The Oxford College of Engineering

10th Milestone Hosur Road, Bommanahalli, Bangalore-560068

Project Synopsis

20MCA44

On

"A PROXY RE-ENCRYPTION APPROACH TO SECURE DATA SHARING IN THE INTERNET OF THINGS BASED ON BLOCKCHAIN"

Submitted By

Name: ASHIK E.D
USN: 1OX21MC016

Department of Computer Application

Under the Supervision of
Dr Puja Shashi
Professor and Head
Department Of MCA

The Oxford College of Engineering

Title: **A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain**

ABSTRACT

With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computationally intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program-based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

EXISTING SYSTEM:

- Due to the restricted resources of Internet of Things devices, an edge device operates as a proxy server to perform computationally expensive activities. Furthermore, by employing information-centric networking capabilities, we successfully disseminate cached content through the proxy, hence improving service quality and effectively utilizing network capacity. It achieves fine-grained data access control while reducing centralized system bottlenecks. As evidenced by the security research and plan assessment, our method for maintaining data security, confidentiality, and integrity shows promise.

DISADVANTAGES OF EXISTING SYSTEM:

- **Scalability:** 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.
- **Performance overhead:** The encryption and re-encryption operations in PRE can introduce additional computational overhead. This overhead may impact the performance of IoT devices with limited computing resources.
- **Key management complexity:** Managing the encryption keys and access control policies in a decentralized blockchain system can be complex. Ensuring secure key distribution and revocation mechanisms is crucial but can add overhead and complexity to the system.
- **Dependency on blockchain consensus:** The security of the system heavily relies on the consensus mechanism employed by the underlying blockchain. If the consensus mechanism is compromised or vulnerable, it can undermine the security guarantees of the entire system.
- **Privacy concerns:** While PRE protects the confidentiality of data during transmission and storage, it does not address privacy concerns related to metadata or data correlation. Additional measures may be required to address these concerns.

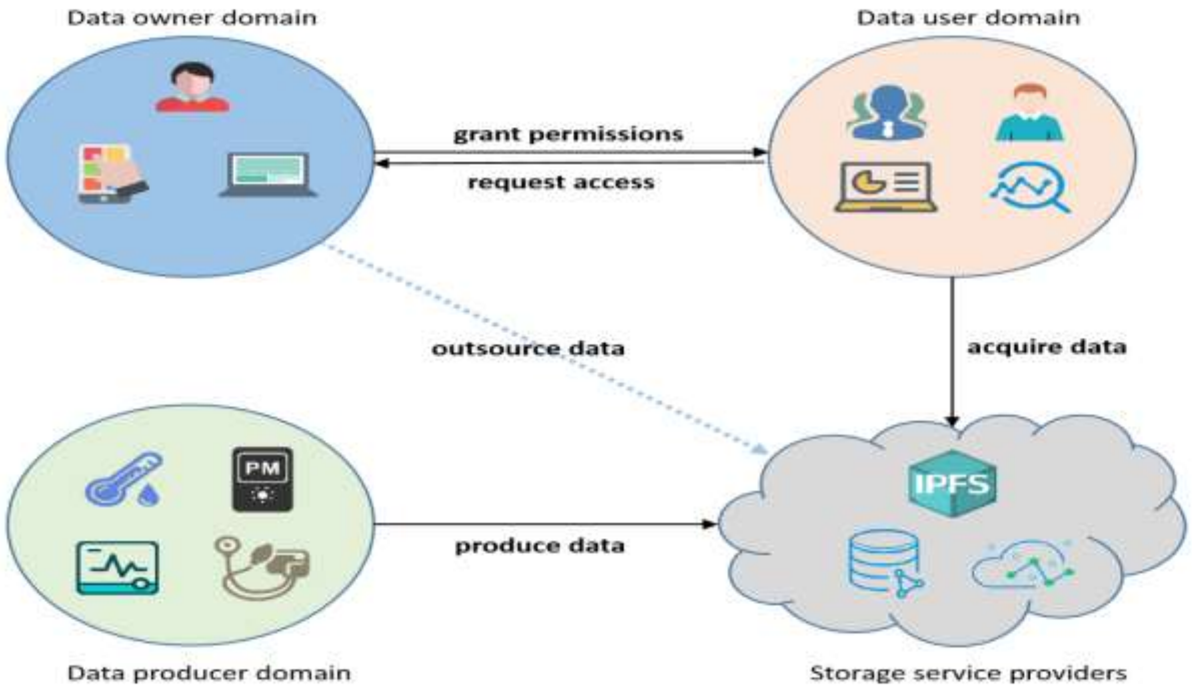
PROPOSED SYSTEM:

- The tool presents a consistent get admission to manage framework to acknowledge data confidentiality, and incredibly fine-grained get admission to records is performed. This may also help to ensure that data owners have complete control over their data.
- The device provides an in-depth description of our prior theme as well as the fruition of a complete protocol that ensures knowledge protection and privacy.
- Factor widgets serve deputy bumps and execute re-encryption on cached records to embellish statistics shipping and properly rent the network information measure. The component widgets are expected to have more calculation capabilities than the IoT widgets and

ADVANTAGES OF PROPOSED SYSTEM:

- **Enhanced security:** The combination of PRE and blockchain provides an additional layer of security for data sharing in the IoT. The encryption and re-encryption processes ensure that data remains confidential throughout the sharing process.
- **Access control:** By leveraging blockchain, access control policies can be defined and enforced transparently. Only authorized entities with the necessary decryption keys can access specific data, ensuring data privacy and integrity.
- **Tamper resistance:** The decentralized nature of blockchain makes it resistant to tampering and unauthorized modifications. This ensures the integrity and authenticity of shared data.
- **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.

SYSTEM ARCHITECTURE:



MODULES:

Data Encryption and Key Generation:

- This module involves the encryption of data generated by IoT devices using appropriate cryptographic algorithms.
- It also includes the generation of encryption keys for each IoT device or data owner.

Access Control and Policy Management:

- This module focuses on defining access control policies for data sharing.
- It involves creating rules or policies that determine which entities are authorized to access specific data.
- Smart contracts can be used to enforce these policies on the blockchain.

Proxy Re-Encryption:

- This module is responsible for the actual re-encryption of data using proxy re-encryption techniques.
- It includes the transformation of encrypted data from one key to another key without revealing the original plaintext.
- The re-encryption operation can be performed by a proxy entity that holds the necessary re-encryption keys.

Blockchain Integration:

- This module involves integrating the blockchain platform into the system architecture.
- It includes the selection of an appropriate blockchain platform that supports smart contracts and data storage.
- The blockchain is used to store encrypted data, access control policies, and transaction records related to data sharing activities.

Key Management:

- This module focuses on secure key management for encryption and re-encryption operations.
- It includes mechanisms for generating, distributing, and revoking encryption keys and re-encryption keys.

- Key management procedures should be designed to ensure the confidentiality and integrity of the keys.

User Interface and API:

- This module provides a user interface or application programming interface (API) for interacting with the system.
- It enables data owners and authorized entities to manage access control policies, request data access, and monitor data sharing activities.
- The user interface or API should be designed to be user-friendly and provide appropriate security controls.

Logging and Auditing:

- This module involves capturing and logging relevant information about data sharing activities.
- It includes recording details such as data access requests, re-encryption operations, and access control policy updates.
- The logs can be used for auditing, troubleshooting, and ensuring accountability.

Performance Optimization:

- This module focuses on optimizing the performance of the system.
- It includes techniques such as parallel processing, caching, and compression to improve the efficiency of encryption, re-encryption, and data retrieval operations.
- Performance optimization is crucial to ensure the system can handle the large volume of data generated by IoT devices.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

➢ System	:	Pentium i3 Processor
➢ Hard Disk	:	500 GB.
➢ Monitor	:	15’’ LED
➢ Input Devices	:	Keyboard, Mouse
➢ Ram	:	2 GB

SOFTWARE REQUIREMENTS:

➢ Operating system	:	Windows 10.
➢ Coding Language	:	JAVA.
➢ Tool	:	NetBeans 8.2
➢ Database	:	MYSQL

CONCLUSION:

The project aims to address the challenges of secure data sharing in the IoT ecosystem by leveraging the cryptographic capabilities of PRE and the decentralized nature of blockchain. It offers advantages such as enhanced security, transparent access control, tamper resistance, and auditability.

However, there are some important considerations and potential disadvantages to keep in mind. These include scalability challenges of blockchain, performance overhead of encryption and re-encryption operations, complexity of key management in a decentralized system, dependency on the security of the blockchain consensus mechanism, and addressing privacy concerns beyond data confidentiality.

To successfully implement this project, key modules or components need to be developed, including data encryption and key generation, access control and policy management, proxy re-encryption, blockchain integration, key management, user interface and API, logging and auditing, and performance optimization.

By carefully addressing these aspects and utilizing appropriate optimization techniques, a pRE-based secure data sharing system in the IoT context can be developed to ensure data confidentiality, integrity, and controlled access. Such a system can offer increased trust and security in the sharing of sensitive IoT data, paving the way for improved IoT applications and services in various domains.

FUTURE SCOPE:

Integration with Edge Computing: As IoT devices generate and process massive amounts of data at the edge of the network, integrating the PRE-based secure data sharing system with edge computing infrastructure can enhance efficiency and reduce latency. This integration can enable secure data sharing and access control closer to the data source, improving real-time decision-making and reducing the burden on centralized systems.

Interoperability and Standardization: In the IoT ecosystem, devices, platforms, and protocols vary widely. Future developments can focus on achieving interoperability and standardization to enable seamless integration of the pRE-based secure data sharing system with diverse IoT devices and platforms. This can facilitate widespread adoption and compatibility across different IoT deployments.

Privacy-Preserving Data Analytics: While PRE ensures data confidentiality during sharing, there is still potential for data correlation and privacy concerns during data analytics. Future advancements can focus on incorporating privacy-preserving data analytics techniques, such as differential privacy or secure multiparty computation, to protect the privacy of sensitive information while allowing meaningful data analysis and insights.

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. A. Shamir, “Identity-based cryptosystems and signature schemes,” inProc.Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984,pp. 47–53.

[3] Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. Int. J. Intell. Syst. Appl. 2018, 10, 40–48.

[4] Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. IEEE Access 2018, 6, 32979–33001.

[5] Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. In Advances in Organometallic Chemistry Volume 60; Elsevier BV: Amsterdam, The Netherlands, 2019; pp. 73–113.

[6] Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763– 768.

[7] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190.

[8] Yin, S.; Lu, Y.; Li, Y. Design and implementation of IoT centralized management model with linkage policy. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015; pp. 5–9.

[9] Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In Intelligent Sensing, Instrumentation and Measurements; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 123–149. 14. Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Nano Things. In Proceedings of the 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018), Barcelona, Spain, 3–5 August 2018; pp. 71–77.

[10]Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of Things: Opportunities & Challenges. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–6.