# A Secured Data Sharing Using Proxy Re-encryption and Blockchain in Cloud Storage

B. Dunesh Madhav(✉), A. Teja Sai Vijaya babu, A. Naga Sai Anil Chowdary, G. Victo Sudha George, and J. Jayaprakash

Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai, Maduravoyal, Tamil Nadu 95, India
duneshmadhav213@gmail.com

**Abstract.** The development of data sharing in cloud computing has proven valuable. The Paper explores the complexities of ensuring data security within cloud environments and proposes a solution centered around proxy re-encryption. The core objective is to strengthen the security aspects related to sharing data within the scope of cloud computing. The proposed system entails data owners securely archive their encrypted data into cloud storage utilizing identity-based encryption. Authorized users can subsequently access the data through proxy re-encryption. To mitigate resource limitations, an edge device acts as a proxy server to manage computationally intensive tasks.

The work leverage information-centric networking to optimize service quality and network bandwidth by delivering cached content through the proxy. The foundational system model relies on blockchain technology, facilitating decentralized data sharing and offering precise access control. A comprehensive security analysis and evaluation of the proposed scheme, illustrate its potential to guarantee data confidentiality, integrity, and overall security Overall, paper presents a holistic strategy to confront data security challenges using proxy re-encryption, edge computing, information-centric networking, and blockchain technology, offering a promising approach for mitigating data security risks in cloud environments.

**Keywords:** Proxy re-encryption · data sharing · blockchain · cloud computing · identity-based encryption · proxy server

## 1 Introduction

In the dynamic world of Information technology, the emergence of cloud storage as a basic paradigm of data storage and sharing has been more dominating. It renders unmatched convenience and scalability. Even though the use of cloud-based services is growing, security concerns and protection of data are at a critical stage. This paper is to tackle these problems head on by introducing an advanced solution for secure data sharing in cloud storage systems. The framework integrates two cutting-edge technologies: Combination PRE and Blockchain provides an effective system for ensuring the data confidentiality and integrity not only but also for traceability [1].


P. Pareek et al. (Eds.): IC4S 2024, LNICST 598, pp. 31–49, 2025.
https://doi.org/10.1007/978-3-031-77078-4_3

Proxy Re-Encryption is a reputable cryptographic technique for sharing data securely by providing an authorized party the ability to transform encrypted data based on one key into ciphertext under another key without decrypting the original encrypted message. This approach has an additional safety feature that cuts to the time of sharing what portion of keys will be decrypted [2]. In addition, there is a layer consisting of Decentralized and unmodifiable PRE modules in the Blockchain system which guarantees the integrity and the transparency of many of the records of the transactions. The implementation of Blockchain guarantees auditable track data access and modifications which materially reduces the occurrence of bailment risks caused by unauthorized access or inappropriate changes to data [3].

In this system, the entities that generate the data are referred to as data producers. They are engaged in protecting the information by themselves encrypting it before handing it over to the clouds service providers (CSPs). A distinction must be made between those who produce data and those who own it. Data owners principally strive to determine who is the owner of the data. The access rights to the data were set up before it is shared with potential users. Though the data owners may also act as the data producers, other entities can also be involved in the data production. The communication between data owners and other entities is considered to occur via a trustworthy intermediary, like an agent or server [4, 5].

## 2 Literature Survey

This paper depicts the role of Blockchain Technology in IoT Data Security. The system is based on a distributed network which eliminates the need for central proxy service providers and thus ensures reliability and correctness. Re-encryption keys are distributed to consensus nodes so that the architecture can fight off collusion attacks by denying unauthorized access to the private key information. System security is enabled by the data confidentiality and integrity that it ensures through a distributed design, which makes it immune to tampering. The analysis of performance and security stresses on the efficiency and scalability of offered scheme, it proposes a reasonable solution for protecting data exchange in IoT [6].

The following paper proposes a model for secure and traceable data-sharing using blockchain technology. This model incorporates three main components: attribute encryption, secure data storage, and smart-contract-based log tracking. The proposed system allows for real-time data sharing between two parties while ensuring high data security. To achieve this, the shared data is first encrypted and then stored off-chain in an Interplanetary File System (IPFS). The hash value of the encrypted data is then encrypted again before being stored on the blockchain. The blockchain data-sharing records are managed and presented visually through a mechanism implemented by smart contracts. Our model offers a solution to the issues of traditional data-sharing models, providing a more secure and efficient way of sharing data [7].

Discusses the features of utilizing blockchain for safe data sharing in IoT, focusing on the decentralized, immutable model. It shows hazards in cloud solutions such as data loss. The authors present smart contracts as a solution for rogue user tracking and for the security of deep learning techniques. Strategies such as granular access controls

are a means of protecting sensitive health information during data sharing. The research proposes applying blockchain to secure IoT data in public clouds to achieve better privacy and access control [8].

Paper presents Identity-based Conditional Proxy Re-encryption (IBCPRE), a new cryptographic notion for confidential data delivery. IBCPRE provides a semi-trusted proxy capable of modifying the ciphertexts of one identity to another identity due to certain specified conditions. Compared with traditional proxy re-encryption, this scheme solves the problems of blind decryption and gives the right to decryption. The proposed IBCPRE scheme is based on the Boneh-Franklin identity-based encryption, however, provides improved security guarantees. Overall, IBCPRE offers a flexible and secure solution of conditional data forwarding in the cryptographic systems [9].

Proposes a new CP-ABE scheme aimed at improving data security and privacy by disguising access policies. It has a constant size ciphertext and reduces storage overhead with the short signature scheme preventing insider attacks. The proposal system ensures access control at a fine-grained level, data confidentiality, authenticity, integrity, and privacy preservation. Performance evaluation is the comparison of the proposed method with the existing CP-ABE schemes illustrating the efficiency of it in encryption, decryption, and memory analysis. The architecture consists of building blocks responsible for access control, insider attack security, and BLS signature verification, which results in a secure and privacy-preserving system for IoT applications with AI [10].

## 3 Existing System

From the above survey, in the current arena of data commerce, centralized servers and cloud-based services dominate their niche in managing deployment, operations, and applications. While these central hubs serve as channels of transmitting and receiving data, one important problem arises because these sources might lack sufficient security measures that leave the entire system open to exploitation. These remain the issues that are exacerbated by the limitations in access control mechanisms and; hence, a danger to data privacy and security [9, 11, 12].

The inadequacy of blockchain technology also worsens the situation since there is no transparency and trust in data transactions [13–16]. The blockchain, decentralized and tamper-proof, could offer a resolution by creating an immutable transactions ledger. This would not only help in transparency and accountability but will also allow stakeholders to validate the integrity as well as original journey of data that has been shared [17–19].

To conclude, there are several serious flaws regarding the current system of data sharing about security, privacy, and trust. For strengthening this ecosystem, a holistic approach needs to be adopted involving efficient security measures, enduring access controls, blockchain technology for transparency and scalable infrastructure solutions Through addressing the above aspects, this goal of achieving a more secure, confidential, and reliable basis for data sharing in heterogeneous ecosystems is sought.

# 4 Proposed System

The proposed method focuses on the minimization of the data exposure due to the delegated access and encryption of the data before its transfer to the cloud servers. A cryptographic scheme called Proxy Re-Encryption (PRE) is offered. It enables a trusted third party to modify the encrypted data while not revealing the decryption keys. This method is of much importance to the implementation of secure data exchange in a unique cloud infrastructure setting.

The framework suggests the incorporation of PRE alongside IBE, ICN, and blockchain for the resolution of data sharing. The article highlights the number of advantages that IBE has over ABE, and it further asserts that it is a suitable option for environments with limited resources.

The platform also deals with ICN, which allows the data owners to label and transfer their data, achieving replication and network cache storage for data delivery. The blockchain technology, as a new concept, is a distributed and decentralized system which solves the many data privacy, storage, and access control problems while ensuring safe and secure data sharing. Proposed system has some advantages like

- Enhanced Data Security
- Detailed access control
- Data Privacy
- Transparency and Trust
- Scalability, Decentralization
- Cost-Efficiency
- Immutable Record Keeping,
- Long-Term Viability

# 5 Methodology

## 5.1 Technologies Used in Data Sharing and Access Regulation in the Cloud Storage.

**Advanced Data Sharing via PRE:**

**KP-ABE and PRE-Integration:** Our proposed system, KP-ABE and PRE are integrated into the cloud-based data exchange platform by means of a proper approach. The data is encrypted through the KP-ABE, where exactly each set of secret attributes keys is needed for its decryption. Cloud is responsible of keeping secret all keys except one which is used for revocation. Such integration enables data to be retained in ciphered form with access strictly permitted based on user's attributes, hence boosting confidentiality and access control. On the one hand, the service provider may be tempted to collude, together with the revoked users, and therefore the third trusted party came up as a suggestion and some schemes were even considered as using CP-ABE to associate encryption policies with ciphertext instead of the secret key. Also, the short-term access control scheme of PRE and ABE has been studied, but they were found to be unsuitable for IoT.

**IBE PRE Data Sharing Scheme:** In our suggested approach, the data is protected when a shared data process pursues the IBE PRE schema. Each session comes with new re-encryption keys that are produced based on user's identity and particular ciphertexts for the sake that public keys are distinct for each pair of user-file identities. Thus, an only allowed people to see certain files which contributes to security enhancement.

Flat PRE with no hierarchy was not found as the best-suited option for handling multiple hard real-time applications. Hence, the access control system utilizes the IBE PRE model for its simplicity and the fact that it is one of the most efficient data access control mechanisms available.

**Combination of IBBE and PRE:** Some schemes in the system, which include conversion from IBE and PRE, give the advantage of seamlessly converting both protocols without revealing the private information. Thus, incorporating the capability gives the organization the right mix of dynamism and versatility in the very process of sharing and transmitting of the data, enforcing it to utilize a particular encryption strategy depending on the security specifications that are available by every data transaction.

Apart from that, an IBPRE protocol is established which provides a zero-one form of proxy server controls all ciphertext whether it is all or none. By means of which they establish full control of encrypted data usage and block unauthorized access, thus keeping sensitive information away from people who could possibly have some malicious intentions.

**Conditional-Based IBE PRE Scheme:** Several new schemes are being proposed regarding conditional secret sharing, such as an identity-based group PRE scheme in which alternative transformations of ciphertexts are allowed across different identities so that the user not have access to the decryption privilege. The security of the protocol is reviewed by the fact that except authorized users do not have the other directory keys information, and they have possibilities only to revoke their own keys not the other gathered data.

The system can be configured to enforce fine-grained access control in which data owners would be able to define detailed access rules which would define policy for variety user groups. This fact increases data confidentiality and integrity which in turn balances the risk of data exposure or changes imposed without any authorization.

The combination of these solutions with the proposed system guarantees resilient data security, data access control, and privacy, leading to a comprehensive solution for data security in cloud environments.

### 5.2 Blockchain-Enabled Data Access Control:

**Decentralized Personal Data Management:** In the proposed system, blockchain-based data access control is automatically implemented to accomplish distributed personal data management. With this integration, the blockchain acts just like an automatic access control system in a decentralized management of individual data. With the help of memory-resident data addresses and a distributed hash table for data storage, the blockchain network keeps data in multiple nodes and does not allow exposure to data. Access control policies are enforced automatically and based on predefined rules and

conditions using smart contracts or decentralized tools. Such approach means that only authorized individuals are allowed to acquire the data that is meant for them which leads to heightened privacy and security. One of the most crucial features of blockchain, and which offers it an edge over other technologies, is the fact that it is decentralized. This means that a compromise in a node would not compromise the integrity of the entire data and access control policies because the blockchain would still serve as a reliable framework for secure management and sharing of sensitive data in cloud environments.

### 5.3 Data Integrity

Data integrity is achieved by incorporating the SHA-1 algorithm into the system. SHA-1 algorithm generates hash values that can serve an identifier for each data; they can be used for checking the integrity of data because the calculation of the hash value of the data which is frozen in time can be compared with the original hash value each time the data is changed. This operation is responsible for the preservation of the information integrity, meaning no data has been modified. This guarantees that all the data is unaltered and accurate. Besides that, SHA algorithm is compatibly used together with asymmetric cryptographic algorithms to create secure digital signatures. Signature can be checked through private and public keys there by data transmissions are protected, which provides authentication and non-repudiation for data transactions. In the system's blockchain technology the SHA algorithm, depending on the mining difficulty, is implemented to hash blocks of data and link them using cryptographic hashes. This guarantees the enduring state of the blockchain by hindering past transactions from being repudiated without causing the whole chain to be altered. In addition, the SHA algorithm is utilized to safely store passwords, sensitive material, and cryptographic keys by converting them into fixed sized hash values. Through this approach, a secure debugging method is introduced that does not require the original data to be disclosed, thereby improving the entire system's security.

### 5.4 AES Algorithm

The AES algorithm will be implemented into the system through the advanced protection system to enhance our level of information and data confidentiality. RSA is a key element in the design of the cryptosystem and is used for encryption and decryption of the data, and to manage the encryption keys. An AES encryption transforms plaintext into ciphertext by utilizing a secret key to keep it safe from unauthorized access before storage or transmission, thus, defending it against potential hackers. The algorithm supports sizes of key 128, 192 and 256 bits that really represent a flexible mode of security. Decryption entails repeating the process in reverse and turning the ciphertext back into plaintext with the use of the same encryption key; which helps to avail authorized access to the data. First and foremost, it is AES which ensures both data security and confidentiality. It is the basic premise behind information sharing and access control in the proposed system as well.

# 6 Proposed System Architecture

## 6.1 Architecture of Proposed Work

Our proposed system framework, as depicted in Fig. 1. It offers a novel technique of data exchange by also utilizing the blockchain-based Proxy Re-Encryption (PRE). It combines edge devices and makes use of blockchain technology. These edge devices act as proxies that perform re-encryption services for authorized users. They are designed to store data at the network edge, thus increasing availability and performance for the users. These devices get re-encryption keys from data owners and obtain ciphertexts from the Cloud Service Provider (CSP) and adjust the ciphertext based on the user's identity. These devices, deemed as trustworthy entities having a pronounced concern for data reliability, are not involved in malicious activities.

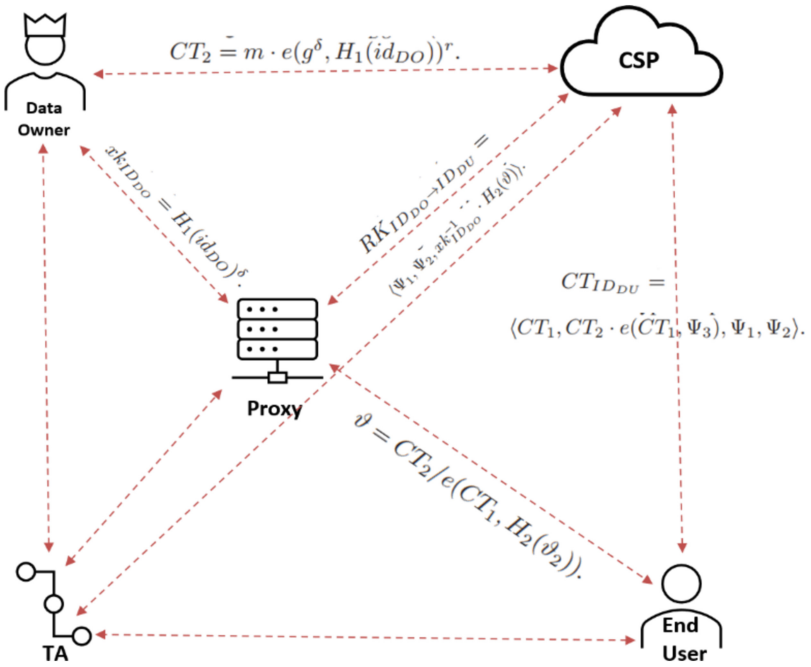


**Fig. 1.** Architecture Diagram of proposed work

A TA runs the setup algorithm during system initialization to get system parameters and the master key. At the same time, the Key Gen algorithm produces keys for users. Upon the Encrypt operation, the data owner produces Ciphertext (CT) which is subsequently securely shared with the CSP by virtue of the metadata stored on the blockchain. One of the benefits of incorporating caches in the forwarding function is network resilience to packet loss which eventually leads to better content availability. This method provides content caching and capabilities like re-encryption.

### 6.2 The Data Flow Between the Different Entities:

The system setup is a fundamental process that establishes the groundwork for secure data transmission and access control. Let us delve into the intricacies of the system setup using bilinear maps and understand each step clearly.

**Bilinear Map Definition:** Bilinear Map Definition: Bilinear map is a fundamental element of the system setup, which is

$$\hat{e} : G1 \times G1 \rightarrow G2. \tag{1}$$

In this context, G1 represents a cyclic group generated by element g, while the order of G2 is denoted by p. Moreover, two hash functions,

$$H1 : G1 \leftarrow (0, 1)* \tag{2}$$

is designed together with G2: G1 $\leftarrow$ G2 that aims at cryptographic operations enhancement.

**Public Parameters Generation:** The public key parameters that encapsulate the essence of the cryptographic system are calculated as params = (G1, H1, g, g$\delta$). Here $\delta$ is a notation for the secret key chosen from the group Z $*$ p.

**Key Generation Process:** Utilizing, public parameters, secret key, and an identifier, the key generation algorithm computes the decryption key for the specified identity. This process yields the data owner's secret key, denoted as

$$\text{xkIDDO} = \text{H1(idDO)}\delta. \tag{3}$$

**Encryption Procedure:** Encryption, a pivotal aspect of secure communication, involves several steps:

Selection of a random number r from set Z $*$ p.

Computation of the ciphertext,

$$\text{CTIDDO} = (\text{CT1},\ \text{CT2}), \tag{4}$$

$$\text{where CT1} = \text{gr and CT2} = \text{m} \cdot \text{e}(\text{g}\delta,\ \text{H1(idDO)})\text{r} \tag{5}$$

This step ensures the confidentiality and integrity of the transmitted message m.

**Re-encryption Key Generation:** Facilitating secure data sharing between different entities necessitates the generation of re-encryption keys:

Selection of an element $\theta$ from G2.

Computation of the tuple

$$\langle \Psi 1,\ \Psi 2 \rangle = \text{Enc(params,\ idDU,\ } \theta). \tag{6}$$

Generation of the re-encryption key as

$$\text{RKIDDO} \rightarrow \text{IDDU} = \langle \Psi 1,\ \Psi 2,\ \text{xk} - 1\text{IDDO} \cdot \text{H2}(\theta) \rangle \tag{7}$$

**Re-encryption Process:** Re-encryption serves as a pivotal operation in enabling secure data transmission:

Re-encrypting the ciphertext CT from the data owner entity to the end user using the re-encryption key

$$\text{RKIDDO} \rightarrow \text{IDDU}. \tag{8}$$

Definition of the re-encrypted ciphertext as.

$$\text{CTIDDU} = \langle \text{CT1},\ \text{CT2} \cdot \text{e}(\text{CT1},\ \Psi 3),\ \Psi 1,\ \Psi 2 \rangle \tag{9}$$

**Decryption Process:** Decryption is the final step, enabling the recipient to retrieve original message m:

For the re-encrypted ciphertext

$$CT'ID = \langle \text{CT3},\ \text{CT4} \rangle \tag{10}$$

$$\text{computation of } \theta 2 = \text{Dec}\big(xkID, CT'ID\big). \tag{11}$$

$$\text{Retrieval of the plain text via } \theta\ =\ \text{CT2/e}\ (\text{CT1},\ \text{H2}(\theta 2)). \tag{12}$$

Computation of the message as

$$\text{m} = \text{CT}\prime 2\text{e}\ (\text{gr},\ \text{H2}(\theta)) = \text{m} \cdot \text{e}(\text{g},\ \text{H2}(\theta))\text{r/e}(\text{gr},\ \text{H2}(\theta)) \tag{13}$$

By meticulously following these steps, cryptographic protocols ensure the confidentiality, integrity, and authenticity of data transmission and access control.

### 6.3 Flow Chart

Figure 2 will outline the operation of the Data Sharing System, facilitating secure file transfer from the Data Owner to an End User.

The system requires a secret key provided by the data owner to access the file, which must be sent alongside the file to the system. Once the file is uploaded, it is stored within a Cloud Service Provider (CSP) for validation of both the file name and secret key. If both matches, the system grants access to the file to the end user.

### 6.4 Modules

**Data Owner Module:** In this phase, the data owner transfers their data to the public cloud server. To ensure security, the data owner symmetrically encrypts the data file and then applies a digital signature to it before loading the data to the cloud. The right to check the integrity of the data file stored on the specific cloud server still rests with the data owner. Besides the data owner can also modify the encrypted data file as he pleases, including updating its content or deleting his own files from the cloud storage.

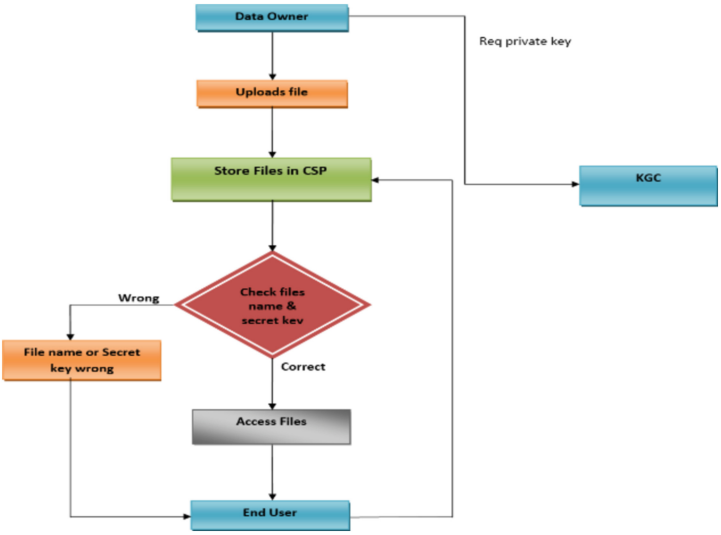


**Fig. 2.** Flow Chart of Proposed System

**Key Generation Centre:** This module involves the Key Generation Centre (KGC), which generates Secret Keys upon user requests. The KGC checks for file presence and generates the appropriate Secret Key accordingly. The KG-CSP (Key Generation-Cloud Service Provider) enables viewing Secret Key-generated files and transactions related to those files.

**Proxy Server:** The server oversees user management, authorization, and facilitates data transactions between the data owner and CSP, as well as end-users.

**Data User Module:** Within this module, the data user logs in using their username and password. Subsequently, the user requests Secret Key for the required file from the CSP, obtaining the Secret Key from the KGC. With the Secret Key in hand, the user attempts to download the file by entering the file name and Secret Key from the cloud server.

**Encryption and Decryption of Data:** All authorized users within the system have the liberty to inquire about any encrypted or decrypted data of interest. Upon receiving the data from the server, the user employs the decryption algorithm to decrypt the ciphertext using their respective secret keys obtained from various users. Access to the content is granted only if the attributes possessed by the user align with the access structure outlined in the ciphertext (CT).

**Attacker Module:** Within the Data User Module, if a remote user enters an incorrect trapdoor or Secret Key during the download process, they are identified as a digital sign attacker or Secret Key attacker.

**Data Integrity Check:** Cloud verification is implemented to check if the data has been tampered with by an attacker. In case of tampering, recovery is initiated by the data owner.

## 7 Implementation

In terms of hardware, the system relies on an Intel Core i5 processor, a 500 GB hard disk, a 24-inch LED monitor, as well as standard peripherals like a keyboard, mouse, and 8 GB of RAM. Software-wise, it mandates the Windows 10 operating system, Java for coding, NetBeans 8.2 as the development environment, and MYSQL for database management.

The operational procedures of the system are elaborated below, illustrating how data is securely stored and accessed through the integration of proxy re-encryption, identity-based encryption, and blockchain technology.

**Ensuring Data Integrity and Encryption:** Data integrity is maintained using the SHA-256 hashing algorithm to generate the data hash. Finally, the data owner encrypts the data with a random encryption key yielding the ciphertext which is securely uploaded to the Cloud Service Provider (CSP).

**Managing Metadata and Digital Signatures:** Metadata including timestamps, keywords, and data types is created to make data retrieval and search much easier. On the contrary, the data owner applies its private key to generate a digital signature attached to the data hash, thus ensuring both data integrity and authenticity.

**Generating Re-Encryption Keys and Access Lists:** A data owner derives re-encryption keys based on user identities requiring data access. These identities are the part of the access lists sent to the proxy server.

**Proxy Server Verification and Data Caching:** The proxy server verifies the sign of the owner belonging to the access list and obtains a URL linked to the ciphertext. Then it makes an identity (ID) for the URL, initially termed as d ID, and adds its own signature to increase the data delivery efficiency.

**Registering on the Blockchain:** Blockchain stores metadata, access control policies, author and proxy signatures, hash values and d ID among others. Blockchain network manages membership keys providing security to the framework for access control.

**Handling User Data Access Requests:** Upon user requests for access to the data, blockchain authenticates the data by verifying the signatures of the data owner as well as the proxy. After successful authentication, the time timestamp is added to the record of historical data.

**Retrieving and Re-encrypting Data:** A request for data is made by the user which in turn causes the proxy server to give Data Digital Signature as reply. The key information is obtained from the cache and the ciphertext from the Cloud Service Provider. Afterwards, the proxy uses the re-encryption key to re-encrypt the CT before making it available to the user.

**User Data Decryption and Blockchain Authentication:** The user decrypts the re-encrypted data by means of their private key and verifies its authenticity using blockchain verification which ensures the correctness of signatures. Timestamp validation happens on a blockchain, with the record kept for audit reasons.


**Fig. 3.** Data Owner Login

Above Fig. 3, a data owner login screen is a web page that enables the owners of data to interact with system, the data owner runs the system parameter setup and generates keys for the users. They encrypt data and officially verify its initial authenticity. The owners of the data generate re-encryption keys to restoring the data of the user. They determine data access through the definition of use policies. Owners verify user requests or grant access, by device. Their function ensures the data security and authenticity remain intact constantly. The data owner sets the rules and control over data sharing as well as accessibility.

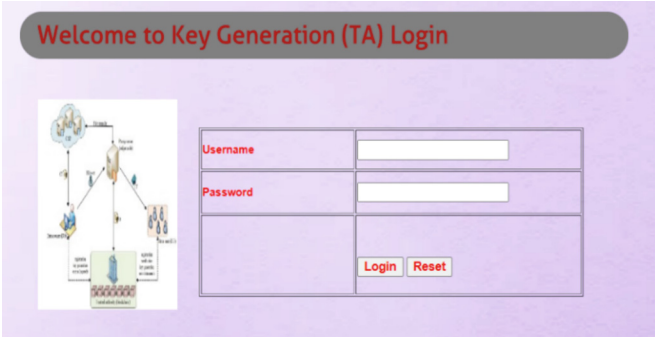


**Fig. 4.** TA Login

Above Fig. 4 shows the homepage of a website for key generation and login. The following elements are visible:

A navigation bar with the following tabs: Home, CSP, Proxy, TA, Data User, Blockchain is a Trusted Authority (TA) as it provides a decentralized and tamper-proof ledger which serves the purpose of system parameter management, secret key issue well as data verification. It plays a role of registering users, creating access control, and enforcing transparent and verifiable data sharing.

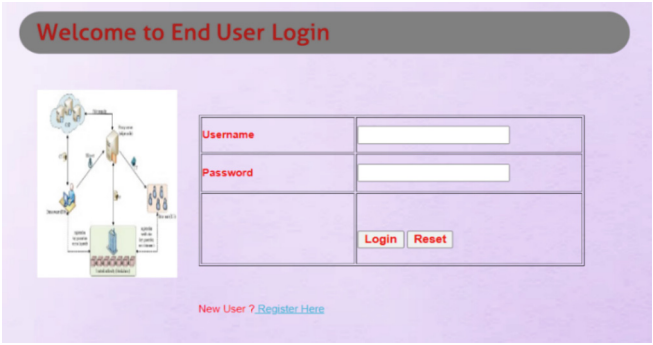


**Fig. 5.** End User Login

Above Fig. 5 login form with the following fields: Username, Password, Login, ResetAbove Fig login page is likely used by users to access a variety of systems and applications, such as cloud security provider (CSP) systems, proxy servers, and data user applications.

The function of the end user is to initiate the interaction by requesting those data that are stored in the system, verify the identity, and after authentication, he or she will receive the probe. They interact with the system to fetch and decrypt ciphered data basing on their individual's private identity keys, enabling them only to access information they have been authorized to view.

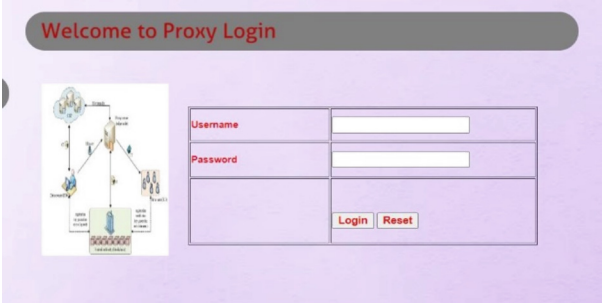


**Fig. 6.** Proxy login

This above Fig. 6 login page is likely used by users to access a web proxy server It can be used to improve security, performance, and privacy.

The checkbox to remember the user's login information allows users to avoid having to enter their username and password each time they need to log in to the proxy server.

The proxy serves as a mediator among three entities: constitutes an interface of the data owner, the CSP, and the end users in general. It represents a crucial element in the provision of a security layer for data transmission as it serves as an intermediary. The data subject passes re-encryption keys to a proxy which proxy than uses these keys to fetch a ciphertext from the CSP. Following that, the proxy will encrypt the ciphertext as

in the function of identity of permitted users. Hence, only authenticated, and authorized users can decrypt the messages.

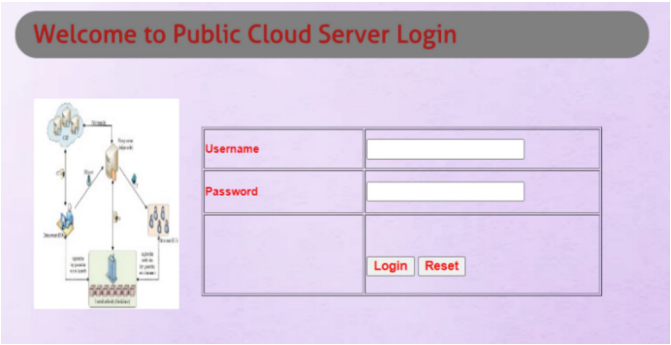


**Fig. 7.** Cloud Server Login

Above Fig. 7, the login form allows users to enter their username and password to authenticate themselves and gain access to their cloud server accounts. The Reset Password link is for users who have forgotten their password. The Create New Account link is for new users who need to create a cloud server account.

The Cloud Service Provider (CSP) functions by encrypting data sent by the data owner and storing it on its servers. When a user requires the specific data, the CSP validates the user's credentials and privileges. After validation the CSP fetches the encrypted data from storage and sends it to the user. The CSP also manages on the encryption and decryption activities, making sure that the data is safe during the period of transmission and storage. Also, CSPs are using security protocols to prevent unauthorized access and data breaches to maintain the confidentiality and integrity of stored data.

## 8 Performance Analysis

### 8.1 Performance Analysis of Proposed System

The proposed solution's security measures will be evaluated in various terms, such as confidentiality, integrity, authentication mechanisms, access policies controls, scalability, resiliency, and usability. These aggregating metrics cover both the cryptographic aspects (for example, encryption effectiveness) and the user experience. An experimental system is set up to duly emulate the real-world situation whereby the sensitive datasets are produced and the solution is deployed under a set of controlled conditions. Different attacks on security are simulated to check the system's resistance level while performance metrics like computational effort is taken into consideration. A quantitative analysis helps to prove the solution's effectiveness, like encryption efficiency, access control effectiveness, attack detection rate, and scalability. Users' satisfaction is also measured by feedback on the effectiveness and ease of use of the security features pointing out areas for modifications and enhancement.

On the other hand, computation time and transaction latency are two quantitative evaluation metrics that must be quantitatively assessed to calculate the proposed solution's security. Computation time is the period required for any computing operation, while transaction latency is the length of time taken by transactions to pass through and get confirmed on the blockchain network. The experimental setup consists of creating an environment virtually resembling real-world scenarios with some cloud servers, edge devices, and blockchain nodes. Different data types and access control strategies are configured to mimic different scenarios of sharing, system performance will be assessed under diverse loads, network conditions and security threats. The results of the security analysis are provided qualitatively, indicating the average time of computation and transaction latency for distinct operations and data sharing, which will shed the light on the system's effectiveness and efficiency. Along with this, base-line systems or existing solutions will be compared to evaluate how the proposed method improves security but at the same time reduces the amount of computation and delaying the transactions.

The analysis of computation time for data encryption, re-encryption, and decryption operations shows distinct growth patterns, indicating differences in performance based on the number of users and encryption methods utilized. This analysis underscores the efficiency and security considerations of the proposed framework in the context of data sharing.

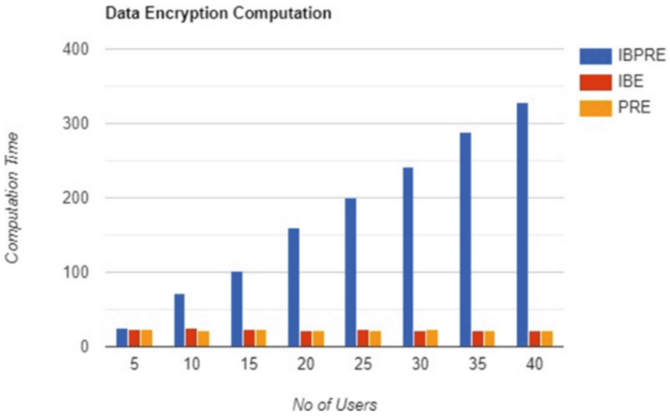


**Fig. 8.** Data Encryption Computation

The Fig. 8 visualizes how the number of users (N) and computational time (ms) in milliseconds are related in encryption at first, the computation time is 350 milliseconds for 5 users, and as the user number rises, the time is reduced. This trend continues to exist until it is getting to a remarkable 10 milliseconds for the user number 40, which means a notable inverse relationship between the computational time and the number of participants. Moreover, the graph contains three data points belonging to the alternative schemes or approaches labeled IBE, PRE and IBPRE. These data points have constantly higher computation times as compared with the scheme represented by the line while the depicted scheme shows clearly the superior efficiency of the designed strategy over these approaches.

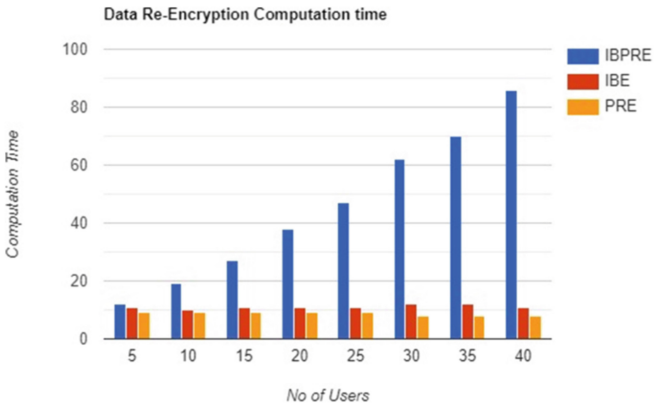


**Fig. 9.** Data re-encryption computation time

Figure 9 highlights the performance of the proposed framework in terms of computational time., particularly for many users. This makes the proposed scheme a more practical and feasible solution for real-world applications in context of data re-encryption.

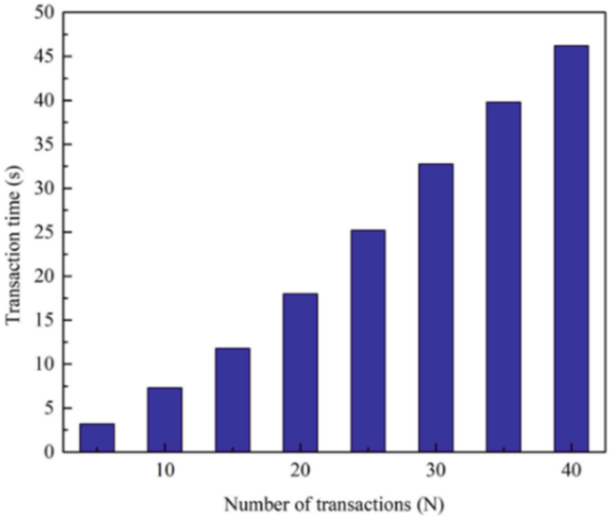


**Fig. 10.** Transaction latency

Figure 10 shows the plot that demonstrates the connection between several transactions (N) and the transaction time (s) in seconds. At first, it will take 50th second period for the first one transaction, and with the increase of transactions, it will become faster and faster. This descending path will be followed until the l0th one, in which it reaches 5 s. On the other hand, we can observe a certain trend in transaction times which is demonstrated by the increase to 30 s for transaction 14. Finally, the graph displays a

general curve showing a fall in transaction time as numbers go up leading to a system that is more efficient over period. Although the ups and downs indicate opportunities to help for improvement and to make such processes smooth and obstacle-free.

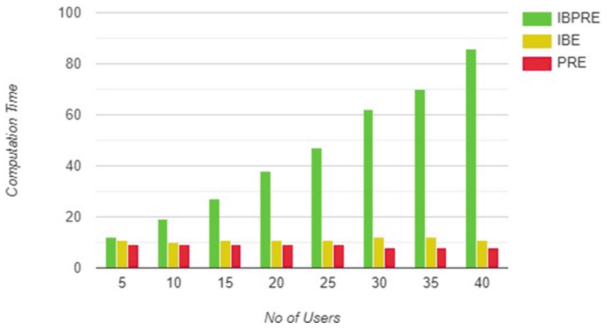


**Fig. 11.** Decryption computation time.

Figure 11 highlights the efficiency of the proposed scheme in terms of computation time, particularly for in terms of Data Decryption.

### 8.2 Attacks Prevented in Proposed System

The solution proposed in the paper is designed to address various security threats within the data exchange system, giving priority to defending against different types of attacks:

**Mitigation of Eavesdropping Attacks:** Through our system, we have created greater protection against these attacks. In a classical setting, attackers use the compromised or CA to give users the wrong public keys, which leads to the decryption of secret data. Therefore, in our approach, it is the blockchain that acts as the CA. The data is saved on publicly accessible blocks; all connections with preceding and succeeding blocks are saved within participating nodes. This immovability of the keys in this blockchain makes it incredibly difficult for attackers to mutate ersatz keys. Furthermore, the distributive component erases a single point of failure.

**Prevention of Data Tampering:** In our adopted blockchain model, each user has the capability to publish a hash associated with their data, safeguarding it against any alterations. In conventional systems compromised by hackers, various versions of the data can be injected, posing challenges in ensuring the integrity of the entire dataset. However, in our model, even if a malicious actor succeeds in breaching the storage and tampering with the data, they are unable to modify the hash stored on the blockchain. This ensures that any tampering with the data is promptly detected by all parties involved.

**Guarding Against Anomalistic Attacks:** In blockchain-based systems, the emergence of forks holds significant importance, particularly when considering the potential for malicious intent. Although attacks may initially focus on a particular device, the risk of them spreading to other devices is a valid concern. In our model, data regarding past

attacks is methodically gathered and added to a blacklist, effectively preventing attacks on entities that remain uncompromised. This proactive strategy strengthens the system's ability to withstand repeated attacks over time.

## 9 Conclusion

The proposed solution provides noteworthy benefits, such as strengthening data security through an integration of Proxy Re-Encryption (PRE), Identity-Based Encryption (IBE), and Blockchain to create a one-stop-shop to promote security and personal confidentiality. This security combination prevents unauthorized data access and breakthrough of the confidentiality, integrity, and access control to meet the established security goals. Moreover, the platform ensures fine-grained authorization operations where data owners can specify access privileges depending on user IDs and characteristic sets, therefore, keeping all data stored secure. Information confidentiality is assured by cryptographic operations such as PRE and IBE, where shared data stay encrypted so that disclosure risks related to data sharing are avoided. Users can confidently engage with Blockchain because in its operation it is transparent and therefore incorruptible by undesirable data abuse. The architecture without a centralized node serves for scaling and resilience to the large-scale data transactions, making it appropriate for a massive network. Notwithstanding these strongholds, the solution might encounter difficulty due to similar constraints such as computational cost, complexity, and adoption. However, possible future progressions may include employing improved cryptographic methods, incorporating leading technologies, enabling ease of use, implementing robust scale-up procedures, maintaining efficient security monitoring, and building consensus about common standards. Compared to existing methods, an analysis of the proposed method should cover security, scalability, usability, and cost effectiveness to provide a thorough report of the solution's strong as well as weak points.

## References

1. Manzoor, A., Braeken, A., Kanhere, S.S., Ylianttila, M., Liyanage, M.: Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. J. Netw. Comput. Appl. **176**, 102917 (2021)
2. Günsay E., Yayla O.: Decentralized anonymous IoT data sharing with key-private proxy re-encryption. Cryptology ePrint Archive (2022)
3. Chinnasamy, P., Deepalakshmi, P., Dutta, A.K., You, J., Joshi, G.: PCiphertext-policy attribute-based encryption for cloud storage: toward data privacy and authentication in AI-enabled IoT system. Mathematics **10**(1), 68 (2021)
4. Yan, L., Ge, L., Wang, Z., Zhang, G., Xu, J., Hu, Z.: Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. J. Cloud Comput. **12**(1), 1–16 (2023)
5. Zhang, W., et al.: Attribute-based proxy re-encryption for secure and fine-grained access control in cloud storage. Futur. Gener. Comput. Syst. **129**, 246–256 (2022)
6. Zhang, M., et al.: Enhanced security and privacy-preserving data sharing in cloud environments using homomorphic encryption. Futur. Gener. Comput. Syst. **126**, 388–398 (2022)

7. Wei, Z., Li, J., Wang, X., Gao, C.-Z.: A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing. IEEE Access **7**, 62785–62793 (2019)
8. Wang, S., Zhang, Y., Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access **6**, 38437–38450 (2018)
9. Obour Agyekum, K.O.B., et al.: A secured proxy-based data sharing module in IoT environments using blockchain. Sensors, **19**(5), 1235 (2019)
10. Fan, K., Ren, Y., Wang, Y., Li, H., Yang, Y.: Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Commun. **12**(5), 527–532 (2018)
11. Singh, M., Kim, S.: Branch based blockchain technology in intelligent vehicle. Comput. Netw. **145**, 219–231 (2018)
12. Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M.: IoT Privacy and security: challenges and solutions. Appl. Sci. **10**(12), 4102 (2020)
13. George, G.S., Meenakshi, K., Begum, A.: Acrse-ik – an attribute-based confidentiality retaining searchable encryption technique using interim keyword for protected cloud storage. Int. J. Recent Technol. Eng. **8**(1S2), 252–256 (2019)
14. Naz, M., et al.: A secure data sharing platform using blockchain and interplanetary file system. Sustainability **11**(24), 7054 (2019)
15. Rawal, B.S., Manogaran, G., Hamdi, M.: Multi-tier stack of block chain with proxy re-encryption method scheme on the internet of things platform. ACM Trans. Internet Technol. (TOIT) **22**(2), 1–20 (2021)
16. Chen, Y., Hu, B., Yu, H., Duan, Z., Huang, J.: A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain. Electronics **10**(19), 2359 (2021)
17. Wang, Z., Guan, S.: A blockchain-based traceable and secure data-sharing scheme. PeerJ Comput. Sci. **9**, e1337 (2023)
18. Zhang, Y., Zheng, D., Deng, R.H.: Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J. **5**(3), 2130–2145 (2018)
19. Nayudu, P.P., Sekhar, K.R.: Dynamic time, and location information in ciphertext-policy attribute-based encryption with multi-authorization. Intell. Autom. Soft Comput. **35**(3), 3801–3813 (2023)