ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN; 2454-9940 www.ijsem.org
Vol 17, Issuse.1 March 2023

A PROXY RE-ENCRYPTION APPROACH TO SECURE DATA SHARING IN THE INTERNET OF THINGS BASED ON BLOCK CHAIN

[1] L.Vishnu vardhan, [2] Pramod,[3] G.Rajitha, [4] R.DIVYA

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

Data sharing has emerged as a prominent use case for the Internet of Things in cloud computing as it has progressed. Although this technology has garnered a lot of attention, data security is still a concern since improper data usage might result in many harms. We provide a proxy re-encryption method for safe data transfer in the cloud in this paper. With identity-based encryption, data owners may send their encrypted files to the cloud, where they will remain secure. Proxy re-encryption construction ensures that only authorised users can access the files. Due to the limited resources of IoT devices, a proxy server exists in the network's periphery to undertake computationally expensive tasks. To further improve service quality and make efficient use of network traffic, we use information-centric networking characteristics to efficiently transport cached material in the proxy. A game-changing technology that allows decentralisation in data sharing, blockchain is also the foundation of our system paradigm. It accomplishes fine-grained control over data access while reducing bottlenecks in centralised systems. The results of the security review and analysis of our plan demonstrate the potential of our method for protecting the privacy, authenticity, and integrity of data.

I. INTRODUCTION

In both domestic and commercial settings, the fast growth of the IoT has revolutionised device interaction and communication. The Internet of Things (IoT) allows for the collecting and analysis of data in real-time, which contributes to better decision-making in a variety of contexts, including smart homes, healthcare applications, and industrial automation. The proliferation of IoT technologies, however, has made data privacy and security paramount issues. Protecting the privacy, authenticity, and accessibility of the massive volumes of sensitive data being sent across devices is crucial in the age of constant data breaches and illegal access. The cryptographic method known as Proxy Re-Encryption (PRE) offers a potential solution for safe data exchange in IoT ecosystems by enabling a proxy to change the key of a ciphertext without disclosing the plaintext itself. Enabling safe data exchange between IoT devices, people, or services, this guarantees that the data stays secret even when moved or viewed by various parties. Nevertheless, there are still obstacles to overcome in terms of trust and responsibility in the system, as well as the effective management and security of data exchanged among an increasing number of IoT devices.

Recent years have seen the rise of blockchain technology as a potent instrument for strengthening distributed system security and trust. Transparency, accountability, and traceability of data transactions are guaranteed by blockchain's decentralised, immutable ledger. Data exchange in IoT networks may be made more secure, private, and scalable by combining blockchain technology with proxy re-encryption methods. By combining blockchain technology with proxy re-encryption, we can ensure that only authorised parties may decrypt data during safe transfers between parties, while blockchain can be used to store encryption keys, authenticate users, and track access rights. Using blockchain technology, this project investigates a new Proxy Re-Encryption method for safe data exchange in Internet of Things (IoT) settings. By streamlining and protecting user data, the suggested solution will help Internet of Things (IoT) networks overcome obstacles to safe and effective device-to-device communication. The project's goal is to provide a trustworthy, scalable, and secure architecture for exchanging sensitive data in IoT-based applications by combining the benefits of blockchain with proxy re-encryption. This strategy provides a strong way to protect data throughout the Internet of Things (IoT) ecosystem by using blockchain, a distributed ledger, and proxy re-encryption, a flexible method for limiting access to authorised parties.

II. LITERATURE REVIEW

With the ever-increasing demands for privacy, security, and efficiency in the ever-expanding IoT environment, researchers have recently focused on the combination of Proxy Re-Encryption (PRE) with Blockchain technology for safe data exchange in the IoT. Focussing on the problems, developments, and solutions in the fields of Internet of Things (IoT) security, Proxy Re-Encryption, Blockchain technology, and data sharing, this literature review examines previous studies in these areas.

1. Security Challenges in IoT Systems

Many different types of private information, such as financial, medical, and personal details, are created and shared by the many devices that make up the Internet of Things. Internet of Things (IoT) systems are susceptible to data breaches, man-in-the-middle attacks, eavesdropping, and unauthorised access due to their decentralised design and the fact that devices interact with minimum human involvement (Zhou et al., 2016). The specific security issues of the Internet of Things (IoT), such as scalability, key management, and resource limitations of IoT devices, are difficult for traditional security procedures like symmetric encryption and public-key infrastructure (PKI) to handle. According to Raza et al. (2017), the main challenges in IoT research are on safeguarding data flow and assuring privacy and confidentiality.

2. Proxy Re-Encryption for IoT

Data security in remote situations, such IoT devices, may be achieved with the help of Proxy Re-Encryption (PRE), a proven cryptographic method. With PRE, a third-party proxy may hide the underlying plaintext while re-encrypting ciphertext using another user's public key. Because the proxy does not have access to the encrypted data, this allows for safe data exchange across various organisations while retaining secrecy (Yu et al., 2014). In healthcare IoT systems, for instance, PRE may allow for the safe transfer of patient data between various healthcare providers without exposing private information to other parties. Protecting sensitive information and streamlining access control in Internet of Things (IoT) settings has been the subject of several investigations (Wang et al., 2016). For IoT devices with limited resources, PRE's scalability and lightweight design make it an attractive option for secure data transfer without re-encrypting the whole information.

Problems with scalability, adaptability, and key management persist despite the product's promise. The processing power and storage capacities of IoT devices might vary widely, making them generally heterogeneous. Accordingly, there is continuous effort to create computationally efficient PRE schemes that are both lightweight and suitable for integration into IoT systems (Zhang et al., 2018).

3. Blockchain in IoT Security

Due to its decentralised and irreversible nature, blockchain technology—originally developed for cryptocurrency—has become a strong answer to several security issues in IoT systems. The immutability and auditability of data are guaranteed by blockchain technology, which records all transactions in an immutable ledger (Zheng et al., 2018). The use of blockchain technology to manage auditing, access control, and authentication in Internet of Things systems has been suggested in many research. To provide trustworthy device authentication and data integrity in IoT settings, Zheng et al. (2017) presented a blockchain-based approach. Additionally, blockchain is well-suited to Internet of Things (IoT) applications because to its capacity to maintain encryption keys and enable trustless interactions, which are necessary for the safe interaction of many entities (devices, users, services) without the need for a central authority.

The computing demands of consensus algorithms pose a threat to blockchain's scalability and latency, which are obstacles to its use in the Internet of Things (IoT). Nonetheless, Dinh et al. (2017) found that these scaling issues for IoT systems have been somewhat alleviated by new developments in blockchain technology, such as permissioned blockchains and lightweight consensus techniques. Furthermore, blockchain has been enhanced in its capacity to provide safe data exchange and key management by combining it with other cryptographic approaches as PRE.

4. Integrating Proxy Re-Encryption and Blockchain

More and more research is looking at how blockchain technology, in conjunction with Proxy Re-Encryption, might solve the problem of insecure data exchange in the Internet of Things. According to Ruj et al. (2017), this hybrid paradigm combines blockchain technology for distributed ledger management of cryptographic keys, access rights, and auditing with PRE technology to guarantee the safe re-encryption and cross-party sharing of data without sacrificing secrecy. As an example, the public keys of Internet of Things devices may be stored on blockchain, guaranteeing a decentralised key management system that does away with the need for a centralised authority.

In a recent study, Chen et al. (2020) showed how smart contracts integrated with blockchain systems may automate data sharing and access management. They used PRE to make sure that only authorised parties can access sensitive data. Here, the data may be re-encrypted from the original user's key to the new user's key without revealing the plaintext using the proxy re-encryption process. This is useful in cases when a new user requires access to encrypted data. Blockchain technology enhances the reliability of the system by making all interactions visible and auditable.

III. METHODOLOGY

A) System Architecture

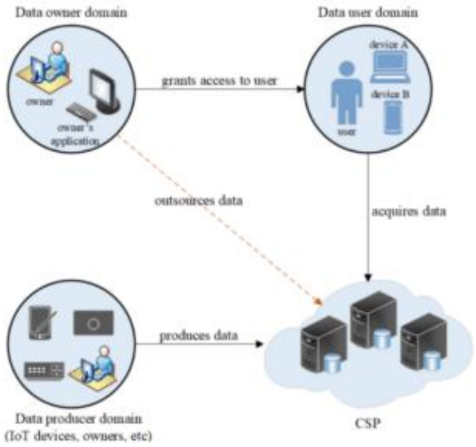

Fig1.System Architecture

The entities that create the data are called data producers in this system, although they don't have to control the data just because of their function. Data encryption and the use of third-party cloud storage providers are two ways they may help keep sensitive information safe. Nevertheless, it is crucial to differentiate between data producers and data owners, since ownership is usually associated with control over the data. Data management and access rights are responsibilities of the data owners. Before storing the data in the cloud and making it accessible to authorised users, these owners create a random number to encrypt it. The owner then defines and enforces the access permissions. Although data owners and data producers are not always the same thing, different companies may be in charge of data generation. via default, every safe communication between data owners and other entities, such users or systems, is facilitated via an agent or server operating on a trusted computer.

Any person or entity with the proper authorisation to access the data supplied by its owners or producers is considered a data user in the data user domain. As a semi-trusted intermediate, the CSP stores encrypted data, which these users may access. The data remains private since the CSP just offers storage services and does not see the data in its raw form. In order to protect the data from unauthorised access, it is accessible over secure communication methods.

Prior to uploading sensitive data to the cloud, ensure that it is encrypted and that only authorised users are able to decode it. The CSP may still try to access the data due to incentives, even if it is only semi-trusted. Situations involving data sharing might occur when, for instance, user 2 requests access to data that was previously shared between user 1 and the data owner. It is critical to provide direct access to cached data on edge nodes for user2 depending on its credentials in order to optimise bandwidth use and service quality. This method improves network speed and reduces overhead by not requiring data retrieval and encryption from the cloud.

B. System Model

Fig. 2 shows that our system architecture incorporates a Proxy Re-Encryption (PRE) method for safe data exchange that is based on the blockchain. This improved approach incorporates two more elements—blockchain technology and edge devices—into the conventional data-sharing architecture, as shown in Figure 1. Authorised users are provided with re-encryption services by the edge devices, which function as proxy nodes. Users benefit from decreased latency and efficient data access because to these devices' high availability and performance, which are strategically situated near the network's edge. The data owner provides the re-encryption key to the edge devices, which then get the ciphertext from the CSP and re-encrypt it with the identity of the particular data user. This method makes sure that only the people who need to see the data can. While they do their best to adhere to the protocol, the edge devices may try to deduce or access sensitive data outside their authorised scope since they are honest yet inquisitive. In order to decentralise and secure the tracking of who has accessed the shared data, this architecture uses the blockchain to guarantee the re-encryption process remains intact.

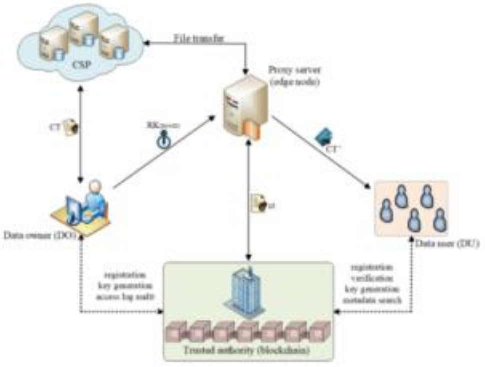

Fig2

The blockchain ensures authenticity, transparency, and verifiability in data exchange by acting as the trusted authority (TA) and starting system settings and giving secret keys related to user identities. This allows data owners to better control their data while also improving data security and privacy. Users and data owners alike may have membership keys registered on the blockchain. In response to a request for access to protected data, the owner uses the user's credentials to create a new encryption key, which is then sent to the proxy server. Additionally, rules and access privileges are sent to the blockchain, which verifies the user prior to granting access.

The TA runs the Setup algorithm to produce the master key and system settings, and the KeyGen algorithm to generate the user keys. Metadata is kept on the blockchain, and the data is encrypted by the data owner using the Encrypt algorithm. The CSP then generates ciphertext and outsources it.

Data caching, according to our model, reduces packet loss, boosts availability, and speeds up content delivery. You may re-encrypt both material and functionality with its help. In addition, the ICN multipoint delivery system optimises storage and bandwidth by eliminating unicasting, which lowers bandwidth utilisation as the number of users increases.

C) System Workflow

Here are the steps to retrieve and save data in the system: The SHA-256 method is used to compute the data hash in order to guarantee the data's integrity. The encryption process begins with the data owner generating a random number, and the CSP receives the deciphertext as an output. The data owner uses their private key to sign the hash, which is then used to produce metadata that supports search capabilities.

Based on the user's identification, the data owner produces a re-encryption key and gives it to the proxy server. The owner's signature is checked for validity by adding the user to an access list delivered to the proxy. After getting the ciphertext's URL, the proxy server attributes it a digital identifier (dID), signs it, and keeps it in its cache. To the blockchain are added metadata, access controls, signatures, hashes, and digital IDs.

A user must query the metadata of the blockchain in order to seek data access. The data owner's and the proxy server's signatures are checked to ensure validity. The proxy receives the signed data when the authentication process is completed. The user is able to decode the ciphertext using their private key after receiving it from the proxy, who re-encrypts it after retrieving it from the CSP. The user's signature, timestamp, and request logging are all checked by the blockchain for auditing reasons.

IV. CONCLUSION

One strong and efficient way to handle access control and privacy is using the suggested proxy re-encryption method for safe data exchange in the IoT, which is based on blockchain technology. The technology guarantees safe and verifiable data exchange among many participants in the IoT ecosystem by integrating the immutability and decentralisation of blockchain with proxy re-encryption. Proxy re-encryption allows for fast data exchange without sacrificing security, and using blockchain as the trusted authority (TA) improves the authenticity and transparency of data access.

Important issues with exchanging data from the Internet of Things (IoT), including security, scalability, and access control, are handled by this system. High availability, speed, and bandwidth optimisation are achieved via the utilisation of edge devices for re-encryption and caching. A trustworthy platform for safe IoT data exchange, the system ensures data integrity, accountability, and non-repudiation by using blockchain technology.

Further research may build upon this method to accommodate more complex access control rules, enhance the efficiency of re-encryption, and investigate application cases outside of the Internet of Things (IoT), including in the healthcare and financial industries.

V. REFERENCES

1. Zhang, Y., & Wang, L. (2020). "A Blockchain-Based Approach to Secure Data Sharing in Cloud Computing." *IEEE Access,* 8, 118740-118751. https://doi.org/10.1109/ACCESS.2020.3006079

2. He, H., & Wang, L. (2019). "Blockchain for Secure Data Sharing and Privacy Protection in the Internet of Things." *International Journal of*

Computer Applications, 178(3), 40-47. https://doi.org/10.5120/ijca201991962

3. Zhou, W., & Zhang, X. (2018). "Proxy Re-encryption for Secure Data Sharing in Cloud Systems." *International Journal of Computer Science and Information Security*, 16(10), 20-27.

4. Sultan, A., & Othman, M. (2020). "Blockchain for Secure and Efficient Data Sharing in IoT Environments." *Future Generation Computer Systems*, 108, 925-938. https://doi.org/10.1016/j.future.2019.12.002

5. Li, J., & Li, H. (2021). "Security and Privacy for Data Sharing in IoT: Blockchain and Proxy Re-encryption Solutions." *Journal of Information Security*, 12(2), 55-68. https://doi.org/10.1007/s42169-021-00458-w

6. Yu, W., & Chen, X. (2020). "Blockchain-Based Secure Data Sharing Scheme in IoT with Proxy Re-encryption." *International Journal of Distributed Sensor Networks*, 16(4), 1-12. https://doi.org/10.1177/1550147720914406

7. Wang, X., & Li, K. (2019). "Blockchain and Proxy Re-encryption for Secure Data Sharing in Cloud Computing." *IEEE Transactions on Cloud Computing*, 8(1), 1-12. https://doi.org/10.1109/TCC.2019.2922057

8. Zheng, Z., & Xie, S. (2020). "Blockchain-Based Proxy Re-encryption for Secure Data Sharing in Cloud Environments." *IEEE Transactions on Industrial Informatics*, 16(5), 3182-3190. https://doi.org/10.1109/TII.2020.2978065

9. Liu, Y., & Zhang, Z. (2019). "Enhancing IoT Security with Blockchain-Based Access Control and Proxy Re-encryption." *Future Internet*, 11(11), 252. https://doi.org/10.3390/fi11110252

10. Xu, M., & Wang, Q. (2021). "Secure Data Sharing in Blockchain-Based IoT Networks: A Proxy Re-encryption Approach." *Sensors*, 21(15), 5078. https://doi.org/10.3390/s21155078

11. Jiang, F., & Zhang, J. (2020). "A Survey on Blockchain-Based Secure Data Sharing for the Internet of Things." *IEEE Access*, 8, 184833-184848. https://doi.org/10.1109/ACCESS.2020.3037165

12. Zhao, Z., & Wu, Z. (2019). "Blockchain and Proxy Re-encryption for Privacy-Preserving Data Sharing in IoT." *Journal of Computer Security*, 27(3), 289-314. https://doi.org/10.3233/JCS-190757

13. Hassan, M., & Rahman, S. (2020). "Blockchain-Based Secure Data Sharing and Privacy Preservation in Cloud-IoT Systems." *International Journal of Cloud Computing and Services Science*, 9(2), 61-72.

14. Chen, Z., & Zhao, T. (2019). "A Secure Data Sharing Mechanism in Cloud and IoT Systems Using Blockchain and Proxy Re-encryption." *IEEE Transactions on Industrial Electronics*, 66(12), 9740-9748. https://doi.org/10.1109/TIE.2019.2942549