BLOCKCHAIN-BASED PROXY RE-ENCRYPTION FOR SECURE DATA SHARING IN IOT NETWORKS

SUBMITTED BY,

ASWINI A J (963321104011)

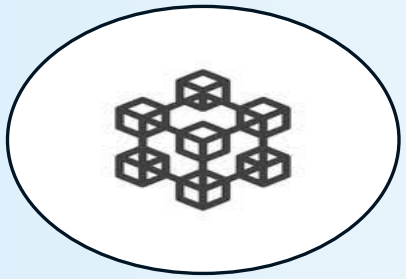
JEMILA R (963321104026)

NIVETHA M (963321104039)

THIVYA R (963321104060)

AGENDA

- Abstract
- Literature Survey
- Existing System
- Disadvantages
- Proposed System
- Advantages
- System Architecture
- Conclusion



ABSTRACT

In the rapidly growing Internet of Things (IoT) ecosystem, ensuring secure data sharing between devices is a significant challenge due to the decentralized nature and limited computational resources of IoT devices. Traditional encryption methods struggle to balance security and performance in these environments. This paper proposes a blockchain-based proxy re-encryption (PRE) scheme to secure data sharing in IoT networks. By leveraging proxy re-encryption, data owners can securely delegate decryption rights to authorized devices without exposing the original encryption keys. Blockchain technology ensures a tamper-proof and transparent mechanism for managing access control and encryption key delegation. The decentralized nature of blockchain enhances security and eliminates the need for a central authority, while proxy re-encryption provides fine-grained access control, allowing efficient and secure data sharing across IoT devices. Experimental results demonstrate that our approach provides strong security guarantees, efficient key management, and scalability suitable for large-scale IoT deployments.

LITERATURE SURVEY

S.NO	TITLE	AUTHOR	YEAR	METHODOLOGY USED	ADVANTAGES	DISADVANTAGES
1	A Proxy Re-encryption approach to secure data sharing in the IoT based on blockchain	Qi Xia	2022	Access control, blockchain, Information-Centric Network	Data Security, Privacy, data confidentiality	Centralized data sharing, Vulnerability to breaches.
2	FairShare: Blockchain for Industrial IoT	Jayasree Sengupta	2023	Fair, accountable, secure sharing, fog nodes, blockchain, proxy re-encryption	Fairness, accountability, security, fraud prevention	Complexity, potential latency
3	Commercializing Medical Records with Blockchain	Phong Tran	2024	Decentralized system, blockchain, IPFS, proxy re-encryption	User control, data integrity, privacy	Scalability, data retrieval efficiency
4	Meta-Key: Secure Protocol	Dagang Li	2017	Blockchain-based storage, proxy re-encryption, secure sharing	No trusted parties, data confidentiality	Collusion risks
5	Secure EMR Sharing Scheme	Jian Liu	2023	Blockchain, proxy re-encryption for medical records	Security, privacy, efficient sharing	Integration challenges

LITERATURE SURVEY

S.NO	TITLE	AUTHOR	YEAR	METHODOLOGY USED	ADVANTAGES	DISADVANTAGES
6	A Survey on Enabling Technologies, Protocols, and Applications	A. Al-Fuqaha	2015	Examines Federated Learning (FL) technologies and applications. FL allows training models without sharing raw data.	Higher security, mitigates data breaches, suitable for diverse industries.	Challenges in implementation across different industries.
7	Divertible Protocols and Atomic Proxy Cryptography	M. Blaze, G. Bleumer	1998	Introduces protocol divertibility and atomic proxy cryptography. Allows secure transformation of encrypted messages using a public proxy key.	Facilitates data re-encryption in untrusted environments, secure data-sharing.	Complexity in implementation.
8	Identity-Based Cryptosystems and Signature Schemes	A. Shamir	1984	Introduces identity-based cryptographic systems. Eliminates traditional key exchanges, leveraging trusted key generation centers.	Reduces complexity of key management, enhances scalability in decentralized networks.	Potential challenges in widespread adoption.
9	Secret Handshakes from Pairing-Based Key Agreements	D. Balfanz	2003	Uses pairing-based cryptography for secure and anonymous authentication protocols. Enables mutual authentication without revealing credentials.	Ensures resistance to collusion and traceability, role-based group membership.	Potential implementation complexity.
10	Blockchain-based Proxy Re-Encryption Scheme	Ahsan Manzoor	(2018)	IoT data in cloud, no TTP, smart contracts, proxy re-encryption	No trusted third parties, scalable, automates	Performance overhead

EXISTING SYSTEM

The existing systems for secure data sharing in cloud computing have made significant advancements in ensuring data confidentiality, integrity, and access control. However, they also come with limitations that hinder their effectiveness in dynamic and resource-constrained environments, such as those enabled by the Internet of Things (IoT). This chapter delves into the current methodologies and their architecture, highlighting the strengths and limitations of the existing approaches.

Existing systems primarily rely on traditional cryptographic techniques and centralized architectures to ensure data security. These systems include symmetric and asymmetric encryption, public key infrastructure (PKI), and access control mechanisms. Although these solutions provide a baseline for data security, their applicability to IoT-enabled cloud environments faces several challenges, including high computational overhead, centralized bottlenecks, and limited scalability.

DISADVANTAGES

- Centralized data sharing.
- Vulnerability to breaches.
- Dependency on trusted third parties.
- Single points of failure.
- Potential data leaks.

Additional :

- Lack of transparency and accountability.
- Difficulty in establishing trust for data handling.
- Significantly pertinent in sensitive industries (e.g., healthcare, finance).
- Critical need for data protection in these sectors.

PROPOSED SYSTEM

The proposed system addresses the limitations of existing data-sharing frameworks by combining advanced cryptographic techniques, fog computing, and blockchain technology to create a secure, decentralized, and efficient data-sharing framework. This system is designed to operate effectively in IoT-enabled cloud environments, with a particular focus on resource-constrained and latency-sensitive applications like e-healthcare.

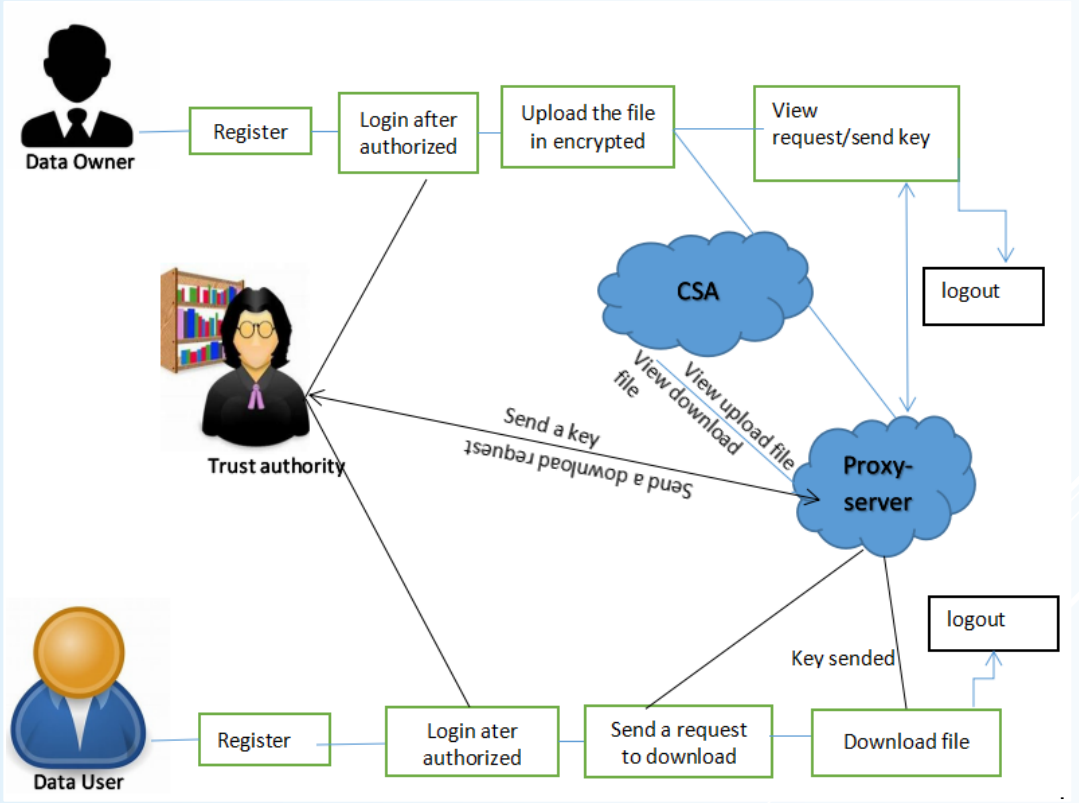
The proposed framework leverages a hybrid architecture combining blockchain and fog computing for decentralized data management. Advanced cryptographic methods, such as proxy re-encryption and identity-based encryption, are integrated to ensure secure data sharing. The primary application of this framework is in e healthcare, but it is adaptable to other domains like smart cities and industrial IoT.

ADVANTAGES

- **Proxy Re-Encryption + Blockchain**
  - Addresses IoT security and privacy.
- **Proxy Re-Encryption**
  - Enables secure data sharing.
  - Protects encryption keys.
  - Uses a proxy server.
- **Blockchain Benefits**
  - Ensures data immutability.
  - Provides transparency.
  - Establishes trustless environment.
- **Enhanced Security**
  - Mitigates IoT data risks.
- **Privacy Assurance**
  - Safeguards shared data.
- **Decentralization**
  - Boosts security by moving away from central systems.
- **Transparency and Trust**
  - Offers visibility and reliability in data transactions.

SYSTEM ARCHITECTURE

- Proxy Re-Encryption and Blockchain Integration
- Data Encryption with Proxy Re-Encryption
- Blockchain Storage
- Node-Based Infrastructure
- Node Functionality



CONCLUSION

Blockchain and proxy re-encryption offer a secure, decentralized solution for IoT data sharing amidst growing device connections and data volumes. Prioritizing privacy and security is crucial, and these technologies provide the means to achieve it and to explore their potential for your IoT projects.

THANK YOU