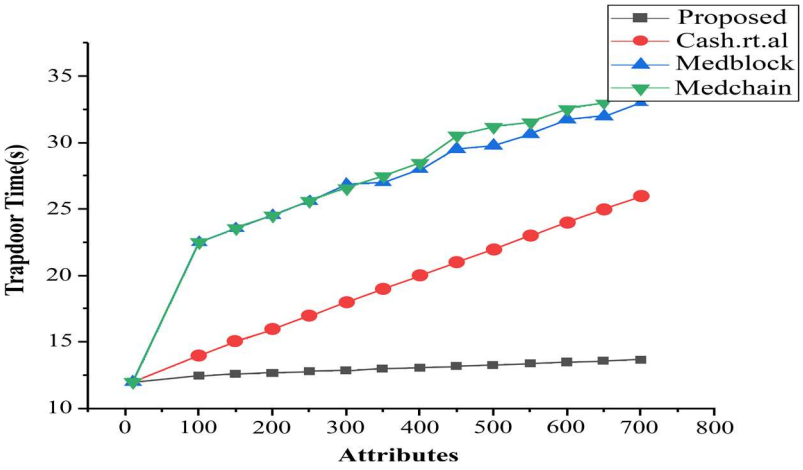


Figure 8. Working Of Proposed Secure Searchable Framework.

8.2 Scenario 2: experiment using variation with block time

We'll check to see if the network has been optimized in this step. When the hyperledger calliper for PHR is configured, an evaluation will be conducted by measuring the block initiate time. This experimentation will help us understand how the simulation findings change over time.

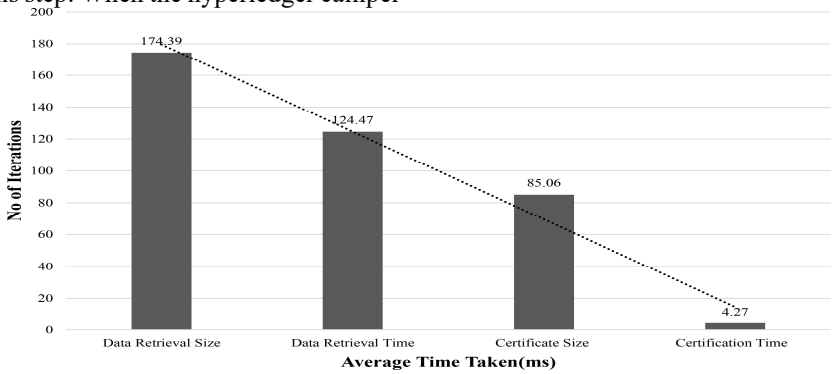
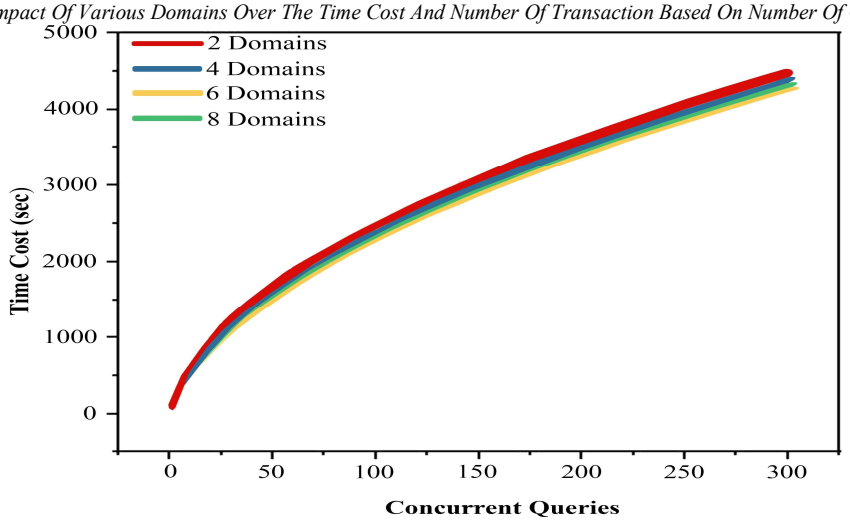


Figure 9. Simulations Results for proposed Method-Confirmation Time vs. no. Transactions.

Figure 10. The Impact Of Various Domains Over The Time Cost And Number Of Transaction Based On Number Of Concurrent



Queries And Requests.

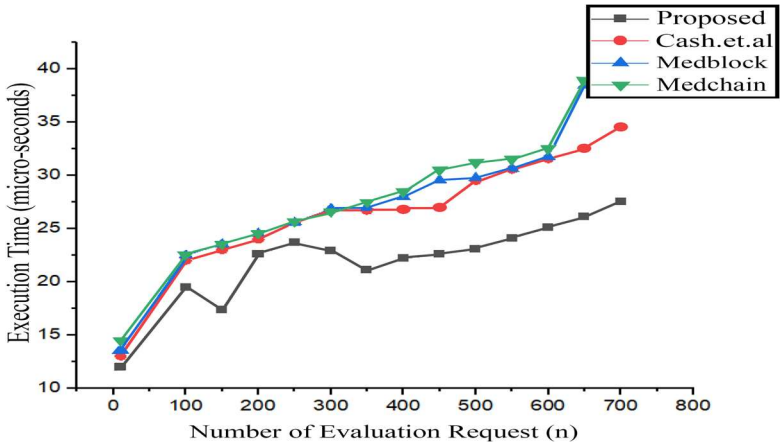


Figure 11. Comparative Analysis Of Access Control Models.

9. DISCUSSION

This paper's primary focus was on the investigation of the mentation of novel security mechanisms that will enhance the security of IoMT edge networks for healthcare monitoring. Blockchain has been identified by both the industry and the research community as a disruptive technology that can significantly contribute to (a) securing IoMT devices and (b) resisting unauthorised access during data transmission. Because of this, the paper's primary focus was on the adoption of blockchain technology in the design and implementation of novel security mechanisms that will (i.e., tamper-proof transmission of medical data). Despite the fact that several blockchain-based security mechanisms have been proposed in the literature for various types of IoT edge networks, there are no blockchain-based security mechanisms for IoMT edge networks. This is the case despite the fact that there are no blockchain-based security mechanisms for IoMT edge net- works. As a consequence of this, additional effort needs to be placed into the design and development of safety procedures for these networks that rely on the technology of blockchains. The two types of blockchain-based security mechanisms that are specifically designed for IoMT edge networks, which are extremely rare, as well as those that are designed for other types of IoT edge networks but have the potential to be adopted in IoMT edge networks due to their similar capabilities and technical characteristics, were the primary focus of this paper. This paper also discussed other types of blockchain-based security mechanisms that are designed for other types of IoT edge networks. To be more specific, our objective was to create a structure for the planning of research activities with the end goal of the creation and development of reliable blockchain-based security mechanisms that ensure authentication and authorization as well as the implementation of AIDSs for IoT edge networks. We want to leverage the findings of this work, in terms of the benefits and drawbacks of the analyzed blockchain-based security mechanisms, to create brand-new blockchain-based security mechanisms that are reliable and efficient in the future. These procedures will ensure authentication and authorization for IoT edge networks, in addition to the installation of AIDSs. Following the creation of blockchain-based security mechanisms, a security analysis will be performed on those mechanisms in order to rank them according to the level of security achieved, with the goal of selecting the most secure mechanism for deployment. Finally, the computational cost, communication overhead, and storage overhead of the developed blockchain- based security measures are assessed as below:

9.1 Security and latency

Although the theoretical security proof in mathematical modeling are demonstrated the correctness and security of our message sharing strategy, other latency's might still influence the distributed healthcare blockchain system that was equipped with this technique. More importantly, it is vital to evaluate the double spending issue, which significantly affected how securely transactions were implemented in the blockchain based IIOMT system. Figure. 15 illustrates the relationships between the proof of successful double spending and the delay with various attacker hash powers under the assumption that the visitor volume for each block was 50 requests per minute (AHP). The simulation results showed that the amount of network security could affect how many confirmations there are for each transaction. If the attacker's hash strength is greater, more confirmations should be handled. We anticipate that the quick validation and

responsiveness are important for high-volume and large- volume blockchain based IIOMT systems.

9.2 Energy consumption

In this section, we provide the comparison of the proposed schemes versus the benchmark model. In the proposed approach we also observed the average energy cost over blockchain actions such as message share, verification share, information retrieval and the reconstruction of the share. Since the energy was primarily utilized by the computing activities, the computing complexity should be taken into account during the creation and restoration phases of the EMR share. Moreover, it was observed that the proposed approach use less energy as compared to the benchmark model in case of energy usage. Due to the integration of IoT sensors devices attached with the blockchain, the battery power was kept into account. using the lightweight homomorphic encryption, the proposed approach used less energy on each EMR processing as compared to the benchmark models. The proposed approach divides EMR into t chunks and each chunk is assigned to a block for specific operations which consume less energy consumption as compared to bi- linear pairing and exponential operations for whole EMR Block.

10. CONCLUSION

Instead of analyzing the usefulness of blockchain technology, this article attempts to familiarise medical professionals with bio-medical device security using blockchain. Since numer- ous cutting-edge research areas surround blockchains, the authors focus on the present threat to medical equipment and how to safeguard it. By detailing the risks, the authors hope that more medical professionals would accept and use blockchain technology to protect medical devices and, consequently, patient safety. It is noteworthy how crucial it is for medical professionals to comprehend the basics of blockchain technology and use that knowledge to incorporate this field into medicine. A comprehensive plan is used to achieve this objective. Furthermore, leveraging cyber-physical systems, we sug- gested a novel secure access control framework based on smart contracts and blockchain. By combining a hybrid deep learning approach with attribute-based access control, we have proposed a novel algorithm that recommends policies for secure access control. However, these access controls include reading, writing, signature creation, and attribute verification. In this study, blockchain is utilized as a security tool, not for data storage. Blockchain offers a framework for validating and encrypting user data into secure ciphertext. The suggested method is assessed and compared to the reference models. It is determined that the proposed model outperforms the existing blockchain-based and centralized systems.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Research No. GrantA445).

RFERENCES

[1] Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. The Open Medical Informatics Journal, 11(1), 37–43. https://doi.org/10.2174/1874431101711010037

[2] Chen, Q., Lambright, J., & Abdelwahed, S. (2016). Towards Autonomic Security Management of Healthcare Information Systems. Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016, 113–118. https://doi.org/10.1109/CHASE.2016.58

[3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), 572.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. Education and Information Technologies, 25(4), 3087-3107.

[5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.

[6] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors, 22(4), 1448.

[7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access, 8, 163209-163224.

[8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect

jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22), 3648.

[10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience, 2021.

[11] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6), 2112.

[12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access, 8, 176495-176520.

[13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A RSS-based localization method using HMM-based error correction. Journal of Location Based Services, 12(3–4), 273–285.

[14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 107-123). Cham: Springer International Publishing.

[15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access, 8, 44459-44469.

[16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In 2021 International Conference on Information Technology (ICIT) (pp. 440-445). IEEE.

[17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access, 8, 148510-148527.

[18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure detection applications acceptance: The case of COVID-19. International Journal of Environmental Research and Public Health, 19(12), 7307.

[19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In 2021 international conference on information technology (ICIT) (pp. 725-731). IEEE.

[20] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 217-234). Cham: Springer International Publishing.

[21] Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-January, 3881–3890. https://doi.org/10.24251/hicss.2020.474.

[23] Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. Risk Management and Healthcare Policy, 9, 75–85. https://doi.org/10.2147/RMHP.S99908.

[24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. Electronics, 11(21), 3571.

[25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng.(IJECE), 10(6), 6461-6471.

[26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception of occupational and environmental risks and hazards among mineworkers: A psychometric paradigm approach. International journal of environmental research and public health, 19(6), 3371.

[27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. Electronics, 11(23), 3926.

[28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20), 3330.

[29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[30] Kemboi, L., & Ronoh, L. (2021). Security Control Model for Electronic Health Records. International Journal of Applied Sciences: Current and Future Research Trends, 12(1), 43-52.

[31] Al-Mejibli, I. S. (2019). A Fuzzy Analytic Hierarchy Process for Security Risk Assessment of Web based Hospital Management System. International Journal of Advanced Trends in Computer Science and Engineering, 8(5), 2470–2474. https://doi.org/10.30534/ijatcse/2019/92852019

[32] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017, September 2018, 112–120. https://doi.org/10.1109/LCN.Workshops.2017.72.

[33] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-agent system combined with distributed data mining for mutual collaboration classification. IEEE Access, 9, 70531-70547.

[34] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT) (pp. 732-738). IEEE.

[35] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In 2021 International Conference on Information Technology (ICIT) (pp. 640-647). IEEE.

[36] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using sem. Sustainability, 15(13), 9908.

[37] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618.

[38] Mohamed, M. A., Shawai, Y. G., Almaiah, M. A., Derahman, M. N., Lutfi, A., & Bakar, K. A. A. (2024). Challenges in data representation for efficient execution of encryption operation. Bulletin of Electrical Engineering and Informatics, 13(2), 1207-1216.

[39] Scientific, L. L. (2024). ENHANCING CLOUD SECURITY BASED ON THE KYBER KEY ENCAPSULATION MECHANISM. Journal of Theoretical and Applied Information Technology, 102(4).

[40] ALKHDOUR, T., ALMAIAH, M. A., ALI, A., LUTFI, A., ALRAWAD, M., & TIN, T. T. (2024). REVOLUTIONIZING HEALTHCARE: UNLEASHING BLOCKCHAIN BRILLIANCE THROUGH FUZZY LOGIC AUTHENTICATION. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[41] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). A NOVEL FEDERATED-LEARNING BASED ADVERSARIAL FRAMEWORK FOR AUDIO-VISUAL SPEECH ENHANCEMENT. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[42] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). BUILDING TRUST IN IOT: LEVERAGING CONSORTIUM BLOCKCHAIN FOR SECURE COMMUNICATIONS. *Journal of Theoretical and Applied Information Technology*, *102*(3).

[43] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, *24*(2), 713.

[44] Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115-127.