IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

Blockchain Based Proxy Re-Encryption for Secure Data Sharing

Gunjal Aditya Ashok[1], Chikane Mayur Sakharam[2], Jadhav Shreyash Ashok[3], Prof Ghodake G. K.[4]
Students, Department of Computer Engineering[1,2,3]
Professor, Department of Computer Engineering[4]
Samarth College of Engineering and Management, Belhe, Junnar, Pune, Maharashtra, India
(AICTE Affiliated)
adityagunjalgil@gmail.com, mayurchikane121@gmail.com
shreyashjadhav533@gmail.com, gitaghodakecomp@gmail.com

Abstract: *This paper proposes a solution to secure data sharing within the Internet of Things (IoT) by combining Proxy Re-Encryption (PRE) and Blockchain. In IoT networks, data must often be shared across multiple devices and users, raising concerns over data privacy and security. Proxy Re-Encryption enables controlled data sharing without disclosing original information, while Blockchain technology offers an immutable, transparent ledger for tracking data transactions. Together, these technologies ensure data integrity, privacy, and efficient access control, making them suitable for modern IoT applications*

Keywords: Access control, Blockchain, Data Security, Proxy Re-Encryption(PRE), Internet of Things (IoT), Data Sharing, Security, Connected Device, Secure Data Sharing, Cryptographic Keys

I. INTRODUCTION

The Internet of Things (IoT) connects billions of devices, each continuously generating and sharing data. However, traditional data-sharing models in centralized cloud environments face limitations in securely handling sensitive data across diverse devices. Key concerns include unauthorized access, data tampering, and privacy breaches. This paper explores a solution where Blockchain and Proxy Re-Encryption are used together to secure and manage data access in IoT.

- **Blockchain's Role:** Blockchain, with its decentralized, tamper-proof structure, can ensure transparent and verifiable transaction records, which is crucial for trust among IoT devices.
- **Proxy Re-Encryption's Role:** PRE allows data originally encrypted by a user to be re-encrypted for a different recipient by a proxy, all without disclosing the original data to the proxy. This enables safe, flexible data sharing between IoT devices.

The integration of these technologies provides enhanced privacy, security, and access management, allowing IoT data to be shared more safely.

Cloud computing has significantly transformed the way we store and manage data, offering users flexibility, accessibility, and scalability. By allowing data to be stored on remote servers, cloud services enable individuals and organizations to access their information from anywhere, at any time. However, with the convenience of cloud storage comes a critical challenge: ensuring data security and integrity. As more sensitive information is stored online, concerns about unauthorized access, data breaches, and tampering have become increasingly prevalent.

The subsequent sections will delve into existing literature, analyze security protocols and frameworks, and propose recommendations for enhancing the security posture of IoT based data sharing systems. Through this exploration, the paper seeks to contribute valuable insights to the ongoing discourse on securing the vast network of interconnected devices in the IoT era.

II. LITERATURE REVIEW

The literature reveals a growing interest in the intersection of blockchain and cloud storage, focusing on several key areas that highlight the potential benefits and challenges of integrating these technologies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

Data Integrity and Security:

Blockchain's immutable ledger records every transaction, ensuring data integrity. Studies such as Zhang et al. (2021) demonstrate that Blockchain's cryptographic protection against tampering provides a foundation for secure IoT networks.

In IoT, data generated by each device can be validated and stored on the Blockchain, allowing verification by users and devices. The use of hashing functions and public-key cryptography strengthens the integrity of shared data.

Many studies emphasize blockchain's significant role in enhancing data integrity and security within cloud storage systems. For instance, Zhang et al. (2021) demonstrated that blockchain's immutable ledger provides a reliable means of tracking changes to data, making it nearly impossible for malicious actors to tamper with stored information without detection. By recording each transaction in a secure and transparent manner, blockchain enables users to verify the authenticity of their data. This transparency fosters trust, as users can independently audit the records stored on the blockchain.

Moreover, the cryptographic methods used in blockchain ensure that data is securely encrypted, further protecting it from unauthorized access. Overall, this combination of features enhances the security posture of cloud storage solutions, addressing one of the most pressing concerns for organizations that rely on cloud services.

Decentralization and Access Control:

Traditional access control systems rely on centralized authorities, which can be a vulnerability in IoT. Blockchain's decentralized nature eliminates this, as Lee and Kim (2020) observed, making it difficult for any single entity to manipulate access permissions.

Attribute-Based Encryption (ABE) and Role-Based Access Control (RBAC) in combination with smart contracts on Blockchain enable automated, secure access control. These techniques allow access based on user roles or attributes, essential for IoT devices with varying permission needs.

Decentralization is another critical advantage of integrating blockchain with cloud storage. Lee and Kim (2020) explored a blockchain-based model that allows users to maintain control over their data while utilizing cloud storage. Traditional cloud services often rely on centralized providers, which can create vulnerabilities and single points of failure. By employing blockchain technology, data is distributed across a network, reducing reliance on any single entity and enhancing security. This decentralized approach empowers users to manage their own data access, enabling them to set permissions and determine who can view or modify their information. As a result, users have greater autonomy over their data, which is especially important in sectors like healthcare and finance, where data privacy is paramount. The ability to control access also helps mitigate risks associated with data breaches, as users can revoke access at any time.

Performance and Scalability:

Blockchain's decentralized storage has inherent scalability issues when processing large volumes of data in real time, as noted by Wang et al. (2022). For IoT, where high transaction speeds are essential, Layer 2 scaling solutions and off-chain processing are emerging solutions. These can help reduce Blockchain's computational load, making it more practical for IoT applications.

While the benefits of blockchain are clear, performance and scalability challenges remain a significant concern. Wang et al. (2022) analyzed the trade-offs between enhanced data security and the efficiency of storage systems. They found that while blockchain can provide superior security features, it may also introduce latency in data retrieval processes. This is particularly problematic for applications requiring real-time access to large volumes of data. The decentralized nature of blockchain can slow down transaction speeds compared to traditional centralized systems, where data retrieval is typically faster. Furthermore, as the volume of data grows, maintaining performance levels becomes increasingly challenging. Researchers are exploring various solutions, such as Layer 2 scaling techniques, to address these issues, but achieving a balance between security and performance continues to be an area of active investigation. Addressing these challenges will be crucial for the widespread adoption of blockchain in cloud storage solutions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

PRE Data Sharing:

Key-policy ABE (KP-ABE) and PRE were coupled by Yu et al. in order to offer a method for the sharing of data in the cloud. Because the data was encrypted using KP ABE, decryption can only be achieved via the use of an adequate collection of the attribute secret keys. In order to manage revocation of users, in addition to the encrypted data, the cloud also handled all attribute secret keys, with the exception of a single unique secret key. When a user's access is revoked, the owner of the data ISSN:0377-9254 must provide new encryption keys to the remaining users and then re-encrypt any material that was previously encrypted.

The system was effective; nevertheless, the re-encryption was carried out in a careless manner, which led to a reduction in the level of security provided by the programme. Park offered an improvement to the approach described in which prevents revoked users and service providers from conspiring together. Their plan was to essentially switch out the service provider with a reliable third party, which suggests that there need to be a greater dependence on the assumption of increased confidence. Other methods have attempted similar efforts, but instead used ciphertext-policy ABE (CP ABE), in which the access policy is connected with the ciphertext rather than the secret keys.

A time-constrained access control strategy that was based on PRE and ABE was also suggested by Liu et al. The time characteristics were kept up to date by ABE while ABE was utilised to construct time-based access control rules. Due to the intensive calculations required for encryption and decryption, these strategies, despite the fact that they provide certain benefits, are not appropriate for use in the context of the internet of things (IoT).

III. DISCUSSION

The integration of blockchain in cloud storage offers several notable advantages and challenges that need to be carefully considered.

ADVANTAGE

Security:

Blockchain employs robust encryption methods to safeguard data against unauthorized access. Transactions are recorded in a way that prevents alteration, ensuring data integrity and reliability. The decentralized storage architecture reduces the risks associated with single points of failure, making data less vulnerable to cyberattacks. Users can perform real-time audits of their data independently, enhancing accountability and oversight. Every change in the data can be tracked, providing a clear audit trail that helps in verifying authenticity. Enhanced security measures allow users to feel more confident about their data's safety. Additionally, smart contracts can automate and enforce access permissions, further securing sensitive data.

Transparency:

A shared distributed ledger allows all users to access the same version of data, enhancing trust. Users can independently verify the authenticity and integrity of their data, fostering confidence. Clear records of transactions increase accountability among users and service providers. The transparent nature of blockchain helps reduce opportunities for fraudulent activities. Organizations can demonstrate compliance with industry standards, boosting confidence among stakeholders. Users can also share data securely and transparently, enhancing collaboration. Furthermore, transparent records contribute to better reputation management for organizations utilizing blockchain.

Tamper resistance:

The decentralized nature of blockchain makes it resistant to tampering and unauthorized modifications. This ensures the integrity and authenticity of shared data.

Blockchain technology, particularly public blockchains like Ethereum, can face

scalability challenges. The large volume of data generated in the IoT ecosystem can strain the transaction processing capabilities of existing blockchain systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

Transparency and Auditability:
The use of blockchain allows for transparent tracking of data access and sharing activities. Auditing and accountability become easier, which can be crucial in compliance-sensitive environments.The encryption and re-encryption operations in PRE can introduce additional computational overhead.

System Architecture

1. Trusted Authority (TA):

- The TA manages the generation and distribution of keys. It authenticates devices and users, issuing encryption and re-encryption keys securely.
- Key Revocation: The TA supports key revocation, an essential feature for IoT security when devices become compromised or obsolete.

2. Proxy Server:

- Proxy Re-Encryption (PRE): The Proxy Server re-encrypts data encrypted by the sender for the recipient using a re-encryption key. This transformation enables data sharing without revealing original content to the proxy.
- Intermediary Role: Acting as an intermediary between IoT devices and the Cloud Service Provider (CSP), the proxy ensures re-encrypted data reaches only authorized recipients.

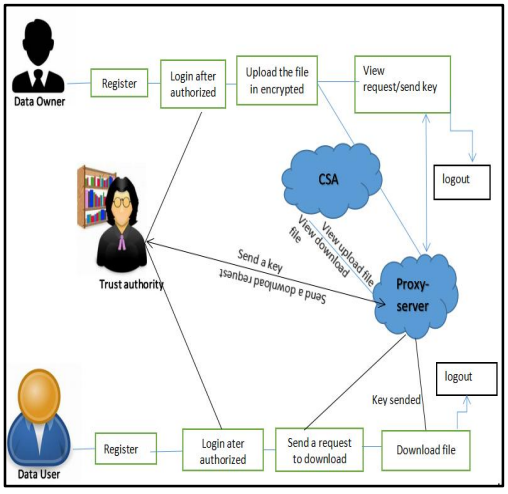
3. Blockchain Ledger:

- Consensus Mechanisms: The Blockchain ledger uses either Proof of Work (PoW) or Proof of Stake (PoS) consensus to ensure that only verified transactions are recorded.
- Smart Contracts: These are programmed on the Blockchain to enforce access policies automatically. For instance, a smart contract could grant data access to devices based on predefined policies stored on the Blockchain.

4. Cloud Service Provider (CSP):

- Secure Data Storage: CSP holds encrypted data, making it accessible only through re-encryption by authorized devices.
- Data Availability: The CSP ensures high availability and redundancy of stored data, allowing devices to retrieve data efficiently while keeping it encrypted at rest.

5. User Interface Module:
This module allows end-users to manage keys, data access policies, and view transaction logs. A simplified interface is crucial to allow non-experts to interact with complex encryption and Blockchain technologies effectively.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

Challenges:

Scalability issues:

Current blockchain architectures may struggle with the efficient handling of large data volumes. Increased network size can lead to slower transaction processing times. Larger block sizes can complicate data management and increase latency in retrieval. High latency in accessing data can hinder the performance of time-sensitive applications. Technologies such as sharding and Layer 2 solutions are still being developed and optimized. Scalability challenges can also increase operational costs, affecting the viability of blockchain solutions. Limited scalability may deter organizations from fully embracing blockchain for cloud storage.

IV. FUTURE DIRECTIONS

Future research should focus on several key areas to enhance the integration of blockchain technology in cloud storage.

1. Hybrid Blockchain Architectures:

Hybrid Models: Integrating traditional databases for high-speed access alongside Blockchain for secure data recording can offer a balanced approach to address performance issues.

2. Improved PRE Algorithms:

Developing more efficient PRE algorithms tailored to IoT environments can reduce computational overhead, enhancing speed while maintaining security.

3. IoT-Specific Blockchain Consensus Protocols:

Investigating new consensus algorithms specifically for IoT data exchanges (e.g., Proof of Authority or Federated Byzantine Agreement) can improve transaction speeds and reduce resource consumption.

4. Regulatory Adaptation for Decentralized Data:

Further exploration into compliance strategies for decentralized data (e.g., privacy-preserving encryption or GDPR-compliant Blockchain designs) is essential to ensure Blockchain and PRE solutions meet legal standards.

V. CONCLUSION

The integration of Proxy Re-Encryption and Blockchain technologies for IoT applications offers a secure, scalable, and efficient method for managing sensitive data. As IoT networks continue to grow, these technologies provide essential features—decentralized control, enhanced privacy, and tamper-proof audit trails—that address critical security challenges. Despite hurdles in scalability and regulation, advances in hybrid models and specialized consensus protocols could soon make these systems viable for widespread IoT use, enabling a future where data integrity, confidentiality, and control are ensured across complex, data-rich IoT networks.

REFERENCES

[1]. 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]. 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.

[4]. Balfanz et al.,"Secret handshakes from pairingbased key agreements," in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

[5]. R. Canetti, S. Halevi, and J. Katz, "Chosenciphertext security from identity-based encryption," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.

[6]. 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

[7]. 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.

[8]. 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.