Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System

Yogesh M. Gajmal* and R. Udayakumar

Bharath Institute of Higher Education and Research, Bharath University, Selaiyur, Chennai, Tamil Nadu 600073, India
E-mail: yogeshmgajmal@gmail.com; rsukumar2007@gmail.com
**Corresponding Author*

Received 06 November 2020; Accepted 03 June 2021;
Publication 28 July 2021

Abstract

Access control is a major factor in enhancing data security in the cloud storage system. However, the existing data sharing and the access control method have privacy data leakage and key abuse, which is a major challenge in the research community. Therefore, an effective method named Blockchain-based access control and data sharing approach is developed in the cloud storage system to increase data security. The proposed Blockchain-based access control and data sharing approach effectively solve single-point failure in the cloud system. It provides more benefits by increasing the throughput and reducing the cost. The Data user (DU) makes the registration request using the ID and password and forwards it to the Data Owner (DO), which processes the request and authenticates the Data user. The information of the data owner is embedded in the transactional blockchain using the encrypted master key. The Data owner achieves the data encryption process, and encrypted files are uploaded to the Interplanetary File System (IPFS). Based on the encrypted file location and encrypted key, the Data owner generates the ciphertext metadata and is embedded in the transactional blockchain.

Journal of Web Engineering, Vol. 20_5, 1359–1388.
doi: 10.13052/jwe1540-9589.2054

The proposed Blockchain-based access control and data sharing approach achieved better performance using the metrics, like a better genuine user detection rate of 95% and lower responsiveness of 25sec with the blockchain of 100 sizes.

Keywords: Data sharing, cloud storage system, Blockchain, smart agreement, interplanetary file system (IPFS).

1 Introduction

In the increasing internet technology era, the cloud storage system becomes a key role in the daily life of the business model. Since the cloud offered various categories of storage services for the enterprise domain and the business individuals to access the cloud resources and share the information anywhere, it is significantly brought a major convenience in human life. The existing data storage system in the cloud has a single failure mark which can be resolved using the decentralized data storage approach, such that it gains more benefits than the centralized model [8, 16, 18]. The decentralized network has high reliability, secrecy, and scalability. Moreover, single-point failure is the major challenging task for the centralized network. To overcome the issue, the decentralized network is used for the business model and in bitcoin, which is fully secured, and hence efficiency can be improved. Moreover, the scalability and trust in the data sharing are enhanced.

The information is stored in a single peer in the decentralized approach, where no user can make any modification [15]. Blockchain is nothing but a decentralized architecture, such that it forms an immutable ledger in a distributed manner to record all the transactions. In general, blockchain is a decentralized and secure data store where all the records are placed in order, including events named blocks [9]. The blockchain is highly resilient; hence no hackers may exploit the system to vulnerable. All the information that is transparent to the nodes is recorded in the blockchain system. It is also apparent to make modifications in data; hence, all users can provide working proof with decentralized trust in blockchain technology. Besides, it is the distributed, transparent, and open ledger that efficiently records all the transactions among two parties in a permanent and verifiable way [11]. Once the information is stored, the information in the blockchain does not get changed unless a record is inserted. In cryptocurrencies, each user has the exact ledger in the network domain, ensuring the complete consensus of nodes or users in the blockchain currencies [4, 17].

Combining the blockchain with IoT technology provides an effective trend in the storage system, as it ensures trust and minimizes the overhead in the IoT system. It makes the IoT system model credible, publicly verifiable, and decentralized databases so that numerous connected devices can achieve trust through blockchain [2]. The blockchain model introduced the data management mechanism [12] to grant permission to the data owner to control and own the data. The storage system can provide better privacy protection to the user data. Besides, to avoid the issues like data privacy, the blockchain system model was introduced [13]. The attribute-based encryption (ABE) model is utilized to perform the access control strategy. The blockchain-enabled access control mechanism was developed to enhance the security in the big data framework [8, 10]. Access control is the most important mechanism to guarantees security in data. Most of the existing access control model, like identity-based access control (IBAC) and discretionary access control (DAC), are not applicable to implement the access control in the IoT system, as it is impossible for all the users to make the access control list (ACL) in IoT system in terms of a large number of unknown identities [2, 22, 23]. The access control model maximizes the integration of the delegation module, such that the role of delegation is to temporarily assign the access rights to the user [5, 24, 25]. Thus, the access control management system effectively simplifies that the number of attributes must be lesser than the number of users [2, 19–21]. The cloud computing helps the students to access the higher learning motivation [26–28].

Motivation

Access control and data sharing in the cloud are essential for the secure transmission and storage of data in the cloud using the secret key. The major challenges associated with the data sharing in the cloud storage system are the low efficient system, failure in the access control system, formal verification, and failure to update the access policy. Hence, there is a need for the access control and data sharing mechanism to enhance the security and to prevent the unauthorized access. Accordingly, this paper proposes a Blockchain-based access control and data sharing approach. The proposed approach involves eight phases, such as setup, user registration, encryption, token generation, control setup, test, validation, and decryption. The proposed approach consists of four entities, like Data owner (DO), Data user (DU), Smart agreement, and Transactional blockchain. The DU sends the registration request to DO with the ID and password of DU. The DO receives the request and forwards it to the smart agreement. The DO generates the secret key based on the Chebyshev polynomial and embedded in the transactional blockchain. The DO encrypts the data and generates the ciphertext metadata. Finally, the DU receives the file from IPFS and decrypts the file using the key.

The major contribution of this research is explained as follows:

- The proposed Blockchain-based access control and data sharing approaches have the facility for distributing the secret keys to the data users. It specifies the access policy to encrypt the shared data. However, the search function of the decentralized system is evaluated using the smart contract of the Ethereum blockchain.

The rest of this paper is organized as follows: Section 2 describes the existing access control methods. Section 3 elaborates on the proposed Blockchain-based access control and data sharing approach. Section 4 explains the results and discussion of the proposed approach, and section 5 concludes the paper.

2 Literature Survey

Various existing access control methods in the cloud storage system are reviewed. Rajput, AR et al. [1] developed an emergency access control management system (EACMS) model based on the hyper ledger composer and fabric. Based on the smart contracts, certain rules were defined for accessing health. The performance was evaluated concerning factors like privacy, security, accessibility, and response time. This method offered better efficiency than the traditional access system. Ding, S et al. [2] introduced an ABAC mechanism to simplify the management system in the IoT environment. The attributes were recorded through blockchain technology to eliminate data tampering and single-point failure. The access control procedure meets the requirements with lightweight computation and high efficiency. Moreover, this model resists multiple attacks but failed to use the consensus algorithm. Ma, M et al. [3] introduced a distributed key management approach (BDKMA) to minimize the multiblock chains and latency in the cloud to attain cross-domain access. Blockchain technology was used to satisfy the requirements, such as high scalability, audit ability, extensibility, and decentralization in IoT. It maximizes the scalability and system performance concerning the network size but failed to achieve persistency in the IoT ecosphere. Ouaddah, A et al. [4] developed a privacy-preserving access control model in IoT based on blockchain technology. It effectively manages the access control concerning the constrained devices. However, this method failed to implement the fair access control model with the bitcoin blockchain and IoT device.

Ali, G et al. [5] developed a permission delegation and access control mechanism in the IoT application. The delegation services were verifiable, trusted, decentralized, and secure by applying blockchain technology. This method attained better integrity, availability, and confidentiality but failed to work with the formal verification and formal modeling. Dagher, G.G et al. [6] introduced a blockchain-based approach for interoperable, efficient, and secure access to medical information by third parties, providers, and patients. It achieves a better decentralization level. However, it failed to meet the legislative standards in the medical data. Lin, C et al. [7] introduced a secure mutual authentication that enforced the access control policies. This approach was designed to offer security and privacy guarantees, like confidentiality, audit ability, and authentication. However, it failed to evaluate the performance using the collaborating and hardware implementation. Wang, S et al. [8] introduced a blockchain-based approach for data sharing through a fine-grained access control model in the decentralized system. Here, the data owner distributes the secret keys to the data users, and the shared data were encrypted through the access policy. This method attained better throughput with less cost but failed to implement the access policy update. The literature review with its inclusion criteria and its findings are given in Table 1.

2.1 Challenges

The major challenges of the research are elaborated below:

- Even though the IoT technology was used to solve various existing problems in real-time, enhancing the privacy and security in the IoT device poses a challenging issue due to the characteristics, such as distributed nature, lack of standardization, and processing power [13].
- Reach the consensus in the cloud environment poses a challenging issue in the network. Solving the access control issues through the full-fledged distribution and append-only ledger in the big data results in a major challenge in blockchain technology [10].
- It was very difficult to solve the data-related issues, like security, multi-tenancy, standardization, and interoperability. Moreover, the pooled resources in cloud computing pose a security challenge in the computing framework [14].

Table 1 Literature review

Authors	Methods	Advantages	Disadvantages	Inclusion Criteria	Findings
Rajput, A.R et al. [1]	Emergency access control management system (EACMS)	This framework provides better efficiency compared with the traditional emergency access system.	The time efficiency of this model was very poor.	The EACMS is accessed with the help of Hyperledger fabric (HF) and Hyperledger composer in blockchain for privacy protection.	Memory usage = 568 B and response time = 5683 ms.
Ding, S et al. [2]	Attribute-based access control scheme	It effectively resists multiple attacks and be efficiently implemented in IoT systems.	It was not suitable for the fine-grained access control system.	The two entities like attribute authorities and IoT devices with five different level of security is used for the access control.	Computation time: 2.87 ms for key generation and 6.34 ms for verification of signature.
Ma, M et al. [3]	Blockchain-based distributed key management approach	The dynamic transaction collection time adjustment enables the performance and system capacity to be optimized for various environments.	However, it failed to facilitate the persistency of the blockchain-based IoT ecosphere.	Fog computung is used for the decentralization and access control in IoT.	When the number of users is 12800, the average collection time is 1.89 s.
Ouaddah, A et al. [4]	Decentralized pseudonymous and privacy preserving authorization management framework	It effectively managed the access control on behalf of constrained devices.	However, it failed to implement the FairAccess with RaspberryPI IoT device and bitcoin blockchain.	Additional security and integrity is added for the access control using token based access control.	None

Ali, G et al. [5]	Decentralized architecture for permission delegation and access control.	This model attained better confidentiality, integrity and availability.	However, this model was failed to work in formal modeling and formal verification of BC.	Used event based and query based permission hybrid delegation method for the analysis of integrity, confidentiality and availablity.	None
Dagher, G.G *et al.*[6]	Blockchain-based framework	It achieves a high-level of decentralization while acknowledging that some nodes ought to be of a higher authority.	This model still offers significant privacy preservation and data integrity.	The Electronic Health Record(EHR) management by Ancile framework for high-level of decentralization. Besides, the encryption and authentication provides access control.	None
Lin, C et al. [7]	Blockchain-based system for secure mutual authentication	It provides privacy and security guarantees such as anonymous authentication, auditability, and confidentiality.	It failed to optimize the performance using hardware implementation, and collaborating with a smart factory operator.	Integrated attribute signature, multi-receivers encryption and message authentication code for secure access control using smart contract.	Initialization, Request Issuance, Chain Transaction, State Delivery, Permission Update phase only cost are 12.123, 4.810, 6.978, 0.013, and 2.559 s respectively.
Wang, S et al. [8]	Blockchain-Based Framework	It attained high throughput with reduced cost.	This model failed to implement the functions of user's attribute revocation and access policy update.	The Ethereum blockchain and attribute-based encryption is used for the decentralization system and to solve fine grained access control system.	None

- To provide the pre-emptive security for the complex and dynamic cloud infrastructure in the cloud provider poses a challenging research issue in the cloud-aware framework. Adapting the security solution to protect the virtual infrastructure results in a major challenge in the cloud.

3 Proposed Blockchain-based Access Control and Data Sharing Approach in Cloud

The proposed Blockchain-based access control and data sharing model is developed for decentralized storage systems in the cloud environment. The proposed decentralized storage approach involves eight phases: setup, user registration, encryption, token generation, control setup, test, validation, and decryption. The decentralized storage system consists of four entities, like Data owner (DO), Data user (DU), Smart agreement, and Transactional blockchain [8]. Each entity performs its operations to perform the access control and data sharing mechanism. DO is the organization or person that owns the files to share. However, DU is DO's data clients that are authorized to view the files. The DO set up the phase by encrypting the master key and embedding the key into the Transactional blockchain. The smart contract is deployed in the Transactional blockchain using the DO. However, the smart contract is used to record the encrypted keyword files and provides effective search to the DU. DU sends the registration request to DO in the setup phase. The DO encrypt and uploads the file to IPFS and embedded the ciphertext metadata in the transactional blockchain. The DU downloads the file from IPFS and decrypts it. Figure 1 portrays the schematic diagram of the proposed Blockchain-based access control and data sharing approach.

3.1 Setup Phase

The setup phase is run by DO such that the DO considers the input as S and generates M and R of the system as output. As R is publicly accessible, the DO publishes the R in the media, like public database and website. The DO encrypted M and embedded M into the Transactional blockchain. Table 2 demonstrates the symbol description of the proposed Blockchain-based access control and data sharing in the cloud.

Moreover, the DO deploys the smart contract in the Transactional blockchain. The smart contract is utilized to record the encrypted keywords and offers an effective search service for the Data user. The $R$and

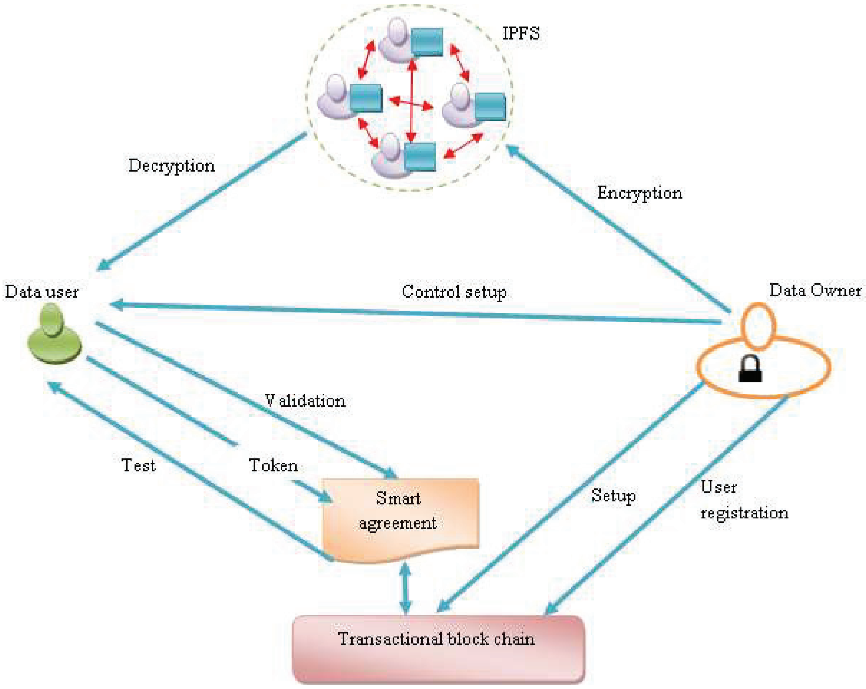


Figure 1 Proposed Blockchain-based access control and data sharing approach.

M generated by the DO is represented as,

$$R = h(S||q) \tag{1}$$

$$M = S \oplus \alpha \tag{2}$$

The S is concatenated with the parameter q and is applied to the hashing function to generate R. q is the parameter that lies between $[0, 1]$ and α denotes the parameter that lies between $[0, 1]$. The master key of the system is generated by performing the Ex-or operation with S and α. The M is encrypted by the DO is represented as,

$$M_{en} = E(M||\alpha)\, mod\, n \tag{3}$$

The M and the parameter α are concatenated together, and the resultant factor is encrypted with the modulus function. The DO embed the encrypted M to the Transactional blockchain. The transactional blockchain receives the encrypted M and records it with the soil database. The transactional

Table 2 Symbol description of the proposed Blockchain-based access control and data sharing approach

Symbol	Description
S	Security parameter
R	System public parameter
M	System master key
h	Hash function
E	Encryption function
//	Concatenation operator
$\oplus$	Ex-or operation
$\otimes$	interpolation
n	random number
D	Soil database
D_{id}	Data user ID
D_{pwd}	Data user password
$D_{s\,pwd}$	Data user session password
T_{id}	Transaction ID
C_{ad}	Contract address
C_{ABI}	Contract Application Binary Interface
C_{src}	Contract source code
D_{en}	Encrypted data
f_k	File encrypted key
s_k	Keyword set
D_{loc}	File location
C_m	Cipher text metadata
D_{en}^{loc}	Encrypted data location
P_{en}	Encrypted key
S_r	Randomly selected key using AES
I_{en}	Encrypted keyword index
t	Search token
$d(.)$	Decryption
$E(.)$	Encryption
D_R	Data retrieved

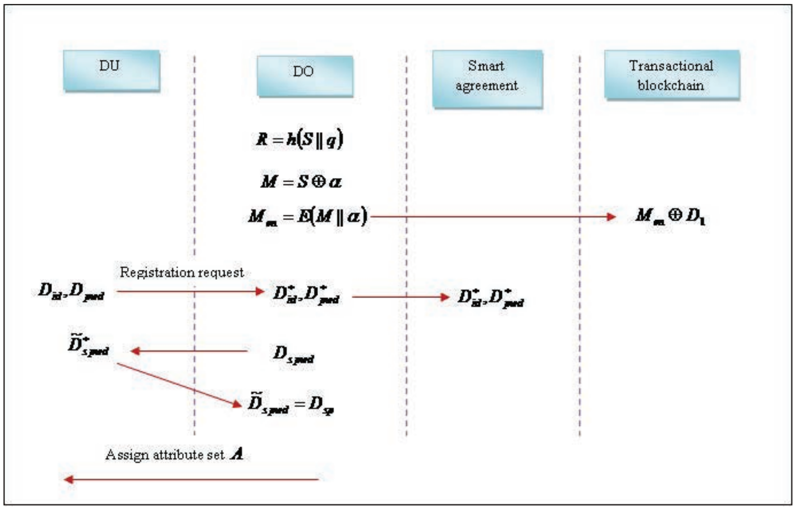


Figure 2 Setup phase of the proposed blockchain framework based access control and data sharing in the cloud.

database performs the Ex-or operation with D_1 and M_{en} and records it for further processing. In this phase, the DU sends the registration request by generating the ID as D_{id} and password as D_{pwd} of DU and sends them to DO. The DO receives the ID and password of DU and records it as D^*_{id} and D^*_{pwd} and forwards them to the Smart agreement. The DO generates the session password for DU as $D_{s\,pwd}$ and forwards it to DU for authenticating the identity. The DU receives and records the session password as $\tilde{D}_{s\,pwd}$ and sends it back to DO after satisfying the identity. The Do authenticates the $D_{s\,pwd}$ and assigns an attribute set $A$to DU. Moreover, the transactional account address of the DU is added as an authorized user in the smart agreement. Figure 2 shows the setup phase of the proposed Blockchain-based access control and data sharing approach.

3.2 User Registration Phase

DO runs the user registration phase. The DO generates the secret key $K$by considering the attribute set and M.

$$y = M \oplus h(A||n) \tag{4}$$

$$K = 8y^4 - 8y^2 + 1 \tag{5}$$

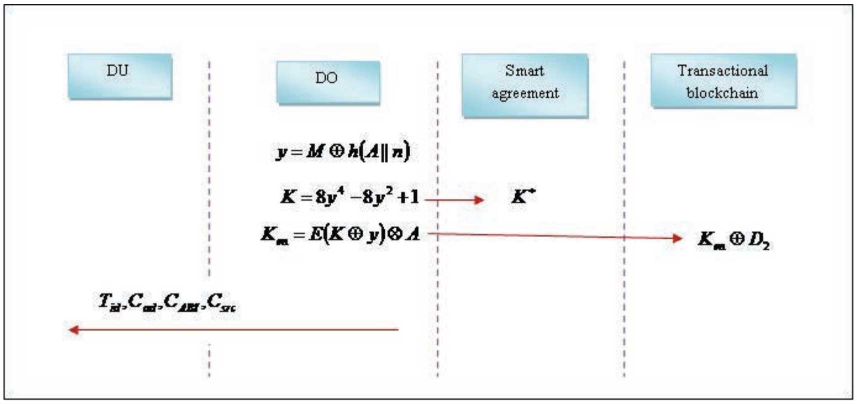


Figure 3 User registration phase of data sharing system.

The attribute set is concatenated with the random number. It is applied with the hashing function, and the resultant factor performs the Ex-or operation with the master key to form the parameter y. K is generated by using the Chebyshev polynomial with the parameter y. The DO generates the secret key K and sends it to the smart agreement, which receives the secret key and stores it K^*. However, the encrypted secret key is represented as,

$$K_{en} = E(K \oplus y) \otimes A \tag{6}$$

The EX-OR operation is done with the secret key and the Chebyshev parameter, and the resultant factor is encrypted and is interpolated with A. The transactional blockchain receives the encrypted secret key K_{en} and embeds it with the soil database. The DO sends the T_{id}, C_{ad}, C_{ABI}, and C_{src} to DU through a secure channel. The user registration phase of the data-sharing system is illustrated in Figure 3.

3.3 Encryption Phase

DO runs the encryption phase, and the encryption phase is carried out at three different stages, such as data encryption, key encryption, and keyword index generation. Initially, the data is encrypted using the keyword set and file encryption key. The DO select the keyword set from data $D$and selects the key using AES to encrypt the data. Moreover, the encrypted data is represented as,

$$D_{en} = E(D||s_k) \oplus f_k \tag{7}$$

The DO uploads the encrypted data to IPFS, which receives the encrypted data and sends the data file location D_{loc} back to DO. At the second stage, the ciphertext for the metadata is created by DO using P_{en} and D_{en}^{loc}. However, the data location of the encrypted data is specified as,

$$D_{en}^{loc} = E(D_{loc}||f_k) \oplus \alpha \tag{8}$$

The encrypted data is Ex-or with the parameter factor α. The Do generates the encrypted key, which is expressed as,

$$P_{en} = E(R \oplus \alpha)||f_k \tag{9}$$

The Ex-or operation is carried out to the R and α, and is encrypted with the concatenation of the file encryption key. The ciphertext metadata generated by DO is represented as,

$$C_m = E(D_{en}^{loc}||P_{en}) \oplus S_r \tag{10}$$

The encrypted data location and the encrypted key are concatenated, and the encryption function is applied to the concatenated data. The randomly selected key using the AES is Ex-or with the encrypted data to form the ciphertext metadata. The DO generates the encrypted keyword index by considering the keyword set and α, which is expressed as,

$$I_{en} = q||E(s_k||\alpha) \tag{11}$$

The keyword set and the parameter α are concatenated and are applied to the encryption function. The encrypted data is concatenated with the factor q to generate the encrypted keyword index. Figure 4 portrays the encryption phase of the proposed data storage sharing in the cloud.

3.4 Token Generation Phase

The DU reads the data connected with the secret key and decrypt K_{en} to get K, which is expressed as,

$$K = D(K_{en}) \tag{12}$$

The encrypted secret key is applied to the decryption function to obtain K. The DU generates the token by considering the keyword set and the secret key as input, which is expressed as,

$$t = a^{s_k} \oplus (K||\alpha) \tag{13}$$

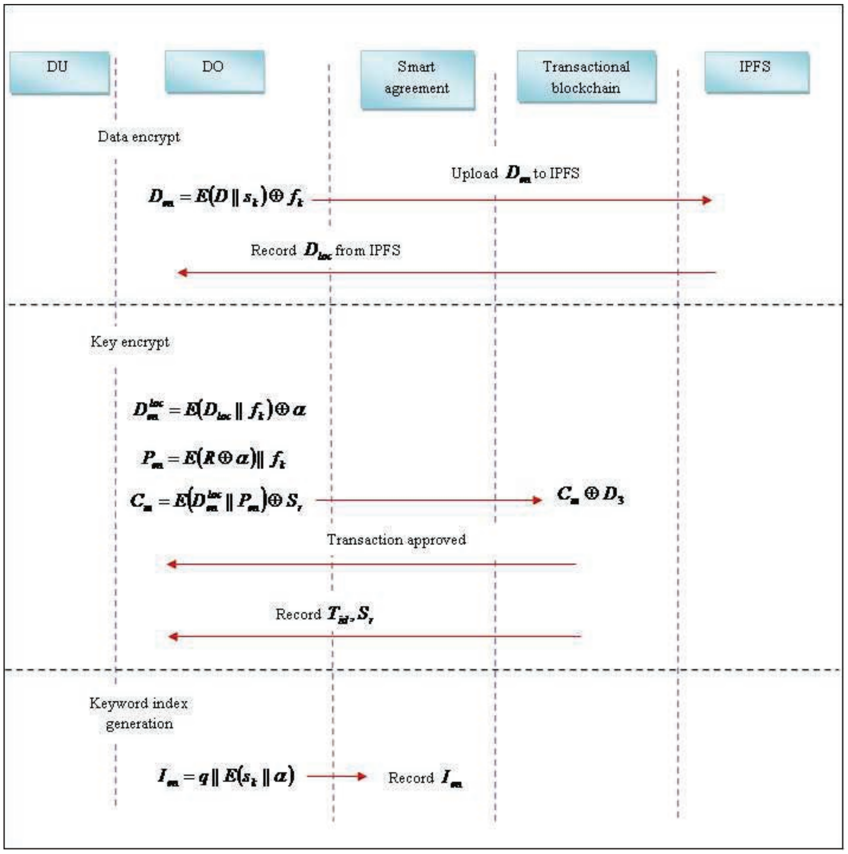

DU
DO
Smart agreement
Transactional blockchain
IPFS
Data encrypt
Upload D_{en} to IPFS
$D_{en} = E(D \| s_k) \oplus f_k$
Record D_{loc} from IPFS
Key encrypt
$D_{en}^{loc} = E(D_{loc} \| f_k) \oplus \alpha$
$P_{en} = E(R \oplus \alpha) \| f_k$
$C_{en} = E(D_{en}^{loc} \| P_{en}) \oplus S_r$
$C_{en} \oplus D_3$
Transaction approved
Record T_{id}, S_r
Keyword index generation
$I_{en} = q \| E(s_k \| \alpha)$
Record I_{en}

Figure 4 Encryption phase of the proposed access control and data sharing system.

The secret key and the parameter α are concatenated and perform the Ex-or operation with keyword set. DU generates the token based on s_k and invokes the smart agreement to search. Figure 5 shows the token generation phase.

3.5 Control Setup Phase

DO runs the control setup phase to performs the data-sharing contract between DO and DU [8]. This phase is responsible for adding a new user, adding an index, deleting the file, deleting the keyword index, searching, and withdrawing the file.

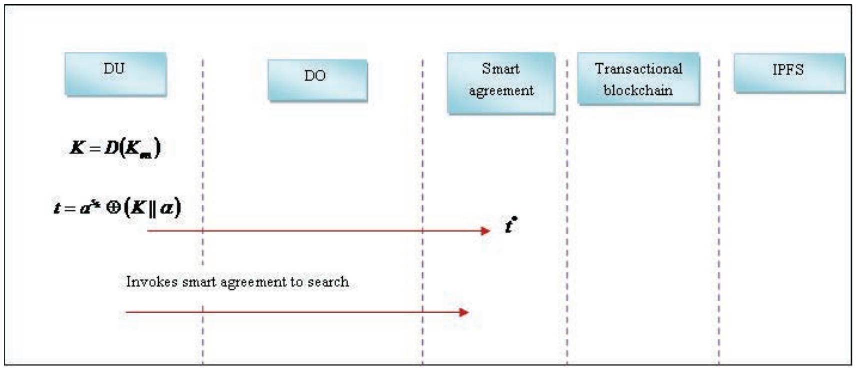

DU
DO
Smart agreement
Transactional blockchain
IPFS
$K = D(K_m)$
$t = a^{s_k} \oplus (K \| \alpha)$
t^*
Invokes smart agreement to search

Figure 5 Token generation phase.

Add user: When the user sends the registration request to DO, the DO receives the request and authenticates it by recording the user information in the smart agreement.

Remove user: The DO can eliminate the user from the authorized user set, bypassing DU's external owned account function.

Add index: When DO uploads the file to IPFS, it selects the keyword set and constructs the keyword index. The keyword indexes stored in the smart agreement are transaction ID, encryption key, and encrypted keyword index.

Delete file: This function is executed by DO, which deletes the file using the keyword index and the transaction ID linked with the file.

Delete the keyword index: This function is executed when required to delete all the files corresponding to the keyword.

Search: This function is executed by passing the encrypted keyword index and returns the key and transaction ID.

Withdraw (): The DO executes this function to withdraw the search service.

3.6 Test Phase

In the test phase, the smart agreement receives the token generated by the DU in the token generation phase and stores it in the smart agreement, which is expressed as,

$$t^* = a^{s_k} \oplus (K^* || \alpha) \tag{14}$$

The token that is recorded in the smart agreement is denoted as t^*. The smart agreement verifies that the token generated by DU is matched with the token recorded in the smart agreement. When $t = t^*$, then the DU is authenticated. When DU sends the request, and if the search option is enabled, then the DU is authorized, which is specified as,

$$X = E(T_{id}||t) \oplus E(S_r||I_{en}) \tag{15}$$

The transaction ID and the token are concatenated and perform the encryption function. On the other hand, the key selected randomly using AES is concatenated with the encrypted keyword index and performs the encryption function. Both the encrypted data are allowed to performs the Ex-or operation, and the resultant term is indicated as X. The smart agreement generates the matched result and forwards it to DU.

3.7 Validation Phase

In the validation phase, the DU validates the user file by generating the validation factor based on the random number, secret key, and the data user ID, which is expressed as,

$$V = X \oplus h(D_{id} \otimes (n||K)) \tag{16}$$

The secret key is concatenated with the random number and is interpolated with the data user ID; the resultant factor is passed to the hashing function. The output of the hash function and the success factor generated by the smart agreement are allowed to perform the Ex-or operation. The DU generates the validation factor and forwards it to the smart agreement for the user to get validated. The smart agreement receives the validation factor from DU and records it as,

$$V^* = X \oplus h(D^*_{id} \otimes (n||K^*)) \tag{17}$$

The smart agreement verifies V with V^*, if it matches, then the user is validated by the smart agreement. Figure 6 shows the Test and Validation phase of the proposed Blockchain-based access control framework.

3.8 Decryption Phase

DU runs the decryption phase. It considers the file encryption key with the retrieved data file and decrypts the data to generate the final data file. DU

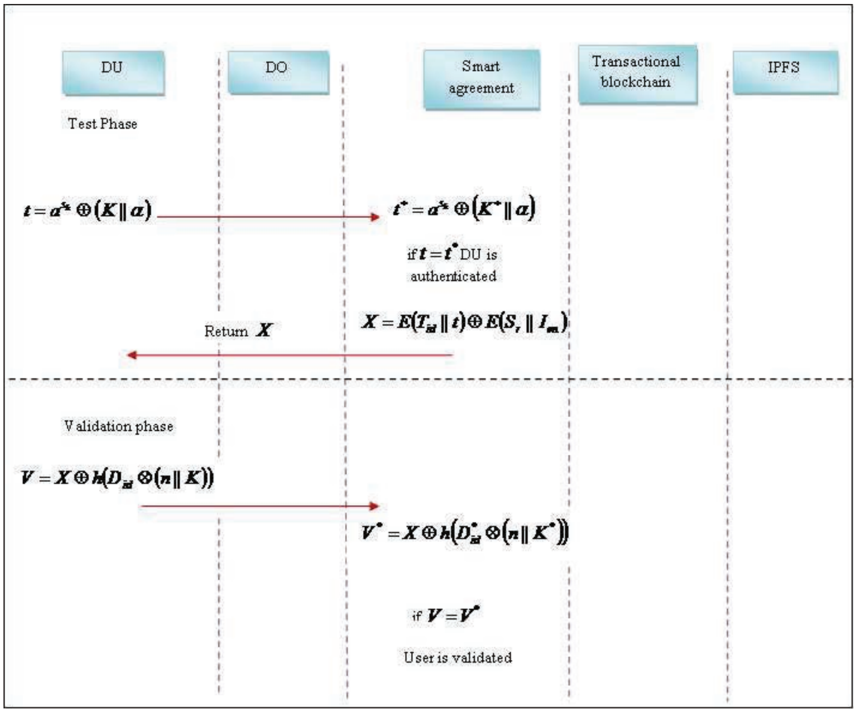

DU
DO
Smart agreement
Transactional blockchain
IPFS
Test Phase
$t = a^{s_k} \oplus (K \| \alpha)$
$t^* = a^{s_k} \oplus (K^* \| \alpha)$
if $t = t^*$ DU is authenticated
Return X
$X = E(T_{id} \| t) \oplus E(S_r \| I_m)$
Validation phase
$V = X \oplus h(D_{id} \otimes (n \| K))$
$V^* = X \oplus h(D_{id}^* \otimes (n \| K^*))$
if $V = V^*$
User is validated

Figure 6 Test and Validation phase of the proposed Blockchain-based access control framework.

sends V and X to DO, which receives the file and recorded in the DO, which is represented as,

$$\tilde{V} = X^* \oplus h(D_{id}^* \otimes (n||K)) \tag{18}$$

The random number and the secret key are concatenated, and the resultant factor is interpolated with the data user ID, which is applied to the hashing function. Finally, the Ex-or operation is performed with X^*. The DO verifies if the validated file generated by DU is matched with the file recorded in DO. DO sends the encrypted data location and encrypted key to DU. The DU stores the encrypted data location and encrypted key and sends them to IPFS along with a^{s_k}. The IPFS receives the data send from DU and records it in IPFS. The IPFS shares the encrypted data with DU. The DU download the file that the IPFS shares and decrypt the retrieved data using the file encryption key, which is expressed as,

$$D = d(D_R \oplus f_k) \tag{19}$$

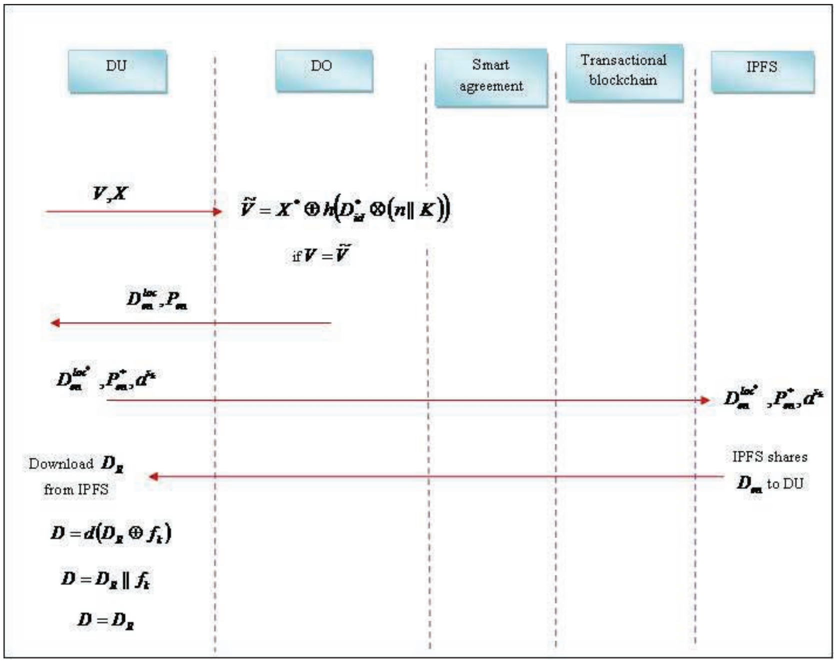

DU
DO
Smart agreement
Transactional blockchain
IPFS
V, X
$\tilde{V} = X^{*} \oplus h(D_{id}^{*} \otimes (n \| K))$
if $V = \tilde{V}$
D_{m}^{loc}, P_{m}
$D_{m}^{loc^{*}}, P_{m}^{*}, d^{k}$
$D_{m}^{loc^{*}}, P_{m}^{*}, d^{k}$
Download D_{R} from IPFS
IPFS shares D_{m} to DU
$D = d(D_{R} \oplus f_{k})$
$D = D_{R} \| f_{k}$
$D = D_{R}$

Figure 7 Decryption phase of the proposed Blockchain-based access control and data sharing approach.

The Ex-or operation is performed with the retrieved data and the file encryption key, and the resultant terms are decrypted using the decryption function.

$$D = D_R || f_k \tag{20}$$

The retrieved data and the file encryption key are concatenated to obtain the data file.

$$D = D_R \tag{21}$$

Finally, the data file is retrieved back by DU. Figure 7 shows the decryption phase of the proposed blockchain for access control and data sharing approach.

4 Results and Discussion

The results and discussion of the proposed Blockchain-based access control and data sharing approaches are explained in this section.

4.1 Experimental Setup

The experimentation of the proposed cloud model is carried out in the PYTHON tool with windows 10 OS, 4 GB RAM, and an Intel processor.

The simulation environment is created using cloudsim with the number of user ranges between 20 to 100 and the blockchain size ranges between 100 to 500 for the experimental evaluation.

4.2 Evaluation Metrics

The performance of the proposed approach is evaluated using the metrics such as responsiveness, bandwidth, and genuine user detection rate.

Responsiveness: It is the promptness with which the cloud services performs the request during the time interval, which is expressed as,

$$R = 1 - \frac{f_{m=1}^{k}(r_m)}{r_{\max}} \tag{22}$$

where, r_m indicates the time between the completion of m^{th} request, and $r_{\max}$ denotes the maximum acceptable time utilized to complete the request, such that $r_{\max} \geq r_m$. k denotes the total number of requests, and f denotes the function that is used to measure the central tendency of data.

Genuine user detection rate: It is termed as the number of users detected as genuine concerning the total number of users.

4.3 Comparative Methods

The performance improvement of the proposed approach is revealed by comparing the proposed with the existing methods, like Emergency Access Control Management System (EACMS) [1], Attribute-Based Access Control (ABAC) [2], and blockchain-based system (BSeIn) for remote mutual authentication [7], respectively.

4.4 Comparative Analysis

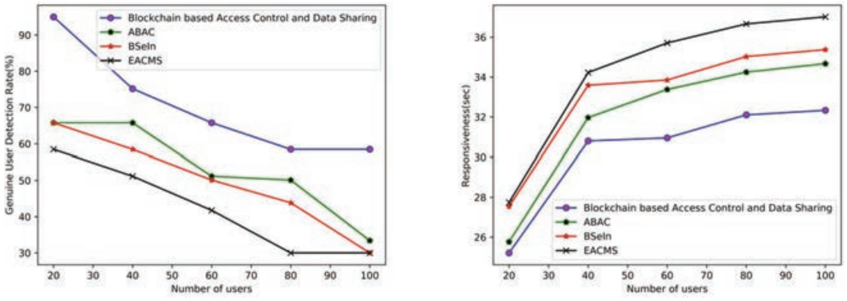
The comparative analysis of the proposed Blockchain-based access control and data sharing approach is made using the performance metrics, such as genuine user detection rate and responsiveness by varying the blockchain size from 100 to 500.

(a) Blockchain size = 100

Figure 8 portrays the comparative analysis of the proposed approach with the Blockchain size as 100. Figure 8(a) represents the comparative analysis of genuine user detection rate concerning the number of users. By considering 20 number of users, the genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 65.7%, 65.76%, and 58.46%, while the proposed blockchain-based access control and data sharing obtained better genuine user detection rate of 95%, respectively. Figure 8(b) depicts the comparative analysis of responsiveness with respect to number of users. When the number of users = 20, the responsiveness obtained by the existing methods, such as ABAC, BSeIn, EACMS is 25 sec, 27 sec, and 27 sec, while the proposed blockchain based access control and data sharing obtained lower responsiveness of 25sec, respectively.

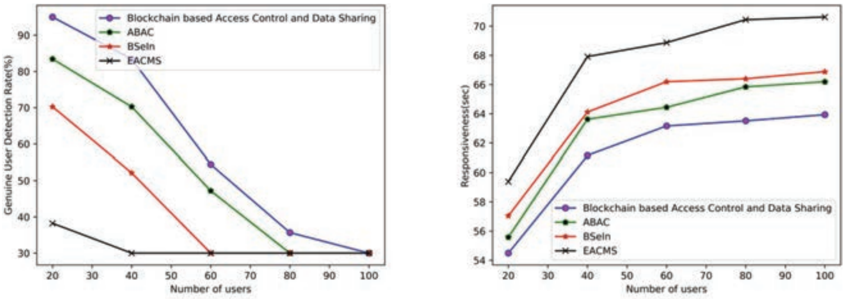
(b) Blockchain size = 200

Figure 9 portrays the comparative analysis of the proposed approach with the Blockchain size as 200. Figure 9(a) represents the comparative analysis of genuine user detection rate. When the number of users = 80, the genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 30%, 30%, and 30%, while the proposed blockchain based access control and data sharing obtained better genuine user detection rate of 35%, respectively. Figure 9(b) depicts the comparative analysis of responsiveness. When the number of users = 80, the responsiveness obtained by the existing methods, such as ABAC, BSeIn, EACMS is 65 sec, 66 sec, and 70 sec, while the proposed blockchain based access control and data sharing obtained lower responsiveness of 63 sec, respectively.



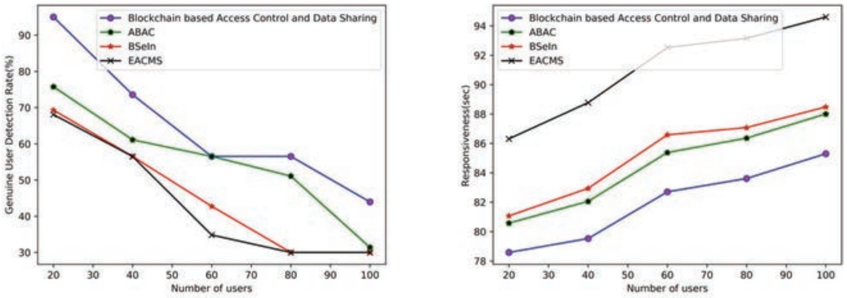
(a) (b)

Figure 8 Comparative analysis with the Blockchain size as 100, (a) genuine user detection rate, (b) responsiveness.



(a) (b)

Figure 9 Comparative analysis with the Blockchain size as 200, (a) genuine user detection rate, (b) responsiveness.

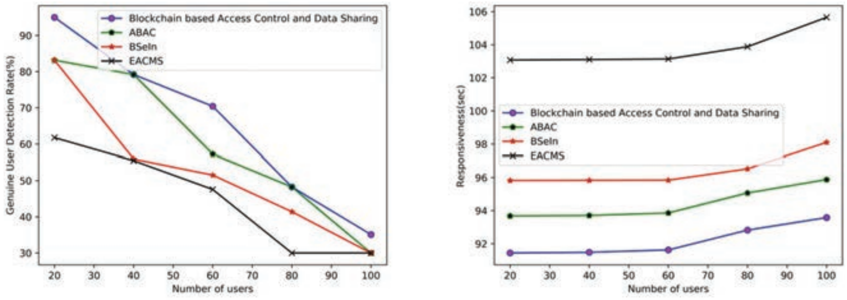


(a) (b)

Figure 10 Comparative analysis with the Blockchain size as 300, (a) genuine user detection rate, (b) responsiveness.

(c) Block chain size = 300

Figure 10 portrays the comparative analysis of the proposed approach with the Blockchain size as 300. Figure 10(a) represents the comparative analysis of genuine user detection rate with respect to the number of users. When the number of users = 40, the genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 61%, 56%, 56%, while the proposed blockchain based access control and data sharing obtained better genuine user detection rate of 73%, respectively. Figure 10(b) depicts the comparative analysis of responsiveness. When the number of users = 20, the responsiveness obtained by the existing methods, such as ABAC, BSeIn, EACMS is 80 sec, 81 sec, 86 sec, while the proposed blockchain based access control and data sharing obtained lower responsiveness of 78 sec, respectively.



(a) (b)

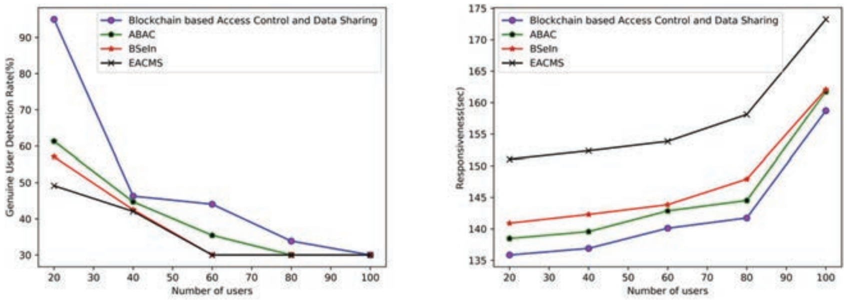
Figure 11 Comparative analysis with the Blockchain size as 400, (a) genuine user detection rate, (b) responsiveness.

(d) Block chain size = 400

Figure 11 portrays the comparative analysis of the proposed approach with the Blockchain size as 400. Figure 11(a) represents the comparative analysis of genuine user detection rate with number of users. By considering 20 number of users, the genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 83%, 83%, 61%, while the proposed blockchain based access control and data sharing obtained better genuine user detection rate of 95%, respectively. Figure 11(b) depicts the comparative analysis of responsiveness to number of users. When the number of users = 20, the responsiveness obtained by the existing methods, such as ABAC, BSeIn, EACMS is 93 sec, 95 sec, 103 sec, while the proposed blockchain based access control and data sharing obtained lower responsiveness of 91 sec, respectively.

(e) Blockchain size = 500

Figure 12 portrays the comparative analysis of the proposed approach with the Blockchain size as 500. Figure 12(a) represents the comparative analysis of genuine user detection rate to number of users. For 20 users, the genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 61%, 57%, 49%, while the proposed blockchain based access control and data sharing obtained better genuine user detection rate of 95%, respectively. Figure 12(b) depicts the comparative analysis of responsiveness with number of users. When the number of users = 20, the responsiveness obtained by the existing methods, such as ABAC, BSeIn, EACMS is 138 sec, 141 sec, 151 sec, while the proposed blockchain based access control and data sharing obtained lower responsiveness of 136sec, respectively.



(a) (b)

Figure 12 Comparative analysis with the Blockchain size as 500, (a) genuine user detection rate, (b) responsiveness.

Table 3 Comparative discussion

Blockchain Size	Metrics	ABAC	BSeIn	EACMS	Proposed Blockchain-based Access Control and Data Sharing
100	***Genuine user detection rate (%)***	65	65	58	95
	responsiveness (sec)	25	27	27	25
200	***Genuine user detection rate (%)***	83	70	38	95
	responsiveness (sec)	138	141	151	136
300	***Genuine user detection rate (%)***	75	69	68	95
	responsiveness (sec)	80	81	86	78
400	***Genuine user detection rate (%)***	83	83	61	95
	responsiveness (sec)	93	97	103	91
500	***Genuine user detection rate (%)***	61	57	49	95
	responsiveness (sec)	138	141	151	136

4.5 Comparative Discussion

Table 3 represents the comparative discussion. With the Blockchain size of 100, the genuine user detection rate obtained by the existing methods, like ABAC, BSeIn, and EACMS is 65%, 65%, and 58%, while the proposed obtained better genuine user detection rate of 95%, respectively. The

Table 4 Comparative discussion of the proposed Blockchain-based access control and data sharing with the existing techniques

Metrics	ABAC	BSeIn	EACMS	Proposed Blockchain-based Access Control and Data Sharing
Tamper-proof	Y	Y	Y	Y
Access Revocation	N	N	Y	Y
Non-Repudiation	Y	Y	Y	Y
Privacy-preserving	Y	N	N	Y
Attack Resistance	Y	N	Y	Y
Block search	N	N	N	Y
Access control	N	N	Y	Y
Metadata update	N	N	N	Y
Storage space recycling	N	N	N	Y
Data privacy	N	N	N	Y
Mutual authentication	N	N	N	Y
Data stream support	N	N	N	Y
Encrypted location search	N	N	N	Y

responsiveness obtained by the existing methods, such as ABAC, BSeIn, and EACMS is 138 sec, 141 sec, and 151 sec, whereas the proposed obtained lower responsiveness of 136 sec for 200 Blockchain size. Therefore, it is clearly depicted that the proposed Blockchain-based access control and data sharing approach attained better genuine user detection rate of 95%, and the lower responsiveness at 25 sec using the Blockchain size as 100.

The comparative discussion of the proposed approach with respect to the existing techniques by evaluating the some of the parametric factors is discussed in Table 4.

From Table 4, the proposed blockchain-based access control and data sharing approach obtained improved performance compared to the state of art techniques. For the data access, the tamper-proof is provided; hence the transparency of transaction is achieved. The access revocation provides enhanced security; non-repudiation is the evidence of the transaction and hence very useful in settling disputes. The attack resistance in the system improves the performance of the system. Moreover, the block search, access control provides another additional level of security, and metadata update has the information about the distribution of data block and the size, which helps to access the data faster. The storage space recycling improves the storage capacity, data privacy enhances secure data sharing, and mutual authentication provides the data sharing among two parties using the key for secure data sharing. The data stream support enables the full data storage referred by the hash function and can use as a general-purpose append-only database. The encrypted location search enables the secure search. Thus the secure and authentic data sharing is achieved by using the access control mechanism in the blockchain.

Besides, the proposed blockchain-based access control and data sharing technique uses eight different phases and four entities for secure data sharing and access control. Thus, the privacy of data is enhanced with reduced key abuse. The consensus protocols provide reliability and trust among the blockchain network. Moreover, the risk of attacks is also reduced with the help of a consensus algorithm named Proof of work (PoW). In our proposed work, the experimental evaluation shows a better genuine user detection rate with reduced responsiveness. Thus the bottleneck is reduced.

4.6 Threats to Validity

Internal Validity: The proposed blockchain-based access control and data sharing are used to secure data transmission. In this, hashing is performed for the encryption of the data. By using different layers of encryption, some of the values may vary.

External validity: For the performance evaluation, the simulation environment is created using cloudsim. Sometimes, the performance may vary because of software issues.

Construct Validity: The performance of the proposed blockchain-based access control and data sharing approach is evaluated based on the performance metrics like responsiveness and genuine user detection rate. However, more evaluation is possible, like throughput, delay, load, and energy consumption.

Conclusion Validity: In calculating the responsiveness and genuine user detection, some functions were used, which may vary concerning the simulation environment.

5 Conclusion

In this research, an effective method named Blockchain-based access control and data sharing approach is developed to increase data security in the cloud model. The system master key is generated and encrypted by the Data owner and is embedded in the transactional blockchain. The Data owner deploys the smart agreement in the transactional blockchain. The Data user sends the registration request to the Data owner, which creates the secret key and encrypts the secret key based on the Chebyshev polynomial, and embedded the encrypted secret key to the transactional blockchain. The Data owner sends the transaction ID, contract address, contract Application Binary Interface, and contract source code to the Data user with the secure channel. The Data owner selects the keyword set, encrypts the file, and uploads the encrypted file to the Interplanetary File System. The data owner generates the encrypted keyword index and records it in the smart agreement. Finally, the Data user downloads the encrypted file from Interplanetary File System and decrypts the file. The proposed named Blockchain-based access control and data sharing approach achieved better performance using the metrics, such as a better genuine user detection rate of 95% and lower responsiveness of 25sec with the blockchain of 100 sizes. The proposed blockchain-based access control and data sharing are widely used in security related applications like secure medical data sharing, real time IoT-related applications, monitoring services, etc. In the future, the performance of the access control and data sharing model in the cloud storage system is enhanced by incorporating some additional features.

References

[1] Rajput, AR, Li, Q., Ahvanooey, M.T. and Masood, I., "EACMS: Emergency Access Control Management System for Personal Health Record based on Blockchain", IEEE Access. 2019.

[2] Ding, S., Cao, J., Li, C., Fan, K. and Li, H., "A Novel Attribute-Based Access Control Scheme Using Block chain for IoT", IEEE Access, vol. 7, pp. 38431–38441, 2019.

[3] Ma, M., Shi, G. and Li, F., "Privacy-Oriented Blockchain-based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario", IEEE Access, vol. 7, pp. 34045–34059, 2019.

[4] Ouaddah, A., Elkalam, A.A. and Ouahman, A.A., "Towards a novel privacy-preserving access control model based on blockchain

technology in IoT", In Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523–533, Springer, Cham, 2017.

[5] Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H. and Ali, Q.E., "Blockchain based Permission Delegation and Access Control in Internet of Things (BACI)", Computers & Security, 2019.

[6] Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B., "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustainable Cities and Society, vol. 39, pp. 283–297, 2018.

[7] Lin, C., He, D., Huang, X., Choo, K.K.R. and Vasilakos, A.V., "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0", Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2018.

[8] Wang, S., Zhang, Y. and Zhang, Y., "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems", IEEE Access, vol. 6, pp. 38437–38450, 2018.

[9] Benchoufi, M. and Ravaud, P., "Blockchain technology for improving clinical research quality", Trials, vol. 18, no. 1, p. 335, 2017.

[10] Es-Samaali, H., Outchakoucht, A. and Leroy, J.P., "A blockchain-based access control for big data", International Journal of Computer Networks and Communications Security, vol. 5, no. 7, p. 137, 2017.

[11] Iansiti, M. and Lakhani, K.R., "The truth about blockchain", Harvard Business Review, vol. 95, no. 1, pp. 118–127, 2017.

[12] R. Chen, I.P. Tu, K.E. Chuang, Q.X. Lin, S.W. Liao and W. Liao, "Endex: Degree of Mining Power Decentralization for Proof-of-Work Based Blockchain Systems," IEEE Network, vol. 34, no. 6, pp. 266–271, 2020.

[13] Rahulamathavan, Y., Phan, R.C.W., Rajarajan, M., Misra, S. and Kondoz, A., "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption", IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6, December 2017.

[14] Dillon, T., Wu, C. and Chang, E., "Cloud computing: issues and challenges", IEEE international conference on advanced information networking and applications, pp. 27–33, April 2010.

[15] Ammar Ayman Battah, Mohammad Moussa Madine,Hamad Alzaabi, Ibrar Yaqoob, Khaled Salah, And Raja Jayaraman, "Blockchain-Based

Multi-Party Authorization for Accessing IPFS Encrypted Data", IEEE Access Vol. 8, 2020.

[16] Umesh Bodkhe, Sudeep Tanwar, Karan Parekh, Pimal Khanpara, Sudhanshu Tyagi, Neeraj Kumar, and Mamoun Alazab, "Blockchain for Industry 4.0: A Comprehensive Review", IEEE Access, vol. 8. 2020.

[17] Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, Alireza Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria", Expert Systems with Applications, Vol. 154, 2020.

[18] Adia Khalid, Muhammad Sohaib Iftikhar, A.s. Al-Mogren, Rabiya Khalid, Muhammad Khalil Afzal, and Nadeem Javaid, A Blockchain-based Incentive Provisioning Scheme for Traffic Event Validation and Information Storage in VANETs", Information Processing & Management, vol. 58, No. 2, 2020.

[19] Christidis, K. and Devetsikiotis, M., "Blockchains and smart contracts for the internet of things", IEEE Access, vol. 4, pp. 2292–2303, 2016.

[20] Islam, S.H., Khan, M.K. and Al-Khouri, A.M., "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing", Security and communication networks, vol. 8, no. 13, pp. 2214–2231, 2015.

[21] Hong Xu, Qian He, Xuecong Li, Bingcheng Jiang, and Kuangyu Qin, "BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control", IEEE Access, vol. 8, 2020.

[22] Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud", IEEE Access, vol. 8, 2020.

[23] Hernández-Ramos, J.L., Jara, A.J., Marín, L. and Skarmeta Gómez, A.F., "DCapBAC: embedding authorization logic into smart things through ECC optimizations", International Journal of Computer Mathematics, vol. 93, no. 2, pp. 345–366, 2016.

[24] Alam, M., Zhang, X., Khan, K. and Ali, G., "xDAuth: a scalable and lightweight framework for cross domain access control and delegation", In Proceedings of the 16th ACM symposium on Access control models and technologies, pp. 31–40, June 2011.

[25] Maesa, D.D.F., Mori, P. and Ricci, L., "Blockchain based access control", In IFIP international conference on distributed applications and interoperable systems, pp. 206–220, Springer, Cham. June 2017.

[26] N. T. Hung, "Deciphering the increased popularity of Vietnamese students' choice of Asian countries for overseas studies: The influence

of motivation for studying abroad on career planning and decision-making process of Vietnamese students in Taiwan", The International Conference on Higher Education in Vietnam and Asia: Similarities and Possibilities of Cooperation, 2020.

[27] Nguyen Tan Hung, "A Model of International Students' Choice: A Mixed-Methods Study", International Virtual Conference on Public Administration, Social Science & Humanities, 2020.

[28] Nguyen Tan Hung, and Jen-Chia Chang, "Preliminary Investigation of the Current Situation and Influencing Factors of International Students in Taiwan under the Background of New Southbound Policy", Taiwan Educational Review, vol. 8, no. 2, 2019.

Biographies

Yogesh M. Gajmal is currently working as Research Scholar in Bharath Institute of Higher Education and Research, Bharath University, Selaiyur, Chennai, Tamil Nadu 600073. He attended the Bharati Vidyapeeth Deemed University, Pune, India where he received his M-Tech in Computer Engineering in 2014. His Ph.D. work centers on Access Control in Cloud and discusses the Access control to develop new efficient and effective solution.

R. Udayakumar is currently working as Professor in Bharath Institute of Higher Education and Research, Bharath University, Selaiyur, Chennai, Tamil Nadu 600073.He has published 224 research papers in Scopus and SCI indexed journals and he is supervisor for research scholar at BIHER.