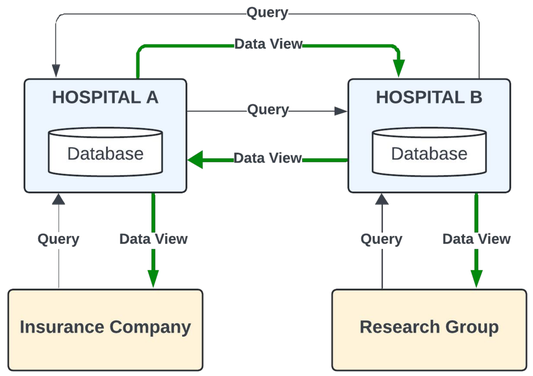
Secure Data Sharing with Decentralised Data Ring Fencing

Aditya Nangia, IIIT-Delhi
Saksham Bhupal, IIIT-Delhi
Kushagra Mittal, IIIT-Delhi
Mukesh Mohania, IIIT-Delhi
Ashish Kundu, Cisco Research

Traditional Multi-Party Data Sharing has several policy, efficiency and security related issues.
We leverage the idea of Ring Fencing borrowed from the financial world coupled with Decentralised Trust to foster efficient and secure data sharing.

Background

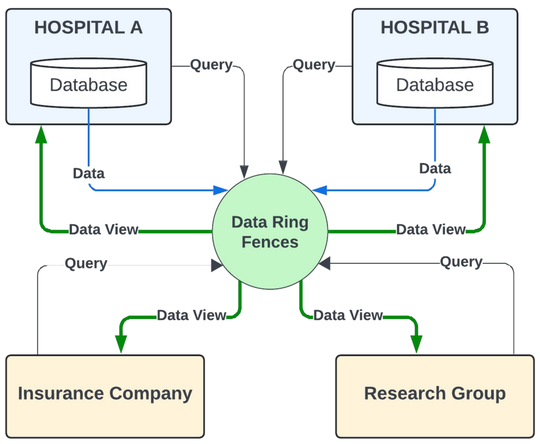
Traditional Multi-Party Data Sharing



Traditional data sharing relies on Access Control, which while helping to mitigate data breaches doesn't address:

- Vulnerability to **Insider Threats**
- Difficulty in Managing **Complex Access Policies**
- **Lack of Flexibility** for Dynamic Data Sharing

Centralised Data Ring Fencing



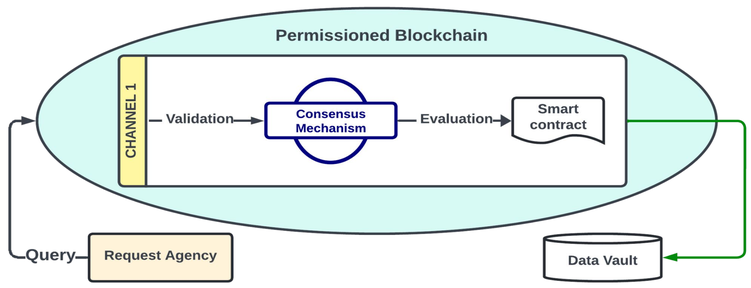
Data Ring Fencing builds on the ring fencing concept borrowed from the the financial world to create a centralized model which solves the above problems however introduces:

- A **single point of failure**
- The need for **absolute trust** in a central authority.

Decentralised Ring Fencing

Therefore, we need Decentralised Trust based data ring fencing.

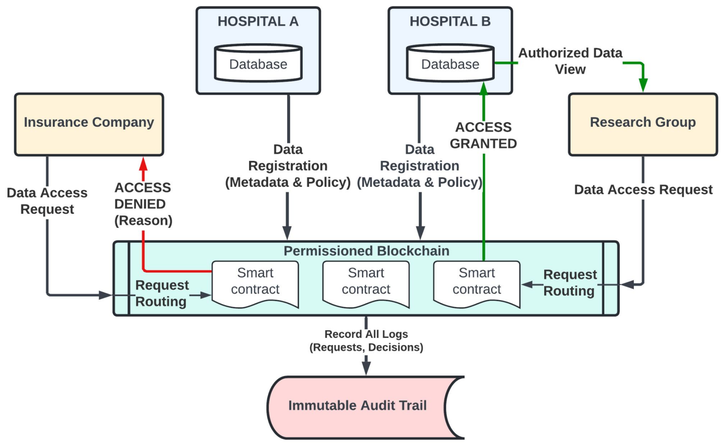
- Even internal data requests are routed through and recorded on the blockchain mitigating **Insider Threats**.
- **Complex Internal Access policies** as well as data sharing agreements are modeled through smart contracts.
- Considerations of data access cost based on predefined conditions allow for **flexible dynamic data sharing.**
- Data vaults private to the data providers ensure there is **no single point of failure.**
- Decentralised architecture allows for a **trustless** data sharing.



Data-Sharing Workflow

- **Data Registration:** Data providers register their data assets - metadata and corresponding ring fences - with the network.
- **Data Access Request:** Data consumer submits data access request to the relevant network channel.
- **Smart Contract Evaluation:** Request is routed to the appropriate smart contract for evaluation against the ring fencing policy.
- **Policy Enforcement:** Based on the following factors, the smart contract determines whether to grant or deny access.
  - **User Authentication:** Based on network **identity** and **role**.
  - **Purpose Alignment:** Verify intended purpose.
  - **Cost Consideration:** Incorporate financial/computational costs.
  - **Pre-defined Conditions:** Verify all dynamic policy conditions.
- **Data Access and Usage:** Data Vault provides access to the applicable data view if approved.
- **Immutable Audit Trail:** Record all actions on the blockchain.

Application



Our model can seamlessly replace existing data management models in multi-party data sharing environments:

- **Healthcare:** Hospitals, insurers, and researchers can securely share patient data to improve care.
- **Finance:** Banks, credit bureaus, etc. can collaborate to enable loan verification and fraud detection without compromising customer privacy.
- **Government Services:** Government agencies can share data for public services (e.g., social welfare) while safeguarding citizen privacy.

Conclusion

Enhanced Control and Privacy: Decentralized trust and distributed ownership gives data owners enhanced control promoting a more private data governance model.
Trust and Transparency: The transparency and auditability provided by the blockchain foster trust and accountability within data sharing ecosystems

References

[1] Nangia, A., Bhupal, S., Mohania, M., & Kundu, C. (2023, November). 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)* (pp. 370-379). IEEE.