Secure Data Sharing with Decentralised Data Ring Fencing

Aditya Nangia
IIIT Delhi
India
aditya20168@iiitd.ac.in

Saksham Bhupal
IIIT Delhi
India
saksham20573@iiitd.ac.in

Kushagra Mittal
IIIT Delhi
India
kushagra20075@iiitd.ac.in

Mukesh Mohania
IIIT Delhi
India
mukesh@iiitd.ac.in

Ashish Kundu
Cisco Research
USA
ashkundu@cisco.com

***Abstract*—The explosion of data and digital technologies has exacerbated privacy concerns. Traditional access control struggles to keep pace with the complexity of multi-party data sharing, where varying data access rules and privacy policies across institutions create significant challenges - leading to unauthorized and unintended access, especially in multi-party scenarios.**

Data Ring Fencing, inspired by the financial sector's concept of isolating assets, offers a multi-layered security framework for secure data sharing. It governs data access privileges, regulating who can access what data, for what purpose, and at what cost. However, the current model relies on a central system, requiring complete trust from all participating institutions.

This paper addresses these limitations by proposing a Decentralized Data Ring Fencing approach that leverages permissioned blockchains. This eliminates the need for a central authority, a critical factor as it removes the inherent single point of failure and the requirement for absolute trust in a central system.

***Index Terms*—Permissioned Blockchain, Data Ring Fencing, Data Privacy, Secured Data Sharing.**

I. Introduction

The exponential growth of data, fueled by advancements like the Internet of Things (IoT) and sensor technology, has created a data deluge. While this presents immense opportunities for innovation, it also raises critical privacy concerns. Individuals are increasingly vulnerable to data breaches, identity theft, and other privacy violations as the collection and analysis of personal information intensifies. Recognizing data privacy as a fundamental right, regulatory bodies worldwide have enacted stricter data privacy legislation like the General Data Protection Regulation (GDPR) [1] and the California Consumer Privacy Act (CCPA) [2] to empower individuals and hold organizations accountable.

Traditional access control mechanisms, which dictate who can access specific data resources, are essential for data security but have limitations. They rely on user identification and pre-defined permissions, creating a binary "access" or "deny" relationship. While this helps mitigate the risk of breaches, it doesn't address:

Vulnerability to Insider Threats: Authorized users with malicious intent can exploit loopholes or misuse credentials.

Difficulty in Managing Complex Access Policies: Complex data sharing agreements with multiple institutions and nuanced access needs based on roles, data subsets, and use cases are challenging to manage with static access control policies.

Lack of Flexibility for Dynamic Data Sharing: Existing mechanisms struggle to adapt to temporary or conditional access needs and lack the granularity to control how data is used after access is granted.

These limitations necessitate access control mechanisms that move beyond the traditional "who-what" paradigm [3]. Our earlier paper, Data Ring Fencing [4], emerges as a promising solution by incorporating additional factors like access purpose and cost. It utilizes a multi-layered security approach with a Three-E architecture (Evaluate, Enforce, Execute) to ensure data privacy and security. However, the current model relies on a central system, introducing a single point of failure and trust concerns.

This paper proposes Decentralized Data Ring Fencing, a framework that leverages permissioned blockchains, a distributed ledger technology for secure and trustworthy data sharing. Utilizing the enhanced security, immutability, and auditability of permissioned blockchains to eliminate the central authority. Our framework distributes data ownership and enforces access control through smart contracts on the secure blockchain network. Secure data access techniques further minimize data exposure while enabling collaboration. This approach has the potential to revolutionize data sharing by fostering trust and accountability through blockchain-based transparency and immutability.

II. Architecture

This section outlines a novel approach to Data Ring Fencing by leveraging the secure and controlled environment offered by permissioned blockchains. This Decentralized Data Ring Fencing architecture aims to enhance data security, transparency, and automation within data-sharing collaborations.

A. Data Sharing Workflow

The data-sharing workflow within this decentralized Data Ring Fencing architecture is designed to be secure, automated, and transparent. This section delves into the step-by-step process, highlighting how permissioned blockchains and smart contracts secure data access.

Data Access Request: Consumer submits data access request to the network.

This work has been partly funded by Cisco Systems Inc.

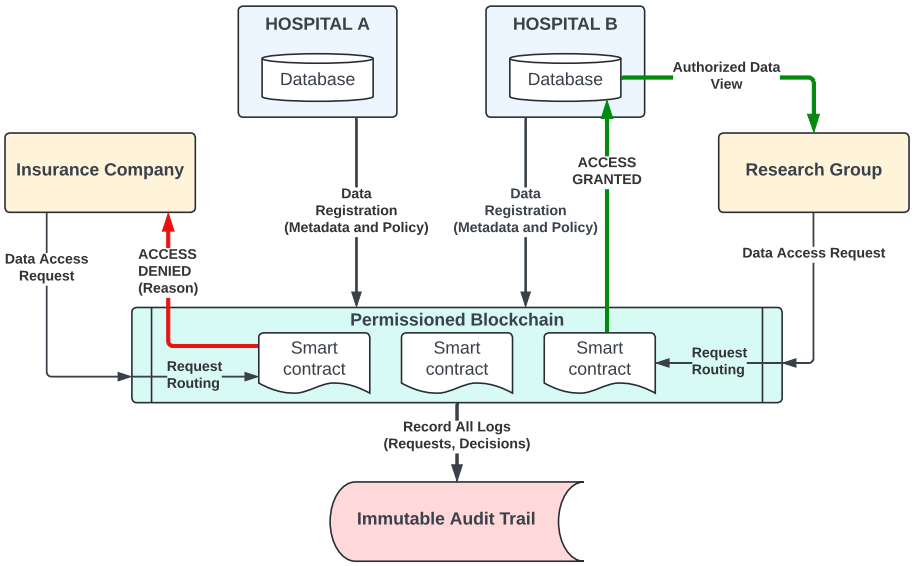

Fig. 1. Decentralized Data Management Model

Smart Contract Evaluation: The submitted request is routed to a relevant smart contract which evaluates it against the access policy.

Policy Enforcement: Based on the evaluation, the smart contract determines whether to grant or deny access. Factors considered during this evaluation include:

1) *User Identity and Role:* User authentication via network identity and role.
2) *Purpose Alignment:* Verify intended purpose aligns with access policy.
3) *Cost Considerations:* Incorporation of potential financial/computational costs.
4) *Pre-defined Conditions:* Verification of all stipulated and flexible access policy conditions.

Data Access and Usage: Provide secure and temporary access if approved (applicable data view from data vault).

Immutable Audit Trail: Record all actions immutably on the blockchain.

B. Data Management

In our decentralized Data Ring Fencing approach, data ownership is distributed. Institutions/individuals (denoted as party x) control their data assets (database D_x) stored within secure enclaves. Access control policies ($P(D_x)$) specifying authorized parties (y), access purpose, and any associated costs/conditions are defined by party x and registered on the permissioned blockchain network. Smart contracts enforce policies and data access occurs without transferring raw data. This empowers data owners and enables secure sharing.

C. Trust Model

In our approach, each party (x) maintains autonomy over their data (D_x) stored in secure enclaves, including defining access policies and ensuring data integrity. Parties trust the system to process authorized queries based on pre-defined policies ($P(D_x)$), but no trust relationship exists beyond the scope of the query. The permissioned blockchain enforces access control and fosters trust through cryptography. Secure data access techniques minimize trust assumptions.

D. Conclusion

Decentralized Data Ring Fencing uses blockchains to empower data owners with precise control over data access. It overcomes limitations of centralized control by distributing ownership and access rules on a secure blockchain. Smart contracts enforce these rules, granting access only to authorized users for specific purposes. Secure data access techniques minimize data exposure while enabling collaboration. This approach fosters trust and transparency through secure, decentralized data governance. While an initial implementation is under evaluation, Our framework has the potential to revolutionize secure data sharing in collaborative environments.

REFERENCES

[1] M. Goddard, "The eu general data protection regulation (gdpr): European regulation that has a global impact," *International Journal of Market Research*, vol. 59, no. 6, pp. 703–705, 2017.

[2] S. L. Pardau, "The california consumer privacy act: Towards a european-style privacy regime in the united states," *J. Tech. L. & Pol'y*, vol. 23, p. 68, 2018.

[3] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[4] A. Nangia, S. Bhupal, M. Mohania, and C. Kundu, "Secured data movement using data ring fencing," in *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE Computer Society, 2023, pp. 370–379.