ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 12 N. 1 (2023), e28612
eISSN: 2255-2863
DOI: https://doi.org/10.14201/adcaij.28612

# Healthcare Data Collection Using Internet of Things and Blockchain Based Decentralized Data Storage

M. Sumathi[a], S. P. Raja[b], N. Vijayaraj[c] and M. Rajkamal[d]

[a] Assistant Professor, School of Computing, SASTRA Deemed to be University, Thanjavur, Tamil Nadu.
[b] Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.
[c] Associate Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sangunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.
[d] Application Developer, IBM Bangalore, Karnataka, India.
sumathi@it.sastra.edu, avemariaraja@gmail.com,vijaycseraj@gmail.com, rajkamalmurugasean@gmail.com

KEYWORDS

*blockchain; IoT; cloud; cryptography; SHA256; healthcare; certificateless access*

ABSTRACT

*With the increase in usage of Internet of Things devices (IoT), IoT is used in different sectors such as manufacturing, electric vehicles, home automation and healthcare. The IoT devices collected large volumes of data on different parameters at regular intervals. Storing a massive amount volume of IoT data securely is a complicated task. Presently, the majority of IoT devices use cloud storage to store the data, however, cloud servers require large storage and high computation. Due to third party cloud service provider (CSP) interaction, the management of IoT data security fully depends on the CSP. To manage these problems, a decentralized blockchain based secure storage is proposed in this work. In the proposed scheme, instead of CSP storage location, the patient health information is stored in the blockchain technique and the blockchain miners verify the transactions with the help of Elliptic Curve Cryptography (ECC). The miner verification process dynamically avoids adversary access. Similarly, the certificateless access is used in the proposed system to avoid certificate based issues. The blocks in the blockchain is going to be stored patient details in a decentralized storage location to avoid unauthorized access and ensure the authenticity of data. The use of blockchain eliminates the need for third party public auditing process through immutable storage. This work illustrates secure communication and immutable data storage without the intervention of CSP. The communication overhead reduced by nearly 10 to 40% and authentication improved by 10 to 20% while confidentiality increased by 5% in comparison to existing techniques. Through this technique, data confidentiality, integrity and availability is ensured.*

# 1. Introduction

Internet of Things (IoT) consists of network of physical objects which are used to collect data in healthcare, agriculture, smart home, electric vehicles, manufacturing and other sectors, at frequent time intervals. IoT sensors produce a massive volume of data in different variables. Currently, IoT data is stored in cloud storage. However, cloud storage leads to unprotected storage and unauthorized access (Sumathi *et al.,* 2018). This is because in cloud storage, data are collected and stored in distributed servers. These servers are managed and controlled by third party CSP. This has drawbacks, namely, unprotected storage and adversaries (Ã) access. Specifically, healthcare data contains highly sensitive personal and disease information of the patient. The primary task of healthcare organization is to protect the patient's sensitive information. To satisfy this requirement and to overcome the cloud storage issues, a decentralized blockchain (BC) storage structure has been used in this work. The BC provides an efficient platform for the protection and distributed storage of sensitive data (Sumathi *et al.,* 2021).

The BC stores information in a block in an ordered manner. The element of a BC is a block. A block is a logical unit which holds the information. Hence, it would be impossible for Ã to modify, manipulate or hack the blocks. A BC contains a distributed digital public ledger of transactions which are available to the entire network on the BC in a sequential order. The proposed work, BC acts as a medium between IoT devices and storage structure, which ensures data security and immutability. In a BC, every node has previous block hash value (PBHV) which, if tampered, can change the hash of every block. So, every user is notified of a change in data and therefore verifies the change. BC offers high level security to patient sensitive information (Sumathi *et al*., 2020). In a BC, a block can add data but cannot alter it. The major benefits of BC technique are greater transparency enhanced security and authentication, certificateless cryptography, no central server, true traceability, high efficiency, efficient data management, and improved speed. Hence, BC is a preferable technique for the handling of sensitive data in all sectors. Likewise, the limitations of the BC technique are limited system capacity, no feedback mechanism, no optimized storage, scalability and complex structure. To overcome these limitations, new techniques are used in the BC technique (Ruinian Li *et al.,* 2019).

Two different types of BC networks are used for storing the user information such as public and permissioned BC. In a public BC network anyone can participate in the transaction and is able to access the information. In this network, the immutability property is maintained; however, the user's information is not protected from others. Likewise, the winner is able to create the next block and add it to BC ledger. No one can control the block creation and updating of ledger. In a permissioned BC, the network is created between the registered and authorized users only. The unauthorized users are unable to participate in the permissioned network. Likewise, only the registered users are able to create and add a block to the BC network. Hence, data immutability and security are maintained in the permissioned BC network. Due to these benefits, the permissioned BC network has been constructed between the authorized users in the proposed work. At present in healthcare sectors, the treatments are dependent on the individual expert knowledge of a particular organization, not dependent on the experts of other organization. This system works well for normal cases, not for emergency cases. In cases of emergency, the patient's life is dependent on the availability of experts. The unavailability of experts increases disease complexity or leads to patient death. Hence, an inter organization collaboration is required. The primary requirement of BC network is that, minimally, fifty percent of members should be active in a network to verify the information which is shared in the network. In emergency cases, the information is updated in the BC network. Then, the information is immediately verified by experts and is shared with the requester. This requirement is achieved thanks to BC technology. Hence, the BC technology is of preference among the healthcare organizations.

The overall organization of the proposed work is as follows: In section 2, the existing techniques have been discussed with their merits and demerits. In section 3, the proposed technique is explained with the necessary architecture and algorithm. The experimental results of the proposed technique are explained in section 4. In section 5, conclusions are drawn regarding the proposed technique and its future enhancement is discussed.

# 2. Related Work

In this section, the latest literature regarding IoT based healthcare data collection and storage challenges are discussed with possible solutions and limitations.

## IoT Based Data Collection and Processing

Lo ai Tawalbeh *et al.* (2022). had focused the edge enabled IoT system on healthcare. In an IoT based healthcare data collection multiple factors are affecting the communication security, storage, power consumption, latency, transmission, monitoring, data integrating and computation. The power consumption and latency are the key factors for selecting the sensors, gateway and network topology. Waleed Noori Hussein *et al.* (2022). proposed the usage of cloud and IoT in healthcare applications. Cloud and IoT were combined to analyze the health data of the patient. Several issues had to be considered when combining the cloud and IoT devices, given the multiple IoT services offered by cloud computing. Hence, the careful selection of IoT devices plays a vital role in IoT implementation. Prajoona Valsalan *et al.* (2020). proposed the IoT based data collection system based on wearable sensors and mobile phones from the remote locations. Basic health information such as temperature, heartbeat and pressure have been measured by the wearable devices and transferred to health centers. Through this process, the doctors are able to diagnose the diseases from the remote areas.

Tamilselvi *et al*. (2020). had discussed the IoT based health monitoring system using smart sensors. The sensors had been used to collect the eye blink, heartbeat and temperature of the patients. The collected information had been stored in a cloud based storage location and smart phones had been used for information transfer. Mohd. Hamim *et al*. (2019). used IoT sensors in the remote health monitoring system for patients. The skin response sensor, temperature sensor and heart pulse sensor have been used to measure the patient health conditions. For continuous real time database updation, the collected information was transferred to cloud storage. The IoT sensors are assembled in the wearable devices for the collection of patient data. This process has been helpful to monitor the remote location of patients in an efficient way. Shivam Gupta *et al.* (2017). proposed the IoT based health monitoring system. The proper and timely monitoring process is possible through the IoT devices. The IoT devices monitor the patient health condition continuously and collect the information from the patient. The collected information was transferred to doctors so that immediate remedy could be provided to the patient.

## Data Storage Using Blockchain Techniques

Ruinian Li *et al*. (2019). proposed the BC based large scale IoT data protection technique. The cloud data storage issues were overcome thanks to the use of BC and cryptographic techniques. BC provides an efficient storage structure for storing the data in a distributed way. The cryptographic algorithm provides an efficient authentication system through BC for IoT based data storage. Rekha Goyal *et al*. (2020). had used the BC based data storage with privacy and authentication in IoT. The difficulty associated with protecting IoT data in face of illegal network access has been discussed. In addition, the efficiency of secure data storage has been considered as it is very low in terms of data management and secures algorithms. Therefore, secure communications in a wireless sensor network were enabled by a decentralized BC network which was integrated with authentication and privacy preserving scheme.

Mingxin ma *et al*. (2019). discussed the privacy oriented BC based on a distributed key management architecture (BDKMA) for hierarchical access control in the IoT scenario. The BDKMA uses fog computing to reduce the latency and multichain BC operated in the cloud. This scheme has achieved highly decentralized, scalable and extendable requirements. Moreover, the authors discussed the achievement of fine-grained auditability with privacy preserving principles by using BC for hierarchical access control in IoT. Alia Al Sadawi *et al*. (2021). analyzed the integration of BC with IoT to eliminate challenges and enhance the performance. IoT plays a vital role in healthcare, agriculture, banking, smart girds and supply chain management. The major problems and challenges faced by IoT systems are authenticity, reliability, security and scalability. These challenges are overcome by BC. The author evaluated the latest implementation stages and the position of current researches in merging BC with IoT networks. Also, the issues associated to the IoT-BC integration had been discussed.

Ch. V. N. U Bharathi Murthy *et al*. (2020). had discussed the BC based cloud computing research challenges and architecture. The BC has been used to resolve the issues faced by cloud computing. An architecture integrating cloud and BC was developed to derive the meaningful communication between the two technologies. Guipeng Zhang *et al*. (2022). had proposed the BC-based e-health management system. The pairing based cryptographic technique was used to provide tamper proof record maintenance. This tamper proof record maintenance avoids the illegal modification and access. The BC payment transaction was also discussed. Marah R. Bataineh *et al*. (2022). had discussed the BC framework in health applications. The IoT data has been collected from different locations and distributed evenly in the BC network. Thin and rich clients have been used for the load balancing process. The data collection and access have been done by both the clients and an analysis was performed on the rich client only. This technique effectively manages the difficulties associated with IoT. Hemant B. Mahajan *et al*. (2023). proposed the healthcare 4.0 for storing the e-health record in BC. The health information was collected from the IoT devices and stored in the fog layer. The fog storage reduces security and processing overhead of cloud. The less sensitive and high volume data was stored in the cloud. The meta-data and log information was stored in the BC network to avoid different types of vulnerable activities.

## Motivation and Justification of the Proposed Work

The motivation of the proposed work is to store the highly sensitive healthcare data in a decentralized BC providing interorganizational access to members, providing a quick response to care takers at the time of emergency cases. The key advantages of the BC storage are to provide immutable storage, dynamic access control and to prevent third parties from managing the stored data. The BC network is created with the registered members and BC miners. Whenever a new transaction is established by the member, the miner verifies the transaction based on existing registration and allows the transactions. When a transaction is successfully completed, a block is created and added to the BC network. So that it is visible to the members involved in the network and the miner receives a reward. Through this process, the data availability is ensured to all the registered users and data integrity is ensured through the immutable storage.

Another requirement of healthcare data is to provide data security to patient information. It is an essential and foremost requirement in healthcare. Hence, the patient information is encrypted by ECC based encryption process and transfer to receiver. Thus, data confidentiality has been achieved in the proposed system.

## Contribution

The novelty of the proposed work is listed as follows: In the present cloud based storage technique, all are able to store and access the information without any restriction and it is managed by CSP. In the proposed work, the IoT devices and members must register prior to becoming involved in the transaction and accessing the information on the network. This process, prevents the involvement of unauthorized parties and ensures data availability to authorized users without access denial. The analysis of the related work evidences the many security issues of cloud storage, including CSP data management and access. Hence, there is a growing trend to use BC-based data storage in different sectors. This tendency has motivated us to make this proposal. In the proposed work the healthcare information is fully stored and managed in the BC to provide fully decentralized storage and prevent third party involvement. The existing cloud storage does not provide complete confidentiality, integrity and authenticity to user data. In the proposed system, the information stored in a block is encrypted by random key based ECC encryption technique which ensures data confidentiality and the immutability of BC for data integrity and decentralized storage, providing access to data to authorized users. Thus, data confidentiality, integrity and authenticity have been ensured in the proposed technique. The existing access control technique is dependent on the certificate authority, not on the data owner (DO). In the proposed system, certificateless data access is enabled by the knowledge of the DO. Thus, the DO has complete control over their data. In the existing technique, the public auditor (PA) needs to verify the access log. Occasionally, PA behaves as an adversary and can change the log history. In a proposed work, these issues have been overcome by the immutable storage and timestamp (TS) value. The TS values automatically tell the transaction time and also verify the access to information in a dynamic manner. Thus, dynamic auditing is achieved in the proposed technique.

## Outline of the Proposed Work

Generally, BC is used for crypto-currency transactions through Ethereum and bitcoin. In the proposed system, BC is used as the storage and as an access medium to IoT data. The major benefit of BC is miner award. When the transaction is successfully completed, the miner can get the rewards. Similarly, whenever a successful transaction is completed the miner gets the rewards immediately. The proposed technique consists of IoT device registration, key and signature generation for the IoT devices, Elliptic Curve and SHA256 based block generation and block storage mechanisms. Figure 1 shows the flow diagram of the proposed system.

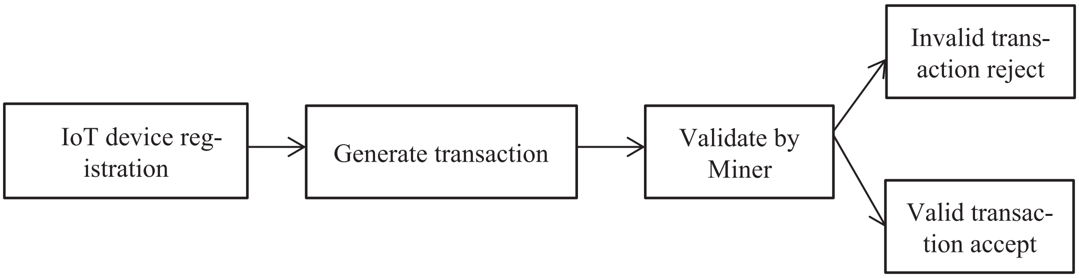


*Figure 1. Flow diagram of the Proposed Work*

## 3. Working Principle of the Proposed System

The working principle of the proposed system is discussed as follows:

- **Registration of IoT Device:** IoT devices are registered in the BC using Elliptic Curve Cryptography (ECC). The basic ECC equation $y^2 = x^3 + ax + b$ satisfies the basic condition $4a^3 + 27b^2 \neq 0$ and is used for the private and public key pair generation for each IoT device.
- **Key Generation:** The key pair for an IoT has been generated an ECC. Using Elliptic Curve Digital Signature Algorithm (ECDSA) library, private and public key pairs were generated for each IoT devices. In an ECDSA algorithm each public key Pu has derived from the private key Pr. The random number generator was used to generate the Pr value for each IoT device. Afterwards, the generated Pr value was used to compute the Pu key value. The Pu is the multiplication of the base point and Pr value. A similar process has been used to generate the Pu key value of all IoT devices.
- **Signature Generation:** After generating the key pair for the addition of data to the BC, a signature is required to verify the transaction and the authenticity of the message by the authenticator's Pu. In the signature generation, the variable length message has been converted to fixed length message digest h(m) by the Secure Hash Algorithm (SHA). The digital signature consists of two integer values 'r' and 's'. Initially, r is computed from the random value 'k' and the base point 'B'. Equation 1 has been used to calculate the 'r' value.

$$(x_1,y_1) = k * B \; mod \; p \text{ and } r = x_1 \; mod \; n \qquad (1)$$

Now, the calculated 'r' value has been used to compute the 's' value of the signature. Equation 2 has been used to calculate the 's' value.

$$s = (k^{-1} \, (h\,(m) + d * r) mod \; n \qquad (2)$$

In the validation, the 'r' and 's' value 0. If the values are equal to zero, new random number should be used to generate the new 'r' and 's' values. This generated signature has been verified in the receiver side for the authenticity verification. The SHA algorithm had used for signature verification process. In a proposed work, Equation 3 had used for signature verification.

$$w = s^{-1} \; mod \; n \text{ and } u_1 = (h\,(m) * w) mod \; n \text{ and } u_2 = (r * w) mod \; n$$
$$(x_2, y_2) = (u_1 * B + u_2 * B) mod \; n \qquad (3)$$

If the generated x2 is equal to the 'r' value, the signature is accepted.

- **Blockchain Implementation:** A block of a BC consists of three components. Those are:
  1. Previous Block Hash Value (PBHV) (to form a chain structure) – To maintain data immutability. If any changes need to be made in a specific block, the previous block all previous blocks must be changed. Changing an entire chain is an impossible task. Hence, the data integrity is maintained in the BC.
  2. Transaction data – the processing data. In the proposed technique, the patient information has been collected and transferred to blocks so that authorized users can access it.
  3. Time stamp – Ensures the transaction time. The timestamp shows the date of the transaction. Through the TS, log verification has been performed without PA.

- **Elliptic Curve Cryptography:** The ECC algorithm was used to generate Pu and Pr value for digital signature generation.
  1. In general, public key cryptography involves the generation of unique Pr for a user and generates Pu by previously generated Pr.
  2. Then the message was digitally signed by the sender using ECC to generate Pr and Pu.
  3. The digitally generated message was transferred to receiver, then the receiver was verified the message using ECDSA. If it passes, the digitally signed message has been accepted otherwise the receiver would have rejected the message.
  4. The working process of ECDSA is as follows:
     a. The sender generates 320 bytes digital signature for a message.
     b. The receiver knows all the public parameters and the sender's Pu.
     c. The receiver receives the sender's message and it is digitally signed and verified.
- **Secure Hash Algorithm (SHA-256):** SHA-256 has been used to generate the hash value of the data which is stored in the block.
  1. The BC has to be secure, because hashing is the most important part in the development of BC. SHA-256 has been used to generate the hash value (HV) of the sensor data. The feature of the HV is to produce fixed size HV for variable size input and every data produces a unique non-duplicate HV for any piece of data.
  2. The SHA-256 algorithm takes an input and produces a 256-bit unique HV which cannot be traced back.

Algorithm 1 shows the working principle of the proposed technique.

**Algorithm 1: IoT Data Collection and Storage in Blockchain**

```
Input: ID, TA, ACL
Output: Pr, Verified TA
Procedure:
1. Procedure Keygen(ID)                  //Key generation of IoT device
2. SignatureGen(ID)                      //Signature generation of ID
3. Verify(ID)                                 // Verify the IoT devices is valid or not
4. if (ID == Valid) then:
     Pr ← Keygen(ID, K)                       // Private key generation of ID
     Pu ← Keygen(ID, Pr, B)              // Public key generation of ID
5. if(Trans(TA, PU)==Valid) then         // If the transaction is valid based on ID
     Accept Transaction
   Else
     Abort Transaction
6. if(Trans == Accept) then
     Create TA = (Pk, ID, ACL, Addr)          // Transaction contains Public key, ID,
     Broadcast(TA)                       // Access Control List(ACL) and address
7. if (ID ∊ ACL) then                       //ID having ACL to access block
     Allow to access
   Else
     Reject Access
End procedure
```

In a proposed system, the Access Control List (ACL) clearly says who is able to access data in the BC. Each transaction contains the Pu, ID of the device, ACL and address of the device. The BC miners verify the transaction is valid or not through the senders Pu. If the transaction is valid, the corresponding transaction is updated to BC by the miner and gets the reward. In the receiver side, the doctors or other authorized persons are willing to access the data; they are creating a transaction with their ID, senders ID and address. This transaction has been verified by the miner and checks the ACL list of the receiver. If the receiver belongs the ACL, the miner allows the receiver to access the block else the receiver stopped by the miner. If any unauthorized user tries to access the patient information, the miner does not allow them to access the block. Their transaction is cancelled by the miner. In a proposed work, the ACL has been created and modified by the DO. The DOs are having complete control over their data and the miners are having the control to allow or stop the transactions. Through this process the unauthorized access has been completely eliminated.

# 4. Methodology

The proposed method has been implemented following methodology described in this section.

### 1. IoT Device Registration Using Blockchain

BC nodes have been used to store all the nodes' (IoT devices') information. The attributes are represented in this storage are shown in table 1.

*Table 1. BC Node*

| Attribute Name | Description of the Attributes |
|---|---|
| **ID** | IoT device index. |
| **Public key** | The IoT device Pu, added to the BC. |
| **Private key** | The IoT device Pr, which is used to sign the data and can be used to verify the data when sent across the BC. |
| **Nodes** | The name of the IoT-Device |

### 2. IoT Data and Transaction Storage in Blockchain

Implement a storage mechanism to store all the BC data i.e IoT device information, transaction details and block details. Using MySQL server to store all the data. The database has been divided into 4 storage representations such as BC_chain, BC_chain_enc, BC_transaction and BC_nodes. The information has been stored in each format as follows:

1. **BC_chain:** Stores the complete BC in the form of a table. The attributes are shown in table 2.

*Table 2. BC_chain representation*

| **Attribute Name** | **Description of the Attributes** |
|---|---|
| **Block_id** | Index of block in the BC |
| **Prev_hash** | The PBHV in the BC, it helps user to authenticate upcoming transactions in a BC. |
| **Hash** | The current transaction HV. |
| **Imp_stamp** | The TIME when the block is added to the BC. |
| **data** | The data is stored in the current block. |

2. **BC_chain_enc:** Stores the fully encrypted BC in the form of a table. The attributes are shown in table 3.

*Table 3. BC Encryption*

| **Attribute Name** | **Description of the Attributes** |
|---|---|
| **Block_id** | Index of block in the BC |
| **Prev_hash** | The PBHV in the BC, it helps user to authenticate upcoming transactions in a BC. |
| **Hash** | The current transaction HV. |
| **Imp_stamp** | The TIME when the block is added to the BC. |
| **Eny_data** | The data stored in the current block is represented through encryption. |

3. **BC_transaction:** Used to store all transactions of an each block. The attributes are shown in table 4.

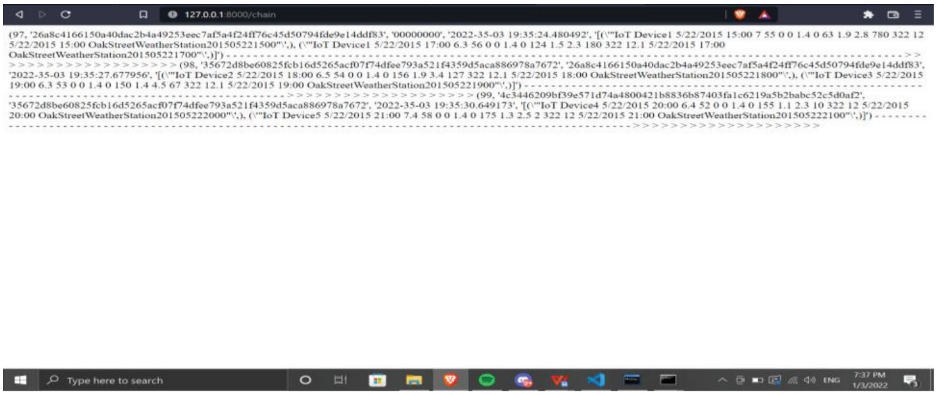
*Table 4. BC Transaction*

| **Attribute Name** | **Description of the Attributes** |
|---|---|
| **ID** | Index of the transaction |
| **Public key** | The IoT device Pu, which creates the transaction. |
| **Signature** | The signature of transaction which is used to verify whether the transaction is legal or not. |
| **Transaction** | Represents all the transaction data. |

# 5. Experimental Results

In this section, the experimental setup and the dataset used in the proposed technique are described in detail. The proposed technique has been implemented in the anaconda based Jupiter notebook python code. The backend data has been stored in MySql. The ECC and ECDSA algorithms have been implemented in python language. The IoT node and members are authenticated by the ECDSA algorithm for secure and authenticated network generation. The IoT medical data has been collected from the Kaggle dataset (https://www.kaggle.com/caesarlupum/iot-sensordata). The dataset contains IoT sensor data collected from patients. The IoT implementation involves the IoT nodes, BC miners and receivers. The IoT sensors are allow the patients and doctors to collect the information at regular intervals. The BCminer verifies the IoT node and the members involved in the process. The IoT data communication is provided by the Giga Ethernet. The experiments were carried out at a maximum of 1200 seconds with 150 watt CPU power utilization.

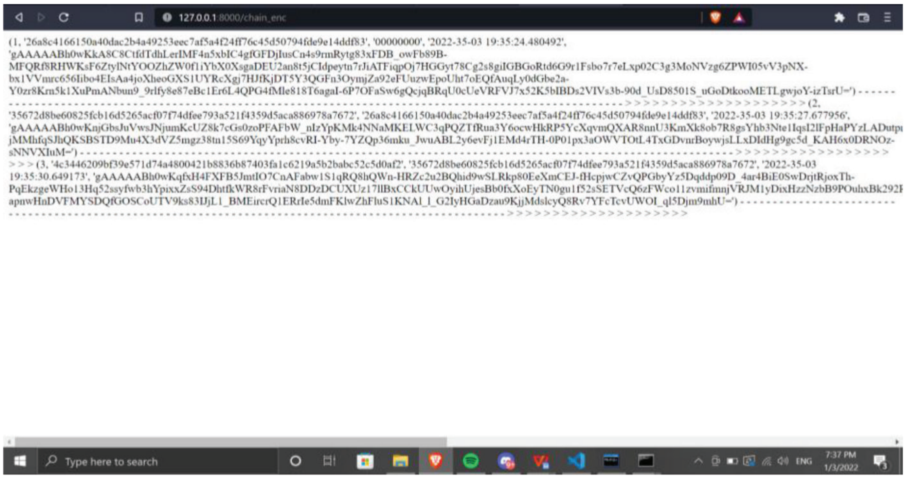
The execution and node creation of the proposed system is shown in figure 2. This figure shows the block creation process with previous block hash value, none and present block information. Each block represents separate data storage and it is immutable in future.



```
(97, '26a8c4166150a40dac2b4a49253eec7af5a4f24ff76c45d50794fde9e14ddf83', '00000000', '2022-35-03 19:35:24.480492', '[(\'"IoT Device1 5/22/2015 15:00 7 55 0 0 1.4 0 63 1.9 2.8 780 322 12
5/22/2015 15:00 OakStreetWeatherStation201505221500"\',), (\'"IoT Device1 5/22/2015 17:00 6.3 56 0 0 1.4 0 124 1.5 2.3 180 322 12.1 5/22/2015 17:00
OakStreetWeatherStation201505221700"\',)]') - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > >
> > > > > > > > > > > > > > > > > > > > (98, '35672d8be60825fcb16d5265acf07f74dfee793a521f4359d5aca886978a7672', '26a8c4166150a40dac2b4a49253eec7af5a4f24ff76c45d50794fde9e14ddf83',
'2022-35-03 19:35:27.677956', '[(\'"IoT Device2 5/22/2015 18:00 6.5 54 0 0 1.4 0 156 1.9 3.4 127 322 12.1 5/22/2015 18:00 OakStreetWeatherStation201505221800"\',), (\'"IoT Device3 5/22/2015
19:00 6.3 53 0 0 1.4 0 150 1.4 4.5 67 322 12.1 5/22/2015 19:00 OakStreetWeatherStation201505221900"\',)]') - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > > > > > > > > > > > > > > > > > > > > (99, '4c3446209bf39e571d74a4800421b8836b87403fa1c6219a5b2babc52c5d0af2',
'35672d8be60825fcb16d5265acf07f74dfee793a521f4359d5aca886978a7672', '2022-35-03 19:35:30.649173', '[(\'"IoT Device4 5/22/2015 20:00 6.4 52 0 0 1.4 0 155 1.1 2.3 10 322 12 5/22/2015
20:00 OakStreetWeatherStation201505222000"\',), (\'"IoT Device5 5/22/2015 21:00 7.4 58 0 0 1.4 0 175 1.3 2.5 2 322 12 5/22/2015 21:00 OakStreetWeatherStation201505222100"\',)]') - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > > > > > > > > > > > > > > > > > > > >
```

*Figure 2. Block Creation*

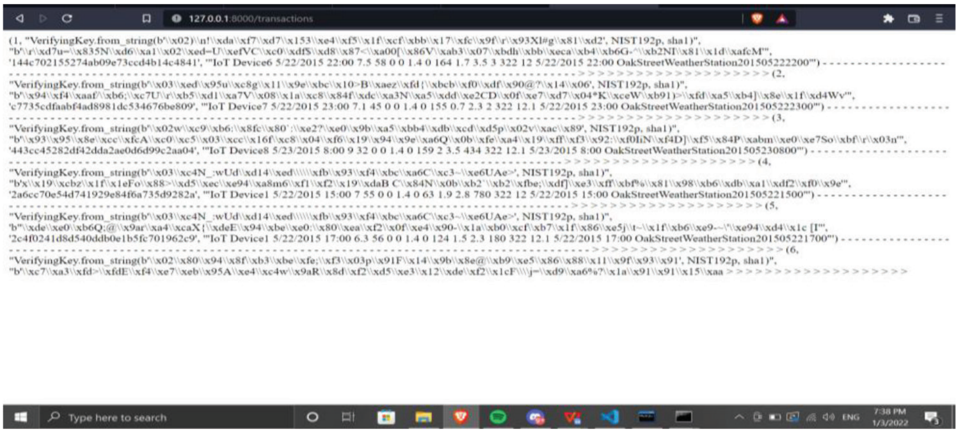
Figure 3 shows the block encryption process using the ECC algorithm. ECC is a public key cryptographic technique and it is suitable for creating a block in a blockchain network.



```
(1, '26a8c4166150a40dac2b4a49253eec7af5a4f24ff76c45d50794fde9e14ddf83', '00000000', '2022-35-03 19:35:24.480492',
'gAAAAABh0wKkA8C8CtfdTdhLerIMF4n5xbIC4gfGFDjIusCn4s9rmRytg83xFDB_owFb89B-
MFQRf8RHWKsF6ZtylNtYOOZhZW0f1iYbX0XsgaDEU2an8t5jCIdpeytn7rJiATFiqpOj7HGGyt78Cg2s8giIGBGoRtd6G9r1Fsbo7r7eLxp02C3g3MoNVzg6ZPWI05vV3pNX-
bx1VVmrc656Iibo4EIsAa4joXheoGXS1UYRcXgj7HJfKjDT5Y3QGFn3OymjZa92eFUuzwEpoUht7oEQfAuqLy0dGbe2a-
Y0zr8Krn5k1XuPmANbun9_9rlfy8e87eBc1Er6L4QPG4fMle818T6agaI-6P7OFaSw6gQcjqBRqU0cUeVRFVJ7x52K5bIBDs2VIVs3b-90d_UsD8501S_uGoDtkooMETLgwjoY-izTsrU=') - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > > > > > > > > > > > > > > > > > > > > (2,
'35672d8be60825fcb16d5265acf07f74dfee793a521f4359d5aca886978a7672', '26a8c4166150a40dac2b4a49253eec7af5a4f24ff76c45d50794fde9e14ddf83', '2022-35-03 19:35:27.677956',
'gAAAAABh0wKnjGbsJuVwsJNjumKcUZ8k7cGs0zoPFAFbW_nIzYpKMk4NNaMKELWC3qPQZTfRua3Y6ocwHkRP5YcXqvmQXAR8nnU3KmXk8ob7R8gsYhb3Nte1IqsI2lFpHaPYzLADutp
jMMhfqSJhQKSBSTD9Mu4X3dVZ5mgz38tn15S69YqyYprh8cvRI-Yby-7YZQp36mku_JwuABL2y6evFj1EMd4rTH-0P01px3aOWVTOtL4TxGDvnrBoywjsLLxDIdHg9gc5d_KAH6x0DRNOz-
sNNVXIuM=') - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > > > > > > > > > > > > > > > > > > > >
> > > (3, '4c3446209bf39e571d74a4800421b8836b87403fa1c6219a5b2babc52c5d0af2', '35672d8be60825fcb16d5265acf07f74dfee793a521f4359d5aca886978a7672', '2022-35-03
19:35:30.649173', 'gAAAAABh0wKqfxH4FXFB5JmtIO7CnAFabw1S1qRQ8hQWn-HRZc2u2BQhid9wSLRkp80EeXmCEJ-fHcpjwCZvQPGbyYz5Dqddp09D_4ar4BiE0SwDrjtRjoxTh-
PqEkzgeWHo13Hq52ssyfwb3hYpixxZsS94DhtfkWR8rFvriaN8DDzDCUXUz17llBxCCkUUwOyihUjesBb0fXoEyTN0gu1f52sSETVcQ6zFWco11zvmifmnjVRJM1yDixHzzNzbB9POuhxBk292F
apnwHnDVFMYSDQfGOSCoUTV9ks83IJjL1_BMEircrQ1ERrIe5dmFKlwZhFluS1KNAl_l_G2IyHGaDzau9KjjMdslcyQ8Rv7YFcTcvUWOI_ql5Djm9mhU=') - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - > > > > > > > > > > > > > > > > > > > >
```

*Figure 3. Block Encryption Using ECC*

Figure 4 shows the transaction verification process of the proposed system by the miner. The transaction verification process helps to check the transactions are performed in a particular time. It works like a log in other file transactions. Through this process, the access history of the block is identified.



```
(1, "VerifyingKey.from_string(b'\\x02)\\n!\\xda\\xf7\\xd7\\x153\\xe4\\xf5\\x1f\\xcf\\xbb\\x17\\xfc\\x9f\\r\\x93Xl#g\\x81\\xd2', NIST192p, sha1)",
"b'\\r\\xd7u=\\x835N\\xd6\\xa1\\x02\\xed=U\\xefVC\\xc0\\xdf$\\xd8\\x87<\\xa00[\\x86V\\xab3\\x07\\xbdh\\xbb\\xeca\\xb4\\xb6G-^\\xb2NI\\x81\\x1d\\xafcM'",
'144c702155274ab09e73ccd4b14c4841', '"IoT Device6 5/22/2015 22:00 7.5 58 0 0 1.4 0 164 1.7 3.5 3 322 12 5/22/2015 22:00 OakStreetWeatherStation201505222200"') - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - >>>>>>>>>>>>>>>>>>>>(2,
"VerifyingKey.from_string(b'\\x03\\xed\\x95u\\xc8g\\x11\\x9e\\xbc\\x10>B\\xaez\\xfd{\\xbcb\\xf0\\xdf\\x90@?\\x14\\x06', NIST192p, sha1)",
"b'\\x94\\xf4\\xaaf/\\xb6;\\xc7U\\r\\xb5\\xd1\\xa7V\\x08\\x1a\\xc8\\x84f\\xdc\\xa3N\\xa5\\xdd\\xe2CD\\x0f\\xe7\\xd7\\x04*K\\xceW\\xb91)>\\xfd\\xa5\\xb4]\\x8e\\x1f\\xd4Wv'",
'c7735cdfaabf4ad8981dc534676be809', '"IoT Device7 5/22/2015 23:00 7.1 45 0 0 1.4 0 155 0.7 2.3 2 322 12.1 5/22/2015 23:00 OakStreetWeatherStation201505222300"') - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - >>>>>>>>>>>>>>>>>>>>(3,
"VerifyingKey.from_string(b'\\x02w\\xc9\\xb6:\\x8fc\\x80`;\\xe2?\\xe0\\x9b\\xa5\\xbb4\\xdb\\xcd\\xd5p\\x02v\\xac\\x89', NIST192p, sha1)",
"b'\\x93\\x95\\x8e\\xcc\\xfcA\\xc0\\xc5\\x03\\xcc\\x16f\\xc8\\x04\\xf6\\x19\\x94\\x9e\\xa6Q\\x0b\\xfe\\xa4\\x19\\xff\\xf3\\x92:\\xf0IiN\\xf4D]\\xf5\\x84P\\xabm\\xe0\\xe7So\\xbf\\r\\x03n'",
'443cc45282df42dda2ae0d6d99c2aa04', '"IoT Device8 5/23/2015 8:00 9 32 0 0 1.4 0 159 2 3.5 434 322 12.1 5/23/2015 8:00 OakStreetWeatherStation201505230800"') - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - >>>>>>>>>>>>>>>>>>>>(4,
"VerifyingKey.from_string(b'\\x03\\xc4N_:wUd\\xd14\\xed\\\\\\xfb\\x93\\xf4\\xbc\\xa6C\\xc3~\\xe6UAe>', NIST192p, sha1)",
"b'x\\x19\\xcbz\\x1f\\x1eFo\\x88>\\xd5\\xec\\xe94\\xa8m6\\xf1\\xf2\\x19\\xdaB C\\x84N\\x0b\\xb2`\\xb2\\xfbe;\\xdf]\\xe3\\xff\\xbf%\\x81\\x98\\xb6\\xdb\\xa1\\xdf2\\xf0\\x9e'",
'2a6cc70e54d741929e84f6a735d9282a', '"IoT Device1 5/22/2015 15:00 7 55 0 0 1.4 0 63 1.9 2.8 780 322 12 5/22/2015 15:00 OakStreetWeatherStation201505221500"') - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - >>>>>>>>>>>>>>>>>>>>(5,
"VerifyingKey.from_string(b'\\x03\\xc4N_:wUd\\xd14\\xed\\\\\\xfb\\x93\\xf4\\xbc\\xa6C\\xc3~\\xe6UAe>', NIST192p, sha1)",
'b"\\xde\\xe0\\xb6Q;@\\x9ar\\xa4\\xcaX{\\xdeE\\x94\\xbe\\xe0:\\x80\\xea\\xf2\\x0f\\xe4\\x90-\\x1a\\xb0\\xcf\\xb7\\x1f\\x86\\xe5j\\t~\\x1f\\xb6\\xe9-~\\"\\xe94\\xd4\\x1c [I"',
'2c4f0241d8d540ddb0e1b5fc701962c9', '"IoT Device1 5/22/2015 17:00 6.3 56 0 0 1.4 0 124 1.5 2.3 180 322 12.1 5/22/2015 17:00 OakStreetWeatherStation201505221700"') - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - >>>>>>>>>>>>>>>>>>>>(6,
"VerifyingKey.from_string(b'\\x02\\x80\\x94\\x8f\\xb3\\xbe\\xfe;\\xf3\\x03p\\x91F\\x14\\x9b\\x8e@\\xb9\\xe5\\x86\\x88\\x11\\x9f\\x93\\x91', NIST192p, sha1)",
"b'\\xc7\\xa3\\xfd>\\xfdE\\xf4\\xe7\\xeb\\x95A\\xe4\\xc4w\\x9aR\\x8d\\xf2\\xd5\\xe3\\x12\\xde\\xf2\\x1cF\\\\j=\\xd9\\xa6%?\\x1a\\x91\\x91\\x15\\xaa >>>>>>>>>>>>>>>>>>>>
```

*Figure 4. Transaction verification Process*

Based on above experimental process, the evaluation of the performance of the proposed system is discussed as follows.

# 6. Performance Analyses

In this section, the performance of our proposed system is evaluated. The simulation was performed in a 64-bit operating system with 16GB RAM. SHA256 had been used for the HV based block generation and the ECC algorithm had been used for the data encryption.

## Key Generation Computation Overhead

The proposed system's key generation overhead is shown in figure 5. The key generation computation overhead increased when the number of IoT devices increased. Similarly, when the number of members involved in the BC network grows it means that the number of generated keys also increases.

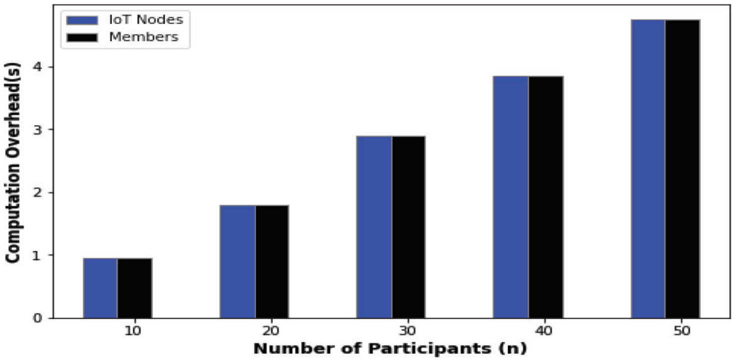


*Figure 5. Key Generation Overhead*

## Block Generation Overhead Analysis

The proposed system's block generation overhead is shown in figure 6. When the number of IoT devices increased, the data collection and block generation overhead also increased. The number of blocks the miner generates depends on the success of the transactions. Thus, the increment in device count is reflected in the block generation count.

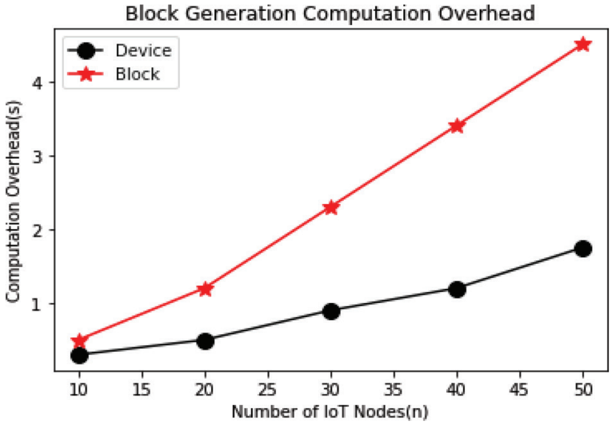


*Figure 6. Block Generation Overhead Analysis*

## Parallel Access Computation Overhead

The proposed system's concurrent access computation overhead is shown in figure 7. When the number of requests from registered member increased, the verification and access time also increased. By means of verification, the miner authenticates each user and controls access. If a greater number of users try to access the block concurrently, the increase in the number of requests increases the access time.

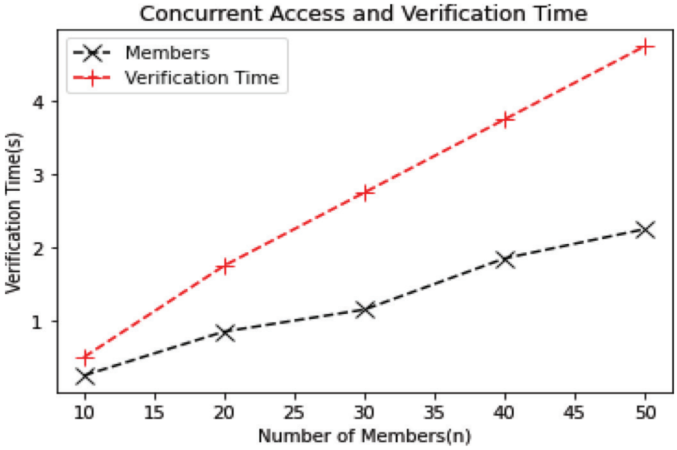


*Figure 7. Concurrent Access Member Verification Time Analysis*

## Communication Overhead Analysis

Communication overhead represents the time taken for signature generation and verification process. The duration of signature generation and verification time depends on the memory consumed. The proposed ECDSA signature generation and verification technique has been compared to other existing techniques such as Light Weight and Anonymous Mutual Authentication and Key Agreement (LAMAKA) and Lamport Signature using PRNG technique. When compared to these techniques, the proposed technique communication overhead decreased from 10 to 40% and from 5 to 20% (Marah *et al*., 2022, Hemant *et al*., 2023). Depending on the number of nodes, the communication overhead is increased. Table 5 shows the communication overhead analysis of the proposed and existing techniques.

*Table 5. Communication Overhead Analysis*

| Number of IoT nodes | LAMAKA | LDMS | Proposed Technique |
|---|---|---|---|
| **10** | 27 | 23 | 19 |
| **20** | 56 | 47 | 39 |
| **30** | 81 | 69 | 57 |
| **40** | 108 | 92 | 76 |
| **50** | 135 | 115 | 95 |

## Authentication Accuracy Analysis

In a proposed system, the authentication accuracy was measured in terms of the ratio of correctly authenticated members from the total number of participants. Figure 8 shows the comparative analysis of the proposed technique with the existing LAMAKA and LDMS technique. When compared to these techniques, the proposed technique's authentication accuracy rate is increased in the range of 10% to 20%.

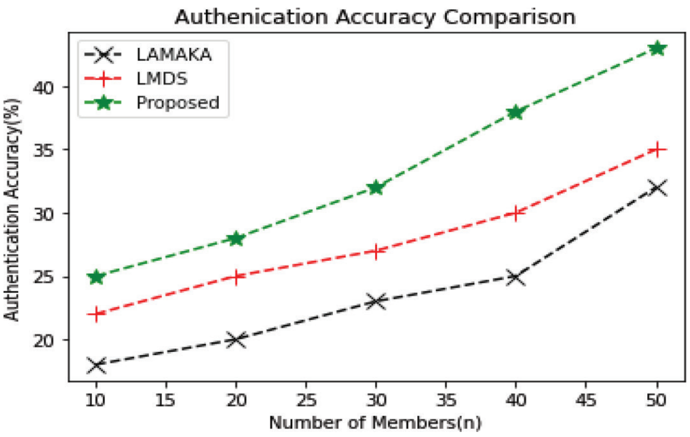


*Figure 8. Authentication Accuracy Comparison*

## Data Confidentiality Analysis

In a proposed technique, the data confidentiality rate was measured by the number of correctly accessed blocks by the authorized members in the BC network. When compared to the existing LAMAKA and LDMS techniques, the proposed technique's data confidentiality is higher than 5%. The authorized users are verified by the miners in each and every transaction. Thus, the malicious users are unable to access and modify the data in the proposed system. Similarly, the BC approach does not allow to modify the data content which is present in the blocks. Hence, the improved confidentiality is achieved in the proposed system. Table 6 shows the comparison of the confidentiality rate of the proposed and existing techniques.

*Table 6. Data Confidentiality Analysis*

| Number of IoT nodes | LAMAKA | LDMS | Proposed Technique |
|---|---|---|---|
| **10** | 72 | 76 | 82 |
| **20** | 79 | 84 | 93 |
| **30** | 85 | 90 | 95 |
| **40** | 82 | 87 | 94 |
| **50** | 90 | 92 | 97 |

Based on the above analysis, the proposed BC data storage and access provides better performance in key generation, block generation, concurrent access, communication overhead, authentication accuracy and data confidentiality etc. Thus, it has been proven that the proposed system provides better results than the existing technique.

## Security Analysis

1. **Privacy –** Whenever the data is transferred in the network for transaction or storage, unauthorized users try to access the patient information. To avoid unauthorized access, the data is encrypted before transfer. In a proposed technique, the patient information was encrypted by senders Pr before transfer and access through Pu. Thanks to this process, the data privacy has been achieved in the proposed technique.
2. **Traceability and Accountability –** In a proposed technique, every node must register in the network before initiating a transaction. This registration avoids the denial of service attack. Thus, every registered user is able to access the blocks and unauthorized access is easily identified through the malicious attempts. The identified malicious devices which had attempted access are permanently removed from further transactions.
3. **Protocol Security –** In a proposed technique, the random Pr and Pu key pairs had generated for each IoT device. It is impossible for adversaries to predict the random keys. Hence, the Pr's may not be found by the adversary. Thus, the generation of a forged digital signature is an impossible task in the proposed technique.
4. **Forward and Backward Secrecy:** In the proposed work, both forward and backward secrecy have been achieved. When a new member or node enters the BC, they need to register before

becoming involved in transactions. Thus, forward secrecy has been achieved. In a backward secrecy, the existing user has been removed from the network; they are unable to access the information from the BC. In each and every transaction, the member's access rights are verified by the miner and then the transaction is enabled. Hence, backward secrecy has been maintained in the proposed work.

Table 7 compares the security of the proposed technique with the existing techniques.

*Table 7. Security Comparison of Proposed and Existing System*

| **Scheme** | **Patra *et al.* 2012** | **Ilokah *et al.* 2020** | **Zhang *et al.* 2018** | **Cao *et al.* 2019** | **Guipeng *et al.* 2022** | **Proposed scheme** |
|---|---|---|---|---|---|---|
| Introduction of Entity | CSP | CSP+CA | CSP+KS | CSP+BC | CSP+BC | BC |
| Privacy Protection Support | N | Y | Y | Y | Y | Y |
| Tampering Attack | N | Y | Y | Y | Y | Y |
| Man-in-the-Middle attack | N | N | N | Y | Y | Y |
| Collusion Attack | N | N | N | N | Y | Y |
| Accountability | N | N | N | N | N | Y |
| Protocol Security | N | N | N | N | N | Y |
| Denial of Service Attack | N | N | N | N | N | Y |
| Distributed Denial of Service Attack | N | N | N | N | N | Y |

## 7. Conclusions and Future Work

To store the IoT sensor information securely, this research proposed a decentralized and secure solution for IoT data storage based on blockchain. The private and public key for the registered IoT devices were generated using the Elliptic Curve Cryptography technique and the blocks containing IoT data were constructed using the SHA256 algorithm. The generated blocks were stored in a blockchain by means of a MySql server. The blockchain miner verified, through an access control list, the user's authenticity to provide them with access to the block and also verified the IoT node's authenticity when validating the node and creating a block in the blockchain. When a node successfully added to the blockchain, the miner gets the reward. When compared to exiting centralized storage, the proposed technique provides high data confidentiality, integrity and availability of patient data. This decentralized technique provides improved results in confidentiality, authenticity, and communication and computation overhead analysis. Thus, it has been proven that the proposed system is able to handle patient information efficiently through the experimental results. To create a user friendly environment, a simple GUI has been developed in a web application.

In the future, a peer-to-peer system will be added to establish interaction with each other. An improved Graphical User Interface will be developed to make the use of blockchain more user friendly and also deal with Dynamic Data/

## 8. References

Bataineh, M. R., Mardini, W., Khamayseh, Y. M. & Yassein, M. M. B, 2022. Novel and Secure Blockchain framework for health applications in IoT. *IEEE Access, 10*, 14914 -14926. https://doi.org/10.1109/ACCESS.2022.3147795

Cao, S., Zhang, G., Liu, P. *et al*., 2019. Cloud-assisted secure eHealth systems for tamper proofing HER via blockchain. *Inf. Sci. 485*, 427-440. https://doi.org/10.1016/j.ins.2019.02.038

Goyal, R., Kumar, G., Saha, R., & Conti, M., 2020. Blockchain-based Data Storage with Privacy and Authentication in Internet-of-Things. *IEEE Internet of Things Journal, 9(*16), 14203-14215. https://doi.org/10.1109/JIOT.2020.3019074.

Gupta, S., Kashaudhan, S., Pandey, D. C., Gaur, P. P. S. G., 2017, IoT based Patient Health Monitoring System. *International Research Journal of Engineering and Technology, 4*(3).

Hamim, M., Paul, S., Hoque, S. I., Rahman, M. N., & Baqee, I. A., 2019. IoT based Remote health monitoring system for patients and Elderly people. *2019 International conference on robotics, electrical and signal processing techniques*, pp. 533-538. https://doi.org/10.1109/ICREST.2019.8644514

Hussein W.N., Hussain H.N., & Humod I. M., 2022. A proposed framework for healthcare based on cloud computing and IoT applications. *Materials today: Proceedings, 60*(3), 1835-1839. https://doi.org/10.1016/j.matpr.2021.12.505

Ilokah, M., & Eklund, J. M., 2020. A secure privacy preserving cloud based framework for sharing electronic health data. *Proceedings of the 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society*, pp. 5592-5597. https://doi.org/10.1109/EMBC44109.2020.9175792

Li., R, Song, T., Mei, B, Li, H, Cheng, X., & Sun, L., 2019. Blockchain for large-scale Internet of Things data storage and Protection. *IEEE Transactions on services computing*, 12(5), 762-771. https://doi.org/10.1109/TSC.2018.2853167

Ma, M., Shi, G., & Li, F., 2019. Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. *IEEE Access, 7*, 34045-34059. https://doi.org/10.1109/ACCESS.2019.2904042

Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., Alkhayyat, A., & Alhayani, B., 2023. Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience 13*, 2329-2342. https://doi.org/10.1007/s13204-021-02164-0

Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. 2020, Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access, 8*, 205190-205205. https://doi.org/10.1109/ACCESS.2020.3036812

Patra, M. R., Das, R. K., & Padhy, R. P., 2012. CRHIS: Cloud based rural healthcare information system. *Proceedings of the International Conference on Theory and Practice of Electronic Governance*, pp. 402-405. https://doi.org/10.1145/2463728.2463805

Sadawi, A. A., Hassan, M. S., & Ndiaye, M., 2021. A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. *IEEE Access, 9*, 54478-54497. https://doi.org/10.1109/ACCESS.2021.3070555

Sumathi, M., Rajkamal, M., Gomathy, B., Infant raj, I., Jaiswal, S., Swathi, D., 2021. Secure Blockchain based data storage and Integrity Auditing in Cloud. *Turkish journal of Computer and Mathematics Education, 12*, 159-165.

Sumathi, M., Sangeetha, S., 2018. Enhanced Elliptic Curve Cryptographic Technique for Protecting Sensitive Attributes in Cloud Storage, *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*. 433-438. https://doi.org/10.1109/ICCIC.2018.8782295

Sumathi, M., Sangeetha, S., 2020. Blockchain based sensitive attribute storage and access monitoring in banking system, *International Journal of Cloud Applications and Computing, 10*(2), 77-92. https://doi.org/10.4018/IJCAC.2020040105

Tamilselvi, V., Sribalaji, S., Vigneshwaran, P., Vinu, P., GeethaRamani, J., 2020. IoT based health monitoring system. *6th International conference on Advanced computing & Communication systems (ICACCS)*, pp. 386-389. https://doi.org/10.1109/ICACCS48705.2020.9074192

Tawalbeh, L., Muheidat, D., Tawalbeh, M., Quwaider, M., & Abd El-Latif, A. A., 2022. Edge enabled IoT system model for secure healthcare. *Measurement, 191*, 110792. https://doi.org/10.1016/j.measurement.2022.110792

Valsalan, P., Tariq Ahmed Barham Baomar, T. A. B., Baabood, A. H. O., 2020. IoT based health monitoring system. *Journal of Critical reviews, 7*(4). https://doi.org/10.31838/jcr.07.04.137

Zhang, G., Yang, Z., Liu, W., 2022. Blockchain based privacy preserving e-health system for healthcare data in cloud. *Computer Network, 203*, 108586. https://doi.org/10.1016/j.comnet.2021.108586

Zhang, Y. Xu, C., Zhang, C. *et al*., 2018. HealthDep: an efficient and secure deduplication scheme for cloud assisted ehealth systems. *IEEE Transaction ind. Inf. 14*(9), 4101-4112. https://doi.org/10.1109/TII.2018.2832251