

# A Blockchain-Based Delegatable Re-Enciphering Mechanism for Trusted Information Exchange in the Web of Things

Syed Arshad Moinuddin<sup>1</sup> Md Ateeq Ur Rahman<sup>2</sup> Mohammed Mohammed Sirajuddin<sup>3</sup>

<sup>1</sup> Research Scholar, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

<sup>2</sup> Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

<sup>3</sup> Professor, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

**Abstract** - The advancement of the Web of Things has seen information sharing as perhaps of its most helpful application in distributed computing. As eye-getting as this innovation has been, information security stays one of the impediments it faces since the illegitimate utilization of information prompts a few harms. In this article, we propose an intermediary re-encryption way to deal with secure information partaking in cloud conditions. Information proprietors can re-appropriate their scrambled information to the cloud utilizing character based encryption, while intermediary re-encryption development will give genuine clients admittance to the information. With the Web of Things gadgets being asset compelled, an edge gadget goes about as an intermediary server to deal with escalated calculations. Likewise, we utilize the elements of data driven systems administration to convey reserved content in the intermediary actually, subsequently working on the nature of administration and genuinely taking advantage of the organization transfer speed. Further, our framework model depends on blockchain, a problematic innovation that empowers decentralization in information sharing. It mitigates the bottlenecks in concentrated

frameworks and accomplishes fine-grained admittance control to information. The security examination and assessment of our plan show the commitment of our methodology in guaranteeing information classification, respectability, and security. We propose division and replication of data in the cloud for ideal execution and security that in general approaches the security and execution issues. In this procedure, we segment a record into segments, and reproduce the isolated data over the cloud center points. All of the centers stores simply a singular part of a particular data record that ensures that regardless of whether there ought to emerge an event of a successful attack, no significant information is uncovered to the attacker. Likewise, the centers taking care of the pieces are detached with specific division.

**Index Terms** — Access control, blockchain, data security, identitybased proxy re-encryption, information-centric network (ICN), Internet of Things (IoT).

## I. INTRODUCTION

The Web of Things (IoT) had evolved as a platform with a significant current-day application, and its adoption has resulted in a

sustained increase in network traffic levels over time. In the next years, many more gadgets are anticipated to become linked. Data performs a variety of functions in applications like Medical, mobile Adhoc networks, green infrastructure, enterprises, and manufacturing, among others, making it a key concept in the IoT paradigm [1]. For all parties concerned, the sensor detects a wide range of characteristics that are highly helpful. So, despite how alluring the Internet of Things may appear, it has created new security and privacy issues. In addition to risks to the authenticity, reliability, and confidentiality of data, IoT must be protected from assaults that prevent this from delivering the required services. Encrypting all data prior to outsourcing to cloud servers is a workable method. Only when conventional security measures are ineffective may attackers see the information in its encrypted form. Any information that is shared must be encrypted at the origin and only be decoded by authorized individuals in order to maintain its security. The decryption key can be shared by all the data users chosen by the data owner when using conventional encryption techniques. The adoption of symmetric encryption means that the data owner and users share the same key, or at the very least that the parties have decided on a key. This answer is quite ineffective. The encrypted data must first be decrypted with a key that is known both to the cloud data provider and the consumers since the data providers do not always know who the targeted data users are. The data owner would need to remain online constantly with this decrypt-and-encrypt approach, which is virtually impossible. When there are several data sets and various data owners and consumers, the issue gets more complicated. Although straightforward, standard encryption techniques need intricate key management methods and are therefore inappropriate for data sharing. Blaze et al. [2] initially presented the idea of proxy re-encryption (PRE), which enables a proxy to convert a file calculated using a delegator's digital certificate into an encrypted meant for a delegate. Let the user of the data by the delegate and the owner of the data by the delegator. In such a plan, the data owner is able to give the user temporary encrypted messages without

disclosing his secret key. The re-encryption key is created by the data owner or a reliable third party. Before providing the updated ciphertext to the user, a proxy executes the re-encryption algorithm using the key. Because it is unaware of the data owner's secret key, the proxy in a PRE scheme cannot be entirely trusted. This is viewed as the best option for securely granting others access to encrypted data, which is essential in any scenario involving data sharing. Additionally, PRE enables the sharing of encrypted cloud data with authorized users while protecting its privacy from unauthorized individuals. Since only users authorized by the data owner may successfully access the outsourced data, data disclosures can be reduced by the use of encryption. In response to this scenario, the author of this paper suggests integrating PRE with personality cryptography (IBE), information-centric networking (ICN), and blockchain-based technique to improve IoT data exchange.

The idea of ICN [8]–[11], where data providers may distribute and provide unique identities to their data so that it can be duplicated and kept in network caches [12], [13], was first presented in response to the need for low-latency applications. This guarantees effective data transmission and network bandwidth utilization, which are requirements for the IoT ecosystem despite the phenomenal surge in network traffic. Regarding trust, Nakamoto [14] proposed a decentralized, distributed architecture that can provide secure and trustworthy data sharing. This refers to blockchain technology, which has attracted a lot of interest since it can protect data privacy. However, new system applications have exploited the blockchain for access control, despite optimization problems when storing enormous amounts of data. Blockchain technology can also be used to achieve user revocation and data confidentiality. Data-sharing systems' security and privacy will be improved by PRE, IBE, ICN's features, and blockchain technology. PRE and IBE will ensure fine-grained data access control, however, the idea of ICN offers a suitable quality of service in data delivery since the in-network caching makes data distribution more effective. The blockchain is tailored to avoid storage and data-sharing

overheads and to provide a trustworthy network between businesses. In our essay, the owner of the data disseminates an access control list that is kept on a blockchain. Access to the data is restricted to authorized users only. The accomplishments of this project are outlined in the sections below.

- 1) To ensure data security and quite well access to data, we offer a secure user access architecture. Additionally, this will ensure that data owners have total control over their information.
- 2) We provide a thorough explanation of our PRE system and the implementation of a comprehensive protocol that ensures data security and privacy.
- 3) Edge devices act as proxy nodes and re-encrypt the cached data to enhance data delivery and efficiently use the network bandwidth. In order to provide high-performance networking, it is expected that the edge devices have more computational power than the IoT devices.
- 4) We show our scheme's security analysis and test it against other schemes to see how well it performs.

## II. SYSTEM ANALYSIS

### Objective:

Although straightforward, standard encryption techniques need intricate key management methods and are therefore inappropriate for data sharing. The idea of proxy re-encryption (PRE), which was initially put out by, enables a proxy to convert a file encrypted for a delegate into one calculated under a delegator's public key. Let the user of the data by the delegate and the owner of the data by the delegator. In such a plan, the data owner is able to give the user temporary encrypted communications without disclosing his secret key. The re-encryption key is created by the data owner or a reliable third party. Before providing the updated ciphertext to the user, a proxy executes the re-encryption algorithm using the key. Because it is unaware of the data owner's secret key, the proxy in a PRE scheme cannot be entirely trusted. This is viewed as the best option for securely granting others access to encrypted

data, which is essential in any scenario involving data sharing. Additionally, PRE enables the sharing of encrypted cloud data with authorized users while protecting its privacy from unauthorized individuals.

### EXISTING SYSTEM

There are essentially two types of distributed data integrity checking techniques. The deterministic guarantee-based systems that check each block of data need a lot of storage and processing power. Data access control possession (DACP) is a different class of methods that uses a probabilistic verification mechanism in which a small sample of blocks is randomly chosen to look for tampering. DACP, which uses sampling technique of just a few units for integrity checking, is introduced in [8].

### Drawbacks of Existing System

- Due to a lack of verification, outsourced data is less secure.
- The access to data is no longer secure.

### PROPOSED SYSTEM

PRE method based on blockchain for data sharing. The smart objects and the blockchain are the extra elements to the data-sharing architecture mentioned in Fig. 1. The edge devices act as proxy nodes and give the authorised user access to re-encryption services (s). The edge devices deliver high reliability and performance services to consumers whenever the data is retained at the network's edge. They get the re-encryption token from the owner of the data, get the encrypted message from the CSP, and change the ciphertext to reveal the user's identity. It is a trustworthy yet inquisitive creature. The trustworthy authority (TA) that starts the system parameters is the blockchain. Additionally, the TA offers private keys that are linked to the identities of the users. Utilizing this distributed ledger improves the security and privacy of data by achieving authenticity, transparency, and verifiability inside the network. Owners of data can properly manage their data as a result. The user and/or owners of the data are registered by the

blockchain network and given membership keys (s). The owner creates a re-encryption key using the user's identity and transmits it to the proxy server whenever a user wants access to data. The blockchain network receives instantiated access permissions and data usage guidelines. Before access is provided, a data user is validated.

#### **Advantages of Proposed System:**

- Fully outsourced cipher-text policy attribute based proxy re-encryption.
- To achieve data sharing, various server-based access control mechanisms have been proposed where a trusted access control server is employed to act as a supervisor.
- The Data Security is been improvised due to Data integrity check.

### **III. PROPOSED MODULAR IMPLEMENTATION**

#### **The Algorithm/ Technique used:**

Applications of the technology mentioned in this article in terms of cloud access control and data sharing.

- Access Control Schemes for ICN
- Identity-Based Proxy Re-Encryption
- Blockchain-Based Access Control and Data Sharing
- PRE Data Sharing; Security Model

Below is the proposed modular implementation of the project. It consists of five modules:

- **Data Owner Module**

The information owner transmits their information to the cloud server in this module. The information owner encrypts

the squares of the information record for security purposes before storing it in the cloud. The owner of the information may review a copy of the squares on the document. matching cloud server. The owner of the data may be able to regulate the squares of the encoded information record, as well as to check the cloud information for replication of the specific document's squares and to create remote clients for registered cloud servers. The information owner also verifies the veracity of the proof on which the aggressor has changed the square.

- **Cloud Server Module**

The cloud specialist cooperative uses a cloud to provide information archiving management. Squares from information documents are encoded by information owners and stored in the cloud for distribution to remote users. Information buyers download encoded information record's squares of their choice from the cloud, then decode them to access the mutual information document's squares.

- **End User**

The remote client enters his client name and secret key to sign in to this module. After that, he will request the discharge key for the squares of the necessary document from cloud servers and obtain the emit key. After receiving the emit key, he is attempting to download the squares from the document by inputting the squares' name and the discharge key from the cloud server.



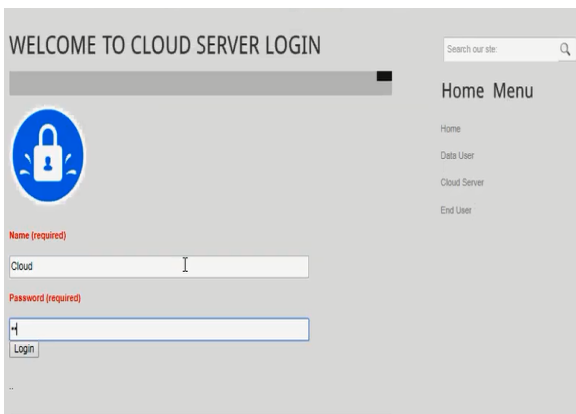
• **Data Encryption and Decryption**


All of the system's legitimate clients are free to inquire about any intriguing decrypted information. The client uses the mystery keys from different Users to conduct the unscrambling calculation Decrypt after receiving the data from the server in order to decode the figure message. Only if the client's attributes match the entrance structure detailed in the figure content CT can the client obtain the substance key.

• **Attacker Module**

The client who assaults or adjusts the square substance called assailant. The aggressor may the client who attempts to get to the document substance by wrong mystery key from the cloud server.

**IV. PROJECT EXECUTION**





### View All Data Fragmentations !!!

File Name	Owner Name	MAC-1	MAC-2
OwnerFragments.jpg	Robiuh	60a1744969577b9c30634d9bdf8c54a2b66a90	2a8838bc45e1009499e1768dce5d
Android.txt	Robiuh	-780bd2e20908ed5e1f31aae01708029088a13a	-1378732e4196e72ee042c8d14dc76ca7a1
BloodBank.txt	Robiuh	757f0ab533d6c4098c82845c415ef1284446a211	139d68892ba17704844139191a94c
Google_Map.txt	Robiuh	7a3210564f2883d1ea8a47579a161650f721411	108e785f71c138427a6de49394772

Back



### View All Data Replication Details !!!

File Name	Owner Name	MAC-1	MAC-2
Android1.txt	Robiuh	-780bd2e20908ed5e1f31aae01708029088a13a	-1378732e4196e72ee042c8d14dc76ca7a1


Back



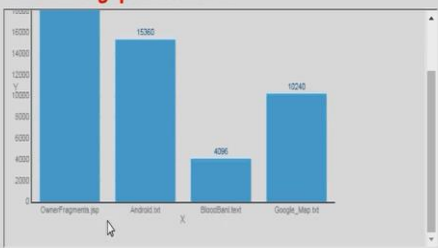
### View All File Requests !!!

EndUser Name	File Request	Req Date Time	Processed Status
Mohan	Android.txt		Response

Back



### View Throughput Results !!!




Back



### View All Transactions !!!

ID	User	File Name	St	Task	Date and Time
1	Robiuh	OwnerFragments.jpg	(B@154097)	Upload	
2	Robiuh	Android.txt	(B@154444)	Upload	
3	Robiuh	BloodBank.txt	(B@10c4c9)	Upload	
4	Robiuh	Google_Map.txt	(B@132c45)	Upload	
5	Mohan	Android.txt	(B@154444)	Download	

Back



### Upload Your Data Fragments !!!

Select File :-	Choose File   SocialNetwork.txt
File Name :-	OSN.txt
	<p>A social network is a social structure made up of a set of social actors (such as individuals or organizations), sets of dyadic ties, and other social interactions between actors. The social network perspective provides a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures.[1] The study of these structures uses social network analysis to identify local and global patterns, locate influential entities, and examine network dynamics.</p> <p>Social networks and the analysis of them is an inherently interdisciplinary academic field which emerged from social psychology, sociology,</p>
MAC1 :-	
MAC2 :-	
MAC3 :-	
MAC4 :-	
	Encrypt

Owner Main Menu

Home

Logout



## CONCLUSION

Data sharing has become one of the IoT's most well-known uses as a result of its development. In a cloud computing context, we provide a secure identity-based PRE data-sharing mechanism to ensure data confidentiality, integrity, and privacy. The IBPRE technology enables secure data sharing and enables data owners to effectively share their encrypted data with authorised users while storing it in the cloud. An edge device acts as a proxy to manage the intense calculations due to resource limitations. The plan also makes advantage of ICN's capabilities to effectively serve cached material, enhancing service quality and optimising network capacity. Then, we describe a system paradigm built on a blockchain that enables flexible permission for encrypted data. It is possible to implement fine-grained access control, which can effectively assist data owners in preserving privacy. The analysis and outcomes of the suggested model demonstrate how effective our plan is when compared to other plans.

### Future Improvement:

Software that fulfils every user demand cannot be created. However, this system has some room for improvement in the future, including: Will focus on the creation of better PRE schemes that operate in distributed environments.

## REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tut.*, vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.
- [2] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, May 1998, pp. 127–144.
- [3] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, Springer, Aug. 1984, pp. 47–53.
- [4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, May 2004, pp. 506–522.
- [5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in *NDSS*, vol. 4. Citeseer, Feb. 2004, pp. 5–6.
- [6] D. Balfanz *et al.*, "Secret handshakes from pairing-based key agreements," in *Proc. IEEE, Symp. Secur. Privacy*, 2003, pp. 180–196.
- [7] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, 2004, pp. 207–222.
- [8] T. Koponen *et al.*, "A data-oriented (and beyond) network architecture," in *Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun.*, Aug. 2007, pp. 181–192.
- [9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to pursuit," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.*, Springer, Oct. 2010, pp. 1–13.
- [10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in *Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops*, 2010, pp. 1–6.