A Proxy Re-Encryption Approach To Secure Data Sharing In The Internet of Things Based on Blockchain

T. Shalini[1], B. Abinaya[2], M. Mohamed Rafi[3]
[1, 2, 3] Dept of Master of Computer Application
[1, 2, 3] Mohamed Sathak Engineering College

Abstract- *The rapid evolution of the Internet of Things (IoT) has enabled massive data generation and sharing across cloud platforms. However, data security remains a critical challenge, as unauthorized access or misuse can lead to severe consequences. To address this, we propose a Proxy Re-Encryption (PRE) based approach for secure data sharing in IoT environments, integrated with blockchain for decentralization and trust. Data owners can encrypt their data using identity-based encryption and outsource it to the cloud. A proxy server, typically an edge device, handles intensive computations to re-encrypt the data for authorized users, enabling secure access without revealing the original content. Blockchain is integrated to record data access requests, approvals, and transactions in a tamper-proof and decentralized manner, ensuring transparency and trust. By splitting data into multiple blocks and enforcing trusted authority validation for users and owners, the system enhances confidentiality, integrity, and availability. Overall, this approach provides a scalable, efficient, and secure solution for IoT data sharing with minimal delay and reduced computational overhead on IoT devices.*

Keywords: Access Control, Blockchain, Cloud Storage, Data Integrity, Data Privacy, Encryption, Key Management, Secure Communication

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has led to the generation and sharing of massive volumes of data across cloud environments, making secure data management a major concern. Traditional security mechanisms often struggle to provide confidentiality, fine-grained access control, and scalability, especially for resource-constrained IoT devices.

To address these challenges, this project presents a secure data sharing framework based on Proxy Re-Encryption (PRE), Identity-Based Encryption (IBE), and blockchain technology. In the proposed system, data owners encrypt IoT data using IBE and store it in the cloud, while computationally intensive re-encryption tasks are delegated to a proxy server, such as an edge device, enabling secure data access for authorized users without exposing the original data.

Blockchain is integrated to record data access requests, approvals, and transactions in a tamper-proof and decentralized manner, ensuring transparency and trust. By splitting data into multiple blocks and enforcing trusted authority validation for users and owners, the system enhances confidentiality, integrity, and availability. Overall, this approach provides a scalable, efficient, and secure solution for IoT data sharing with minimal delay and reduced computational overhead on IoT devices.

II. PROCEDURE FOR PAPER SUBMISSION

A. Review Stage

The main objective of this stage is to assess the quality, originality, clarity, and technical correctness of the research work or improvements to enhance the overall standard of the paper.

B. Final Stage

After successfully completing the review process and incorporating all suggested revisions, the manuscript enters the final stage. In this phase, the paper is approved for publication and undergoes final formatting, proofreading, and validation checks. The authors may receive a confirmation or acceptance letter.

C. Figures

Figures are visual representations such as diagrams, graphs, charts, and images that help in better understanding of the content. All figures should be clear, properly labeled, and relevant to the topic. Each figure must be numbered consecutively and should include a descriptive caption below the figure. Figures must be referred to in the text before they

appear, and their quality should be high enough for clear visibility.

III. MATHEMATICAL FORMULATION

The proposed system utilizes cryptographic techniques, particularly Proxy Re-Encryption (PRE), to ensure secure data sharing in Internet of Things (IoT) environments integrated with blockchain.

Let the data owner encrypt a message M using their public key PK_A, resulting in ciphertext C_A = Enc(PK_A, M). A proxy re-encryption key RK_{A→B} is generated using the data owner's private key and the receiver's public key. The proxy uses this re-encryption key to transform C_A into C_B = ReEnc(RK_{A→B}, C_A), without accessing the original message.

IV. SYSTEM ARCHITECTURE AND UNITS

This approach focuses on providing secure and efficient data sharing in Internet of Things (IoT) environments using a combination of proxy re-encryption and blockchain technology. In IoT systems, devices continuously generate and share sensitive data, which makes security and privacy a major concern.

Proxy re-encryption allows a third-party proxy to transform encrypted data from one user to another without accessing the original data, ensuring confidentiality. At the same time, blockchain technology is used to maintain a decentralized and tamper-proof record of data transactions, improving trust and transparency.

V. HELPFUL HINTS

A. Figures and Tables

Figures and tables play a crucial role in presenting information in a clear and concise manner in research papers. Figures such as system architecture diagrams, flowcharts, and graphs help to visually explain the working of the proxy re-encryption mechanism and blockchain integration. Tables are used to organize and compare data, such as performance metrics, security features, or experimental results. All figures and tables should be properly numbered and must include descriptive captions. They should be referenced in the text before they appear, ensuring a logical flow of information. Proper formatting, clarity, and alignment should be maintained to enhance readability and understanding of the proposed system.

B. References

The references section lists all the sources that have been used or cited in the research paper. It provides credibility to the work by acknowledging the contributions of previous researchers in the fields of Internet of Things, blockchain technology, and data security. All references should be arranged in a standard format and numbered sequentially as they appear in the text. Each reference must include complete details such as author name, title of the paper, journal or conference name, volume, issue, year of publication, and page numbers. Proper citation ensures authenticity, avoids plagiarism, and helps readers to locate the original sources for further study.

C. Abbreviations and Acronyms

All abbreviations and acronyms used in the research paper should be defined clearly when they are first introduced in the text. This helps readers understand the terminology without confusion. Common terms such as IoT (Internet of Things), PRE (Proxy Re-Encryption), and BC (Blockchain) should be written in full form initially, followed by the abbreviated form in parentheses.

D. Equations

All equations used in the research paper should be presented clearly and formatted properly. Equations must be centered and numbered consecutively (e.g., (1), (2), etc.) for easy reference within the text. Each variable, symbol, and constant used in the equation should be defined clearly when it first appears. Equations should be referred to in the text before or after they are displayed to maintain a logical flow. Proper spacing and alignment must be maintained to ensure readability, and complex equations should be briefly explained to help readers understand their significance in the proposed system.

VI. PUBLICATION PRINCIPLES

Publication principles ensure that research work is conducted and presented with honesty, transparency, and integrity. Authors must submit original work that has not been published or submitted elsewhere. Proper acknowledgment of sources through accurate citation is essential to avoid plagiarism. The data presented in the paper should be genuine, and any form of fabrication, falsification, or manipulation is strictly prohibited.

All contributors who have significantly participated in the research should be listed as authors. In addition, authors

must follow ethical guidelines during the submission and publication process. Conflicts of interest, if any, should be clearly disclosed. The paper should comply with the journal's formatting and submission rules. Authors are responsible for responding to reviewers' comments and making necessary revisions in a timely manner. Once accepted, copyright requirements and publication policies must be followed strictly to ensure smooth and ethical dissemination of the research work.

VII. CONCLUSION

This paper presents a secure and efficient data sharing mechanism using proxy re-encryption integrated with blockchain technology for the Internet of Things. The proposed approach ensures data confidentiality, access control, and integrity. The integration of blockchain provides transparent and tamper-proof transaction records, while proxy re-encryption enables data owners to maintain control over their sensitive information. Overall, this approach enhances secure communication and trust among IoT devices in a decentralized environment.

VIII. APPENDIX

This paper presents a secure and efficient data sharing mechanism using proxy re-encryption integrated with blockchain technology for the Internet of Things. The proposed approach ensures data confidentiality, access control, and integrity. Overall, it enhances secure communication and trust among IoT devices.

IX. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all those who supported the successful completion of this research work. Special thanks are extended to the faculty members and project guides for their valuable guidance, encouragement, and continuous support. The authors also acknowledge the institution for providing the necessary resources and environment to carry out this work. Finally, heartfelt thanks to friends and family for their motivation and support throughout the project.

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.