IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207101 |

An Approach to Secure Data Sharing in the Internet of Things Using Blockchain-Based Proxy Re-Encryption

Darshan G S[1], Dr. Prabhudeva S[2]

PG Student, Dept. of Master of Computer Applications, Jawaharlal Nehru New College of Engineering, Shivamogga, India[1]

Director and Professor, Dept. of Master of Computer Applications, Jawaharlal Nehru New College of Engineering, Shivamogga, India[2]

ABSTRACT: Data sharing has come one of the most profitable pall computing operations as the Internet of Effects has grown. Indeed, though this technology has a nice look, data security is still one of its challenges because indecorous data operation can have a lot of negative consequences. A deputy re-encryption result for safe data conveyance in pall surrounds is described in this paper. Data possessors can use identity-grounded encryption to outsource translated data to the pall, and authorized druggies can pierce the data via deputy-encryption construction. Due to the confined coffers of Internet of effects bias, an edge device operates as a deputy garcon to perform computationally precious conditioning. Likewise, by employing information-centric networking capabilities, we successfully circulate cached content through the deputy, hence perfecting service quality and effectively utilizing network capacity. It achieves fine-granulated data access control while reducing centralized system backups. As substantiated by the security exploration and plan assessment, our system for maintaining data security, confidentiality, and integrity shows a pledge.

KEYWORDS: deputy re-encryption, deputy garcon, data security, confidentiality

I. INTRODUCTION

With the rapid growth of the Internet of Things (IoT), there is an increasing need for secure data sharing among IoT devices and applications. However, traditional security mechanisms face several challenges in this context, such as scalability, trust, and data integrity. To address these challenges, the integration of blockchain technology and proxy re-encryption can provide a promising solution for secure data sharing in the IoT.

Blockchain Technology:

Blockchain is a decentralized and distributed ledger technology that ensures transparency, immutability, and security in data transactions. It operates on a peer-to-peer network, where multiple participants, or nodes, collectively maintain and validate the block chain's integrity. The use of consensus algorithms ensures that all participants agree on the validity of transactions, making it difficult for malicious actors to tamper with data.

Proxy Re-encryption:

Proxy re-encryption is a cryptographic technique that allows a proxy entity to transform ciphertext encrypted under one key into ciphertext encrypted under a different key without revealing the underlying plaintext. This enables a secure delegation of decryption rights from one party to another, without compromising the confidentiality of the data.

II. RELATED WORK– (LITERATURE SURVEY)

1. S. Yu, et al, [1], PRE and key-policy ABE (KP-ABE) were combined to suggest a mechanism for cloud data sharing. KP-ABE encryption was used to encrypt the data, making decryption feasible only with the right set of attribute secret keys. In addition to managing the encrypted data, the cloud also controlled all attribute secret keys with the exception of one unique secret key for handling user revocation.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207101 |

2. Q. Liu, et al, [2], Also put forth a PRE and ABE-based time-limited access control mechanism Time- based access was designed using ABE.PRE was used to update the time characteristics while controlling policies. Despite these schemes' benefits, their high computational costs for encryption and decryption make them unsuitable for use in the IoT.

3. h.-y. Lin et al [3], address the access control function for a secure networked storage system by proposing a fine-grained access control mechanism. in this mechanism, a user cannot only read or write data but also grant the reading permissions of a single file or a whole directory of files to others with low cost. Moreover, these functions are supported in a confidential way against honest-but-curious storage servers. our technical contribution is to propose a hybrid encryption scheme for a typical structure of a file system by integrating a hierarchical proxy re-encryption scheme and a hierarchical key assignment scheme.

4. Y. Zhou et al, [4], To ensure that only data disseminators whose attributes satisfy access policy can disseminate the data to their own social space, we use attribute-based conditional proxy re-encryption. The dispersed ciphertexts can be subject to fine-grained access controls thanks to the re-encryption key's association with a set of attributes that prevents all except the matching ciphertext from being re-encrypted.

5. G. Zyskind et al, [5], needed because the blockchain was used as an autonomous access control manager. On the blockchain, just the data address was kept, and the mechanism for data storage was a distributed hash table. Thus, there was a lower chance of data leaking. However, their plan included no explicit recommendations for access control models.

III. METHODOLOGY

Due to the decentralized nature of IoT networks and the requirement for strong security procedures, securing data sharing in the IoT is a critical concern. Combining proxy re-encryption and blockchain technology is one way to overcome this problem. Let us investigate this approach:

Blockchain technology: A distributed ledger that is decentralized and offers a safe environment for recording data or transactions. It consists of a chain of blocks, each of which has a list of verified transactions with timestamps. Blockchain's decentralized structure guarantees that no single party has control over the data, making it impervious to manipulation or unlawful changes.

Proxy Re-encryption: A proxy is a person who can change ciphertext from one key to another without knowing the plaintext using the cryptographic technique of proxy re-encryption. This makes it possible for organizations to share data securely without having to directly access the encryption keys.

To secure data sharing in IoT using blockchain-based proxy re-encryption, we can follow these steps:

Step 1: In the IoT data encryption process is for each IoT device to encrypt its data with a special encryption key and a symmetric encryption method like AES (Advanced Encryption Standard). This guarantees that the data is secure and confidential throughout transmission.

Step 2: The blockchain network receives the uploaded, encrypted IoT data. The blockchain stores each data transaction as a block that contains all essential metadata, including the device ID, timestamp, and encrypted data.

Step 3: A recipient requests specific IoT data from the blockchain when they need access to it. The recipient is located via the blockchain network, which also retrieves the corresponding encrypted data.

Step 4: The recipient, who is in possession of the associated private key, can use their decryption key to decrypt the newly encrypted data. This guarantees that the original IoT data may only be accessed by authorized user.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207101 |

DATA FLOW DIAGRAM:

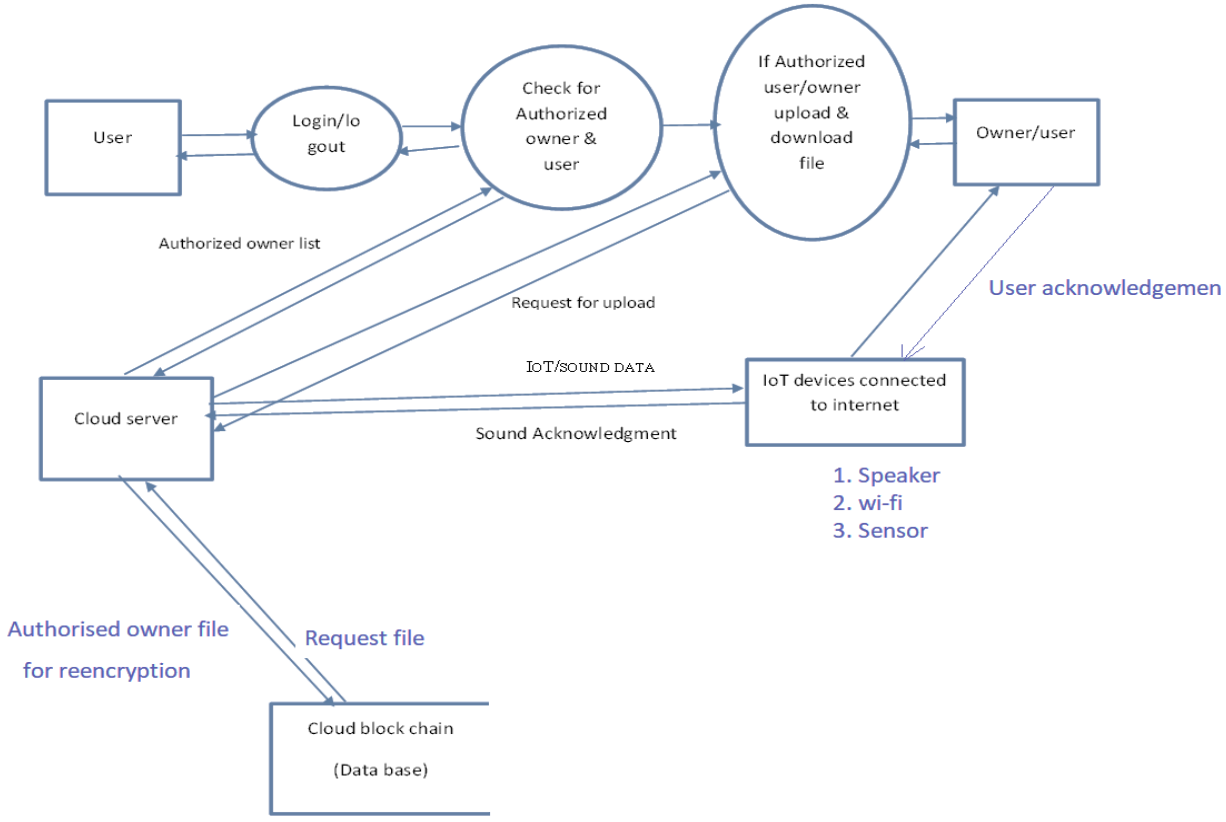

Figure 1: Data Flow Diagram

IV. IMPLEMENTATION AND RESULT ANALYSIS

In this project data owners can outsource their encrypted data to the cloud using identity based encryption and this process is referred as re-encryption. Further, in this project works, we used java programing language for implementation.

In this work we have consider three modules for the software design, they are:

Module 1 - for owner,
Module 2 - for user and
Module 3 -for server,

The following diagram shows modules of this project work:

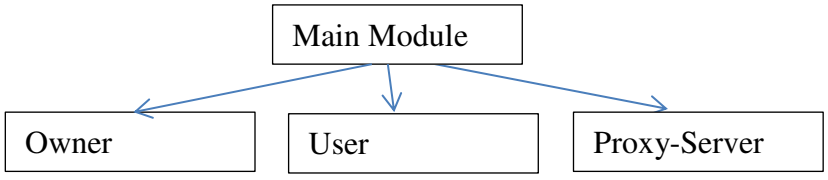

Figure 2: Software modules diagram

Sample screen shots are listed bn for the user and owner accounts login respectively.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207101 |

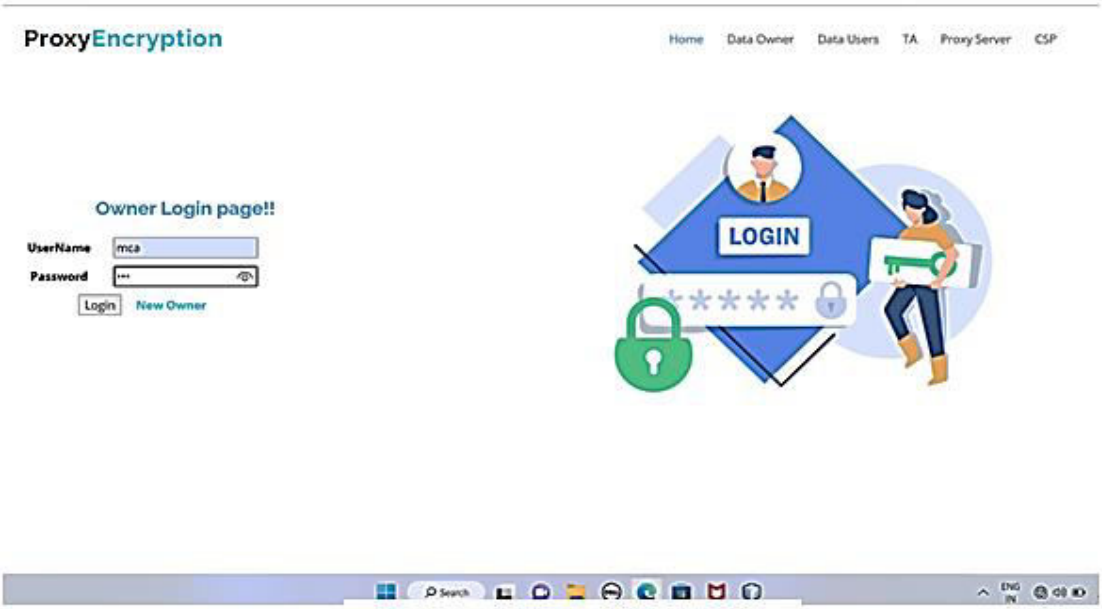

Figure 3: Owner login page

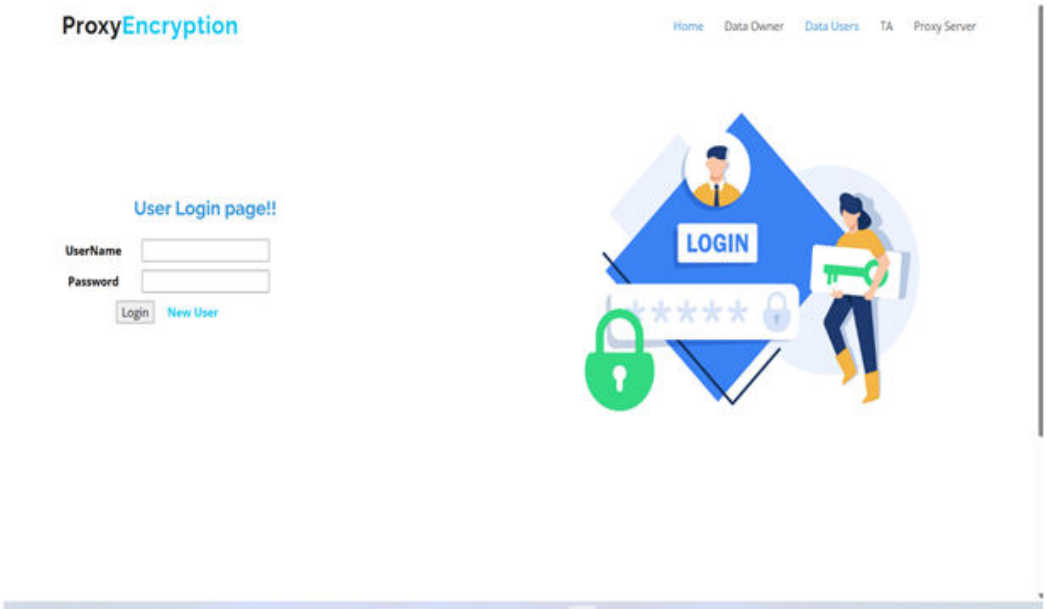

Figure 4: User login page

V. CONCLUSION AND FUTURE WORK

In this project work, we designed for owner and user login credentials separately for security point of view and implemented using JAVA. Using blockchain-based proxy re-encryption is a best strategy for safeguarding data exchange in the Internet of Things (IoT), in conclusion. Several advantages are realized by fusing proxy re-encryption's

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207101 |

cryptographic prowess with the decentralized nature of blockchain. Firstly, the adoption of blockchain provides an immutable and transparent record that protects data integrity. This improves the system's overall security by preventing unauthorized changes or tampering with IoT data. Secondly, proxy re-encryption enables safe data transfer without the requirement for key sharing. In order to guarantee the confidentiality of the data, this makes sure that only authorized recipients with the proper decryption keys can access and decrypt the data. This strategy is appropriate for IoT deployments with a large number of devices due to the scalability of blockchain networks. The decentralized nature of blockchain further improves the overall security of the data exchange process by lowering the possibility of a single point of failure. Furthermore, auditability and traceability of data transactions are provided by the blockchain and proxy re-encryption combination. Better accountability, openness, and systemic trust are made possible as a result. Overall, using blockchain-based proxy re-encryption to ensure data integrity, secrecy, scalability, decentralization, and audibility presents a potential solution to the security issues in IoT data sharing.

REFERENCES

1. S. Yu, C. Wang, K. Ran, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. IEEE INFOCOM,Mar. 2010, pp. 1–9.
2. Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.
3. H.-Y. Lin, J. Kubiatowicz, and W.-G. Tzeng, “A secure fine-grained access control mechanism for networked storage systems,” in Proc. IEEE 6th Int. Conf. Soft. Secure. Rel., Jun. 2012.
4. Y. Zhou et al., “Identity-based proxy re-encryption version 2: Making mobile access easy in cloud,” Future Genre. Compute. Syst., vol. 62, pp. 128–139, Sep. 2016.
5. G. Zyskind et al., “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Secure. Privacy Workshops, May 2015, pp. 180–184.
6. 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.
7. M. Ma, D. He, N. Kumar, K.-K. R. Choo, and J. Chen, “Certificate searchable public key encryption scheme for industrial Internet of Things,” IEEE Trans. Ind. Inform., vol. 14, no. 2, pp. 759–767, May 20.
8. L. Zhang, Q. Wu, Y. Mu, and J. Zhang, “Privacy-preserving and secure sharing of PHR in the cloud,” J. Med. Syst., vol. 40, no. 12, pp. 1–13, Dec. 2016.
9. A. Carzaniga, M. J. Rutherford, and A. L. Wolf, “A routing scheme for content-based networking,” in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.
10. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. Available: https://bitcoin.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details