Computing and Informatics, Vol. 41, 2022, 1207–1239, doi: 10.31577/cai_2022_5_1207

INTERNET OF THING BASED CONFIDENTIAL HEALTHCARE DATA STORAGE, ACCESS CONTROL AND MONITORING USING BLOCKCHAIN TECHNIQUE

Muruganandam Sumathi

School of Computing
SASTRA Deemed to be University
Thanjavur, Tamilnadu, India
e-mail: sumathi@it.sastra.edu, sumathishanjai.nitt@gmail.com

Natarajan Vijayaraj

Department of Computer Science and Engineering
Vel Tech Rangarajan Dr. Sagunthala Research
and Development Institute of Science and Technology
Chennai, Tamilnadu, India
e-mail: vijayaraj@veltech.edu.in, vijaycseraj@gmail.com

Soosaimarian Peter Raj Raja

School of Computer Science and Engineering
Vellore Institute of Technology
Vellore-632 014, Tamilnadu, India
e-mail: avemariaraja@gmail.com

Murugesan Rajkamal

IBM, Bangalore, Karnataka, India
e-mail: rajkamalmurugasean@gmail.com

Abstract. Internet of Things plays a significant role in multiple sectors like agriculture, manufacturing and healthcare for collecting information to automation. The collected information is in different diversity and consists of confidential and non-confidential information. Secure handling of confidential data is a crucial task in cloud computing like storage, access control and monitoring. The blockchain based storage technique provides immutable data storage, efficient access control and dynamic monitoring to confidential data. Thus, the secure internet of things data storage, access control and monitoring using blockchain technique is proposed in this work. The patients health information that are in different formats are pruned by a decision tree algorithm and it classifies the confidential data and non-confidential data by the fuzzy rule classification technique. Depending on data owner's willing, the fuzzy rule is framed and the confidential and non-confidential data collected by internet of things sensors are classified. To provide confidentiality to confidential data, Attribute Based Encryption is applied to confidential data and stored in an off-chain mode of blockchain instead of entire data encryption and storage. The non-confidential data is stored in a plaintext form in cloud storage. When compared to support vector machine, K-nearest neighbor and Naive Bayes classification techniques, the proposed fuzzy rule based confidential data identification produces greater than 96 % of accuracy based on data owner willing and confidential data storage takes lesser than 20 % of storage space and processing time in an entire data storage. Additionally, the blockchain performances like throughput, network scalability and latency is optimized through minimal block size and transactions. Thus, our experimental results show that the proposed blockchain based internet of things data storage, access control and monitoring technique provides better confidentiality and access control to confidential data than the conventional cloud storage technique with lesser processing time.

Keywords: Internet of things, secure data storage, access control, access monitoring, blockchain, smart contract, attribute based encryption, e-healthcare, data pruning

1 INTRODUCTION

At present automation plays a key role in human life and is done by electrical, mechanical and computerized devices. These devices are producing different diversity of data and need to be analysed in multiple aspects for providing better services to end user. Thus, the data collection, analysis and storage are an essential task in automation. Presently, Internet of Things (IoT) sensors collect the data, machine learning (ML) algorithms do the analysis and cloud storage is used for storing the data [1]. The IoT sensors are linked together to collect data from various locations in various sectors such as healthcare, agriculture, manufacturing, home automation, banking, electric power grid, supply chain, and vehicle monitoring [2]. The IoT devices produce massive volume of data in different formats. To analyse this large

volume of data is a time consuming task. Hence, data pruning is required to identify the exact data which is required for analysis and needs protection [3].

The identified precious data needs to be stored in a secure manner in the cloud storage (CS). Conventionally, user data is stored in the user personal storage location, but nowadays the size of data is very large. Hence, the maintenance cost is very high. To reduce the cost of storage and maintenance, CS is used in the present storage technique [4]. The secure storage of semi-structured and unstructured data in the cloud is a challenging task. The storage cost depends on the size of data and Cloud Service Providers (CSP). To reduce storage and maintenance cost, the data preparation is applied to IoT data for identifying the confidential data (CD) in the collected data. Afterwards, the CD is to be stored in CS locations. Due to third party CSP interaction, security issues are high in cloud storage [5]. To overcome these issues, the blockchain (BC) based data storage (BCDS), access control (AC) and monitoring techniques are proposed in this work. Figure 1 shows the overall organization of the proposed work.

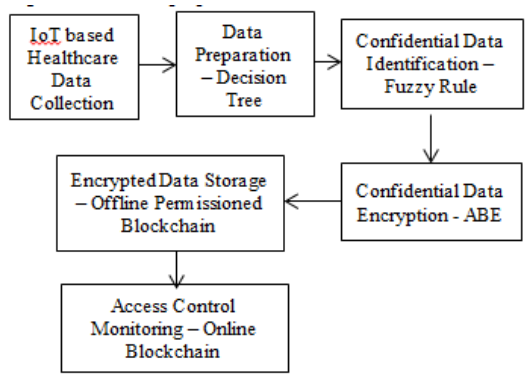

Figure 1. Workflow of the proposed system

Currently, BCDS is more trusted data storage technique than the conventional secure data storage. The major characteristics of BC are decentralized, immutability, enhanced security, distributed ledgers, consensus, provenance, smart contract (SC), finality and faster settlement. Due to these characteristics, BC is used in different sectors like banking, healthcare, education, manufacturing, land registration, crime register management, electronic voting, etc. [6]. The major benefits of BC are transparency, trustability, identification, credibility, collaboration and organization. Usually BC data are stored in the distributed ledger and viewed by every registered user in a network. This public visibility leads to higher security risk. The BC storage is broadly classified as permissionless and permissioned BC. The permissionless BC stores all information and the information is visible to all the members involved in a network. The permissioned BC is vice versa, the members who are all involved in the registered network are able to access the data available in the network and

others are not able to view and access. Hence, permissioned BC is preferred in secured data management [7].

One more issue of CS is access control (AC) and monitoring process. In CS, the AC and monitoring depends on CSP. Occasionally, the CSP also behaves as a malicious attacker (A) and distributes the user CD to others. To overcome this issue, permissioned BC based AC and monitoring technique is used in present security system [8]. The limitation of BC is storage size of the block. Every block size is equal to or lesser than 1 MB. When the data size is higher than 1 MB, it cannot be fitted in a single block. Hence, an alternate storage technique is proposed as on-chain and off-chain based storage [9]. The storage capacity of on-chain is very less, thus the limited size data is stored in an on-chain mode. The storage capacity of off-chain is vice versa and it is maintained outside the BC. Hence, the data needs to be classified before storing it in the block. Likewise, the on-chain data is the recent and frequently accessed data by the members involved in the network and the off-chain storage information is accessed rarely by authorized members [10]. Furthermore, the BC data is stored in two different ways, namely hot and cold storage. The hot storage handles the frequently changing data and cold storage handles the permanent data. In the proposed technique, the cold is preferred to store the confidential medical records. Hence, the cold storage with off-chain based permissioned network is used for CD storage.

Motivation and contribution of the proposed work:

- To collect patient's health data through IoT sensors and to avoid the security issues of CS, the BCDS, AC and monitoring of IoT data is proposed in this work.
- To collect data from patients by IoT sensors and to prune the data using decision tree (DT).
- To classify the data as CD and non-confidential data (NCD) by using data owner (DO) defined fuzzy rule (FR) classification.
- To apply attribute based encryption (ABE) to CD instead of ED for reducing the processing complexity and to store CD in off-chain.
- To create a CS based off-chain block by using SC in a permissioned network which avoids public access and overcomes block size limitations.
- To effectively monitor the authorized user access through on-chain network.
- To reduce storage space and access time (AT) complexity, to provide efficient AC and monitoring and to optimize the BC metrics like throughput, latency and network scalability.

The remaining sections are organized as follows. In Section 2, the existing works are related to IoT data collection, data classification, secure data storage, AC and monitoring system in cloud and BC is discussed with merits and limitations. In Section 3, the proposed secure IoT data storage, AC and monitoring system using BC technique is discussed with system architecture and necessary algorithms. In

Sections 4 and 5, the mathematical analysis and experimental results of the proposed system are discussed with necessary comparisons. Finally, in Section 6, the proposed technique is concluded with the future enhancements.

2 RELATED WORKS

The existing works related to IoT based data collection, storage, AC and monitoring system in cloud and BC are going to be discussed with its merits and limitations.

2.1 Blockchain Based IoT Data Collection and Storage

Shafagh et al. proposed the BC based IoT data sharing technique. The time-series data has been divided into a number of continuous chunks and are linked together through hash functions. The time series based IoT data was stored in a locality aware decentralized storage area and access information has been stored in on-chain mode. It allows fine-grain AC that leads to moderate overhead [11]. Li et al. discussed the large scale IoT data storage and protection in BC technique. The IoT devices data has been collected from different devices and stored in the distributed hash table. The hash table pointers have been stored in BC storage locations for rapid identification. The AC has been assigned to the hash table pointers for the authorized user's access. The data storage is performed in a proficient but not in an authentication scheme [12]. Casado-Vara et al. used the BC technique for IoT data sharing using edge computing. The smart controller collecting data from different IoT devices and storing the data in an edge computing device takes lesser power than conventional storage. The SC is used for validating the data collecting IoT devices. The information collected by IoT sensors is stored in a side-chain and it is linked to the main-chain [13].

Xu et al. proposed the BC based IoT data storage and analysis. The IoT data has been collected from different objects by using object ID, methods, policies and attributes. Sapphire dependent BC created by using OSD-SC reduces IoT data analysis overhead and optimizes the storage space better than the other techniques [14]. Goyat et al. discussed the IoT data storage with privacy authentication in BC. By using cluster head, the IoT information has been collected from various locations and sent to base station node. The base station node maintains the records about the data which is forwarded to cloud and BC. The base station based BC generation and monitoring process eliminates the malicious revoked certificate usage [15]. Javed et al. analyzed the e-health record storage in BC technique. The health records stored in the electronic form is a more challenging task than the conventional storage regarding the security aspects. The conventional storage allows the access to the authorized users and not to the unauthorized users, but in the electronic form, everyone is able to access the record without knowing who is DO. Hence, the healthcare records are encrypted and stored in CS and data secrecy depends on CSP. To avoid this issue, the medical records are stored in blocks in the BC technique for providing better AC than the cloud based data storage [16].

Zhang et al. discussed the IoT based smart manufacturing and BC based trusted data management. The data which is generated in a manufacturing sector is collected through IoT devices and stored in blocks. This storage technique provides smart manufacturing system and increases the transaction efficiency with quality assurance [17]. Dwivedi et al. proposed the healthcare based BC generation using IoT data. In the current situation, user's medical data needs to be stored and shared in an electronic form for the quickest response to handle emergency cases and to provide treatment on time. Due to confidentiality, the patient's healthcare data needs to be stored and shared in a confidential manner. The existing CS has higher security issues. To overcome these issues, the BC based secure storage and sharing are used in the present system [18]. Wang used the BCDS for IoT based clinical data management and transfer. The clinical data has been collected by IoT devices directly from patients and stored in blocks. Based on DO AC, the data is accessed by authorized members. This DO based monitoring technique provides better AC and monitoring to CD than the conventional AC and monitoring technique [19].

Hinze et al. proposed the wearable IoT device based healthcare data collection from the forestry workers. The people who work in remote areas are able to monitor their health by the wearable devices. The rule based data analysis measures the deviations in the health conditions and communicates the information to health centers for providing immediate remedies to them [20]. Mutanu et al. discussed the IoT based health monitoring technique to enhance the healthcare sectors. The IoT sensors collecting data in different diversity and formats like CVS, JSON, etc., are an efficient way. The data privacy, accuracy level and communication efficiency have been improved in this work [21].

2.2 Blockchain Based Access Control and Monitoring

Liu et al. proposed the IoT data AC using BC technique. The Attribute Based Access Control (ABAC) and hyper-ledger fabric BC technique have been used for AC and monitoring. Three different types of SCs have been used for AC generation like device, policy and access contract. These SCs have been integrated for the generation and management of AC. This system ensures data consistency in an efficient way [19]. Ali et al. used the BC based permissioned network for the IoT data AC. Based on query based permissioned delegation, the AC has been created in a BC. This BCAC technique provides the decentralized, verifiable, trusted and secure services to authorized users. The Simple Promela Interpreter model is used for the AC implementation [22].

Wang et al. discussed the BC based data sharing and fine grained AC system. The BC based decentralized storage technique eliminates the issues of CS. The DO's have the complete control over their data in a BC technique. Ethereum based framework has been used for data sharing and AC generation provides better AC and monitoring than the CS [23]. Ma et al. proposed the BC based hierarchical AC in an IoT with distributed key management using fog computing to reduce the latency and cross domain access. This AC scheme provides high scalability,

extensibility, decentralized and fine grained auditability to IoT data. The group access and authorization process have been done [24]. Shi et al. discussed the BCAC technique in a distributed IoT. Each node in an IoT has been identified through node account address and stored in a block. The symmetric encryption algorithm is used to achieve the privacy preserving, authorization and authorization revocation [25].

Sun et al. discussed the IoT data AC with security, cross domain and lightweight process with BC. The permissioned BC with ABAC and identity based signature scheme have been used for providing security, cross domain access and lightweight process. The IoT devices are divided into different functional domains. Each functional domain data is stored in a separate local block and local blocks are combined to generate the final BC [26]. Feng et al. proposed the 5G enabled IoT data based BC dependent AC framework. Three different types of chain-codes are constructed, such as policy management, credit evaluation and AC chain-code. The chain-codes have been used for the AC generation and the two-step credit-based raft consensus is used for block construction. It takes lesser computational time and lower hardware resource consumption than the existing techniques [27].

Ding et al. proposed an ABAC scheme using BC in IoT data. The ABAC technique based IoT data management simplifies the access management and the BCDS scheme avoids the single point on failure and data tampering process for the management of medical records. This technique provides higher storage and security efficiency and lightweight calculations on IoT data [28]. Zhang et al. proposed the AC scheme based on BC using IoT device based data storage. The ABAC provides fine-grained AC, flexible and decentralized AC of IoT devices. Authority nodes based BC has been constructed for major computations and also provides scalability, efficient IoT device data management [29]. Tanwar et al. proposed the healthcare record based IoT data maintenance with BCAC. The ABAC technique is used to control the accessibility of healthcare record with hyper-ledger based data storage. The chain-code based BC is used to create the blocks in a BC [30]. Maseleno et al. used the BC technique to maintain the healthcare based IoT data. The healthcare data is classified as CD and NCD. Afterwards, the CD has been stored in different layers of encryption and decryption [31].

Cerchione et al. designed the BC based distributed healthcare ecosystem. The healthcare data has been stored in the private, permissioned BC location and the information processing theory has been used to validate the BC records. This BC record maintenance reduced the medical errors and improved the quality of service [32]. Xiang and Zhao discussed the BC based searchable encryption in healthcare applications. The searchable and fine-grained AC technique provides data confidentiality. The ABE and BC features have been combined to provide better confidentiality to healthcare CD [33]. Poongodi et al. constructed the BC network between hospitals, medical centers, insurance companies and patients. The individual patient record has been stored in BC for quick access of the members involved in the network. This quick access reduces latency and increases the throughput and quality of the transactions [34].

Based on the above literature review analysis the following points are summarized:

- The BCDS management is a more efficient way of storage than the CS.
- The DO have the control over their data instead of CSP.
- The ABAC scheme has been used for the generation AC in a BC.
- In another side, the chain-code and hyper-ledger based block generation is used for the IoT data storage.
- The permissioned BC is used to store CD and permission-less BC is used to monitor the off-chain.

Limitations of the existing techniques:

- The storage size of the blocks is not analysed deeply. The major limitation of the BC is the block size. Hence, data analysis is required before storing the data in a block.
- The ABAC is not sufficient for providing better AC. Hence, further control verification is required in a BCAC.

To overcome the abovementioned limitations, the secure IoT data storage, AC and monitoring system using BC technique are proposed in this work.

3 PROPOSED BC BASED STORAGE, AC AND MONITORING

The proposed technique collects IoT based healthcare data from the patients and sends the data for pruning using DT technique. The pruned data is classified as CD and NCD by using FR based classification. Subsequently, the classified CD is encrypted by ABE technique, and hash code (HC) is generated from the encrypted CD by using secured hash algorithm (SHA-256). The generated HC is used for block generation in an off-chain mode. The DO generates and stores the AC in an on-chain mode. By using the AC rules, the on-chain mode controls and monitors the off-chain mode access. In this process, the DOs have the complete control over their data. Figure 2 shows the overall system architecture of the proposed BCDS, AC and monitoring technique. Table 1 lists the notations and their corresponding abbreviations are used in the proposed technique.

The overall organization of the proposed system is discussed as follows.

3.1 Internet of Things Data Collection and Pruning

Different types of sensors are fixed on the patients body to measure the health condition like blood pressure, temperature and heart beat, etc. In the proposed system, the Threshold Value (T_V) is fixed for each sensor by the DO. If the Measured

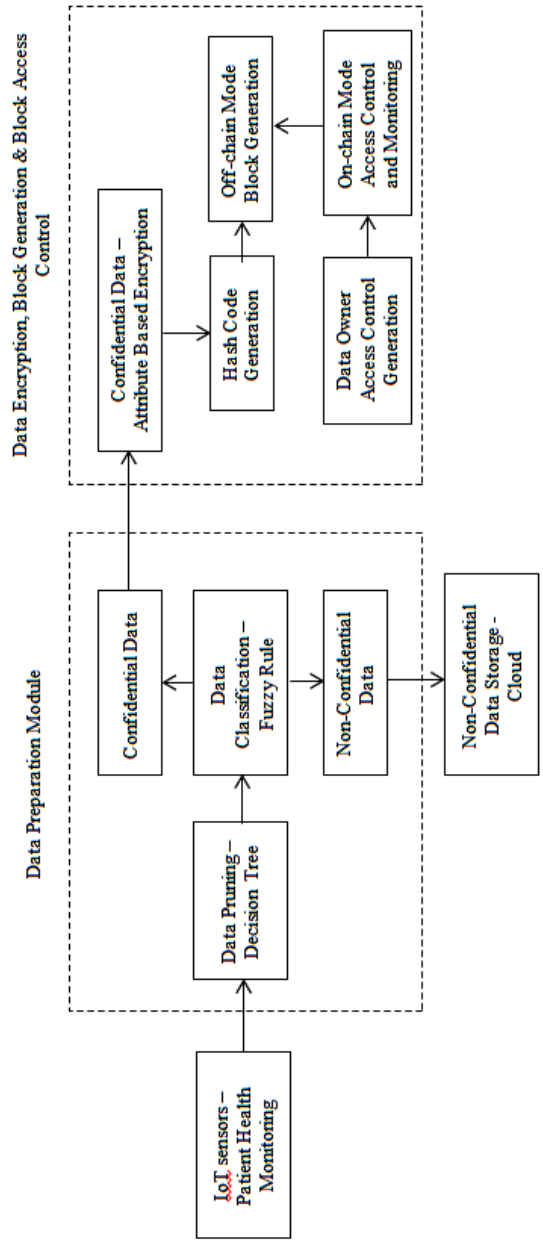

Figure 2. System architecture – BCDS, AC and monitoring technique

Terms	Abbreviations	Terms	Abbreviations
IoT	Internet of Things	DO	Data Owner
ABE	Attribute Based Encryption	PR	Private Key
SC	Smart Contract	PU	Public Key
ABAC	Attribute Based Access Control	T_V	Threshold Value
P_D	Pruned Data	M_V	Measured Value
VID	Verifier ID	CD	Confidential Data
D	Deviation	B_P	Base Point
FV	Fuzzy Value	T_T	Time Taken
TS	Time Stamp	N	Nonce
PT	Plain Text	RID_i	Role ID of ith User
CT	Cipher Text	ML	Machine Learning
FR	Fuzzy Rule	ECC	Elliptic Curve Cryptography
LT	Life Time	NCD	Non-Confidential Data
HC	Hash Code	AL	Attribute Label
ED	Entire Data	AC	Access Control
ST_{space}	Storage Space	BCAC	Blockchain Based Access Control
CS	Cloud Storage	CSP	Cloud Service Provider
A	Attacker	BCDS	Blockchain Based Data Storage
A_T	Access Time	PBHC	Previous Block Hash Code
BC	Blockchain	CSP	Cloud Service Provider

Table 1. Notations and abbreviations

Value (M_V) of specific sensor is higher or lower than the specific T_V, the M_V is transferred to data collection device. Equation (1) is used to calculate the Deviation (D) of T_V and M_V value.

$$D = T_V - M_V \Longrightarrow \pm T_V. \tag{1}$$

Rarely the collected data may have missing or error values. To remove these values, the data pruning process is applied to the collected data. The DT based data pruning technique is applied to sensor data to remove the missing or error values. The DT classifies the data as lesser than T_V and greater than T_V. Subsequently, the pruning technique is applied to specific branch instead of complete tree.

The pruning process removes the error value from the M_V and missing values are filled by an average value of a particular sensor data. Now, the Pruned Data (P_D) is sent to classification. E.g. blood pressure of a patient is a significant data to save a life. If the pressure value is higher or lower than T_V it leads to death. Hence, the M_V is compared to T_V to store the changes of M_V in the particular time period.

3.2 Confidential and Non-Confidential Data Classification

Now, the P_D is classified as CD and NCD by FR. In healthcare domain, every user's health information needs to be maintained in a confidential manner. Usually, healthcare information consists of CD and NCD. For specific diseases, its treatment

information is highly confidential in comparison to the normal treatment information. To protect the CD is a more essential task than the NCD. In other aspects, the ED protection leads to higher computational complexity and reduces data usage of authorized users. Therefore, the CD is classified from the NCD before applying security techniques. The FR based CD classification rules are framed by the DO based on if-then-else condition and the T_V. Considering the list of attributes in a dataset like name, age, address, mobile number, income, email id, type of disease, and stage of the disease (initial, final and middle), etc. From these attributes, selected attributes are considered as CD and remaining attributes are considered as NCD. Depending on FR, the attributes are classified as CD and NCD like YES/NO, TRUE/FALSE or 0/1. The YES/NO condition is taken for the classification of CD in a proposed work. The DO assigns YES/NO values to each attribute at the time of FR rule formation. Table 2 shows the attributes and their corresponding fuzzy values (FV).

Attribute Label	**Attribute Name**	**Fuzzy Value**
AL_1	Patient Name	Yes
AL_2	Age	Yes
AL_3	Address	Yes
AL_4	Phone Number	Yes
AL_5	Email ID	No
AL_6	Disease	Yes
AL_7	Income	Yes
AL_8	Insurance Amount	No
AL_9	Stage of Disease	No
AL_{10}	Doctor's Name	No
AL_{11}	Hospital Name	No
AL_{12}	Zip Code	No
AL_{13}	Bill Amount	No

Table 2. List of attributes and fuzzy values

Equations (2) and (3) are used for generating of FR by using Table 2 values for which the attribute is classified as CD or NCD.

$$\text{CD} = \text{IF}(AL_1 \text{ AND } AL_2 \ \ldots \ \text{AND } AL_n) \tag{2}$$

else

$$\text{NCD} = \text{IF}(AL_1 \text{ AND } AL_2 \ \ldots \ \text{AND } AL_n). \tag{3}$$

If the attribute is identified as CD, then it is sent for encryption, otherwise it is stored in CS in PT form. Compared to ML techniques, FR based classification provides better results for CD identification. Hence, FR classification is used for CD and NCD identification. Now, the identified CD is transferred to ABE.

3.3 Attribute Based Encryption of Confidential Data

After identifying CD, the ABE is applied to CD instead of ED. The ABE is more suitable for DO based CD encryption and decryption. The major characteristics of ABE are flexible, fine-grained AC, key sharing and management is not required, collision free attack technique. Likewise, the ABE technique provides higher scalability, security and privacy to patients CD. Therefore, the DO(PU, PR) based ABE technique is used for CD encryption. The elliptic curve cryptography (ECC) algorithm is used to generate the PU and PR of DO by solving the basic ECC equation $y^2 = x^3 + ax + b$. The ECC algorithms security strength depends on the random value and base point. The generated PU and PR are used for the encryption and decryption of CD in Equations (4) and (5). Each CD contains the list of attributes which require protection from authorized access. The i^{th} DO, CD consists of (AL_1 AND AL_2 AND ... AND AL_n).

$$\text{Eny}(\text{CD}_i) = \text{PU}_i(\text{DO}_i(\text{CD})) \Longrightarrow \text{CT}(\text{CD}_i), \tag{4}$$

$$\text{Dey}(\text{CD}_i) = \text{PR}_i(\text{DO}_i(\text{CD})) \Longrightarrow \text{PT}(\text{CD}_i). \tag{5}$$

The i^{th} DO PU is used for the encryption of i^{th} DO, CD. Similarly, the i^{th} DO PR is used for the decryption of i^{th} DO, ciphertext (CT) $\text{CT}(\text{CD}_i)$. Algorithm 1 is used for the CD encryption and decryption.

Algorithm 1 CD Encryption and Decryption

Input: CD, PU, PR
Output: Eny(CD), Dey(CD)
for all DO Generate (PU, PR) **do**
  Encryption(CD)
  if $\text{CD}_i \in \text{DO}_i$ **then**
    $\text{Eny}(\text{CD}_i) = \text{PU}_i(\text{DO}_i(\text{CD})) \Longrightarrow \text{CT}(\text{CD}_i)$
  else
    $\text{Eny}(\text{CD}_{i+1}) = \text{PU}_{i+1}(\text{DO}_{i+1}(\text{CD}_{i+1})) \Longrightarrow \text{CT}(\text{CD}_{i+1})$
Decryption(CD)
if $\text{CD}_i \in \text{DO}_i$ **then**
  $\text{Dey}(\text{CD}_i) = \text{PR}_i(\text{DO}_i(\text{CD})) \Longrightarrow \text{PT}(\text{CD}_i)$
else
  $\text{Dey}(\text{CD}_{i+1}) = \text{PR}_{i+1}(\text{DO}_{i+1}(\text{CD}_{i+1})) \Longrightarrow \text{PT}(\text{CD}_{i+1})$
return $\text{CT}(\text{CD}) \setminus \text{PT}(\text{CD})$

Now, the encrypted CD is transferred to hash code (HC) generation.

3.4 Hash Code and Block Generation

The major features of hash function are to generate fixed length output for various sizes input and to provide collision free, one-way function, pre-image resistance and pseudo randomness. The one-way function takes input and produces an output in one direction only. The reverse process is an impossible task. Due to these characteristics, the hash function is used for block generation in a BC technique. In a proposed technique, the Eny(CD_i) is taken as an input for the HC generation. Depending on number of AL's present in a CD, the size of Eny(CD_i) varies from user to user. The Double SHA-256 is a suitable algorithm for the BC based HC generation because, the double SHA-256 algorithm is a collision free algorithm and produces hexadecimal values which is suitable for block generation process. Hence, the double SHA-256 algorithm is used for the HC generation in the proposed work. Equation (6) is used for the HC generation of Eny(CD_i).

$$\text{HC}(\text{CD}_i) = \text{Double\_SHA\_256}(\text{Eny}(\text{CD}_i)). \tag{6}$$

The generated HC of Eny(CD_i) is stored in a block. Likewise, all users Eny(CD) based HC is generated and stored in a block for the BC generation. Every block in the BC consists of HC of the Previous Block (PBHC), HC of the current block, Time Stamp (TS), Nonce (N) and AC. Equation (7) is used for the generation of block based on HC. In the block, TS is used to identify the block generation time, Nonce indicates the unique identification and AC represents AC limit.

$$\text{Block}(\text{CD}_i) = (PB_{HC} + H(\text{CD}_i) + AC + TS + N) \tag{7}$$

Algorithm 2 is used for generating of HC and block based on Eny(CD_i).

Algorithm 2 Hash Code and Block Generation

Input: Double SHA256, Eny(CD_i)
Output: HC(CD_i), Block(CD_i)
for all Eny(CD_i) **do**
  Generate HC(CD_i)
  HC(CD_i) = Double_SHA_256(Eny(CD_i))
  return HC(CD_i)
  Generate Block(CD_i)
  Block(CD_i) = (PB_{HC} + HC(CD_i) + $AC + TS + N$)
  return Block(CD_i)

Now, the generated block is added to the BC.

3.5 Smart Contract and Blockchain Construction

SC plays a key role in the BC construction and is executed automatically when predetermined conditions are met. The major benefits of SC are backup, auto

saving, safety, speed and accuracy. In the proposed healthcare data management, the SC is executed when the T_V variations occur. The following code is the solidity based SC routine to generate a BC. Now, the generated blocks are added into the BC. Figure 3 shows the BC structure of the proposed system.

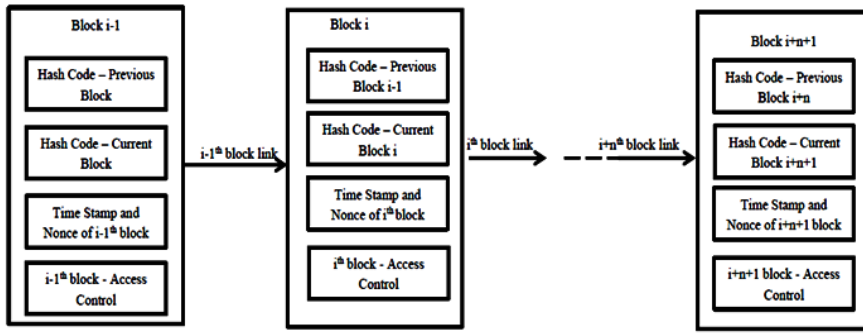

Figure 3. BC construction BCDS, AC and monitoring

Each block consists of the following components:

- Previous Block Hash Code (PBHC): The PBHC is used to maintain data integrity. When a particular block needs to be changed in BC, the PBHC also needs to be changed. This is an impossible task in BC. Hence, the data integrity is maintained in BC through PBHC.
- Current Block Hash Code (H(CDi)): In the proposed work, the encrypted data is stored in a block, it is in the form of HC. The HC maintained data integrity and data size are equal in all the blocks.
- Time Stamp (TS) and Nonce (N): The TS and N are used to uniquely identify the time of block generation.
- Access Control (AC): The AC defines the access rights of authorized users.

Algorithm 3 shows the SC representation of the proposed system.
Now the generated BCAC and monitoring is done through SC.

3.6 Access Control and Monitoring

The SC automatically verifies the authorized users AC. In the proposed system, the BC is constructed in a permissioned off-chain mode and allows only registered users access. The DO have the complete control over their CD and assign the AC to authorized users. The proposed technique doctors, nurse, medical student, representative and administrators are involved in block access. Each role has different kind of access rights. Before accessing a data in a permissioned network, the members need to register their role in the permissioned network. Table 3 shows the members

Algorithm 3 Solidity Routine to SC

```
Function addblock(address blockaddress, string HC, String AC) only DO public
{
Require(status = true);
Uint id = blockId[blockaddress];
if (id == 0) then {
    blockid[blockaddres] = block.length;
    id = block.length++; }
    Blockadded(blockaddress, HC, AC);
    Numberofblocks++;
}
```

involved in BC based IoT data storage, AC and monitoring technique and their roles.

The access types are:

- Read Only: To read content in a specific block.
- Write: To write content in a block and to create a block.
- Transfer: To transfer the particular block to authorized user.

The on-chain mode is used to monitor the off-chain mode block access. The members involved in the proposed system create the on-chain mode of BC. When a particular member needs to access a block in an off-chain mode, they need to send a request to on-chain mode. The request and authorization is verified by the members involved in an on-chain network and the access permission is provided to them. Equations (8), (9) and (10) are used to verify the AC of an authorized user.

Role ID	**Members**	**Access Type**	**Members Role**
R_1	DO	AC_1	Generate HC and Block Access and Transfer Block
R_2	Doctor	AC_1	Generate Block and BC Access and Transfer Block
R_3	Nurse	AC_2	Access Block
R_4	Medical Student	AC_2	Access Block
R_5	Medical Representative	AC_2	Access Block
R_6	Medical Administrator	AC_3	Access and Transfer Block

Table 3. Members access rights and roles

$$AC_1 = R_1 \text{ and } R_2 \Longrightarrow \text{Read, Write, Transfer.} \tag{8}$$

$$AC_2 = R_3 \text{ and } R_4 \text{ and } R_5 \Longrightarrow \text{Read,} \tag{9}$$

$$AC_3 = R_6 \Longrightarrow \text{Read, Transfer.} \tag{10}$$

Figure 4 shows the on-chain and off-chain representation of the proposed system. Algorithm 4 shows the AC and monitoring process. In the on-chain, the role identification number (RID) is verified by the members involved in the network. One third of the members need to accept the RID for accessing on off-chain blocks, otherwise the requester is unable to access the blocks.

Through the abovementioned design, the IoT sensor data is collected and performed data pruning by DT. Then the pruned data is classified as CD and NCD by FR. The CD is encrypted by ABE technique and the HC is generated for construction of off-chain blocks and block access is monitored by an on-chain network.

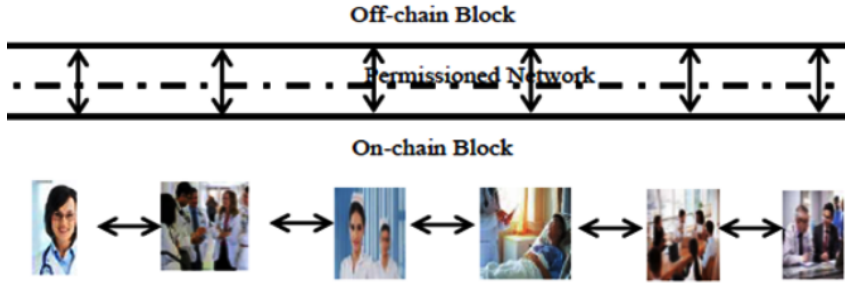

Figure 4. Representation of on-chain and off-chain block

Algorithm 4 Access Control and Monitoring

Input: Role, Access Type
Output: Allowed or Not
Register RID_i to on-chain network
Send Block_ID Access Requests to on-chain network
Check RID_i by Members in an on-chain network
if (RID_i == valid) **then**
    Assign $\text{AC}_i \Longrightarrow \text{RID}_i$;
else
    Reject Request
$\text{AC}_i = \text{HC}\{TS, N, \text{RID}_i, \text{Block\_ID}\}$
AC_i to off-chain network
Compute HC of AC_i in off-chain $\Longrightarrow \text{AC}_i^{'}$
if ($\text{AC}_i == \text{AC}_i^{'}$) **then**
    Allow Access
else
    Reject Access
Return Allow \ Reject

4 MATHEMATICAL BACKGROUND

This section consists of the functions involved in key generation, encryption and decryption, HC generation, block access time and space complexity analysis of the proposed technique.

4.1 Key Generation, Encryption, Decryption and HC Generation

Cryptography algorithms work behind the mathematical concepts. The proposed BCDS, AC and monitoring technique uses ABE encryption and SHA-256 based HC generation. The ECC equation $y^2 = x^3 + ax + b(\mathrm{mod}\, y)$ is used for DO(PU, PR) key generation. The variables a and b values depend on random numbers from 0 to $n-1$. The DO generate their own (PU, PR) key pair using ECC algorithm based on the following process.

- **Initial Key Generation Setup** (1^{α}) – $(\mathbf{BP}, \mathbf{PR})$**:** This initial key generation setup takes α as the initial value for the identification of Base Point (BP) and PR values. The PR is known to the DO and is hidden from others.
- **Key Generation PUGen(BP, PR)** – PU_i: The BP and PR values are used for the generation of PU of an i^{th} user such as $PU_i = \mathrm{PR}_i * BP$. In an ECC algorithm, the scalar multiplication is used for the PU generation instead of multiplication. In a scalar multiplication, the BP is added repeatedly to the PR to generate the PU.

The generated PU and PR are used for an encryption and decryption of CD for a particular DO. The following functions are used for the encryption and decryption of CD.

- $\mathrm{Eny}(\mathrm{CD}_i \in \mathrm{PT}(\mathrm{CD}_i), PU)$ – $\mathrm{CT}(\mathrm{CD}_i)$: The encryption of CD_i depends on PU of DO_i for producing the $\mathrm{CT}(\mathrm{CD}_i)$. In an encryption, the PT is XOR with the PU for producing the CT. The $\mathrm{PT}(\mathrm{CD}_i)$ consists of $\mathrm{PT}(\mathrm{CD}_i) \Longrightarrow A_1,\ A_2, \ldots, A_n$. Equation (11) shows the CT(CD) generation.

$$\mathrm{CT}(\mathrm{CD}_i) \Longrightarrow (\mathrm{PT}(\mathrm{CD}_i) \oplus PU). \tag{11}$$

- $Dey(\mathbf{CD}_i \in \mathbf{CT}(\mathbf{CD}_i), \mathbf{PR})$ – $\mathrm{PT}(\mathrm{CD}_i)$: The decryption of CD_i belongs to the $\mathrm{CT}(\mathrm{CD}_i)$ and PR of DO_i. Equation (12) shows the decryption of CD.

$$\mathrm{PT}(\mathrm{CD}_i) \Longrightarrow (\mathrm{CT}(\mathrm{CD}_i) \oplus \mathrm{PR}). \tag{12}$$

- $\mathrm{HashGen}(\mathrm{CD}_i)$ – $(\mathrm{HC}(\mathrm{CD}_i) \in (\mathrm{CT}(\mathrm{CD}_i), \mathrm{Double\_SHA\_256})$: The HC generation depends on $\mathrm{CT}(\mathrm{CD}_i)$ and Double SHA_256 algorithm shows in Equation (13).

$$\mathrm{Double\_SHA\_256}(\mathrm{Eny}(\mathrm{CD}_i)) \Longrightarrow \mathrm{HC}(\mathrm{CD}_i). \tag{13}$$

- AccBlock(HC(CD_i)): AccessHC(CD_i) in a block starts from the block request to gain specific block access permission. Equation (14) shows the block access.

$$\mathrm{Block}_{req}(\mathrm{DO}_i) = \mathrm{Token}\{\mathrm{RID}_i, \mathrm{TS}_i, \mathrm{AC}_i\}. \tag{14}$$

The block request for i^{th} DO consists of RID of i^{th} person along with TS and i^{th} block AC. This block request is given to on-chain and verified by the members involved in on-chain and the block access permission is granted to the requester. The grant permission shows in Equations (15) and (16):

$$\mathrm{Access}_{grand}(\mathrm{Block}_i) \;=\; \mathrm{Token}\{\mathrm{RID}_i, \mathrm{TS}_i, \mathrm{Acc}_{perm}, \mathrm{VID}\}, \tag{15}$$

$$\mathrm{Acc}_{perm} \Longrightarrow \{\mathrm{Block}_{id}, \mathrm{Acc}_{Limit}, \mathrm{LT}_{perm}\}. \tag{16}$$

Access grant consists of RID of the i^{th} user, TS of i^{th} block request, access permission and verifier ID (VID). Due to access limit and life time (LT) of the token, the long-time access of a block with the same token is controlled by the LT of a token.

4.2 Time Complexity Analysis

The time complexity of the proposed work depends on IoT data collection (DC), data pruning (PD), data classification (D_{cla}), CD encryption (Eny(CD)), HC generation and block generation (Blk_{gen}). The total time required (TT_{Req}) for the proposed technique is calculated by Equation (17):

$$CD(TT_{Req}) = \sum(T_{taken}\{D_C + CD + D_{cla} + \mathrm{Eny}(\mathrm{CD}_i) + \mathrm{HC}(\mathrm{Eny}(\mathrm{CD}_i)) + \mathrm{Blk}_{gen}\}). \tag{17}$$

If n number of patient records are involved in a process then the time requirement for processing n records is $TT_{Req} * n$. The proposed technique time requirement is compared to ED encryption and block generation time. Equation (18) is used for calculating the ED processing time.

$$\mathrm{ED}(\mathrm{TT}_{Req}) = \sum(T_{taken}\{D_C + \mathrm{ED} + \mathrm{Eny}(ED) + \mathrm{HC}(\mathrm{Eny}(ED)) + \mathrm{Blk}_{gen}\}). \tag{18}$$

In a proposed CD based encryption and Blk_{gen} time depends on the number of attributes involved in the CD. The attribute count of CD is lesser than ED and varies for each DO. Hence, the time taken for $\mathrm{Eny}(ED) > \mathrm{Eny}(\mathrm{CD})$ and the $\mathrm{ED}(\mathrm{TT}_{Req}) > \mathrm{CD}(\mathrm{TT}_{Req})$. Likewise, the TT for the proposed technique block request to access is calculated by Equation (19) which consists of the block request time (Block_{req}) to block access grant (Access_{grand}) and access time (Access_{Time}) = $\mathrm{Block}_{size} * n$.

$$\mathrm{BlockAcc}_{Time} = \sum(\mathrm{Block}_{req} + \mathrm{Access}_{grand} + \mathrm{ED} + \mathrm{Access}_{time}). \tag{19}$$

If n number of transactions is requested concurrently, the block access time duration varies. Hence, the Average Access Time (AvgAcc_{Time}) for each block is

calculated by Equation (20).

$$\text{AvgAcc}_{Time} = \left(\frac{\text{BlockAcc}_{Time}(B_1 \ldots B_n)}{n} \right). \tag{20}$$

The Total Access Time (TotalAcc_{Time}) of n request is calculated by Equation (21).

$$\text{TotalAcc}_{Time} = \text{BlockAcc}_{Time} * n. \tag{21}$$

In a proposed technique CD is encrypted and used for HC generation and Blkgen instead of ED. Hence, it is proven that the processing time required for CD is lesser than ED processing time.

4.3 Space Complexity Analysis

The storage size (ST_{space}) requirement of CD based blocks is calculated by Equation (22).

$$\text{ST}_{space}(\text{HC}(\text{CD}_i)) = \text{Size}(\text{CD}(A_1 \ldots A_n)). \tag{22}$$

The storage size requirement is lesser than ED such as $\text{Space}_{Req}(\text{CD}) < \text{Space}_{Req}(ED)$. The storage size of ED depends on the total number of attributes and the CD depends on the number of attributes in a CD, whereas the attribute counts in CD are lesser than ED. Hence, $ST_{space}(\text{CD}) < ST_{space}(ED)$ is proven. Based on this analysis the key generation, encryption, decryption, HC generation, time and space complexity, block AT and storage size requirement is estimated in the proposed system.

5 SECURITY ANALYSIS

The major role of cryptography algorithm is to provide secure storage to patient's information in all aspects without compromising any security attacks. Similarly the BC technique maintains data integrity and provides better AC and monitoring to CD without third party public auditors. Hence, the cryptography technique is integrated to BC technique. This section focuses on various security attacks analysis of the proposed technique.

IoT node and data based attacks: The major security issues in IoT devices and data are node capture attack, replay attack, side channel attack, eavesdropping, false data injection, spoofing, sinkhole attack, DoS attack, unauthorized attack, phishing attack, malicious attack and authentication. These issues are avoided through secure storage of IoT data in BC such as the node capture attack, side channel attack, replay attack are avoided through DO based AC. The spoofing, sinkhole attack, DoS attack, data injection, phishing, malicious attack and authentication issues are overcame through permissioned BC based AC and monitoring. The permissioned BC allows only authorized registered users, and

the encrypted data HC is stored in an off-chain. Hence, the unauthorized users are unable to access the IoT node and data without the knowledge of DO.

Data privacy and authentication: The data privacy and authentication is achieved by SC and encrypted HC. The SC provides perfect AC, self-monitoring, auto decision making and to update the access policies in an efficient way and encrypted HC is accessed by authorized users only. Hence, the data privacy and authentication is achieved effectively.

Data confidentiality and integrity (modification attack): The fundamental security requirements are data confidentiality, integrity and authentication. In the proposed system, the data privacy and authentication is achieved through SC. Similarly, the data confidentiality and integrity is achieved through encrypted HC storage in BC. The major advantage of BC technique is to maintain data integrity through PBHC and one-way property. If the particular block information needs to be changed, the PBHC also need to be changed. This HC depends on TS and it is a continuous process. Hence, the modification of specific block is an impossible task in BC. Similarly, the data confidentiality is achieved through DO based encryption. This DO based encryption avoids third party storage and management. Hence, the data confidentiality and integrity is achieved and proved.

Resistance against reply attack, man-in-the-middle attack and impersonation attack: In the proposed BC based secure storage, TS is added to every block and transaction. Depending on TS value, the freshness of data and transaction is identified. The freshness of TS avoids the reply attack. Similarly, the on-chain based BC controls the man-in-the-middle attack. The authorized registered users are able to participate in the process. Thus, the man-in-the-middle attack is avoided. The impersonate attack is avoided by the DO based data collection, storage and AC such as the AC policy generation is an impossible task for an A. Due to DO based key pair generation, the A is unable to generate the PR and AC policy. Hence, the proposed technique against the reply attack, man-in-the-middle attack and impersonation attack avoidance is proven.

Resist double-spending attack: The DO defines the AC and number of times access for a particular block by a particular user. The same AC ID will not be used more than once by the same user. Due to this limitation, the double-spending is avoided. Table 4 shows the security analysis of proposed and conventional technique.

Based on the above analysis, it is proven that the proposed technique against the IoT node and data based attacks provides data privacy and authentication to patient information, data confidentiality and integrity is maintained against the resistance reply attack, man-in-the-middle attack, impersonate attack and double spending attack.

Parameter	**Third Party Storage and AC**	**Proposed BC Based Storage and AC**
Confidentiality	Low	High
Privacy	Low	High
Integrity	Low	High
User Control	No	Yes
Auditing	Static	Dynamic
Access Control	Service Provider	Data Owner
Medical Record Control	Incomplete Control	Complete Control

Table 4. Security analysis of proposed and conventional technique

6 EXPERIMENTAL RESULTS

The experimental evaluation of the proposed BC based secure IoT data storage, AC and monitoring technique is conducted through solidity 0.4.11 package and java. The ECC and Double_SHA256 algorithms are used for encryption, decryption and HC generation process on IoT based healthcare data. In the proposed technique `https://data.world/datasets/ehr` dataset is used for an analysis [35]. The FR classification is applied to classify CD and NCD in the dataset. The dataset contains information about the patients heart diseases, which is highly confidential in comparison to other diseases. Hence, this dataset is taken for an analysis.

6.1 Classification Time Analysis

In FR classification, the classification time depends on the number of rules and the DO's. In the proposed technique, single if-then-else condition used for identifying the CD for a single DO takes 3 seconds for classification. Totally 1 000 DO's are presented in a proposed technique. Hence, $1\,000 \times 3 = 3\,000$ seconds are required for the CD classification. Likewise, classification accuracy depends on DO willingness, thus, the if-then-else rule is based on DO willingness. Hence, FR classification technique produced greater than 96 % classification accuracy. The classification time and accuracy is compared to the ML algorithms SVM, KNN and NB. The ML algorithms classification time and accuracy depends on training data. Figure 5 shows the comparison of proposed and ML algorithm classification accuracy. When compared to SVM, KNN and NB classification, it is proven that the proposed FR classification produces higher classification accuracy rate such as greater than 96 % in all DO willingness. Hence, the FR classification technique is used for CD classification.

6.2 Storage Space Analysis

The maximum size of a single document is 50 MB. This is applicable to 1000 users hence, $1\,000 \times 50 = 50\,000$ MB for ED. To store 50 000 MB size document in blocks leads to highest processing time and needs more storage space in blocks. The major

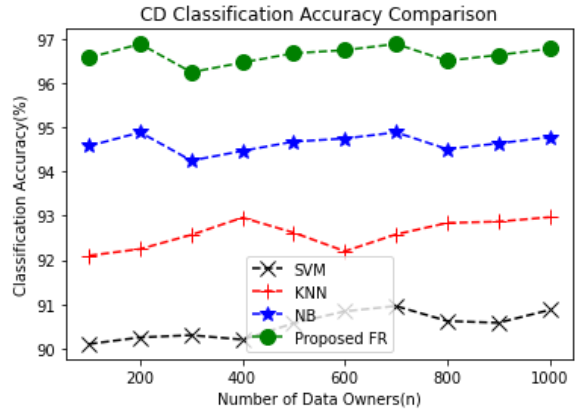

Figure 5. Classification accuracy comparison

constraint of BC is block size such as the maximum size of each block is 1 MB. To handle this issue, the CD is stored in a block instead of ED. The CD size varies from 15 MB to 30 MB depending on DO willingness. Thus, the proposed technique storage size requirement is from 30 % to 60 % instead of 100 %. Table 5 shows the storage space requirement analysis of the proposed and ED storage for 10 DO's. The similar process continues to all DO's. The ED storage takes higher storage space than the proposed CD storage space requirement. Hence, the storage space requirement is reduced and the proposed technique is proven.

DO ID	ED Storage Space Requirement (MB)	CD Storage Space Requirement (MB)	% of Storage Space Required
DO_1	50	15.37	30.74
DO_2	50	18.25	36.50
DO_3	50	28.78	57.56
DO_4	50	22.69	45.38
DO_5	50	17.89	35.78
DO_6	50	15.48	30.96
DO_7	50	16.52	33.26
DO_8	50	19.63	39.26
DO_9	50	20.45	40.90
DO_{10}	50	29.36	58.72

Table 5. Storage space utilization analysis

The storage space utilization reflects in the storage cost and processing time. The ED requires 100 % storage space thus it is proven that ED takes higher processing time and storage cost. It is proven that the proposed CD takes 30 % to 60 % of storage space and processing time.

6.3 Encryption and Decryption Time Analysis

Generally, the encryption and decryption time depends on document size. If document size is increased, the encryption and decryption time is also increased. To reduce the encryption and decryption time, in a proposed system 30 % to 60 % of data CD is encrypted instead of 100 % ED. Figure 6 shows the encryption time analysis of the proposed technique. Single ED encryption time is 4.5 seconds and CD encryption is from 0.3 to 1.5 seconds. Thus, 1 000 users ED encryption takes 4 500 seconds and CD encryption takes 300 seconds to 1 500 seconds. Thus, it is proven that the proposed CD based encryption requires 30 % to 60 % of encryption time. Likewise, the decryption time also depends on a document size. In the proposed CD technique, 30 % to 60 % of data is decrypted instead of 100 % of data. Figure 7 shows the decryption time analysis of the proposed technique with ED decryption time. Based on this analysis, it has been proven that the encryption and decryption time requirement is lesser than ED encryption and decryption time. Hence, the proposed CD encryption and decryption is preferable to the large size document encryption and decryption.

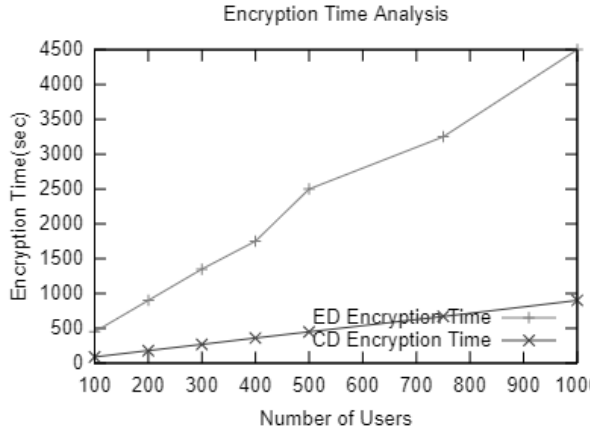

Figure 6. Encryption time analysis

6.4 Block Generation and Access Time Analysis

In the proposed technique, the block generation and A_T depends on HC. Generally, the input to HC varies in size. Thus, the block generation cost varies for each size. The block generation consists of the HC generation and block generation time. Figure 8 shows the block generation time for the proposed technique. In hashing technique, the output HC is equal for all documents. The block A_T starts from access request to block access. The block A_T for the proposed technique is lesser

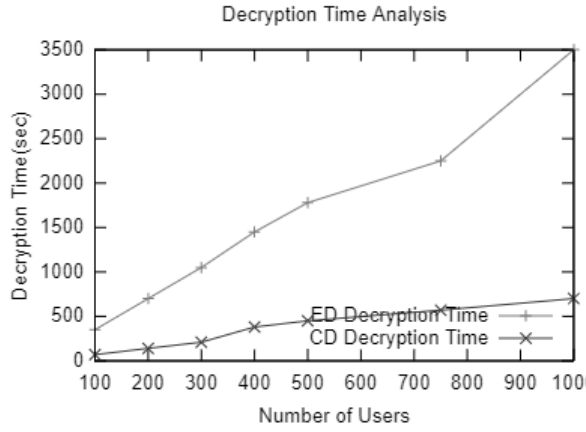

Figure 7. Decryption time analysis

than 30 % of ED A_T. Figure 10 shows the block generation time for the proposed technique.

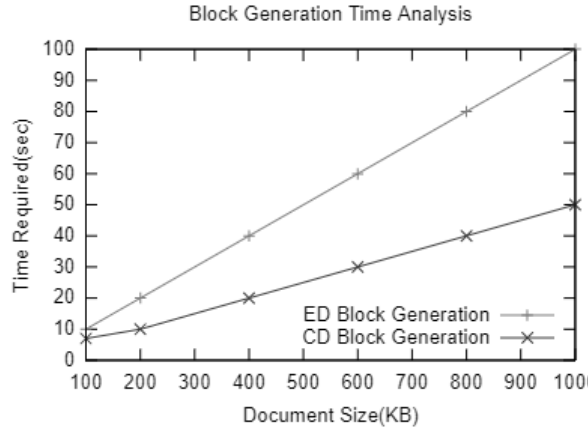

Figure 8. Block generation time analysis

6.5 Blockchain Latency Time and Throughput Analysis

The latency time (L_T) analysis is a key performance indicator of the BC based data process. The BC latency is the time duration between two blocks generation in the BC. The ED based block generation takes higher time than the CD data based block generation. When a block size is large, the average L_T is also high. Similarly, the

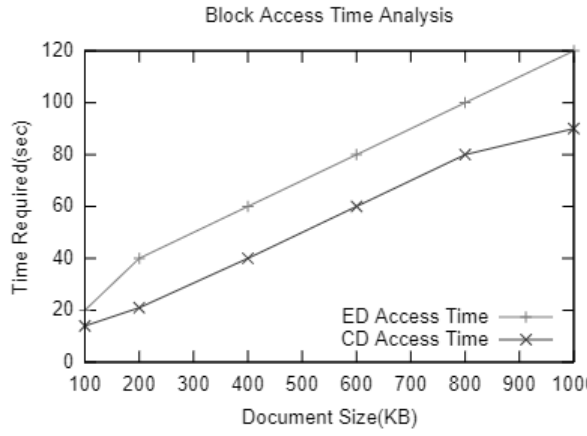

Figure 9. Block access time analysis

L_T depends on the throughput also. If the throughput rate is high, latency rate will be low. Thus, latency and throughput are inversely proportional. The transaction latency and throughput is measured by Equations (23) and (24).

$$\text{Latency} = (\text{CNT} * \text{NT}) - \text{ST}, \tag{23}$$

$$\text{Throughput} = \left(\frac{\text{CT}}{\text{TTT}}\right) * \text{CNT} \tag{24}$$

where

- CNT – Confirmation Time,
- NT – Network Threshold,
- ST – Submit Time,
- CT – Committed Transactions,
- TTT – Total Transaction Time and
- CNT – Committed Node Transactions.

Figure 10 shows the average L_T analysis of the proposed system and ED. The basic measurements taken in the proposed system are based on the number of rounds, the number of transactions per round, the transaction mode and the rate of transaction. Five rounds are taken for the process, each with 1 000 transactions for write operation and the transaction rate varies from 100 to 250 tps. The proposed system is compared to ED processing. In Figure 10, x axis shows the throughput in transaction per second (tps) and y axis shows the average L_T in seconds. Compared to ED processing, the proposed CD processing takes lesser L_T due to the data size. When the block size is increased, the L_T is also increased. In the proposed technique,

instead of ED, the CD based process performed. Thus, it has been proven that the proposed technique L_T is lesser than the ED L_T.

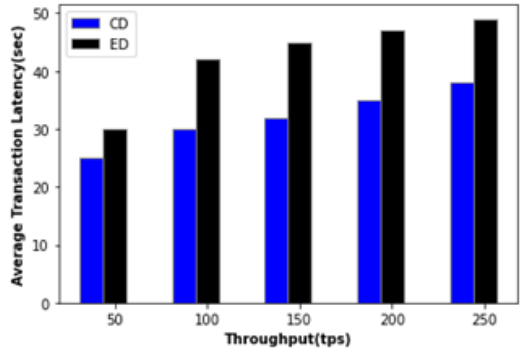

Figure 10. Transaction average latency

6.6 Processing Time Analysis of Entire Document and Confidential Data

The overall processing time (P_T) of the ED is compared to CD based classification, encryption, HC generation, block generation and block A_T. Table 6 shows the comparison of the proposed and ED process. In a proposed CD process, single document classification takes 3 sec, encryption takes 0.5 sec, HC generation takes 2 sec, block generation takes 1.5 sec and block access takes 3.5 sec. Depending on CD size the P_T varies from 10 sec to 12.57 sec. Hence, 1000 users' document takes 10 500 seconds. The ED encryption takes 4.5 sec, HC generation takes 3 sec, block generation takes 4.8 sec and block access takes 3.5 sec for single document and 15 800 sec for 1000 users. The proposed CD takes 66 % to 80 % P_T. Thus, it has been proven that the ED takes 20 % higher processing time than the proposed CD.

Thus, it is proven that the overall P_T is lesser than ED. Based on the experimental results, the proposed CD based Secure IoT data storage, AC and monitoring technique storage space utilization, encryption and decryption time requirement, block generation and A_T, it has been proven that the average L_T is lesser than ED P_T.

6.7 BCDS, AC and Monitoring Technique Key Features Comparison to Conventional Techniques

The proposed technique's key features are compared to the conventional secure storage, AC and monitoring technique [36]. Table 7 shows the comparison process of the proposed and the existing techniques such as hierarchical AC, group key AC, public key certificate, pre-shared key access and BC based key management

DO ID	**ED P_T(Sec)**	**CD P_T (Sec)**	**% of P_T Required**
DO_1	15.8	10.50	66.45
DO_2	15.8	11.23	71.07
DO_3	15.8	12.45	78.79
DO_4	15.8	11.86	75.06
DO_5	15.8	11.15	70.56
DO_6	15.8	10.23	64.74
DO_7	15.8	10.98	69.49
DO_8	15.8	12.12	76.70
DO_9	15.8	12.25	77.53
DO_10	15.8	12.50	79.11

Table 6. Processing time comparison of ED and CD

(BDKM). The parameter values are indicated as LOW (L), Medium (M), High (H), None (N), Untrust (U) and Yes (Y). Based on this analysis the proposed CD based secure storage, AC and monitoring technique provides higher scalability, lower key updation and decentralized storage and auditing. Likewise, the proposed technique provides higher extendability and resilience, lesser computation and communication overhead and eliminates centralized storage overhead issues. Hence, it has been proven that the proposed system provides better results in all aspects.

Key Features	Hierarchical Access	Group Key Access	Public Key Certificate	Pre-Shared Key Access	BDKM	Proposed BCAC
Scalability	L	M	M	L	M	H
Decentralized	N	N	N	N	Y	Y
Auditing	U	U	U	U	Y	Y
Key Update	M	H	H	H	L	L
Centralized Storage Overhead	M	M	M	M	N	N
Extendability	L	L	L	L	H	H
Computation and Communication Overhead	H	H	L	L	H	L
Resilience	M	L	M	L	M	H

Table 7. Key features comparison of proposed and conventional techniques [36]

The proposed BCAC technique's running time and storage space is compared to the existing tuCP-ABE and BC based cipher policy ABE (BCAS) techniques. Table 8 shows the comparison of proposed and existing techniques running time and storage space [37]. Due to sensitive attribute process, both the running time

and storage space requirement of the proposed technique is lesser than the existing technique. Thus, it is proven that the proposed technique is better than the existing technique.

Run Time of Proposed and Existing Technique (Sec)				
Algorithm	Setup	KeyGen	Encryption	Decryption
tuCP-ABE	0.14801	0.07155	0.44139	0.65323
BCAS	0.14801	0.04601	0.43787	0.67775
Proposed BCAC	0.14801	0.04325	0.35287	0.48524
Storage Space Utilization of Proposed and Existing Techniques (KB)				
Algorithm	Setup	KeyGen	Encryption	Decryption
tuCP-ABE	3.14062	1.24275	11.0379	6.54142
BCAS	3.14062	0.57812	10.7773	6.41016
Proposed BCAC	3.14062	0.45715	8.4523	5.92432

Table 8. Run time and storage space comparison [37]

Summary of the proposed technique:

- The FR based classification technique provides above 96 % classification accuracy based on DO preferences.
- The CD based storage technique requires 30 % to 60 % storage space than ED storage technique.
- The CD based encryption and decryption takes 66 % to 80 % of P_T.
- The CD based HC generation takes lesser P_T than ED based HC generation time. i.e. the overall P_T of proposed technique is 20 % lesser than ED.
- In security aspects, the proposed technique provides DO based AC and monitoring through BC.

Thus, secure storage, AC and monitoring to patient's healthcare records without compromising confidentiality, integrity and availability is achieved in the proposed system.

7 CONCLUSIONS

In a proposed system the IoT based data is collected from patients and the measured value is deviated from the predefined threshold value. The measured value is stored in the IoT devices. Then, the measured value is pruned by decision tree by removing the error and missing values. Now, the pruned data is classified as confidential and non-confidential data by a fuzzy rule classification technique. These fuzzy rules are framed by data owners. Hence, above 96 % accuracy is achieved in the proposed technique when compared to SVM, KNN and NB classification techniques. The

classified confidential data is encrypted by attribute based encryption technique. When compared to the entire document encryption, the confidential data based encryption takes lesser than 20 % storage space and encryption time in ED. Now, the encrypted data is taken for hash code and block generation. Due to collision resistance and one-way function property, the double SHA_256 is used for hash code generation. The generated hash code is stored in a block along with time stamp; previous block hash code and nonce values for avoid data integrity issues. When compared to the entire document process, the proposed confidential data based processing takes lesser than 20 % of processing time and takes lesser latency than the entire data processing in the cold storage method. Hence, the proposed system utilizes lesser storage space, and the processing time has been proven without compromising confidentiality, integrity and availability.

In future, the unstructured and semi-structured document based confidential data classification can be done in the integrated classification technique for improving the classification accuracy and to create a BC network between clinical care providers for taking quick decisions about the diseases in emergency cases. It is planned to develop the wearable kit for helping remote patients. Additionally, when BC is integrated with artificial intelligence (AI), the classification accuracy will be improved. AI provides better understanding of problem and provides the solution instead of a normal classification. Hence, better decision will be taken through BCAI technique.

REFERENCES

[1] Cai, H.—Xu, B.—Jiang, L.—Vasilakos, A. V.: IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. IEEE Internet of Things Journal, Vol. 4, 2017, No. 1, pp. 75–87, doi: 10.1109/JIOT.2016.2619369.

[2] Rahman, M. S.—Islam, M. A.—Uddin, M. A.—Stea, G.: A Survey of Blockchain-Based IoT eHealthcare: Applications, Research Issues, and Challenges. Internet of Things, Vol. 19, 2022, Art. No. 100551, doi: 10.1016/j.iot.2022.100551.

[3] Ravikumar, S.—Kavitha, D.: IoT-Based Home Monitoring System with Secure Data Storage by Keccak-Chaotic Sequence in Cloud Server. Journal of Ambient Intelligence and Humanized Computing, Vol. 12, 2021, No. 7, pp. 7475–7487, doi: 10.1007/s12652-020-02424-x.

[4] Prabhu Kavin, B.—Ganapathy, S.: A Secured Storage and Privacy-Preserving Model Using CRT for Providing Security on Cloud and IoT-Based Applications. Computer Networks, Vol. 151, 2019, pp. 181–190, doi: 10.1016/j.comnet.2019.01.032.

[5] Kamruzzaman, M. M.—Yan, B.—Sarker, M. N. I.—Alruwaili, O.—Wu, M.—Alrashdi, I.: Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities. Journal of Healthcare Engineering, Vol. 2022, 2022, Art. No. 9957888, doi: 10.1155/2022/9957888.

[6] Dujak, D.—Sajter, D.: Blockchain Applications in Supply Chain. In: Kawa, A., Maryniak, A. (Eds.): SMART Supply Network. Springer, Cham, EcoProduction Book Series, 2019, pp. 21–46, doi: 10.1007/978-3-319-91668-2_2.

[7] Leible, S.—Schlager, S.—Schubotz, M.—Gipp, B.: A Review on Blockchain Technology and Blockchain Projects Fostering Open Science. Frontiers in Blockchain, Vol. 2, 2019, Art. No. 16, doi: 10.3389/fbloc.2019.00016.

[8] Helliar, C. V.—Crawford, L.—Rocca, L.—Teodori, C.—Veneziani, M.: Permissionless and Permissioned Blockchain Diffusion. International Journal of Information Management, Vol. 54, 2020, Art. No. 102136, doi: 10.1016/j.ijinfomgt.2020.102136.

[9] Hepp, T.—Sharinghousen, M.—Ehret, P.—Schoenhals, A.—Gipp, B.: On-Chain vs. Off-Chain Storage for Supply- and Blockchain Integration. IT – Information Technology, Vol. 60, 2018, No. 5-6, pp. 283–291, doi: 10.1515/itit-2018-0019.

[10] Xiao, Y.—Zhang, N.—Li, J.—Lou, W.—Hou, Y. T.: PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Attested Off-Chain Contract Execution. In: Chen, L., Li, N., Liang, K., Schneider, S. (Eds.): Computer Security – ESORICS 2020. Springer, Cham, Lecture Notes in Computer Science, Vol. 12309, 2020, pp. 610–629, doi: 10.1007/978-3-030-59013-0_30.

[11] Shafagh, H.—Burkhalter, L.—Hithnawi, A.—Duquennoy, S.: Towards Blockchain-Based Auditable Storage and Sharing of IoT Data. Proceedings of the 2017 on Cloud Computing Security Workshop (CCSW '17), ACM, 2017, pp. 45–50, doi: 10.1145/3140649.3140656.

[12] Li, R.—Song, T.—Mei, B.—Li, H.—Cheng, X.—Sun, L.: Blockchain for Large-Scale Internet of Things Data Storage and Protection. IEEE Transactions on Services Computing, Vol. 12, 2019, No. 5, pp. 762–771, doi: 10.1109/TSC.2018.2853167.

[13] Casado-Vara, R.—de la Prieta, F.—Prieto, J.—Corchado, J. M.: Blockchain Framework for IoT Data Quality via Edge Computing. Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems (BlockSys '18), ACM, 2018, pp. 19–24, doi: 10.1145/3282278.3282282.

[14] Xu, Q.—Aung, K. M. M.—Zhu, Y.—Yong, K. L.: A Blockchain-Based Storage System for Data Analytics in the Internet of Things. In: Yager, R. R., Pascual Espada, J. (Eds.): New Advances in the Internet of Things. Springer, Cham, Studies in Computational Intelligence, Vol. 715, 2018, pp. 119–138, doi: 10.1007/978-3-319-58190-3_8.

[15] Goyat, R.—Kumar, G.—Alazab, M.—Conti, M.—Rai, M. K.—Thomas, R.—Saha, R.—Kim, T. H.: Blockchain-Based Data Storage with Privacy and Authentication in Internet of Things. IEEE Internet of Things Journal, Vol. 9, 2022, No. 16, pp. 14203–14215, doi: 10.1109/JIOT.2020.3019074.

[16] Javed, M. U.—Rehman, M.—Javaid, N.—Aldegheishem, A.—Alrajeh, N.—Tahir, M.: Blockchain-Based Secure Data Storage for Distributed Vehicular Networks. Applied Sciences, Vol. 10, 2020, No. 6, Art. No. 2011, doi: 10.3390/app10062011.

[17] Zhang, Y.—Xu, X.—Liu, A.—Lu, Q.—Xu, L.—Tao, F.: Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System. IEEE Transac-

tions on Computational Social Systems, Vol. 6, 2019, No. 6, pp. 1386–1394, doi: 10.1109/TCSS.2019.2918467.

[18] Dwivedi, A. D.—Srivastava, G.—Dhar, S.—Singh, R.: A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors, Vol. 19, 2019, No. 2, Art. No. 326, doi: 10.3390/s19020326.

[19] Liu, H.—Han, D.—Li, D.: Fabric-iot: A Blockchain-Based Access Control System in IoT. IEEE Access, Vol. 8, 2020, pp. 18207–18218, doi: 10.1109/ACCESS.2020.2968492.

[20] Hinze, A.—Bowen, J.—König, J. L.: Wearable Technology for Hazardous Remote Environments: Smart Shirt and Rugged IoT Network for Forestry Worker Health. Smart Health, Vol. 23, 2022, Art. No. 100225, doi: 10.1016/j.smhl.2021.100225.

[21] Mutanu, L.—Gupta, K.—Gohil, J.: Leveraging IoT Solutions for Enhanced Health Information Exchange. Technology in Society, Vol. 68, 2022, Art. No. 101882, doi: 10.1016/j.techsoc.2022.101882.

[22] Ali, G.—Ahmad, N.—Cao, Y.—Asif, M.—Cruickshank, H.—Ali, Q. E.: Blockchain Based Permission Delegation and Access Control in Internet of Things (BACI). Computers and Security, Vol. 86, 2019, pp. 318–334, doi: 10.1016/j.cose.2019.06.010.

[23] Wang, S.—Zhang, Y.—Zhang, Y.: A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. IEEE Access, Vol. 6, 2018, pp. 38437–38450, doi: 10.1109/ACCESS.2018.2851611.

[24] Ma, M.—Shi, G.—Li, F.: Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. IEEE Access, Vol. 7, 2019, pp. 34045–34059, doi: 10.1109/ACCESS.2019.2904042.

[25] Shi, N.—Tan, L.—Yang, C.—He, C.—Xu, J.—Lu, Y.—Xu, H.: BacS: A Blockchain-Based Access Control Scheme in Distributed Internet of Things. Peer-to-Peer Networking and Applications, Vol. 14, 2021, No. 5, pp. 2585–2599, doi: 10.1007/s12083-020-00930-5.

[26] Sun, S.—Du, R.—Chen, S.—Li, W.: Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. IEEE Access, Vol. 9, 2021, pp. 36868–36878, doi: 10.1109/ACCESS.2021.3059863.

[27] Feng, Y.—Zhang, W.—Luo, X.—Zhang, B.: A Consortium Blockchain-Based Access Control Framework with Dynamic Orderer Node Selection for 5G-Enabled Industrial IoT. IEEE Transactions on Industrial Informatics, Vol. 18, 2022, No. 4, pp. 2840–2848, doi: 10.1109/TII.2021.3078183.

[28] Ding, S.—Cao, J.—Li, C.—Fan, K.—Li, H.: A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, Vol. 7, 2019, pp. 38431–38441, doi: 10.1109/ACCESS.2019.2905846.

[29] Zhang, Y.—Li, B.—Liu, B.—Wu, J.—Wang, Y.—Yang, X.: An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. Electronics, Vol. 9, 2020, No. 2, Art. No. 285, doi: 10.3390/electronics9020285.

[30] Tanwar, S.—Parekh, K.—Evans, R.: Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications. Journal of Information Security and

Applications, Vol. 50, 2020, Art. No. 102407, doi: 10.1016/j.jisa.2019.102407.

[31] Maseleno, A.—Hashim, W.—Perumal, E.—Ilayaraja, M.—Shankar, K.: Chapter 8 – Access Control and Classifier-Based Blockchain Technology in e-Healthcare Applications. In: Singh, A. K., Elhoseny, M. (Eds.): Intelligent Data Security Solutions for e-Health Applications. Academic Press, Intelligent Data-Centric Systems, 2020, pp. 151–167, doi: 10.1016/B978-0-12-819511-6.00008-X.

[32] Cerchione, R.—Centobelli, P.—Riccio, E.—Abbate, S.—Oropallo, E.: Blockchain's Coming to Hospital to Digitalize Healthcare Services: Designing a Distributed Electronic Health Record Ecosystem. Technovation, 2022, Art. No. 102480, doi: 10.1016/j.technovation.2022.102480.

[33] Xiang, X.—Zhao, X.: Blockchain-Assisted Searchable Attribute-Based Encryption for e-Health Systems. Journal of Systems Architecture, Vol. 124, 2022, Art. No. 102417, doi: 10.1016/j.sysarc.2022.102417.

[34] Poongodi, T.—Sujatha, R.—Kiruthika, M.—Suresh, P.: Chapter 9 – IoT-Based Health Care Data Analytical Paradigm Using Blockchain Technology. In: Bhattacharyya, S., Mondal, N. K., Mondal, K., Singh, J. P., Prakash, K. B. (Eds.): Cognitive Data Models for Sustainable Environment. Academic Press, Cognitive Data Science in Sustainable Computing, 2022, pp. 203–230, doi: 10.1016/B978-0-12-824038-0.00001-8.

[35] Electronic Health Record (EHR) Datasets. `https://data.world/datasets/ehr`.

[36] Sumathi, M.—Sangeetha, S.: Blockchain Based Sensitive Attribute Storage and Access Monitoring in Banking System. International Journal of Cloud Applications and Computing (IJCAC), Vol. 10, 2020, No. 2, pp. 77–92, doi: 10.4018/IJCAC.2020040105.

[37] Zuo, Y.—Kang, Z.—Xu, J.—Chen, Z.: BCAS: A Blockchain-Based Ciphertext-Policy Attribute-Based Encryption Scheme for Cloud Data Security Sharing. International Journal of Distributed Sensor Networks, Vol. 17, 2021, No. 3, doi: 10.1177/1550147721999616.

Muruganandam Sumathi completed her B.Eng. in computer science and engineering in 2003 from the Shri Angalamman College of Engineering and Technology, Tiruchirappalli. She completed her M.Tech. in information technology in 2008 from the Bharathidasan University, Tiruchirappalli. She completed her Ph.D. in 2021 in the area of data security from the National Institute of Technology, Tiruchirappalli. Currently she is working as Assistant Professor in the School of Computing in SASTRA Deemed University, Thanjavur, Tamilnadu, India.

Natarajan Vijayaraj is currently working as Associate Professor in the Department Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed University), Chennai. He obtained his UG in the Roever Engineering College, Perambalur and PG degrees in the Jayaram College of Engineering and Technology, Trichy. He received his Ph.D. degree from the Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed University), Chennai in 2021. He has been in the teaching profession for the past 14 years and handled various courses for both UG and PG programs. He is guiding 5 research scholars. He has more than 12 publications in national and international journals. He has also published 3 book chapters. He is a life member of various bodies such as ISTE, IAENG.

Soosaimarian Peter Raj Raja completed his schooling in the Sacred Heart Higher Secondary School, Sathankulam, Tuticorin, Tamilnadu, India. He completed his B.Tech. in information technology in 2007 from the Dr. Sivanthi Aditanar College of Engineering, Tiruchendur. He completed his M.Eng. in computer science and engineering in 2010 from the Manonmaniam Sundaranar University, Tirunelveli. He completed his Ph.D. in 2016 in the area of image processing from Manonmaniam Sundaranar University, Tirunelveli. Currently he is working as Associate Professor in the School of Computer Science and Engineering in Vellore Institute of Technology, Vellore, Tamilnadu, India.

Murugesan Rajkamal completed his B.Eng. in computer science and engineering in 2019 from the K. Ramakrishnan College of Engineering, Tiruchirappali. He is pursuing his M.Tech. in data science and engineering in BITS Pilani, Rajasthan. Currently he is working as Application Developer in IBM, Bangalore.