# Block-chain based Secure Data Access over Internet of Health Application Things (IHoT)

**A. Ezil Sam Leni[1*], R. Shankar[2], R. Thiagarajan[3] and Vishal Ratansing Patil[4]**
[1]Department of CSE, KCG College of Technology
Chennai- 600097, India
[e-mail: Lenisatish@gmail.com]
[2]Department of ECE, Teegala Krishna Reddy Engineering College
Hyderabad -5000972, India
[e-mail:ece.dr.ram.shankar@gmail.com]
[3]Department of Information Technology, Prathyusha Engineering College,
Thiruvallur - 602025, India
[e-mail:rthiyagarajantpt@gmail.com]
[4]Computer Department, Rizvi College of Engineering,
Bandra, Mumbai 400050, India
[e-mail: vishalpatil@eng.rizvi.edu.in]
[*]Corresponding author: A. Ezil Sam Leni

*Received September 18, 2022; revised December 2, 2022; revised January 11, 2023; accepted April 25, 2023; published May 31, 2023*

## Abstract

The medical sector actively changes and implements innovative features in response to technical development and revolutions. Many of the most crucial elements in IoT-connected health services are safeguarding critical patient records from prospective attackers. As a result, BlockChain (BC) is gaining traction in the business sector owing to its large implementations. As a result, BC can efficiently handle everyday life activities as a distributed and decentralized technology. Compared to other industries, the medical sector is one of the most prominent areas where the BC network might be valuable. It generates a wide range of possibilities and probabilities in existing medical institutions. So, throughout this study, we address BC technology's widespread application and influence in modern medical systems, focusing on the critical requirements for such systems, such as trustworthiness, security, and safety. Furthermore, we built the shared ledger for blockchain-based healthcare providers for patient information, contractual between several other parties. The study's findings demonstrate the usefulness of BC technology in IoHT for keeping patient health data. The BDSA-IoHT eliminates 2.01 seconds of service delay and 1.9 seconds of processing time, enhancing efficiency by nearly 30%.

***Keywords:*** BlockChain, Distributed System, Security, IoT, Healthcare service, Privacy.

**http://doi.org/10.3837/tiis.2023.05.010** **ISSN : 1976-7277**

## 1. Introduction

The blockchain idea is well-known for its application in crypto currencies such as bitcoin. It has received much interest from many people because of its vast business opportunity and uses in various applications like finance, medical, and logistics [1-3]. Healthcare industry services are the most visible and essential services that must be completed on time, reliably, and confidentially. As a fully decentralized technology, blockchain can play a significant role in the provision of such medical services. The healthcare industry benefits significantly from blockchain-based, which guarantees safe data storage and sharing between stakeholders, countrywide data interoperability, and customizable and rapid invoicing modalities [4].

We are currently living in a new technological era. After mobile Network techniques and the Internet dominated the last two decades, the Internet of Things (IoT) explosion has arrived. Every element is uniquely determined and reachable, becoming a part of the Web in the IoT technology. Gadgets that generate, analyze, and exchange privacy-sensitive data make up the IoT, and Medication management, home automation, transport, farming, and environmental sensing are just several solutions available. In addition, a wide range of cognitive IoT devices uses on each layer of IoT. Because these IoT devices gather and process many sensitive documents, data privacy and security are critical. In addition, IoT systems are thin and compact, with reduced power consumption.

Because the limited quantity of power generated is typically required to accomplish core program operations, addressing other issues like privacy and data security. Traditional data security and data privacy measures are ineffective due to gadgets' dispersed architecture and resource limits. As a result, IoT requires scalability, compact and decentralized data security protection. Because of its encrypted, decentralized, unchangeable, open, and publicly available record, the blockchain system that supports Cryptocurrency [5] can resolve the difficulties listed above. The blockchain protocol organizes all data into a series of linked blocks that record transactions relating to their purpose. It forms a chain when blocks connect to the original existing block. It also needs a mining technique to attach the blocks to the chain when it is full of transactions.

Miners do the mining procedure who solve a resource-intensive computational challenge referred to as Proof of Work (PoW) [6]. Nevertheless, using blockchain in the field of IoT is not simple. It faces several issues, including low scalability, high resource consumption, and traffic congestion, to name a few. We present a novel blockchain architecture tailored for IoT devices in this study, and we use the example of Remote Medical Surveillance to demonstrate our point (RPM). RPM allows healthcare providers to interact with patients outside of a traditional clinical environment. Patients wear Wearable intelligent gadgets, and these gadgets can send communication among healthcare professionals such as blood sugar levels, pulse rate, and respiration patterns, among other things.

In the context of current security needs for medical systems, there is a specific need for a robust and reliable blockchain-based medical service that will offer easy and secure access to patient information. Also, many key stakeholders are involved, such as doctors, who can extract and attach information only with the patient's consent. Simultaneously, the platform must adhere to essential security aspects like secrecy, consistency, and authenticity [7]. This study suggests a blockchain-based health service in which authorized physicians can safely append or retrieve patients' health information with the patient's authorization. Furthermore, our developed scheme can provide scalability, a critical necessity in today's medical systems.

## 2. Motivation

Modern internet medical services, including Digital Health/Medical Records (EHR/EMR), serve an important in saving, exchanging, and keeping individuals' private medical information. However, there seem to be a variety of flaws that could result in the leakage of patients' confidential health information. For example, patients may find tracking which party receives patient records and use different techniques to manage medical systems. In such circumstances, distributed ledger technology can be critical since it delivers data-ledger-based capabilities disseminated to all communicating nodes. A patient can keep track of which entities access information and allow access to only those who are permitted. As a result, the main aim of this project is to use private blockchain in health services and address possible flaws in present medical systems. This work's novelty is that it contributes much too securing patient records using a blockchain-based N2N network technique. While transferring, the patient information gathered from the sensing device must be protected. Patient records unboxing are done only, satisfying the wise agreement policy, so we are motivated to work on proof of agreement (PoA). The technical soundness of this work is much more focused on securing patient data over the blockchain network.

## 3. Related Work

Conoscenti et al. [8] examine how to use blockchain technology and peer-to-peer (P2P) techniques in a personal IoT. Their analysis uncovered significant flaws in blockchain technologies' integrity, invisibility, and flexibility. They conclude that while large blockchain networks (such as Bitcoin) are trustworthy, they are not suitable for IoT due to capacity difficulties. Moreover, [9] shows how blockchain might help with several common IoT issues. Blockchain-based smart agreements, for illustration, can enhance safety in IoT supply chain operations. Finally, Reyna et al. [10] investigate the problems of IoT and blockchain incorporation. The study compiles and analyzes IoT applications as blockchain subsystems, significant technology, and the latest IoT-Blockchain deployments. Ethereum is the most widely used IoT with a blockchain-based platform.

Patient information is regarded as very confidential and must be protected safely and adequately. As a result, healthcare information should be stored, shared, and managed safely. Different methods offer to handle these concerns. For instance, [11-13] presents several authentication protocols to meet the demand for robust and reliable health information retrieval, management, and other critical safety needs. Such methods helped meet multiple security needs in targeted occupational health & safety to a certain level. However, despite recent improvements in medical technologies, these techniques are no longer adequate since numerous parties have abused patients through various means, even without one‘s permission [14]. Therefore, experts are eager to identify multiple security systems relying on blockchain-based medical solutions in this context [15].

Huh, et al. [16] suggest a new Ethereum-based PKI management platform based on intelligent agreements. The security plan employs Public key cryptographic encryptions, with credentials kept on Ethereum and secret keys possessed on personal devices. However, there are two issues with the suggested system. The primary issue is that each transaction takes a long time to accomplish. The next issue is a huge storage need for IoT customers' restricted equipment. The level of protection reduces by fixing this issue with a proxy gateway that's the third trusted party. Ethereum is an open, decentralized platform [17] that allows users to build intelligent contracts that concentrate on advancing Distributed ledger BC technology. An intelligent agreement is a computer-based framework that consists of principles that participants decide upon to meet the specific needs and a Turing complete structure for protecting patient information and regulations that may update by the juristic person their identity is on the agreement [18]. An intelligent agreement may also communicate with the BC and health professionals based on individual needs. It can also maintain the hospital's patient records by administering the stakeholder's security controls and safe management of the medical history [19].

Multiple research investigations on the possible use of BC in medicine have now been reported in several studies by numerous investigators [20]. The most prominent sectors of implementation where BC technologies can provide value are digital medical care procedures for physical and remote monitoring of patients' record and preserving the privacy of health records [21]. The research in [16] presented MedRec, a distributed approach to EHR/EMR management based on BC technologies. The researchers also included a possible case analysis of BC use in medicine, which serves as a model for EHR/EMR systems. Furthermore, a study in [22] shows that MedShare gives the permissionless approach of exchanging health information across diverse service suppliers utilizing blockchain. As a result, the academics are proposing several techniques for safe data accessible in a blockchain-based health service.

Dorri et al. [23] demonstrate a simple BC implementation in an intelligent house. Local private BCs define as unchangeable ledgers that record policies and transactional content, and the proprietor controls the suggested private blockchain that does not use PoW. Each home automation has its blockchain, which a resident miner administers. These miners get a list of products and evaluate all home automation activities. A public key secures unicast connectivity between mobile, whereas the host miner creates these credentials. Another Dorri et al. study [24] proposes an identical general model blockchain-based for larger IoT systems.

By employing personal BC for safer and speedier healthcare information retrieval, this work contributes to a more effective and efficient detail accessing strategy. As a result, this study provides an approach for data acquisition and access from other parties dependent on the patient's identity management. Medical information maintains in a repository on N2N networks, which addresses records on the ledger. The accessibility determines the content that patients are authorized to access, whereas doctors require patient permission. This research suggests a blockchain-based protection system for a clinical networking application in which individuals securely and privately communicate their healthcare information with hospitals and doctors.

## 4. System Model

This chapter summarizes a BC-based authentication scheme for real-world IoT devices, such as an intelligent health monitoring network. We'll look at a basic remote healthcare setup where patients utilize health monitoring IoT devices. These gadgets will collect patients' health records, such as heart rate, body temperature, and sleeping habits. Any other individuals, such as healthcare workers, must be granted or denied, and we can achieve revoked data access by the patient through PoA. If a person requires medication, he may exchange his information with the medical practitioners of his choice. He can disable network file sharing once the treatment has ended. The suggested framework, seen in **Fig. 2**, consists of five stages: patient enrollment, data appending or retrieval across a blockchain-connected N2N channel, smart agreement deployment, patient records storage in the cloud, and proof of agreement (PoA).

### 4.1 Local Block Chain Network

Fig 1 shows the implementation of the local blockchain network, which uses the degree of care. The black thick line on the graph represents the primary private blockchain network. The hospitals or medical centers are responsible for maintaining the crucial network components and must sync with global databases. To keep their database up-to-date and accurate, the clinics merely need to synchronize with the nodes of the local blockchain network.

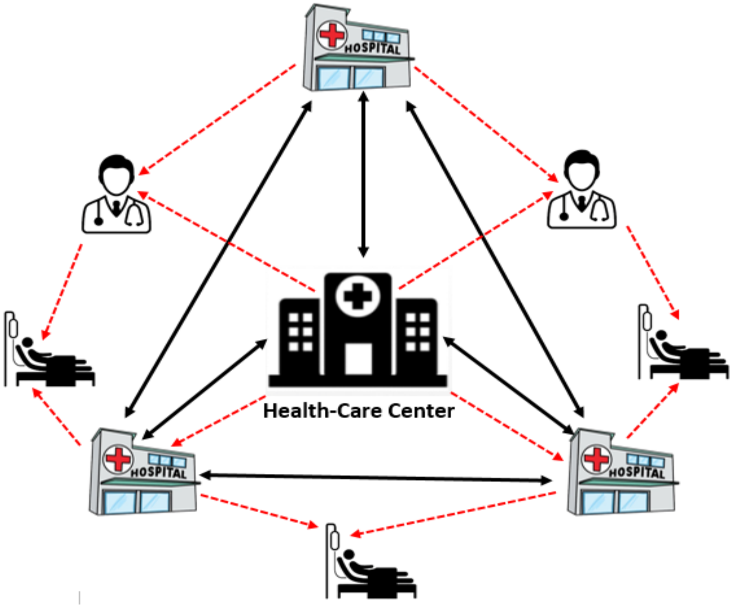

Fig. 1. Simple Local Block Chain Network Architecture

Red Dotted lines represent data queries from patients looking for medical records to the blockchain network. Since their network infrastructure can handle the high data traffic brought on by many requests, the primary blockchain network nodes in this situation (such as the hospital or healthcare center) manage the queries. Therefore, the speed and accuracy of the synchronization should be ensured as a central node in the blockchain network.

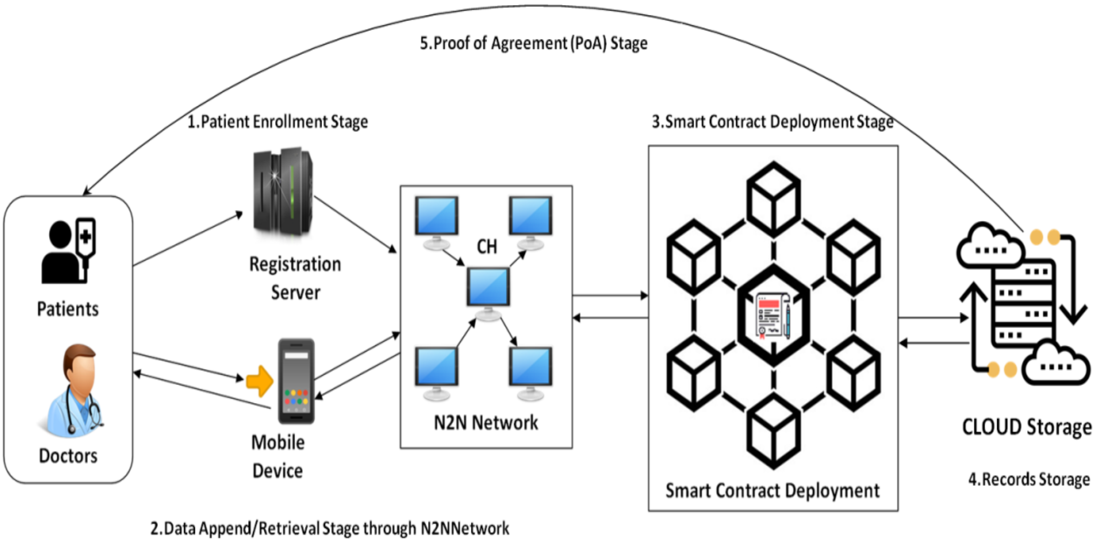
5.Proof of Agreement (PoA) Stage
1.Patient Enrollment Stage
3.Smart Contract Deployment Stage
Patients
Doctors
Registration Server
Mobile Device
CH
N2N Network
Smart Contract Deployment
CLOUD Storage
4.Records Storage
2.Data Append/Retrieval Stage through N2NNetwork

Fig. 2. Proposed BSDA-IoHT Architecture

### 4.2 Patient Enrollment Phase

Before seeing a physician, a new patient needs to enroll with the RS. Customers must submit their identification ($iP_t$), public key ($P_{tK_{pu}}$), and also the public key of physician(s) serving patients ($P_{nK_{pu}}$) via their tablet or smartphone because it is a one-time enrollment. We only examine one physician for the sake of clarity. Families can participate in the plan in the same way physicians can, with only viewing privileges. The RS then transmits ($iP_t$,$P_{tK_{pu}}$,$P_{nK_{pu}}$) to a BC via the N2N network, verified by the patients and the RS. First, it must be cross-verified that ($iP_t$ and$P_{nK_{pu}}$) are already transmitted to the BC. Next, the BC checks the patient's and RS's registrations and records ($iP_t$,$P_{tK_{pu}}$,$P_{nK_{pu}}$) over that N2N connected BC. **Table 1** depicts the notations and meanings.

**Table 1.** Notations and Meanings

| S.No | Notation | Meaning |
|---|---|---|
| 1. | $P_n$ | Physician / Doctor |
| 2. | $P_t$ | Patient |
| 3. | $k$ | Key |
| 4. | $En_k$ | Encryption Key |
| 5. | $De_k$ | Decryption Key |
| 6. | $K_{pu}$ | Public Key |
| 7. | $K_{pr}$ | Private Key |
| 8. | $iP_n$ | Physician Identity |
| 9. | $iP_t$ | Patient Identity |
| 10. | $R_s$ | Registration Server |
| 11. | $h(f)$ | Hash Function |
| 12. | $T_s$ | Time Stamp |
| 13. | $RP_t$ | Patient Record |
| 14. | $P_{nK_{pu}}$ | Physician Public Key |
| 15. | $P_{nK_{pr}}$ | Physician Private Key |
| 16. | $P_{tK_{pu}}$ | Patient Public Key |
| 17. | $P_{tK_{pr}}$ | Patient Private Key |
| 18. | $Ed_T$ | Encrypted Text / Cipher text |
| 19. | $G_d$ | Medical Gadgets |
| 20. | $\veebar$ , ǁ | XOR , Concatenation |

### 4.3 Data Block Append or Retrieval Phase

With the client's permission, the physician needs to rewrite/append patient record ($RP_t$) to the BC in this step. We assume that both the physician and the client have their Smartphone's ($G_d$) with healthcare software application installation. As a result, the physician encodes the information with a shared key that the client can deduce. Following that, the client verifies the encryption's correctness and, if it is, signs the encoded value. Ultimately, the physician signs the patient's consent and transfers the message to the BC. To become even more specific, this resulted in the following actions:

- Use $T_s$ to represent the present timing. The physician calculates M=m$P_t$ by determining m=$h\left(iP_n, P_{nK_{pr}}, T_s\right)$. The physician then calculates the symmetric cryptographic key $k$= m$P_{tK_{pu}}$and the symmetric encryption $Ed_T1$= $En_k(RP_t$,$T_s)$. The above value, along with T, and R, is communicated to the patients.
- In addition, the client can also calculate $k$= M$P_{tK_{pr}}$which can utilize to decode$Ed_T1$. The communication time compares to the physician's current details (in live time) to the patients.
- If the test is affirmative, the patient issues a signature using the formula $Ed_T2 = P_{tK_{pr}} h\left(iP_n \parallel P_{tK_{pu}} \parallel P_{nK_{pu}} \parallel Ed_T1 \parallel M \parallel T_s\right) \veebar kh(iP_t \parallel Ed_T1 \parallel M \parallel T_s)$ . Also, it calculates $K_s$=$kP_n$, which use to verify signatures. Finally, the patient transmits to the physician the outcome as a capsule CAP = ($iP_n$,$P_{nK_{pu}}$, $K_s$,$Ed_T1$ ,$Ed_T2$, $T_s$).
- Next, the physician verifies whether$Ed_T1$ ,$T_s$,$M$, $iP_t$, $P_{nK_{pr}}$, and $K_s$=$kP_n$ have not altered. Then, it transmits ($iP_t$, $P_{nK_{pr}}$,$T_s$, $M$, $K_s$, $Ed_T1$ ,$Ed_T2$) to that same BC if it is the scenario. Again, remember that it is unnecessary to confirm the signature's trustworthiness because the agreement's miners will be doing it.

The BC then takes different steps after obtaining the capsule:

- First, the BC seeks up the patient's shared key and the related enrollment agreement using the timestamp $T_s$.
- It then checks the equivalence $Ed_T2$ . $P_n$=$P_{tK_{pu}} h\left(iP_n \parallel P_{tK_{pu}} \parallel P_{nK_{pu}} \parallel Ed_T1 \parallel M \parallel T_s\right) \veebar kh(iP_t \parallel Ed_T1 \parallel M \parallel T_s)$ to ensure that the certificate and, consequently, this test verifies which data originated using patient $iP_n$ and that the physician with public key $P_{nK_{pu}}$ is participating.
- If true, the CAP capsule is saved on the BC.
- If a doctor suggests acquiring a patient's information in a proper time frame$T_f$, the physician will transmit ($iP_t$, $iP_n$, $T_f$) to the BC, certified by the physician.

Following the issuance of this information, the BC will take the necessary actions:

- The BC currently examines the$T_f$'s timeliness, the signature's legitimacy, and whether the patient has given the physician right to share the information (as stored on BC).
- If this is the case, it obtains all information for that time frame. CSR0= is the format of the message ($P_{tK_{pu}}$,$T_s$,$M$,$Ed_T1$,$Ed_T2$). Observe that $P_{tK_{pu}}$replaces$iP_t$, and $P_{nK_{pu}}$ is deleted from the recorded capsule because the physician previously knew it. The authenticity is verified by BC already, So it is adequate for the physician to calculate the password $k$ =$h$ ($P_{nK_{pr}}$, $T_s$)$P_{tK_{pu}}$and the simultaneous decoding of $Ed_T1$.

### 4.3 Deployment of Smart Agreement

Smart agreements are a BC-based transactional automating technology. It allows counterparties to define the conditions under which they can complete transactions electronically. We will use smart contracts in several different environments. Smart contracts, in additional terms, enable applications to manipulate a code on a BC system in a verifiable manner, allowing them to make various decisions without the use of the trust. Customers can put their trust straight within precise procedures and guarantees provided in a contract instead of related parties [25-28]. Each intelligent contract does have its location and identity on the

BC. As a result, it can keep all its state and claim ownership of assets on the BC, allowing it to operate as a trusted service. Smart agreements provide the system with an interface of activities that can activate by transmitting transactions to the agreement. Because it will store an agreement on the BC, every node may see and implement its commands and record every transaction. We can use a patient's information generated by an IoT gadget and medical professionals as two examples of entities who need the BC channel's trustworthiness [29-32]. Patients can also provide or remove access to personal information via various innovative agreements, as previously signed by both parties.

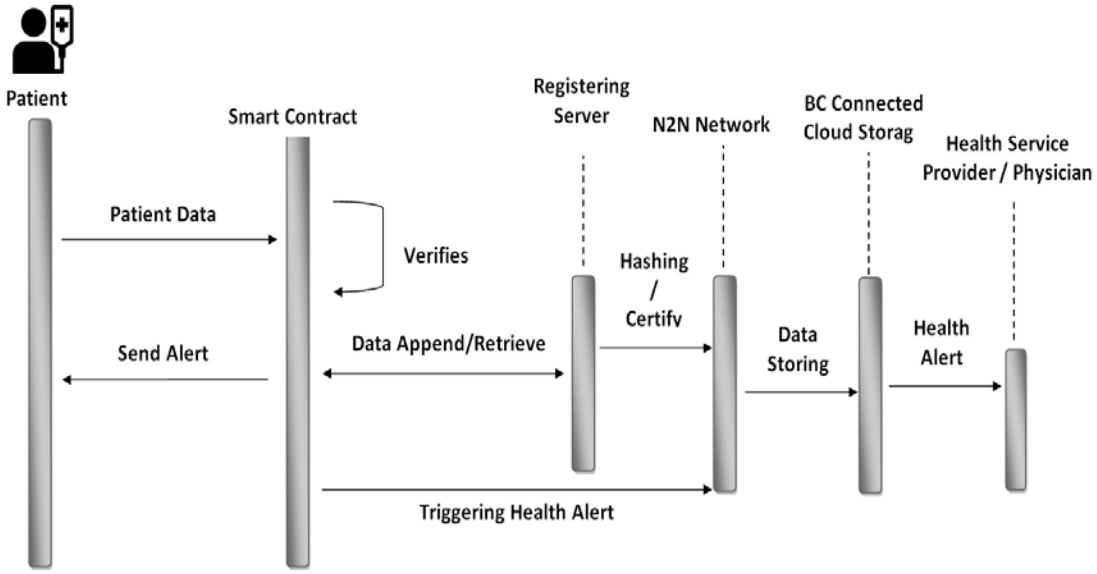

**Fig. 3.** Process Flow Diagram of Smart Contract Deployment

An agreement is activated when a condition is true and information transmits to the blockchain (**Fig. 3**). Try setting a constraint in the smart contract for the patient's peak and minimum sugar levels. If the measurement falls above or below the specified threshold, the smart contract will transmit a notification and information to the BC network. Let's imagine an IoT Sensor is used to track the sugar levels of patients. The patient's sugar levels will be measured regularly by an IoT device, and it will compare information to a smart contract, which might exchange between the Patient and Physician [26]. If a Physician requests that a notification be delivered if sugar levels exceed a specific limit, it records the activity and associated information to a central server by keeping the data hashing on a BC linked to the N2N connection. Finally, as part of the related smart contract, a medical warning is given to the Physician.

## 4.4 Cloud Storage

The information sent by patient gadgets is stored securely. For example, when a smart contract sends a network alarm, it sends pertinent healthcare information to the cloud. The nodes append a digital certificate to the health records before delivering it via the cloud. We are only transmitting data that goes beyond the prescribed Standard area in this case, not all information that an IoT healthcare gadget may generate. Next, the node verifies the digital signatures added to cloud storage. Cloud services will destroy data if the hash value and signature are incorrect or unavailable. Finally, the cloud servers organize the user's information into unique blocks and provide the block's hashes to the N2N network—a hashing of data that can use SHA to compute the hash. The source could be a large text, but the functions return a fixed length, such as 256 or 512 bits. We calculate the aggregate hashes of all data in the structure of a Merkle Tree when a single block involves multiple records or phrases. Merkle trees are a network of hashing that makes things simpler to authenticate data effectively, not a technique for storing data. Merkle trees additionally allow the customer to keep only the tree's base (combination hash), not just the complete history; thus, it will collect original information in the server while sending the cumulative hash to the BC network.

## 4.5 Proof of Agreement (PoA)

Proof of Agreement (PoA) is a class of permissions underlying blockchain techniques that gained popularity leading to enhanced efficiency over traditional Byzantine Fault Tolerant methods due to fewer communication links. We suggest a PoA at the very first for secure networks as an element of the Ethereum blockchain [33-35]. The regulators are a group of N trustworthy nodes that rely on PoA methods. Each authority is identifiable by a unique ID, and most sources, at least N2, are presumed to be reliable. To organize the transactions provided by patients, the regulators run an agreement. We use PoA methods for an extraction rotation framework, a commonly accepted approach to equitably disseminate the ownership of block creation between patients and physicians. Attempting to make it seem less computationally and power-efficient than that of the PoW mentioned above methodologies has gained attention in other blockchain application fields. PoA techniques are far more suitable for IoT devices than their PoW counterparts.

**Algorithm** 1 Algorithm of BDSA-IoHT

```
 if task(verify_rights)=true, Next
verify for the patient and physician
task(retrieve_address)
retrieve_address($RP_t$)
else
Close the transaction;
end if
Data Retrieve Module:
if task(smart_contract)=true, Next
retrieve_data — from the address($RP_t$)
return($RP_t$)
Send to the correct request_ID($iP_n$or$iP_t$)
end if
Data Append Module:
if task(smart_contract)=true, Next
append_data to the particular $RP_t$
return(1)
end if
Change permission Module:
Task(msg.sender==patient)
The patient can modify the physician's particulars or attach.
end task
```

# 5. SECURITY ANALYSIS

Now we'll demonstrate how our suggested technique can provide strong security characteristics.

## 5.1 Confidentiality

Only the patients at any had given time and the physician for a predetermined duration, as indicated in the RC agreement, must be allowed to access the personal health information. The information on the BC is in the form $(iP_t, P_{nK_{pr}}, T_s, M, K_s, Ed_T1, Ed_T2)$. First and foremost, due to ECDHP and ECDLP, this information is made so that only the doctor and patient can deduce the plaintext data. In this context, the physician's private key is $h(P_{nK_{pr}}, T_s)\ P_{tK_{pu}}$, while the patient's key is $P_{tK_{pr}}$R. Since the physician cannot keep all the varied random number of all interactions from multiple patients, we should utilize $h(P_{nK_{pr}}, T_s)$ instead of m. Second, only a physician who meets the requirements of the established agreement recorded on the BC can create such a communication. The physician cannot reproduce the signing request to the patients at a later stage due to the inclusion of the timeframe within the encrypted message [36-40].

## 5.2 Integrity

This property ensures that nobody ever may alter personal health information without the patient's permission. In addition, the integrity of the ciphertext is assured since the patient signs it. Before even being saved, the BC verifies the signature's authenticity. In reality, anybody with access to the patient's public key can verify the signature's authenticity, a characteristic known as public verification. The signature scheme offered is modeled on the Schnorr signature technique.

## 5.3 Authentication

If the person claiming to deliver the communication is accurate, the system provides authenticity. This functionality is intrinsically offered in this situation, especially using a signature-based approach to the well-known Schnorr signature technique. As a result, no one else can do a man-in-the-middle or impersonating threat.

## 5.4 Security Attacks

### 5.4.1 Impersonating Attacks

In IoHT networks, impersonating or identity theft refers to identities that utilize a person's name, image, or other identifying characteristics, such as patients' names or hospitals' logos, for malicious purposes. They are distinct from other acceptable representations of a person or entity, like websites, spoofs, and fake profiles [41]. Attackers mostly impersonate users via bogus accounts, sites, programs, and email accounts. The best defense tactics include using AI, email security measures, and regularly probing and testing corporate systems.

As mentioned in the previous description, this gives insight into how our suggested approach provides secrecy, integrity, and authenticity. We maintain patient confidentiality, and all doctor-patient communications should be encrypted using the cryptography technique. In the suggested algorithm, the patient randomly modifies all the transaction data every time an authentication session takes place. Additionally, a doctor randomly examines them, which can prevent data alteration and secure against impersonation attacks.

### 5.4.2 Stolen Verifier Attacks

The authentication system often keeps the verifications of users' credentials instead of users' actual credentials to limit the threats after it's stolen. The opponent who has acquired the proof for a passcode can employ the stolen-verifier attack to pretend to be that client. The stolen-verifier operation can use the brute-force password if patients use insecure credentials. Robust access control protocols can defend against dictionary attacks, but they may sometimes be immune to attacks with stolen verifiers [42].

In reality, the patient may access multiple servers using the same key $P_{tK_{pr}}$ R for his convenience. If a remote system insider gets his hands on $P_{tK_{pr}}$R, he might use the patient's login to access other servers. In our approach, the verifier instead gets $h(P_{nK_{pr}},T_s)$ during the verification process rather than the patient disclosing $P_{tK_{pr}}$R, to the remote system. However, it is challenging to deduce $P_{tK_{pr}}$R, from its hash value. Furthermore, the remote system doesn't keep a verifier table that attackers may exploit to acquire the patient key. The suggested method can therefore withstand stolen verifier attacks.

### 5.4.3 Replay Attacks

The key to preventing replay attacks is using the proper encryption technique. When the "keys" in encrypted communications decipher at the closing of communication, they allow access to the content. Whether the person who intercepted the initial message can see or interpret the key is irrelevant in a replay attack. They only need to copy everything, including the statement and key, and transmit it again [43-45]. To prevent this from happening, the transmitter and the recipient should create a session key that is purely unpredictable and must be used once per operation. Another way by adding timing information to all communications is another defense against this attempt. It limits the time it takes for attackers to listen, extract data, and resent them by preventing hackers from retransmitting information conveyed more recently than a predetermined amount of time.

From an integrity standpoint, In our mechanism, every communication between patient and doctor has a timestamp and hashes for every other field it includes. In addition, all transactions are linked because every block has a hash connecting it to the block preceding it, preventing replay attacks.

## 6. Performance Analysis

### 6.1 Scalability

Because it is a personal blockchain, the entire procedure takes less time than the current network. It is measured based on transactional responsiveness. The average lifespan for creating the new block is roughly 10 seconds, which is also the case for smart contract transactions. It requires 32 seconds for verification, although this varies on the gas price. After validation, it takes 75-120 seconds to produce the following several blocks. It takes 60 seconds to retrieve the information and 1-2 minutes to update the information, depending on the information.

### 6.2 Access control

In the smart contract, the individual makes decisions about network access suggestions. If a third party or an unknown person attempts to enter the platform, the intelligent agreement will deny the transaction and end the scheme.

**Table 2.** A comparison between the suggested approach with different properties of existing systems

| Feature | [37] | [38] | [39] | [40] | [41] | BSDA-IoHT |
|---|---|---|---|---|---|---|
| Access Control | A | A | A | A | A | A |
| Confidentiality | UA | A | A | UA | A | A |
| Integrity | UA | A | A | A | A | A |
| Patient/Doctor Authentication | UA | UA | A | A | A | A |
| Scalability | A | UA | A | A | UA | A |

## 6.3 Integrity

Integrity is crucial between the patient and the smart agreement. Because the patient has previously signed the agreement, no one else can edit or alter the conformity. In our situation, the physician/3rd parties cannot update or modify the intelligent contract agreement. **Table 2** compares the attributes of our current proposal to those of other blockchain-based health services now in use. In contrast, we have two assessment alternatives: A- Available (it is reliable and available) and UA- Unavailable (it does not have the functionality).

The suggested BDSA-IoHT technique, which uses blockchain mechanisms to efficiently share health records in storage servers, is presented in a tabular and graphical format. The proposed process evaluates how efficient it is to share patient records via an N2N network in a blockchain-connected cloud storage with various factors [46]. In addition, the suggested method compares throughput, service delay, and processing time with existing approaches.

## 6.4 Throughput

The absolute number of health information effectively communicated with the patient and physician in a given time is known as throughput ($\mathrm{T}^{h}$). **Eq. 1** describes the suggested strategy as a mathematical equation for throughput. We compute throughput as follows:

$$\mathrm{T}^{h} = \frac{\sum_{r=0}^{n} RP_t(n)*S}{1000} \tag{1}$$

Where, $RP_t(n)$ is the number of patient record shared securely and S is the Size of Record.

## 6.5Service Delay

Service delay is the difference between receiving a request and receiving a response during health information exchanges. In **Eq. 2**, the suggested method defines a computational formula for service delay. Service Delay($\mathrm{S}^{d}$) is measured as follows:

$$\mathrm{S}^{d} = \sum_{r=0}^{n} \mathrm{T}^{n} r(Req) - \mathrm{T}^{n} r(Rec) \tag{2}$$

Where, $\mathrm{T}^{n} r(Req)$is the Transaction Request,$\mathrm{T}^{n} r(Rec)$ is the Transaction received and r = 0….n.

Table 3. A Comparison of Throughput

| Throughput (%) | | | |
|---|---|---|---|
| Data Size | SEHRTB | MedBloc | BDSA-IoHT |
| 100 | 92.7 | 94.5 | 95.75 |
| 200 | 89.4 | 91.2 | 94.4 |
| 300 | 88.6 | 90.6 | 93.8 |
| 400 | 87.4 | 89.3 | 93.2 |
| 500 | 88.1 | 89.5 | 92.3 |
| 600 | 86.5 | 88.7 | 91.7 |
| 700 | 86.2 | 88.1 | 91.1 |
| 800 | 87.3 | 87.6 | 90.5 |
| 900 | 86.4 | 87.2 | 89.7 |
| 1000 | 86.5 | 87.5 | 89.32 |

## 6.6 Processing Time

The proposed method is described in Eq. 3 as a mathematical equation for processing time. We compute processing time by multiplying the number of patient records by the mean retrieval time for healthcare data. ${T_s}^{rt}$ is the mean retrieval time for patient medical history, and $RP_t(n)$ is the total medical records. In a tabular manner, Table 3, 4 and 5 shows the simulation results of the SEHRTB algorithm and existing techniques.

$$\mathrm{P}^{T} = \sum_{r=0}^{n} RP_t(n) * {T_s}^{rt} \qquad (3)$$

The comparison of other existing methods such as SEHRTB, MedBloc, and our technique BDSA-IoHT is in Fig. 4, 5 and 6.

Table 4. A Comparison of Service Delay

| Service Delay (s) | | | |
|---|---|---|---|
| Data Size | SEHRTB | MedBloc | BDSA-IoHT |
| 100 | 92.7 | 94.5 | 95.75 |
| 200 | 89.4 | 91.2 | 94.4 |
| 300 | 88.6 | 90.6 | 93.8 |
| 400 | 87.4 | 89.3 | 93.2 |
| 500 | 88.1 | 89.5 | 92.3 |
| 600 | 86.5 | 88.7 | 91.7 |
| 700 | 86.2 | 88.1 | 91.1 |
| 800 | 87.3 | 87.6 | 90.5 |
| 900 | 86.4 | 87.2 | 89.7 |
| 1000 | 86.5 | 87.5 | 89.32 |

**Table 5.** A comparison of Processing Time

| Processing Time (s) | | | |
|---|---|---|---|
| **Data Size** | **SEHRTB** | **MedBloc** | **BDSA-IoHT** |
| 100 | 92.7 | 94.5 | 95.75 |
| 200 | 89.4 | 91.2 | 94.4 |
| 300 | 88.6 | 90.6 | 93.8 |
| 400 | 87.4 | 89.3 | 93.2 |
| 500 | 88.1 | 89.5 | 92.3 |
| 600 | 86.5 | 88.7 | 91.7 |
| 700 | 86.2 | 88.1 | 91.1 |
| 800 | 87.3 | 87.6 | 90.5 |
| 900 | 86.4 | 87.2 | 89.7 |
| 1000 | 86.5 | 87.5 | 89.32 |

Finally, based on an assessment of different metrics such as throughput (percent), service-delay(s), and processing-time(s) for clinical outcomes of different sized, our technique claims that the suggested BDSA-IoHT technique delivers the best result against previous approaches.

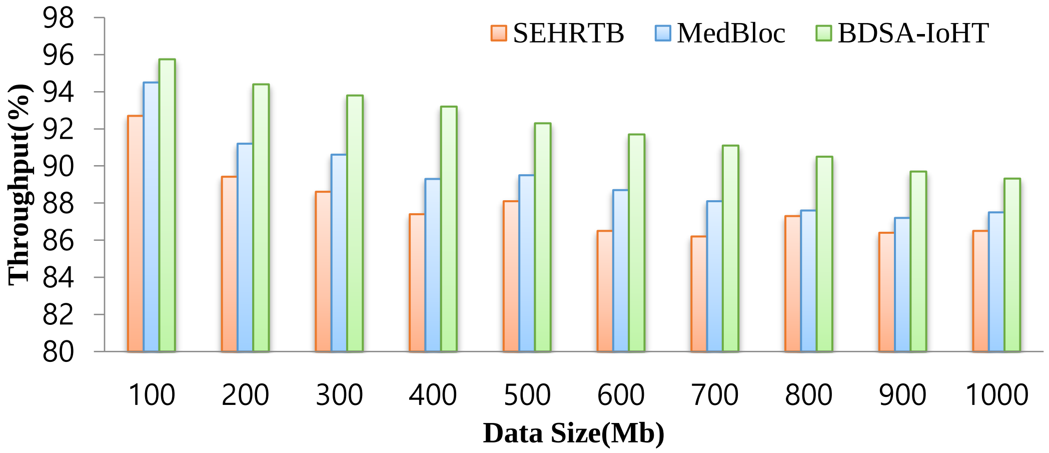

**Fig. 4.** Comparison of Throughput

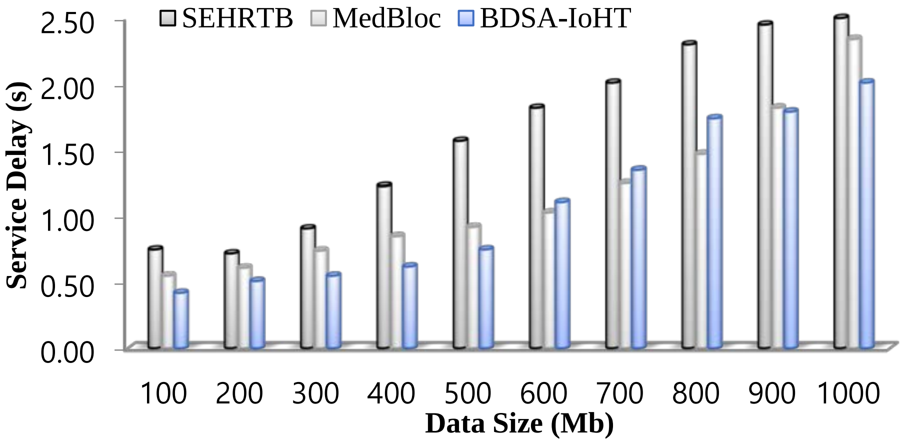

**Fig. 5.** Comparison of Service Delay

The preceding diagrams demonstrate that our BDSA-IoHT method efficiently maintains processing time. The BDSA-IoHT secures health record transactions and manages access to health records stored and processed on storage platforms. The BDSA-IoHT eliminates 2.01 seconds of service delay and 1.9 seconds of processing time and enhances efficiency by nearly 30%. Finally, our findings reveal that the proposed BDSA-IoHT method outperforms all other algorithms on all model checking and input datasets.

Our findings identified that our work is more robust than any other security method. Our security model met the confidentiality, authentication, and integrity, but we need to focus on various attacks like stolen-verifier attacks and replay attacks. We will do in our future work all these attack mitigations. Our entire model relies on intelligent agreement, and we use blockchain for communication with a data hashing method.

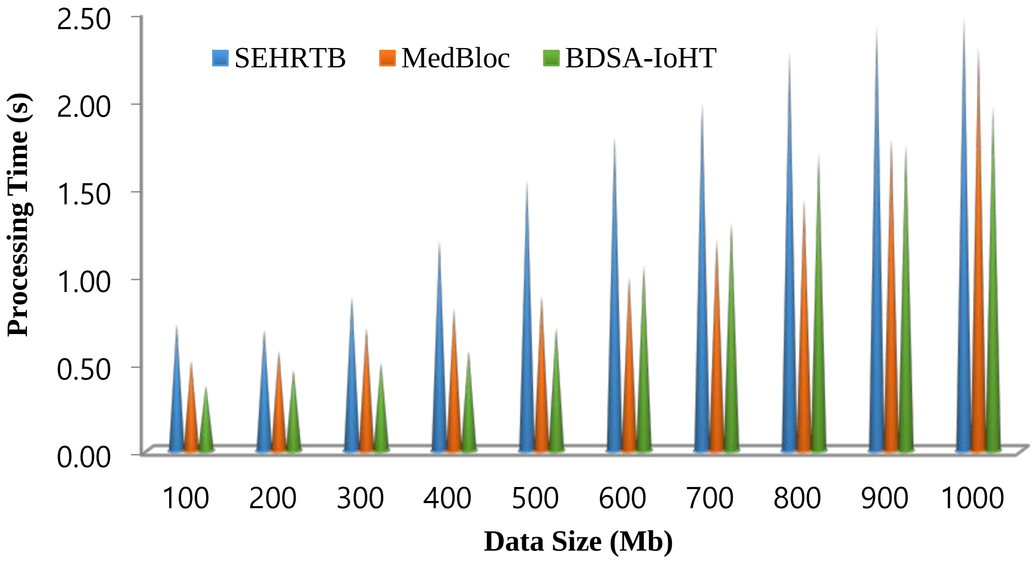

**Fig. 6.** Comparison of Processing Time

## 6. Conclusion and Future Enhancement

Incorporating blockchain technology into IoT is not a manageable undertaking, and such approaches face numerous challenges. As a result, the advantages of using blockchain-based IoT systems must be carefully considered and approached with prudence. Our suggested blockchain-based IoT paradigm eliminates these barriers. It addresses most security and privacy concerns while considering the resource limits that so many IoT devices face.

Blockchain in healthcare systems has created enormous advantages, not just in terms of secure and efficient data storage, exchange, and accessibility, but also in producing a great potential in the medical industry for many stakeholders. The main goal of this study is to use blockchain techniques to construct a secured data accessibility method for present medical systems. We also examined if our suggested approach can meet confidentiality, integrity, and authenticity conditions. We've also offered a possible intelligent contract arrangement in light of this healthcare circumstance. In the future, it would be fascinating seeing this concept evaluated in a controlled research context to assess the system's overall performance. We'll keep this in mind for future projects. The goal of this project was to see if we could use the method to quantify patient involvement. In addition, the project aims to plan the procedure within the same free and open-source platform for future evolution.

## References

[1] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, February 2018. Article (CrossRef Link).

[2] N. Kshetri, "Can blockchain strengthen the internet of things?," *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017. Article (CrossRef Link).

[3] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017. Article (CrossRef Link).

[4] Manzoor, Y. Hu, M. Liyanage, P. Ekparinya, K. Thilakarathna, G. Jourjon, A. Seneviratne, S. Kanhere, and M. E. Ylianttila, "Demo: A Delay-Tolerant Payment Scheme on the Ethereum Blockchain," in *Proc. of 19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2018)*, 2018. Article (CrossRef Link).

[5] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Computer Science*, vol. 113, pp. 73 – 80, 2017. Article (CrossRef Link).

[6] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. of 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, Sept 2016. Article (CrossRef Link).

[7] A. M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in *Proc. of 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, pp. 5–8, Feb 2016. Article (CrossRef Link).

[8] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *Proc. of Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*, IEEE, pp. 1–6, 2016. Article (CrossRef Link).

[9] A. Yksel, A. Kp, and znur zkasap, "Research issues for privacy and security of electronic health services," *Future Generation Computer Systems*, vol. 68, pp. 1 – 13, 2017. Article (CrossRef Link).

[10] A. Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, "On blockchain and its integration with iot. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173-190, 2018. Article (CrossRef Link).

[11] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26 521–26 544, 2017. Article (CrossRef Link).

[12] A. D. Dwivedi, P. Morawiecki, and G. Srivastava, "Differential cryptanalysis of round-reduced speck suitable for internet of things devices," *IEEE Access*, vol. 7, pp. 16 476–16 486, 2019.Article (CrossRef Link).

[13] A. Azeta, D. O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, "Implementing a medical record system with biometrics authentication in e-health," in *Proc. of 2017 IEEE AFRICON*, pp. 979–983, Sept 2017. Article (CrossRef Link).

[14] D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, 2019. Article (CrossRef Link).

[15] Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative ddos mitigation with smart contracts," in *Proc. of IFIP International Conference on Autonomous Infrastructure, Management and Security*, pp. 16–29, 2017. Article (CrossRef Link).

[16] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *Proc. of Advanced Communication Technology (ICACT), 2017 19th International Conference on*, IEEE, pp. 464–467, 2017. Article (CrossRef Link).

[17] W. Liu, S. Zhu, T. Mundie, and U. Krieger, “Advanced blockchain architecture for e-health systems,” in *Proc. of e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on*, IEEE, pp. 1–6, 2017. Article (CrossRef Link).

[18] Y. Hanada, L. Hsiao, and P. Levis, “Smart contracts for machine-tomachine communication: Possibilities and limitations,” in *Proc. of 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*, IEEE, pp. 130–136, 2018. Article (CrossRef Link).

[19] N. Kahani, K. Elgazzar, and J. R. Cordy, “Authentication and access control in e-health systems in the cloud,” in *Proc. of 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 13–23, April 2016. Article (CrossRef Link).

[20] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain,” 2018.

[21] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, “Identity privacy preserving biometric based authentication scheme for naked healthcare environment,” in *Proc. of 2017 IEEE International Conference on Communications (ICC)*, pp. 1–7, May 2017. Article (CrossRef Link).

[22] A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, “Systas: Density-based algorithm for clusters discovery in wireless networks,” in *Proc. of 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, IEEE, pp. 2126–2131, 2015. Article (CrossRef Link).

[23] Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, IEEE, pp. 618–623, 2017. Article (CrossRef Link).

[24] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for iot,” in *Proc. of the Second International Conference on Internet-of-Things Design and Implementation*, ACM, pp. 173–178, 2017. Article (CrossRef Link).

[25] Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, “Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues,” *IEEE Access*, vol. 6, pp. 17 246–17 263, 2018. Article (CrossRef Link).

[26] A. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. K. R. Choo, “Blockchain: A panacea for healthcare cloud-based data security and privacy?,” *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan 2018. Article (CrossRef Link).

[27] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, “Applying software patterns to address interoperability in blockchainbased healthcare apps,” *arXiv preprint arXiv:1706.03700*, 2017. Article (CrossRef Link).

[28] Dhinakaran, D., Prathap, P.M.J, "Protection of data privacy from vulnerability using two-fish technique with Apriori algorithm in data mining," *The Journal of Supercomputing*, 78(16), 17559–17593, 2022.Article (CrossRef Link).

[29] G. Gomathy, P. Kalaiselvi, D. Selvaraj, D. Dhinakaran, A. T. P and D. Arul Kumar, "Automatic Waste Management based on IoT using a Wireless Sensor Network," in *Proc. of 2022 International Conference on Edge Computing and Applications (ICECAA)*, pp. 629-634, 2022. Article (CrossRef Link).

[30] M. Wohrer and U. Zdun, “Smart contracts: security patterns in the ethereum ecosystem and solidity,” in *Proc. of Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop on*, IEEE, pp. 2–8, 2018. Article (CrossRef Link).

[31] Jena Catherine Bel D, Esther C, Zionna Sen G B,Tamizhmalar D, Dhinakaran D, Anish T. P, "Trustworthy Cloud Storage Data Protection based on Blockchain Technology," in *Proc. of 2022 International Conference on Edge Computing and Applications (ICECAA)*, pp. 538-543, 2022. Article (CrossRef Link).

[32] B. Murugeshwari, D. Selvaraj, K. Sudharson and S. Radhika, "Data mining with privacy protection using precise elliptical curve cryptography," *Intelligent Automation & Soft Computing*, vol. 35, no.1, pp. 839–851, 2023. Article (CrossRef Link).

[33] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “Bbds: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, p. 44, 2017. Article (CrossRef Link).

[34] D. Dhinakaran, and P. M. Joe Prathap, "Preserving data confidentiality in association rule mining using data share allocator algorithm," *Intelligent Automation & Soft Computing*, vol. 33, no. 3, pp. 1877–1892, 2022. Article (CrossRef Link).

[35] R. Zhang, R. Xue and L. Liu, "Security and Privacy for Healthcare Blockchains," *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3668-3686, 2022. Article (CrossRef Link).

[36] K. Sudharson, A. M. Sermakani, V. Parthipan, D. Dhinakaran, G. Eswari Petchiammal and N. S. Usha, "Hybrid Deep Learning Neural System for Brain Tumor Detection," in *Proc. of 2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1-6, 2022. Article (CrossRef Link).

[37] Dhinakaran, D., Selvaraj, D., Udhaya Sankar, S.M., Pavithra, S., Boomika, R., “Assistive System for the Blind with Voice Output Based on Optical Character Recognition,” in *Proc. of International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems*, pp. 1-8, 2023. Article (CrossRef Link).

[38] Jin, H., Xu, C., Luo, Y., Li, P, “Blockchain-Based Secure and Privacy-Preserving Clinical Data Sharing and Integration,” in *Proc. of ICA3PP 2020 Algorithms and Architectures for Parallel Processing*, pp. 93-109, 2020. Article (CrossRef Link).

[39] D. Dhinakaran, M. R. Khanna, S. P. Panimalar, A. T. P, S. P. Kumar and K. Sudharson, "Secure Android Location Tracking Application with Privacy Enhanced Technique," in *Proc. of 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, pp. 223-229, 2022. Article (CrossRef Link).

[40] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, “Metrics for assessing blockchain-based healthcare decentralized apps,” in *Proc. of 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–4, Oct 2017. Article (CrossRef Link).

[41] K. Sudharson and S. Arun, "Security protocol function using quantum elliptic curve cryptography algorithm," *Intelligent Automation & Soft Computing*, vol. 34, no.3, pp. 1769–1784, 2022. Article (CrossRef Link).

[42] S.M. Udhaya Sankar, D. Dhinakaran, C. Cathrin Deboral, M. Ramakrishnan, "Safe Routing Approach by Identifying and Subsequently Eliminating the Attacks in MANET," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 219-231, 2022. Article (CrossRef Link).

[43] Mubarakali, A., Bose, S.C., Srinivasan, K. et al., “Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain,” *J Ambient Intell Human Comput*, 2019. Article (CrossRef Link).

[44] Chukwu and L. Garg, "A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations," *IEEE Access*, vol. 8, pp. 21196-21214, 2020. Article (CrossRef Link).

[45] Dhinakaran D, Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B, "Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing," *International Journal of Engineering Trends and Technology*, vol. 70, no. 3, pp. 284-294, 2022. Article (CrossRef Link).

[46] Huang, J., Qi, Y.W., Asghar, M.R., Meads, A., Tu, Y.-C., “Sharing medical data using a blockchain-based secure EHR system for New Zealand,” *IET Blockchain*, 2, 13– 28, 2022. Article (CrossRef Link).

**EZIL SAM LENI** A received B.E. degree in Computer Science and Engineering from Bharathiar University, India, and M.E and Ph.D. degrees in Computer Science and Engineering from Sathyabama Institute of Science and Technology, India. She was an Assistant Professor, in the Department of Computer Science and Engineering from 1997 to 2010. Since 2010 January she has been with JEPPIAAR SRR Engineering College as a Professor in the Department of Computer Science and Engineering. She is currently working as a Professor in the Department of Computer Science and Engineering, KCG College of Technology, India. She has published many papers in refereed journals and international conferences. Her main research interests include Wireless and Mobile Networks, Distributed Systems, Information Retrieval Techniques, Machine Learning models in Image Processing, Text Mining, and Sentiment Analysis.

**Dr. Shankar R.**, has completed his Bachelor of Engineering in Electronics and Communication Engineering (ECE) from Bharathidasan University, Tiruchirapalli, Tamil Nadu, India. He acquired his Master of Technology in ECE from Pondicherry Engineering College. He accomplished his Doctor of Philosophy in ECE from Pondicherry University, Pondicherry. He has around 22 years of experience in the field of teaching and research. He has published various research papers in 12 International Conferences, 4 National Conferences, 23 indexed international journals, 10 patents and 6 books. His areas of interest are Electromagnetics, Microprocessors, Mobile Communication, Computer Networks, Wireless Communication (WC), 6G and beyond WC, Soft computing, IoT, Cyber Security, Machine and Deep Learning. He is a life member of Indian Society for Technical Education and Institution of Engineers.

**Dr. R. Thiagarajan** is working as an Assistant Professor in Department of Computer Science and Engineering, Prathyusha Engineering College. He received his Ph.D. degree under the Faculty of Information and Communication Engineering in Anna University, Chennai, India, in 2020. He pursued his Bachelor degree from Anna University and Master's in Computer Science and Engineering from Dr. M.G.R University, Chennai. His research interests include Wireless Adhoc Networks, Network Security, Machine Learning and Deep Learning techniques. He is a Life time Professional body member of CSI, ISTE.

**Vishal Ratansing Patil** received B.E. degree in Computer Engineering from North Maharashtra University, India, and M.Tech in Software System from Rajiv Gandhi Prodyogiki Vishwavidyala and Ph.D. degrees in Computer Science and Engineering from Madhyanchal professional University, Bhopal, India. He was an Assistant Professor, in the Department of Computer Engineering from 2011 to 2021 Since 2011 November he has worked for many colleges like Sardar patel Institute of engineering, KJ Somaiya Institute of Engineering, Usha Mittal Institute of Engineering College as a Assistant Professor in the Department of Computer Engineering. He is currently working as a Associate Professor in the Department of Computer Engineering, Rizvi College of Engineering, India. He has published many papers in refereed journals and international conferences. His main research interests include Deep learning, Machine Learning., Cloud computing, Blockchain, Data science etc.