Journal of Autonomous Intelligence (2024) Volume 7 Issue 3
doi: 10.32629/jai.v7i3.1332

ORIGINAL RESEARCH ARTICLE

Access control and data sharing mechanism in decentralized cloud using blockchain technology

Yogesh Gajmal[1,*], **Pranav More**[2], **Arvind Jagtap**[3], **Kiran Kale**[4]

[1] *Finolex Academy of Management and Technology, Ratnagiri 415639, Maharashtra, India*

[2] *School of AI & Future Technologies, Universal AI University, Karjat 410201, Maharashtra, India*

[3] *MIT Art Design and Technology University, MIT School of Computing, Pune 412216, Maharashtra, India*

[4] *Presidency University, Itgalpur, Rajanakunte, Yelahanka, Bengaluru 560064, Karnataka, India*

*** Corresponding author:** Yogesh Gajmal, yogeshmgajmal@gmail.com

ABSTRACT

Access control is the most vital aspect of cloud data storage security. Traditional techniques for data distribution as well as access control face noteworthy challenges in the arena of research as a result of extensive abuse and privacy data breaches. The blockchain concept provides security by verifying users by multiple encryption technologies. Collaboration in the cloud improves management but compromises privacy. Consequently, we created an efficient access management and data exchange system for a blockchain-based decentralized cloud. On the basis of an ID and password, the data user (DU) submits a registering request to the data owner (DO). The DO data is incorporated into a transactional blockchain by an encoded master key. The data owner (DO) provides data encryption, and encrypted files are still published to the Interplanetary File System (IPFS). The DO generates ciphertext metadata, which is then published to the transactional blockchain utilizing a secure file location and a secure key. The projected access control and data sharing solution performed better in a decentralized blockchain based cloud, as measured by metrics such as a reduced illegitimate user rate of 5%, and a size blockchain of is 100 and 200, respectively.

Keywords: data sharing; cloud storage system; blockchain; smart agreement; Interplanetary File System (IPFS)

ARTICLE INFO

Received: 10 October 2023
Accepted: 21 November 2023
Available online: 12 January 2024

1. Introduction

The term “cloud” becomes prevalent in the communications industry as clients start utilizing virtual private network (VPN) services to streamline interactions[1]. End users are frequently not required to be aware of the real connections and locations of the network as a whole in order to use cloud computing services like storage, software, installation, and information access. Today’s widely used IT approach, the cloud, moves processing and data away from desktops and enormous server centers[2]. The NIST defines cloud computing as a method intended for rapidly granting on-demand system authorization towards a large number of connected computing sources without requiring any work or communication from the service provider. Due to the rapid expansion of high-speed internet through the universe, it is anticipated that requests will be delivered as services over the internet, thereby decreasing the total price of the system.

Cloud computing’s main objective is to efficiently employ scattered sources, incorporate them for high throughput, and be able to address common computational issues. Scalability, virtualization, interoperability, standards of service, and delivery methods including public, private, and a combination of both are all associated with cloud computing[3].

1.1. Data sharing privacy in cloud

Privacy is the ability of a person or group to secure information and then expose it in a thoughtful manner[4]. The following explanations of privacy's many components: different aspects of privacy are how, when, and how much. Meanwhile, a subject is more associated with the latest data being disclosed than the previous data from the existing years. Users feel comfortable if their friends can manually request their data, but they do not feel happy with often and automatically delivered warning information, and they may choose to keep their information reported as an unclear area rather than a specific place.

The user's context and privacy should be correctly used and protected in a variety of commercial apps. Institutional security necessitates the implementation of rules, guidelines, and procedures for the management of personally identifiable information[5].

1.1.1. Identity management

A big platform can use a maximum number of Internet-based facilities thanks to cloud computing[6]. In addition to its advantages, it increases the threat to privacy if a third party is associated with it. If a dependable third party is added, heterogeneity could occur and have an effect on cloud security. Identity management, a self-determining technique that makes use of identity information on untrusted hosts, is a novel solution to this issue. In order to stop information loss and privacy breaches in cloud storage, various protective phases are used. A business that depends on security needs can access the most recent services through the cloud. However, the virtualization of hardware, software, and databases has been used to create the cloud environment. The updating of cloud services involves a significant amount of trust reputation management and cloud security architecture. Programme authorization security, server access safety, internet access safety, and dataset safety are the main security challenges that occur in the cloud[7].

1.1.2. Privacy issues

The virtual computing method used by cloud computing is completely different from the previous computing technologies. There is a chance that the user's private data will be dispersed across international borders in several virtual data centers. In the present, various legal systems disagree on the issue of data privacy protection. In the meanwhile, customers of cloud computing services can divulge confidential information. Attackers look at crucial tasks that people who are involved in the computing process have submitted. The main privacy restrictions are trust, uncertainty, and conformity, which are defined as environments where information spreads in dynamic, global flows before issues with requirements compliance are resolved. Trust is defined as whether personally identifiable information (PII) is handled improperly. Uncertainty is defined as the process of verifying information that has been destroyed by the person in charge of maintaining information.

1.2. Access control-based data privacy

The primary requirements of cloud computing are privacy and security, which also pave the way for developing a secure and efficient method of accessing control for the information sources[8]. The access control mechanism prevents the requester from having any chance of obtaining the information after the user's authoritative identification has been confirmed. However, the access control approach is often used to safeguard important data resources and stop intruders from gaining unauthorized access.

Some of the current access control techniques are attribute-based access control (ABAC), mandatory access control (MAC), usage control (UCON), and role-based access control (RBAC). The access control paradigm is more prominent than the numerous conventional approaches in cloud frameworks. Users should allow authentication of the cloud service provider (CSP) and maintain proper regulations for allowing the data and the services while using cloud computing's storage and services. It is crucial to provide access control between mutual authentication and service providers in order to validate cloud security. Additionally, cloud users not only manage channel attacks but also integrate relevant measures for confirming the data's privacy. Although CSP has recently used a number of access control measures in the cloud domain to provide greater security protection, there are still significant limitations[8].

1.2.1. Role-based access control (RBAC)

A fundamental requirement of any type of data device is access control. ABAC and RBAC, two common access control techniques for services, are explained. This RBAC system takes into account a group of roles that may be accessed for doing specific tasks in a way that users can access to operate at certain crucial portions. The access control model typically takes into account the existence of a set of authorizations P and a certain type of user U.

1.2.2. Attribute-based access control (ABAC)

The architectural models as well as the policy model are the two requirements that make up the ABAC system. While the architectural model takes into account the rules for data access control, the policy model outlines the properties of ABAC schemes[3]. The following list of ABAC's numerous types of attributes is explained:

a. Subject attributes

A user who advances on a resource is known as a subject. Each topic is made up of the associated values that define its traits and sense of self. These include the subject's name, occupation, employer, and unique identification. In contrast, a resource is a user who moves through a subject. Additionally, the resources' attributes are expanded to allow for control decision-making.

b. Environment attributes

Environmental characteristics describe the functional, technical, and various contexts in which data access is carried out. The values in this case, such as the current date and time, the most recent services, and the data privacy stage, are not linked to a particular resource or subject. Additionally, the policy representation between the ABAC must be fine-grained. It is therefore employed in conjunction with subject, resource, and environmental aspects[9].

1.2.3. Blockchain-based access control

The illustration in the study of Ali et al.[10] demonstrates how a decentralized privacy solution can be used to protect the privacy of information gathered and managed by an external entity. This method is based solely on distributed ledger technology (blockchain), which functions as an access controller to protect pointer privacy, and an off-chain distributed hash table (DHT), which should be authorized by blockchain technology to protect encoded data. When a user logs in, the most recent compound identity is created and aggregated. Using an identifying key, the information is encrypted and decrypted, and the compound identity is composed of login key pairings for the user and the service. The blockchain guarantees both the user's identity also the service's right to access the information. It prepares the hash to retrieve the information from off-chain storage.

The prime aim of this project is to implement a decentralized cloud storage system that usages Blockchain technology to manage data access and sharing. The data owner (DO) handles the registration request then receives the user ID and password from the data user (DU). In addition, the data user is confirmed. Using a master key that has been encrypted, the transactional blockchain encodes data owner information. After the data owner effectively implemented data encryption, the encoded files were transfer to the Interplanetary File System (IPFS). Taking into consideration the location of the encoded key and encoded file, the data owner generates the encrypted text metadata that is unintentionally added to the transactional blockchain.

Incorporating blockchain technologies into the cloud storage system is a beneficial trend since it increases confidence and lowers computing costs. It makes the system model credible, decentralized, and publicly verifiable so that the different connected devices can gain trust through blockchain. The blockchain model created a method for managing data that allows the data owner to have ownership and control. Additionally, the storage system can provide improved privacy protection for the individuals' data. The blockchain system model was designed to do away with issues like data privacy. The access control approach with blockchain support was created to boost security. Access control is a crucial tool for ensuring data privacy.

The rest of the article's arrangement is as follows: The section 2 describes the access control mechanisms currently in use. The third section explains the suggested access control and data sharing strategy. The fourth section describes the findings and discusses the recommended course of action, and the fifth section concludes the paper.

2. Motivation

In this section, analyses a number of current blockchain-based access control strategies, which motivate the researchers to create a method to increase data security.

2.1. Literature survey

The cloud storage model is extremely important to the daily processes of the corporate world in the era of developing internet technologies. The cloud offers a variety of storage options for business people and enterprise domains to access cloud resources as well as exchange the information anywhere, which plays a significant function and provides greater ease in daily life for people. The current cloud data storage model has one major flaw, which can be fixed by using a decentralized approach to data storage, which has more benefits than a centralized model[9–11]. Decentralized networks typically have greater scalability, dependability, and confidentiality. Additionally, a centralized network has a harder time dealing with single-point failure. The commercial strategy heavily relies on bitcoin's decentralized network to avoid single points of failure, making it completely safe and increasing efficiency. The data-sharing method is also made more reliable and scalable. In the decentralized architecture, where no user may make any changes, the information is gathered in a single peer[12]. Additionally, because Blockchain has a decentralized structure and creates an immutable ledger distributed to record every transaction, it is also known as a decentralized structure. A network-based approach called cloud computing makes data available to users[13,14]. Service providers offer software resources that are shared as well as information from non-demand sources. Users can access complex services and amass necessary finances on local platforms in the cloud computing structure once native data is sent to cloud servers. Cloud computing is the smart structure in contrast to cloud computing's cost and services[15,16]. IoT blockchain technology was used Ouaddah et al.[17] to create a privacy-preserving access control system. Here, a new decentralized pseudonymous authorization management mechanism that protects privacy is used to handle access control for controlled devices and to maintain the constancy of the blockchain. Additionally, the access control paradigm used by the emergency cryptocurrency solution, authorization tokens, was adopted. In this case, blockchain was used to confirm that all cooperating parties had guaranteed the access system and policies in distributed structures.

Guo et al.[18] the data owners are allowed to encrypt their information then delegate it to a distributed model. Without the need for a distinct round interface for the production of legal search tokens, the data owner distributes the secret key to authorized users through influencing blockchain smart contracts. Furthermore, the trust problems related with query authorization are efficiently solved by this technique. To offer encrypted keyword search, forwards privacy, and regulated blockhead over-head, a secure local index structure was created.

2.2. Challenges

The challenges experienced by existing block chain approaches are illustrated as below,

EACMS was created for access control in the block chain system in[19], Although this model failed to enhance the performance of a system with less complexity. For a safe cloud data sharing architecture, the blockchain enabled access control solution with various attribute authorities was created in[20]. However, this algorithm did not successfully strike a balance between security and efficiency. The decentralized data storage method based on blockchain was introduced in [21], but this model has not yet maintained the required Quality-of-Service (QoS).

BDKMA was developed for access control in IoT structures[22], Although this solution was not discovered, a feedback model for security access managers (SAMs) and cloud managers was developed to aid in the persistence of blockchain-based IoT in[23]. Although this model does not estimate performance depending on software and hardware implementation, the BSeIn model was created in[24] for a fine-grained access control model.

2.3. Objectives

The major objectives of access control and data sharing mechanism are illustrated as given below:

- To provide a data sharing procedure that is efficient and simple across many cloud storage platforms.
- To protect the integrity of the data and stop unauthorized people from accessing the information on cloud platforms.
- To use a secret key generated via a blockchain-based data sharing technique to get the original image data.
- To provide a solid data-sharing infrastructure that ensures data security on public or untrusted cloud servers.
- To provide flexibility and ensure the data's privacy while maintaining high security.

3. Proposed blockchain-based access control and data sharing technique in cloud

The blockchain provides security by utilizing robust encryption mechanisms to authenticate the identities of users. One of the most important security requirements for sharing data in cloud computing is to guarantee that users have complete control over access to their confidential information, as unauthorized disclosure of this information to individuals or unethical businesses could compromise user security. Therefore, it is essential to protect the data transfer procedure[25]. Block chain-based technologies offer a viable and irretrievable public ledger for recording the transactions of different type and is considered as a core unit for addressing the data origin problem of cloud infrastructures[26]. This paradigm contains of eight stages: the setup phase, the user registration phase, the encryption phase, the token creation phase, the control set-up phase, the test phase, the validation phase, also the decryption phase. Data owner (DO), smart agreement, data user (DU), Interplanetary File System (IPFS), and transactional block chain are the four entities considered in this technique. DU refers to the clients of DO who have access to the files. In order to complete the process of data preservation and information retrieval, each party in this situation must fulfill its responsibilities. Before transferring the assembled files to the DU, the DO encodes the data then transmits it to the IPFS. The final stage in data protection is maintaining the confidentiality of the user's data. The scheme for the cloud's block chain-assisted data retrieval model is shown in **Figure 1**.

Only legal users must have access to the cloud-based information storage in order towards share data. Once the data owner needs to share their data thru the group, the completed data encryption key is provided to each group member. Any member of the group can download encrypted content from the cloud, which is then decrypted using the key. As a consequence, the group member does not require the assistance of the data owner. In addition to privacy and utility characteristics, the technique used them to manage the critical data. In response to requests for encoded data collected in cloud, the CSP controls whether the requested data is present in storage or else whether a data retrieval mechanism that satisfies the demanded index terms exists. During information retrieval, the original data from protected data is retrieved.

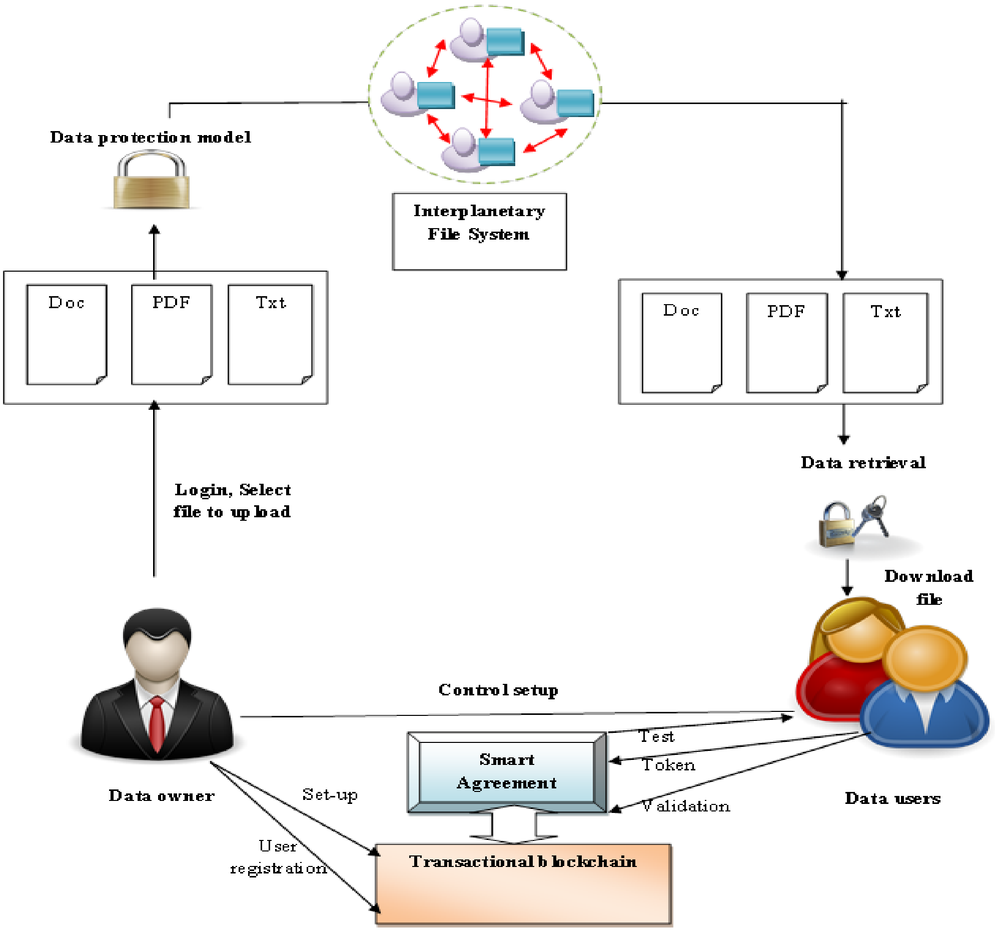

Figure 1. Block diagram of developed approach.

3.1. Setup phase

Setup level is operated by DO such that DO considers input as S and produces M and $R$of system as output. The DO publishes R which is system public parameter in media, such as website and public dataset, since $R$is widely available. The DO encrypted M and embedded M into transactional blockchain (**Table 1**).

Table 1. Symbol description of developed method.

Symbol	Description
S	Security parameter
R	System public parameter
M	System master key

Table 1. (*Continued*).

Symbol	**Description**
h	Hash function
E	Encryption function
//	Concatenation operator
$\oplus$	EX-OR operation
$\otimes$	Interpolation
n	Random integer
D	Soil database
D_{id}	Data user ID
D_{pwd}	Data user password
D_{spwd}	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 based on AES
I_{en}	Encrypted keyword index
t	Search token
$d(.)$	Decryption
$E(.)$	Encryption
D_R	Data retrieved

Moreover, DO use smart contracts for blockchain-based transactions. The smart contract is uses to store encrypted keywords then provides data consumers with effective search capabilities. According to the M and R descriptions produced by DO,

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

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

where, S is concatenated with q parameter and it is employed to hashing function for producing R. Moreover, q is a parameter, which ranges among $[0,1]$ and α symbolizes the parameter ranges from $[0,1]$. The master key of system is formulated by executing EX-OR function with S and α.

DO encrypts the letter M, which is performed as,

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

The term M and parameter α are concatenated with each other, and resultant factor is encrypted with modulus function. The DO implant the encrypted M to transactional blockchain. The transactional blockchain receives encrypted M and records it with soil dataset. The transactional data executes the EX-OR function with D_1 and M_{en} also records it for further processing. In this segment, DU transfers registration request through producing ID as D_{id} and password as D_{pwd} of DU and transfers them to DO. The DO receives DU ID and password as well as records it as D_{id}^* and D_{pwd}^* m moreover, forwards them to smart agreement. The DO produces session password for DU as D_{spwd} and sends it to DU for authenticating the identity. The DU receives and records session password as $\widetilde{D}_{spwd}$ and sends it back to DO after filling the identity. The DO authenticates D_{spwd} and distributes attribute set A to DU. In addition; transactional account address of DU is included as authorized user in smart agreement.

3.2. User registration stage

DO is primarily in charge of managing this stage of user registration, and it creates the secret key K using the attribute set and the value M.

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

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

The DO produces the secret key K and transmits it to the smart agreement, which stores it as K*. But the denotation for a secret key that has been encrypted is,

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

After performing the EX-OR function with a secret key and Chebyshev parameter, the output value is encrypted and interpolated with A. Ken secret encryption key is delivered to the transactional blockchain along with soil data. T_{id}, C_{ad}, C_{ABI}, and C_{src} are sent through protected channel from the DO to the DU.

3.3. Encryption phase

Three independent stages of the encryption process data encryption, key encryption, and keyword index generation are completed during this phase, which is overseen by DO. Initially, a file encryption key also a keyword set is utilized to encode the data. To encrypt the data, the DO selects an AES key and a keyword set from the data. Furthermore, encoded data is characterized as,

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

In the second stage, DO uses P_{en} and D_{en}^{loc} to create ciphertext for metadata. On the other hand, the position of encrypted data is depicted as,

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

The DO generates an encrypted key that is indicated as,

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

The DO-created ciphertext metadata is denoted as,

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

The encrypted key and encrypted data location are concatenated and the encryption function is used to concatenated data. The randomly chosen key based on AES is EX-OR functioned with encrypted data for generating ciphertext metadata. The DO produces encrypted keyword index through including keyword set andα, which is denoted as,

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

Concatenating the keyword set and parameter α also applying an encryption process on it. To create an encrypted keyword index, the encrypted data is concatenated with factor q.

3.4. Token generation phase

For the purpose of getting K, the DU reads a data file associated with a secret key and decrypts K_{en} as follows:

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

The encrypted secret key is employed to decryption function in order to attain$K$. The DU creates a token that is explained as follows:

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

The secret key and parameter$\alpha$are concatenated then, EX-OR function is performed with keyword set. Additionally, DU produces token depends on s_k and invokes smart agreement for searching process.

3.5. Control setup phase

In order to carry out the contract for data exchange between DU and DO, DO manage the control setup step. This part is primarily responsible for adding new users and handling index, file deletion, keyword index deletion, searching, and file withdrawal.

3.6. Test phase

The smart agreement is characterized as, in the test stage, collecting the token created via the DU in the token generation portion and accumulating it into the smart agreement.

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

The token, which is recorded in smart agreement is indicated as t^*. The smart agreement verifies the token produced by DU is coordinated with token recorded in smart agreement. DU is authenticated, while $t = t^*$. When DU sends a request, and search option is enabled, then DU is authorized, which is expressed as,

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

The transaction ID and token are concatenated and executes encryption function. Furthermore, key are chosen randomly based on AES is concatenated with encrypted keyword index and completes encryption function. Both of the encrypted data are permitted to execute EX-OR function, and resultant value is signified as X. The smart agreement produces matched result and transfers it to DU.

3.7. Validation phase

DU validates user files throughout the validation process by creating a validation factor that is dependent on a secret key, a random number, and data user ID, which is indicated as,

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

The secret key is concatenated with random integer and is interpolated with data user ID, thus the resultant value is given to hashing function. The output of hash function and success factor produced by smart agreement is permitted to implement EX-OR function. The DU produces validation factor and transfers it to smart agreement for user in order to become validated. The smart agreement receives validation factor from DU and records it by following equation,

$$V^* = X \oplus \hbar\big(D_{id}^* \otimes (n||K^*)\big) \tag{17}$$

If V and V^* match, the smart agreement validates the user. Otherwise, it does not.

3.8. Decryption phase

DU often handles decryption stage, which involves decrypting a file using the returned data file and the file encryption key to create the final information file and sent from DU to DO. DO get the file and logs them as,

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

The secret key and random integer are concatenated, and resultant value is interpolated with data user ID, which is employed to hashing operator. At last, EX-OR function is carried outwith X^*. The DO verifies if an authenticated file produced by DU is matched with file recorded in DO. DO transfers encrypted data location and encrypted key to DU. The DU accumulates encrypted data location and encrypted key and transfers them to IPFS with a^{s_k}. The IPFS receives data directs from DU and records it in IPFS. The IPFS shares an encrypted data with DU. The DU download the file that the IPFS shares and decrypt retrieved data based on file encryption key, which is illustrated as,

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

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

The data file is constructed by concatenating the file encryption key with the retrieved data.

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

Finally, DU is used to retrieve the data file.

4. Results and discussion

In this section, the findings and discussion of the recently proposed technique are illustrated. This part also includes the experimental design, performance metrics, and performance analysis.

4.1. Experimental setup

An Intel processor, 4 GB of RAM, a PYTHON tool, and Windows 10 OS are used to implement the designed cloud system. For experimental evaluation, the simulation environment is built using CloudSim, with user counts ranging from 20 to 100 and blockchain sizes from 100 to 500.

4.2. Performance metrics

On the basis of metrics such as illegitimate user, the established technique's efficacy is estimated. Users who make legitimate queries to destinations that are permitted by edge routers are illegitimate.

4.3. Performance analysis

Utilizing performance criteria, such as illegitimate user by adjusting blockchain size from 100 to 500, the developed strategy is compared to other approaches.

a) Blockchain size = 100

Figure 2 depicts the comparison study of illegitimate users in terms of user count. Using current methods, such as ABAC, BSeIn, and EACMS, the percentage of illegitimate users is 54%, 52%, and 22%, respectively, when there are 20 users. In contrast, the proposed access control and data sharing mechanism generated only 5% unauthorized users. Using current methods such as ABAC, BSeIn, and EACMS, the percentage of illegitimate users when there are 40 users is 62%, 62%, and 42%, respectively. However, only 32% of illegitimate users utilized the projected blockchain-based access control and data sharing system. For a population of 60 users, current methods like ABAC, BSeIn, and EACMS respectively catch 69%, 62%, and 62% of unauthorized users. In contrast, the proportions of illegitimate users for blockchain-based access control and data sharing solutions were 42% and 12%, respectively. Using current techniques, such as ABAC, BSeIn, and EACMS, the percentage of illegitimate users when there are 80 users is 70%, 70%, and 69%, respectively. In contrast, the proportions of illegitimate users for blockchain-based access control and data sharing solutions were 42% and 12%, respectively. ABAC, BSeIn, and EACMS each provide an unlawful user rate of 70%, 70%, and 70% when there are 100 users. However, the projected blockchain-based access management and data sharing solutions result in only a 70% rate of illegitimate users.

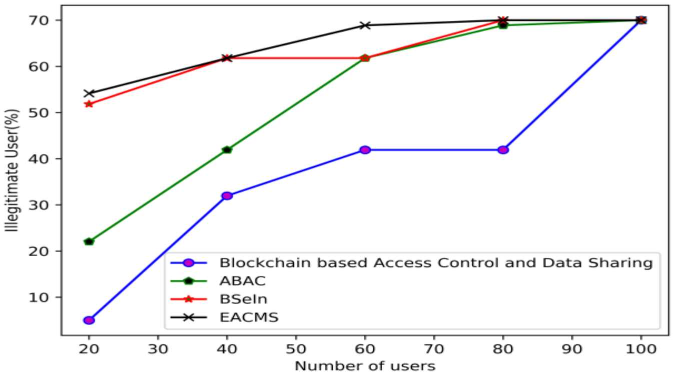

Figure 2. Comparative analysis with the blockchain size as 100, illegitimate user.

b) Blockchain size = 200

Figure 3 depicts the comparison study of illegitimate users in terms of user count. Current techniques, including ABAC, BSeIn, and EACMS, attract 62%, 30%, and 16% of unauthorized users for every 20 users. In comparison, the projected blockchain-based access control and data sharing options generated only 5% and 1% fraudulent users, respectively. Using the current techniques, such as ABAC, BSeIn, and EACMS, the percentage of illegitimate users is 70%, 48%, and 30%, respectively, when there are 40 users. Comparatively, 16% of the projected blockchain-based access control and data sharing users were fraudulent. Using current techniques, such as ABAC, BSeIn, and EACMS, the percentage of unauthorized users attained when there are 60 users is 70%, 70%, and 53%, respectively. The suggested blockchain-based access restriction and data sharing solution reached 45% of illicit users. Using the current techniques, such as ABAC, BSeIn, and EACMS, the percentage of illegitimate users obtained from 80 users is 70%, 70%, and 70%, respectively. In contrast, only 74% and 74% of unauthorized users utilized the proposed blockchain-based access restriction and data sharing system. ABAC, BSeIn, and EACMS each provide an unlawful user rate of 70%, 70%, and 70% when there are 100 users. However, the suggested blockchain-based access control and data exchange solutions result in only a 70% rate of fraudulent users.

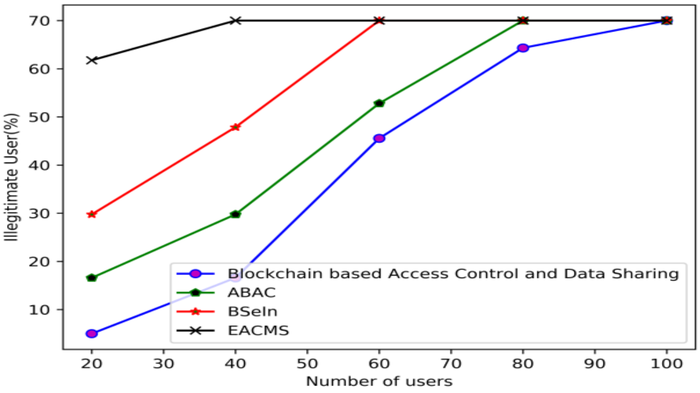

Figure 3. Comparative analysis with the blockchain size as 200, illegitimate user.

c) Blockchain size = 300

Figure 4 depicts the comparison study of illegitimate users in terms of user count. Using the current techniques ABAC, BSeIn, and EACMS it is possible to identify 32%, 31%, and 24% of unauthorized users when there are twenty users. While only 5% of illegitimate users make use of the suggested blockchain-based access control and data sharing solutions. Using current methods such as ABAC, BSeIn, and EACMS, the percentage of unauthorized users when there are 40 users is 43%, 43%, and 39%, respectively. In contrast, 26% of users on the projected blockchain-based access control and data sharing system were fraudulent.

When there are 60 users, the suggested blockchain-based access control and data sharing technique has a lesser percentage of illegitimate users, at 43%, than the current approaches, such as ABAC, BSeIn, and EACMS, which have 65%, 57%, and 43%, respectively.

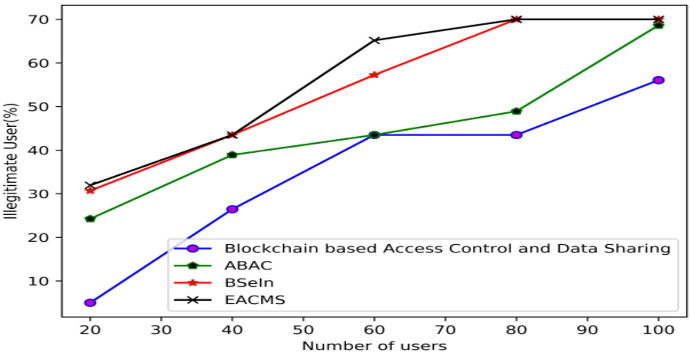

Figure 4. Comparative analysis with the blockchain size as 300, illegitimate user.

d) Blockchain size = 400

Figure 5 compares actual user populations. Using current techniques such as ABAC, BSeIn, and EACMS, the percentage of unauthorized users attained when there are 20 users is 17%, 17%, and 38%, respectively. Only 5% of illicit users were interested in the suggested blockchain-based data sharing and access restriction.

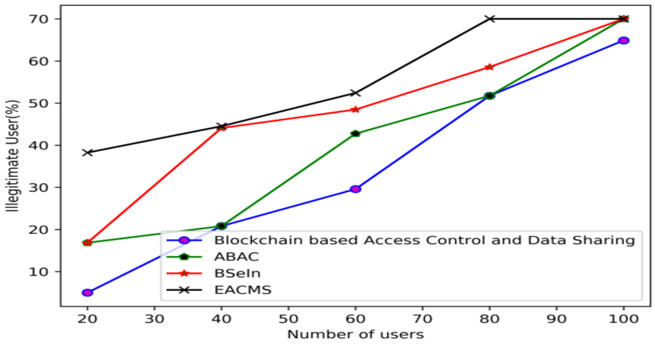

Figure 5. Comparative analysis with the blockchain size as 400, illegitimate user.

e) Blockchain size = 500

The quantity of authorized users is contrasted with the numeral of unauthorized users in **Figure 6**. Current techniques, such as ABAC, BSeIn, and EACMS, detect 39 percent, 43 percent, and 51 percent of unauthorized users when there are 20 users. The suggested blockchain-based access control and data sharing system attracted only 5% of unauthorized users.

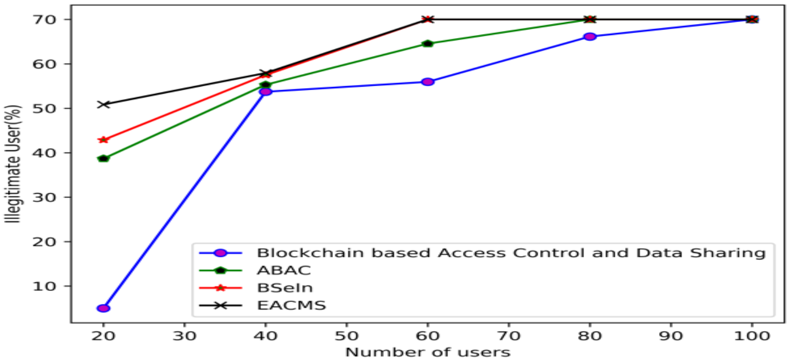

Figure 6. Comparative analysis with the blockchain size as 500, illegitimate user.

4.4. Comparative discussion

Table 2 compares the development of a data sharing as well as access control method based on blockchain of sizes 100, 200, 300, 400, and 500 with regard to the number of illegitimate users (40). ABAC, BSeln, and EACMS all acquire a percentage of illicit users of 62%, 62%, and 42%, respectively. However, the proposed method obtains only 32% of illegal users through a block size of 100. Using a blockchain size of 100, it follows that the established blockchain-based access control and data sharing technique had 32% fewer illegitimate users.

Table 3 presents the analysis of two datasets using methodologies that take into account privacy and information loss. Using the heart disease dataset, the proposed technique measures privacy to a maximum of 82.875%, whereas PSO, CS, BS, and privacy without optimization measure privacy to 74.029%, 72.520%, 71.388%, and 68.566%, respectively. The suggested technique calculates the minimal information loss of 17.124% while the information loss assessed by PSO, CS, BS, and without optimization are 25.970%, 27.479%, 28.611%, and 31.433%, respectively. The proposed method measured maximum privacy of 96.5% and least information loss of 3.5% using the breast cancer dataset.

Table 2. Comparative discussion.

Blockchain size	Metrics	ABAC	BSeIn	EACMS	Blockchain-based access control and data sharing
100	Illegitimate (%)	62	62	42	32
200	Illegitimate (%)	70	48	30	16
300	Illegitimate (%)	43	43	39	26
400	Illegitimate (%)	18	42	43	18
500	Illegitimate (%)	53	56	58	51

Table 3. Comparative analysis.

Dataset	Metrics	Proposed method	PSO	CS	BS	Without optimization
Heart disease dataset	Privacy (%)	82.875	74.029	72.520	71.388	68.566
	Information loss (%)	17.124	25.970	27.479	28.611	31.433
Breast cancer dataset	Privacy (%)	96.5	95.584	93.849	92.849	91.484
	Information loss (%)	3.5	4.415	6.15	7.15	8.515

The lower computation time of 5.84 seconds for the newly created access control and data sharing method based on blockchain is shown in **Table 4**.

Table 4. Computation time.

Metrics	ABAC	BSeIn	EACMS	Blockchain-based access control and data sharing
Computational time(sec)	8.97	8.06	7.36	5.84

4.5. Main findings

The main findings of developed approaches are explicated as below,

- The performance of developed blockchain-based access control and data sharing technique is evaluated using illegitimate users.
- Thus, the devised blockchain-based access control and data sharing method obtained better performance with illegitimate users of a 5% drop.
- In addition, the performance of developed approach in cloud structure is evaluated using for metrics, namely privacy, and information loss.

- Therefore, the introduced model in cloud system achieved enhanced performance with respect to information loss of 3.5% in heart disease database and privacy of 82.87% in breast cancer dataset.

5. Conclusion

Access control is the most essential element for improving data security in cloud storage architecture. Privacy data breaches and key abuse resulting from the existing data sharing and access control technique constitute the greatest challenge in the field of research. As internet technology advances, the significance of the cloud storage system in the day-to-day operations of the business model increases. Due to the cloud's many categories of storage facilities for the enterprise area as well as business people, the ability to access cloud assets from anywhere then send information has significantly enhanced human existence. This research was conducted in response to blockchain-based decentralized cloud access control and data sharing. The DU generates an enrolment request utilizing the user's ID as well as password. A master key that has been encrypted is used to merge the DO data into the transactional block chain. Using the encrypted file location and encrypted key, the DO achieves data encryption before sending the encrypted files to IPFS. The ciphertext metadata produced by the DO is sent to the transactional blockchain. The encoded keyword index is created and added to the smart contract by the data owner. The encrypted file is subsequently downloaded and decrypted by the Data user from IPFS. As a result, when a 100-blockchain setup was used, the effectiveness of the blockchain-based access control and data sharing technique was improved by a 5% drop in illegitimate users and also, the suggested model's better performance in the cloud system led to information loss reductions of 3.5% and privacy improvements of 82.87%.

Author contributions

Conceptualization, YG and PM; methodology, YG; validation, AJ, KK and PM; formal analysis, YG and KK; resources, YG; writing—original draft preparation, YG; writing—review and editing, YG and AJ; visualization, YG and PM; project administration, YG and KK. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Kaufman LM. Data Security in the World of Cloud Computing. IEEE Security & Privacy Magazine. 2009, 7(4): 61-64. doi: 10.1109/msp.2009.87
2. Dikaiakos MD, Katsaros D, Mehra P, et al. Cloud Computing: Distributed Internet Computing for IT and Scientific Research. IEEE Internet Computing. 2009, 13(5): 10-13. doi: 10.1109/mic.2009.103
3. Jadeja Y, Modi K. Cloud computing-concepts, architecture and challenges. In: Proceedings of the IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET). March 2012; pp.877-880.
4. Tsai T, Theera-Ampornpunt N. A study of soft error consequences in hard disk drives. In: Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), June 2012; pp. 1-8.
5. Pearson S, Benameur A. Privacy, Security and Trust Issues Arising from Cloud Computing. 2010 IEEE Second International Conference on Cloud Computing Technology and Science. Published online November 2010. doi: 10.1109/cloudcom.2010.66
6. Ma M, Shi G, Li F. Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. IEEE Access. 2019, 7: 34045-34059. doi: 10.1109/access.2019.2904042
7. Victor N, Lopez D, Abawajy JH. Privacy models for big data: a survey. International Journal of Big Data Intelligence. 2016, 3(1): 61. doi: 10.1504/ijbdi.2016.073904
8. Dillon T, Wu C, Chang E. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications. Published online 2010. doi: 10.1109/aina.2010.187

9. Bodkhe U, Tanwar S, Parekh K, et al. Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access. 2020, 8: 79764-79800. doi: 10.1109/access.2020.2988579
10. Ali S, Wang G, White B, et al. A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). Published online August 2018. doi: 10.1109/trustcom/bigdatase.2018.00179
11. Khalid A, Iftikhar MS, Almogren A, et al. A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs. Information Processing & Management. 2021, 58(2): 102464. doi: 10.1016/j.ipm.2020.102464
12. Battah AA, Madine MM, Alzaabi H, et al. Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data. IEEE Access. 2020, 8: 196813-196825. doi: 10.1109/access.2020.3034260
13. Yang X, Li T, Xi W, et al. A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud. IEEE Access. 2020, 8: 170713-170731. doi: 10.1109/access.2020.3025060
14. Shen B, Guo J, Yang Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences. 2019, 9(6): 1207. doi: 10.3390/app9061207
15. Niu S, Chen L, Wang J, et al. Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain. IEEE Access. 2020, 8: 7195-7204. doi: 10.1109/access.2019.2959044
16. Naz M, Al-zahrani FA, Khalid R, et al. A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. Sustainability. 2019, 11(24): 7054. doi: 10.3390/su11247054
17. Ouaddah A, Elkalam AA, Ouahman AA. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. Europe and MENA Cooperation Advances in Information and Communication Technologies. Published online September 23, 2016: 523-533. doi: 10.1007/978-3-319-46568-5_53
18. Guo Y, Wang S, Huang J. A blockchain-assisted framework for secure and reliable data sharing in distributed systems. EURASIP Journal on Wireless Communications and Networking. 2021, 2021(1). doi: 10.1186/s13638-021-02041-y
19. Rajput AR, Li Q, Taleby Ahvanooey M, et al. EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. IEEE Access. 2019, 7: 84304-84317. doi: 10.1109/access.2019.291797
20. Qin X, Huang Y, Yang Z, et al. A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. Journal of Systems Architecture. 2021, 112: 101854. doi: 10.1016/j.sysarc.2020.101854
21. Wang S, Zhang Y, Zhang Y. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. IEEE Access. 2018, 6: 38437-38450. doi: 10.1109/access.2018.2851611
22. Ding S, Cao J, Li C, et al. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access. 2019, 7: 38431-38441. doi: 10.1109/access.2019.2905846
23. Chinnasamy P, Vinodhini B, Praveena V, et al. Blockchain based Access Control and Data Sharing Systems for Smart Devices. Journal of Physics: Conference Series. 2021, 1767(1): 012056. doi: 10.1088/1742-6596/1767/1/012056
24. Lin C, He D, Huang X, et al. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications. 2018, 116: 42-52. doi: 10.1016/j.jnca.2018.05.005
25. Gajmal YM, Udayakumar R. Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System. Journal of Web Engineering. Published online August 30, 2021. doi: 10.13052/jwe1540-9589.2054
26. Gajmal YM, Udayakumar R. Privacy and Utility-Assisted Data Protection Strategy for Secure Data Sharing and Retrieval in Cloud System. Information Security Journal: A Global Perspective. 2021, 31(4): 451-465. doi: 10.1080/19393555.2021.1933270