International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 08 Special Issue 01 | 2023

Secure Data Sharing In Iot Based On Blockchain Technology

Tejas S. Naphade[1], Tejas R. Mukund[2], Rushikesh P. Suralkar[3], Rahul C. Junare[4], Sudesh L. Farpat[5]

[1,2,3,4] Student, Computer Science and Engineering, VBKCOE, Malkapur, Maharashtra, India
[5] Assistant Professor, Computer Science and Engineering, VBKCOE, Malkapur, Maharashtra, India

ABSTRACT

The development of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. Despite the obviousness of this technology, data security remains one of the obstacles facing, as misuse of data can lead to significant losses. In this paper, we propose a proxy re-encryption method to secure data sharing in cloud environments. Data owners can use identity-based encryption to outsource their encrypted data to the cloud, while proxy encryption structures allow legitimate users to access the data. Because IoT devices have limited resources, high-end hardware acts as a proxy server to handle compute-intensive operations. We also use message-centric network functions to efficiently deliver cached content to proxy servers, improve quality of service, and maximize network bandwidth. In addition, our system model is based on blockchain, which is the disruptive technology that enables decentralized data sharing. It alleviates bottlenecks in centralized systems and allows granular control of access to data. Our analysis and security assessment of Blueprint shows promise in our approach to data confidentiality, integrity and security.

Keyword: *- Access Control, blockchain, data security, proxy re-encryption, IOT*

1. INTRODUCTION

Access Control, blockchain, data security, proxy re-encryption, IOT The Internet of Things (IoT) has become a very important technology in today's world, and its development has led to the growth of network traffic over the years. It is expected that, units will be delivered in the coming years. Data is a central concept of the IoT paradigm, as collected data has multiple uses in applications such as healthcare, automotive networking, smart cities, industry, and manufacturing. Sensors measure a large number of parameters that are very useful for factors. So, as tempting as the Internet of Things may seem, its developments pose new challenges for security and privacy. In addition to attacks that threaten the confidentiality, integrity and confidentiality of data, the Internet of Things must also be protected from attacks that prevent it from providing essential services [1].

A viable solution is to encrypt the data before outsourcing it to cloud servers, and when traditional security measures fail, attackers can only see the data in encrypted form. When sharing data, all information must be encrypted at source and only authorized users can decrypt it to keep it secure. may use traditional encryption techniques, whereby the decryption key is shared between all data users designated by the owner or data and users or at least participants who accept the key. This solution is very ineffective [1]. Also, the data owner does not know in advance who the intended data user is, so encrypted data must be decrypted and then encrypted with a key known to both the owner and the user. This encryption and decryption solution mean that the owner of the data must be online at all times, which is practically impossible with. When there is multiple data and the owners and users of the data are different, the problem will get more complicated. PRE, along with IBE and ICN and blockchain capabilities, will improve the security and privacy of the data exchange system. PRE and IBE guarantee fine-grained control over data access, while the ICN concept promises an adequate quality of service in data delivery. This is because caching in the network enables efficient distribution of data. Blockchain is optimized to avoid the overhead of storage and data sharing and to ensure a system of trust between entities in the network. In this article [1], a data owner propagates the access

control list stored on her blockchain. Only authorized users can access her data. The contributions of this article are summarized as follows: 1) We propose a secure access control framework to ensure data confidentiality and enable granular access to data. This gives data owners full control over their data. 2) Provide a detailed description of the PRE-scheme and updates to the complete protocol that guarantees data security and confidentiality. 3) To improve data delivery and use network bandwidth effectively, edge devices act as proxy nodes and perform re-encryption of cached data. Edge devices are assumed to have more computing power than IoT devices, thus providing high performance networks. 4) A security analysis of our scheme is presented, its performance tested and compared with existing schemes.

2. RELATED WORK

2.1 Pre-Data Sharing

There is a wide variety of research on IoT security and privacy, most of which is devoted to understanding and identifying these threats. Additionally, the use of blockchain to secure various IoT platforms has also been discussed. IoT devices capture, collect, and share massive amounts of data, raising significant security and privacy concerns. In their article, Khan and Salah [5] explored various IoT security challenges and identified insecure transmission of IoT data as a high-level security risk. The authors demonstrated a basic lack of security by hacking smart home IoT devices out of the box. In 1998, Blaze, Bleumer, and Strauss [2] first introduced the concept of proxy rekey and built the first two-way proxy rekey application. The authors [3][4] have proposed a similar scheme, but it is not dynamic and therefore not suitable for cloud data sharing. A highly efficient solution for storing data in the cloud has been proposed using a pair-free proxy re-encryption scheme. However, the plan has not been put into action. The basic structure of the proposed schema is based on this, but includes some important changes, such as including metadata, to ensure practical use of the schema. Most of the previous work partially addresses the issue of secure sharing of IoT data. Developing on-device security that eliminates all security threats to IoT devices is nearly impossible. IoT's limited computing and power resources also make it difficult to run complex security algorithms on the device. We propose to use a combination of blockchain and pairing-free proxy transcoding schemes to provide a trading platform and securely transmit sensor data to users.

2.2 Blockchain-Based Access Control and Data Sharing

Zyskind et al. [6] Blockchain was used to provide decentralized management of personal data and ensure privacy. blockchain was used as an automated access control manager, so no third party was needed. Only data address was stored on the blockchain and a distributed hash table was used as the implementation of data storage. This mitigated the risk of data leaks. However, no specific access control model is proposed in their scheme. Maesa et al. [7] proposed a blockchain-based access control scheme in which a data owner defines his policy for data and stores it on the blockchain. Policies are assigned to users as access rights. Fan et al. [8] designed a model similar to [7] where encrypted data is uploaded to the cloud and access policies for the data are stored on the blockchain as transactions. The blockchain used is public, so access policies can be leaked. Singh and Kim [9] presented a blockchain-based model for sharing data in vehicle networks and enabling secure he communication between vehicles. However, using public blockchains does not work well for peer-to-peer (P2P) data exchange between vehicles due to the high costs associated with setting up public blockchains in resource-constrained vehicles.

2.3 Access Control Schemes for ICN

Several centralized and decentralized access control mechanisms have been proposed in the literature to control content in the ICN framework. Silva and Zorzo [10] presented an access control system for named data networks based on the ABE scheme and proxy servers. Before content is published, data owners encrypt it and generate access policies that bind it. Encrypted data is stored on the closest router and access policies are stored on the server. When a user accesses the content, the user gets the content from the router, gets the access policy from the proxy her server, and then decrypts the data. Their scheme allows user revocation. However, because the proxy server participates in all content access, it presents a single point of failure if the proxy server fails. In al. [11] for access control in ICN he developed a privacy-enhancing scheme that uses ABE and uses trusted third parties to manage attributes. Content publishers generate access policies based on attributes defined by third parties and encrypt data using random symmetric keys. The publisher then hides the random key and access policy in the content name, making it accessible only to authorized users.

3. SYSTEM MODEL

This system model introduces a blockchain-based PRE-approach to data sharing. As illustrated in Figure, additional entities in the data sharing model are the edge device and the blockchain. Edge devices act as proxy nodes and s provide re-encryption services to authorized users. Edge devices provide high availability and high-performance services to users when data is cached at the edge of the network. Obtain the re-encryption key from the data owner, obtain the ciphertext from the CSP, and convert the ciphertext to the identity of the data consumer. It is an honest but curious being.

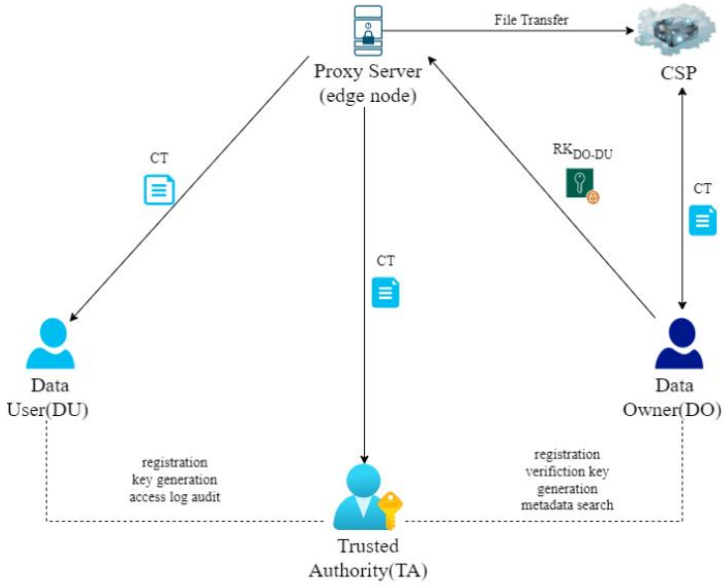

Fig -1: Data sharing system model

Table -1: Notation

Symbol	Meaning
CT	Ciphertext
DO	Data owner
DU	Data user
RK	Re-encryption key
dID	De-encryption ID

Blockchain acts as a Trusted Authority (TA) that initiates system parameters. TA also provides the user her private keys associated with her identity. Using this distributed ledger enables authenticity, transparency, and verifiability within the network, improving data security and confidentiality. Therefore, the data owner can effectively control her data. The blockchain network registers and issues membership keys to data owners and users. When user requests data access, the owner uses the user's identity to generate a re-encryption key and send it to the proxy server. Permissions and guidelines for using data are instantiated and sent to the blockchain network. Data users are validated before access is granted.

TA runs a setup algorithm to generate system parameters and a master key during the system initialization phase. At the same time, use the KeyGen algorithm to create the user's key. The data owner runs the encryption algorithm to create the ciphertext CT. The ciphertext is then offloaded to the CSP and the metadata is stored on the blockchain.

In this model, including a data cache in the transfer process makes content delivery more resilient to packet loss and increases content availability. It supports feature caching (also) as well as content caching (which is encrypted in this case). In addition, ICN's multipoint distribution system ensures efficient use of bandwidth and storage space. As the number of users increases, content is no longer unicast, reducing bandwidth usage.

Regarding storing and retrieving data on the system, the data is hashed using the (SHA − 256) hashing algorithm to ensure data integrity. Data owner generates random numbers used to encrypt data and the resulting ciphertext is uploaded to his CSP. Metadata is created to support search functionality, and the data owner creates a digital signature on the data using private key to sign the hash function.

The data owner generates a re-encryption key based on the user's identity and passes it to the proxy server. User is included in the access list sent to the proxy server. Proxy checks owner's signature for authenticity. After the CT is stored in her CSP, the proxy takes the ciphertext unified resource locator (URL), generates a ID (dID) and assigns it to the URL. The server adds that signature to his dID and caches it on the proxy server. Finally, metadata, access control policies, signatures, hashes and dIDs of both data owners and proxy servers are uploaded to the blockchain.

When a user makes a request for data access, the user queries blockchain metadata. The authenticity of the data is verified by checking the signatures of the data owner and the proxy server. If the authentication succeeds, a timestamp is added and then the signed data is sent to the proxy server with a request for the actual data. The relevant information about the data is obtained from the cache and the relevant ciphertext is also obtained from his CSP. Proxy server performs re-encryption of the ciphertext and the result he sends to user. The user can now decrypt the ciphertext using the private key. Blockchain has previously verified the authenticity of her users based on their signatures. The timestamp is verified and the request is saved on the blockchain for verification.

Blockchain technology is a distributed database that operates in a decentralized and untrustworthy manner. It has gained widespread usage due to its transparency, tamper-resistance, and security features. In the context of the Internet of Things (IoT), blockchain offers a promising solution for data security and privacy issues. However, the combination of IoT and blockchain technology also presents new challenges such as poor scalability, data retrieval efficiency, data mining, and limitations due to blockchain's inherent nature. As a result, data sharing and mining over encrypted data pose significant security and privacy concerns in blockchain-based IoT applications. Therefore, it is essential to develop solutions that can address these challenges and preserve privacy in data sharing and data mining in the IoT context, utilizing blockchain technology.

Possible applications but are not limited to:

- Blockchain-based access control for shared data.
- Public data auditing based on blockchain in IoT.
- Encrypted textual data search.
- Encrypted image search.
- Attacks on searchable encryption schemes.
- Threat model and risk assessment.
- Machine learning algorithms.
- Novel security architectures for data mining.
- Privacy preservation in blockchain-based data mining.
- Defense countermeasures.

4. CONCLUSIONS

The internet of things (IoT) has revolutionized data sharing by making it a crucial application to ensure data confidentiality, integrity, and privacy. To provide secure data sharing in a cloud computing environment, we offer a secure identity-based pre-data exchange system. Our IBPRE technology enables secure data sharing, allowing data owners to store their encrypted data in the cloud and share it efficiently with authorized users. Given the resource limitations of sophisticated hardware, we use proxies to handle computationally intensive operations. Our solution also integrates ICN functionality to skillfully forward cached content, thereby improving the quality of service and maximizing network bandwidth utilization. Additionally, we propose a blockchain-based system model that facilitates flexible delegation of encrypted data and precise access control. This model helps data owners protect their privacy. The efficiency of our scheme is evident in the analysis results and the proposed model, making it more efficient than existing schemes.

5. REFERENCES

[1] Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, and Jianbin Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain", vol. 16, no. 1, march 2022
[2] M. Blaze. G. Bleumer, and M. Strauss. "Divertible protocols and atomic proxy cryptography." in International Conference on the Theory and Applications of Cryptographic Techniques. Springer. 1998. pp. 1277 144.
[3] C.-K. Chu. J. Weng. S. S. Chow. J. Zhou. and R. H. Deng. "Conditional proxy broadcast re-encryption." in Australasian Conference on Information Security and Privacy. Springer. 2009. pp. 3277342.
[4] M. Sun. C. Ge. L. Fang. and J. Wang. "A proxy broadcast re-encryption for cloud data sharing." Multimedia Tools and Applications. vol. 77. no. 9. pp. 10455710469. 2018.
[5] M. A. Khan and K. Salah. "Iot security: Review. blockchain solutions. and open challenges." Future Generation Computer Systems. vol. 82. pp. 395411. 2018.
[6] G. Zyskind et al., "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Secure. Privacy Workshops, May 2015, pp. 180–184.
[7] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in Proc. IFIP Int. Conf. Distributed Appl. Interoperable Syst., Springer, Jun. 2017, pp. 206–220.
[8] K. Fan, Y. Ren, Y.Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.
[9] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," Comput. Netw., vol. 145, pp. 219–231, Nov. 2018.
[10] R. S. Da Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf., Jan. 2015, pp. 128–133.
[11] B. Li, D. Huang, Z.Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," IEEE Trans. Dependable Secure Comput., vol. 15, no. 2, pp. 194–206, Apr. 2016.