e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

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

Prof. Bharat Dhak[*1], Apurva Basule[*2], Arya Goswami[*3], Mujahid Khan[*4], Sahil Armarkar[*5]

[*1,2,3,4,5]Department Of Computer Science And Engineering, Priyadarshini JL College Of Engineering (RTMNU), Nagpur, India.

DOI : https://www.doi.org/10.56726/IRJMETS53208

ABSTRACT

In the world of IoT, sharing data securely is vital. This research presents a new way to do it using proxy Re Encryption (PRE) and blockchain technology. PRE helps owners share data without giving away their secrets, and blockchain ensures this process is secure and easy to track. Through simulations, this approach proves effective for real-world IoT use. It offers a safe and straightforward solution for data sharing in IoT. In our approach, a dynamic and efficient proxy Re Encryption scheme is implemented within the blockchain network. This scheme not only guarantees data confidentiality but also minimizes the computational overhead on resource-constrained IoT devices.

Keywords: Internet Of Things (IoT), Proxy Re-Encryption (PRE), Blockchain, Data Security, Data Sharing, Access Control, Privacy, Encryption.

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others.

The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data.A viable solution is to encrypt the data before outsourcing to the cloud servers.

Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner.

The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users.

II. LITERATURE REVIEW

Paper Name: A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain.

Author Name: Kwame Opuni-Boachie Obour Agyekum

Description: In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive

computations. Also, we make use of the features of information centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. image-based virtual try-on clothes application enhances the online shopping experience by providing users with a realistic and interactive way to try on clothes virtually, saving time and effort in physical dressing rooms.

Paper Name: Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing

Author Name: Ahsan Manzoor, Madhsanka LiyanageT

Description: Data is central to the Internet of Things (IoT) ecosystem. Most of the current IoT systems are using centralized cloud-based data sharing systems. Involvement of such a third party service provider requires trust from both sensor owner and sensor data user. Moreover, the fees need to be paid for their services. To tackle both the scalability and trust issues and to automatize the payments, this paper presents a blockchain based proxy re-encryption scheme. The system stores the IoT data in a distributed cloud after encryption. To share the collected IoT data, the system establishes runtime dynamic smart contracts between the sensor and the data user without the involvement of a trusted third party.

Paper Name: PROXY RE ENCRYPTION APPROACH TO SECURE DATA SHARING IN THE INTERNET OF THINGS BASED ON BLOCKCHAIN

Author Name: Srujana D, Jyothi T.

Description: Data sharing has developed as one of the most important aspects for the internet of things in cloud computing applications. Even though progress of technology is visually attractive but data security becoming a more problem because of its usage of data in inappropriate that leads a result in a variation of bad effects. To overcome this issue We delivered a proxy re-encryption method in this paper that exchanges data in the cloud in a safer way. Identity based encryption allows owners to store their threatened information to the cloud, while proxy reset encryption structure allows approved users to access the data. Due to the limited resources of Internet of Things devices availability, an edge device serves as an intermediary in order to handle demanding calculations. The foundation of our system concept is blockchain, a ground-breaking technology that permits decentralized data sharing.

Paper Name: Data Re-Encryption Approach to Secure Data Sharing using Blockchain

Author Name: Komal Varpe1 , Shraddha Umbarkar2 , Rohit Kalekar

Description: This paper proposes a Data Re-Encryption (DRE) approach to address security and privacy concerns in cloud-based data sharing using blockchain technology. The proposed approach uses smart contracts for access control and re-encryption, ensuring authorized users can access shared data. A trusted third party performs re-encryption without revealing the original data, and a consensus algorithm guarantees integrity. The DRE approach is evaluated through simulation, demonstrating scalability, efficiency, and security.

III. OBJECTIVE

1. To enhance the security and privacy of data exchanged in IoT networks.
2. To provide a secure and decentralized solution for sharing sensitive data in IoT environments.
3. Blockchain technology adds an additional layer of security by providing immutability, transparency, and decentralized control over data sharing.
4. This approach addresses the challenges of data privacy and security in IoT networks, enabling secure and trusted data sharing among IoT devices and stakeholders.

IV. METHODOLOGY

1. Problem Statement:

The problem revolves around the challenges and risks associated with data sharing in IoT ecosystems. These challenges include:

Privacy Concerns: IoT devices collect and transmit sensitive data, raising privacy concerns about unauthorized access and misuse.

Data Integrity: Ensuring the integrity of data during transmission and storage is crucial to prevent tampering or corruption.

Unauthorized Access: IoT networks are vulnerable to unauthorized access, posing risks to the confidentiality

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

and security of the data.

2. Design the Architecture:

System Components:

- IoT Devices: Sensors, actuators, and other smart devices that collect and generate data.
- Gateways: Devices that aggregate data from IoT devices and communicate with external networks.
- Blockchain Network: Distributed ledger technology for decentralized and tamper-resistant data storage.
- Proxy Re-Encryption Module: Software component responsible for encrypting and decrypting data using proxy re-encryption techniques.

Data Flow:

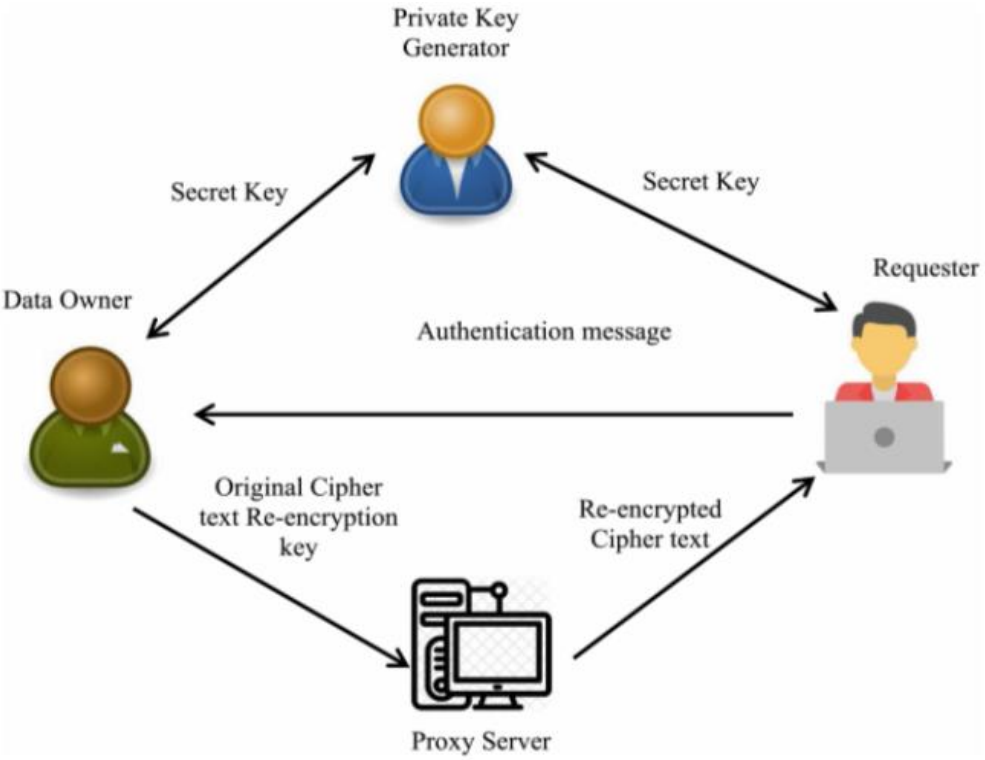
Data Collection: IoT devices collect data from the environment.

Data Encryption: Data is encrypted using proxy re-encryption techniques before transmission.

Data Transmission: Encrypted data is transmitted to the gateway.

Blockchain Storage: Encrypted data and transaction records are stored on the blockchain for decentralized and tamper-resistant storage.

Block Diagram:



3. Implementation Steps:

Implement Proxy Re-Encryption:

- Develop Proxy Re-Encryption Libraries: Implement proxy re-encryption algorithms in software libraries compatible with IoT devices.
- Key Management: Design a secure key management system to generate and distribute public/private keys to IoT devices.
- Encryption/Decryption Process: Implement algorithms for encrypting data with the recipient's public key and decrypting data with the recipient's private key.
- Authentication Mechanisms: Develop authentication mechanisms to ensure that only authorized parties can decrypt the data.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

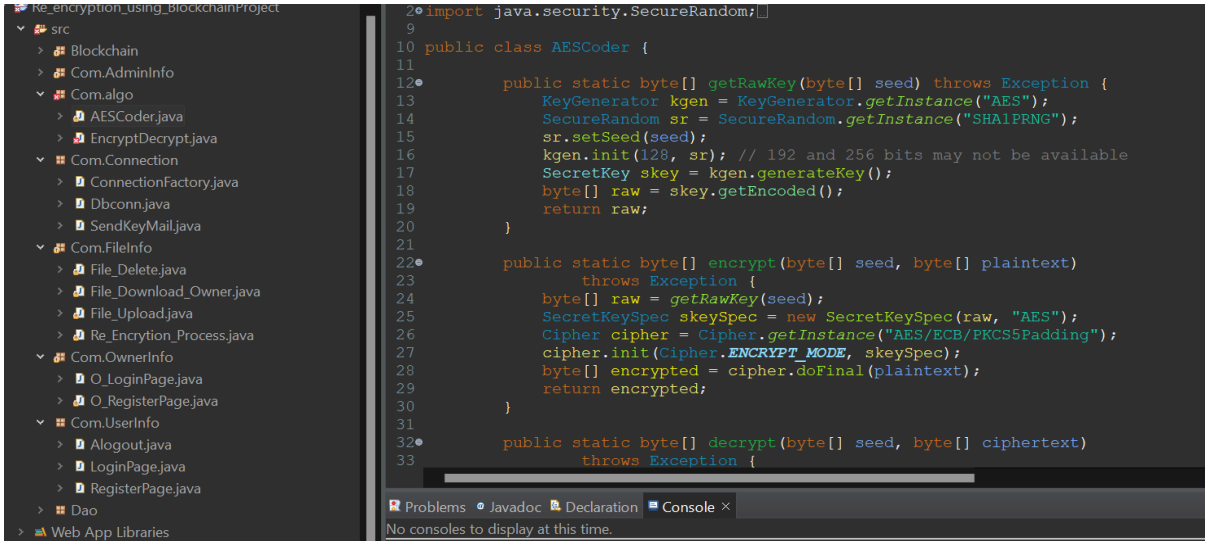


Fig 1: Encryption with AES

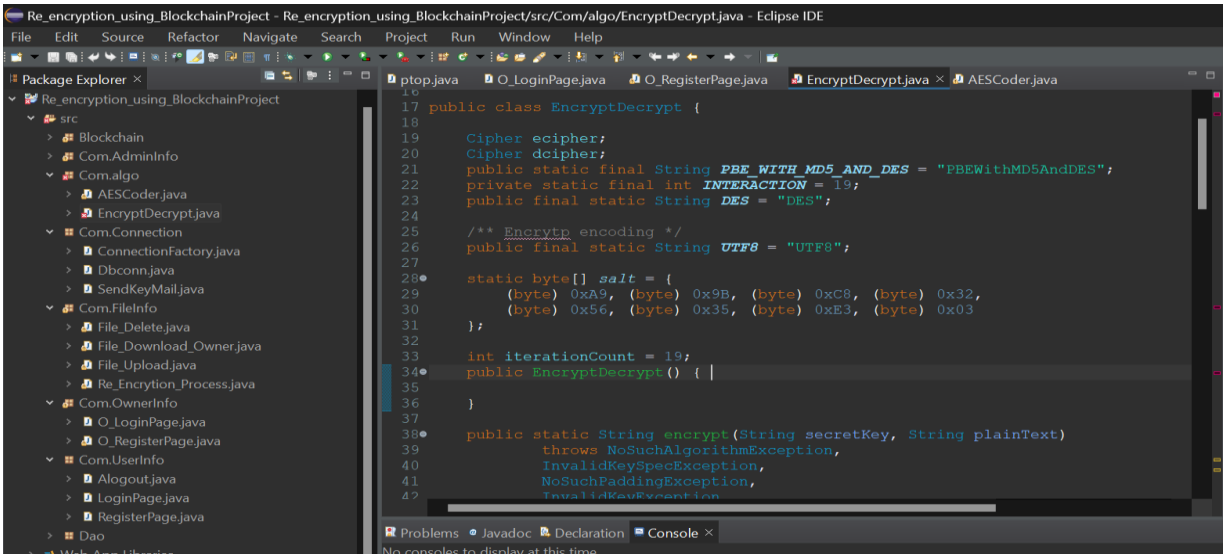


Fig 2: Decryption with MD5 and DES

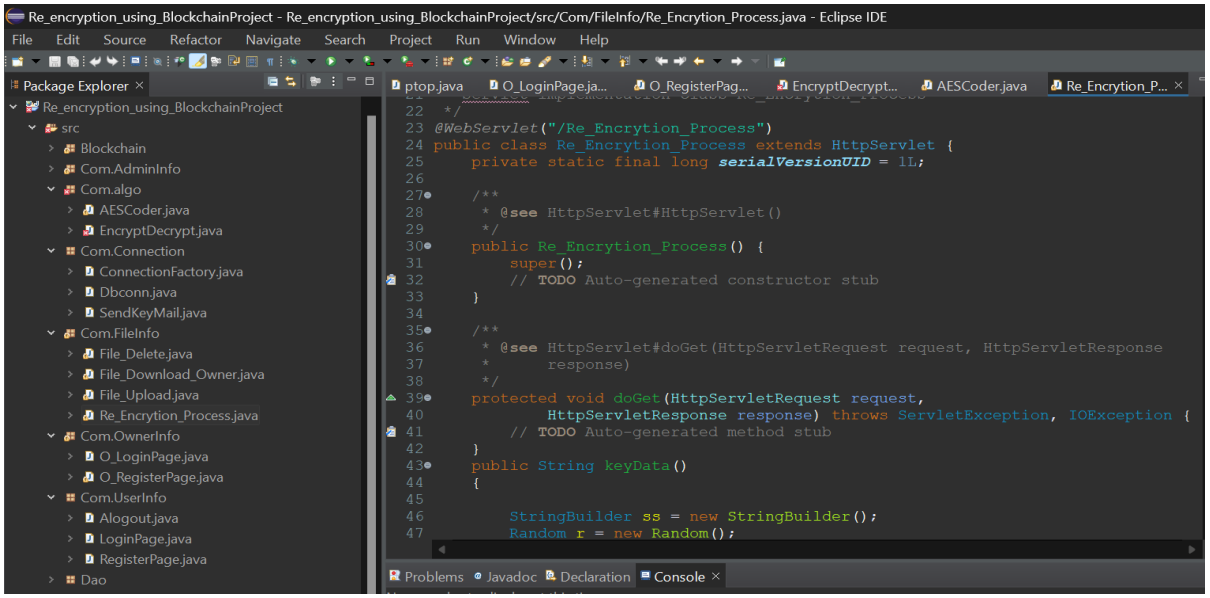


Fig 3: Re-encryption key generation

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

4. Utilize Blockchain for Data Management:

- Blockchain Network Setup: Configure and deploy a blockchain network with multiple nodes distributed across the IoT environment.
- Smart Contract Development: Write smart contracts to define data storage, access control, and auditability rules on the blockchain.
- Encrypted Data Storage: Encrypt data before storing it on the blockchain to maintain confidentiality.
- Transaction Recording: Record transactions related to data sharing, access requests, and permissions on the blockchain for transparency and traceability.

5. Establish Smart Contracts:

- Rule Definition: Define rules and permissions for data sharing in smart contracts.
- Access Control Policies: Implement access control policies based on predefined conditions, such as user roles or data sensitivity.

6. Test and Evaluate:

- Performance Testing: Measure the performance of the system in terms of data encryption/decryption speed, transmission latency, and resource utilization.
- Scalability Testing: Evaluate the system's ability to handle a large volume of data and concurrent access requests as the IoT network scales.
- Security Audits: Conduct security audits to identify vulnerabilities and assess the robustness of the system against potential attacks.

7. Deployment and Monitoring:

- Real-World Deployment: Deploy the system in a real-world IoT environment, such as a smart city or industrial IoT deployment.
- Continuous Monitoring: Implement monitoring tools to track system performance, detect anomalies, and respond to security threats promptly.
- Update and Maintenance: Regularly update the system with patches and security fixes to address emerging vulnerabilities and ensure long-term security.

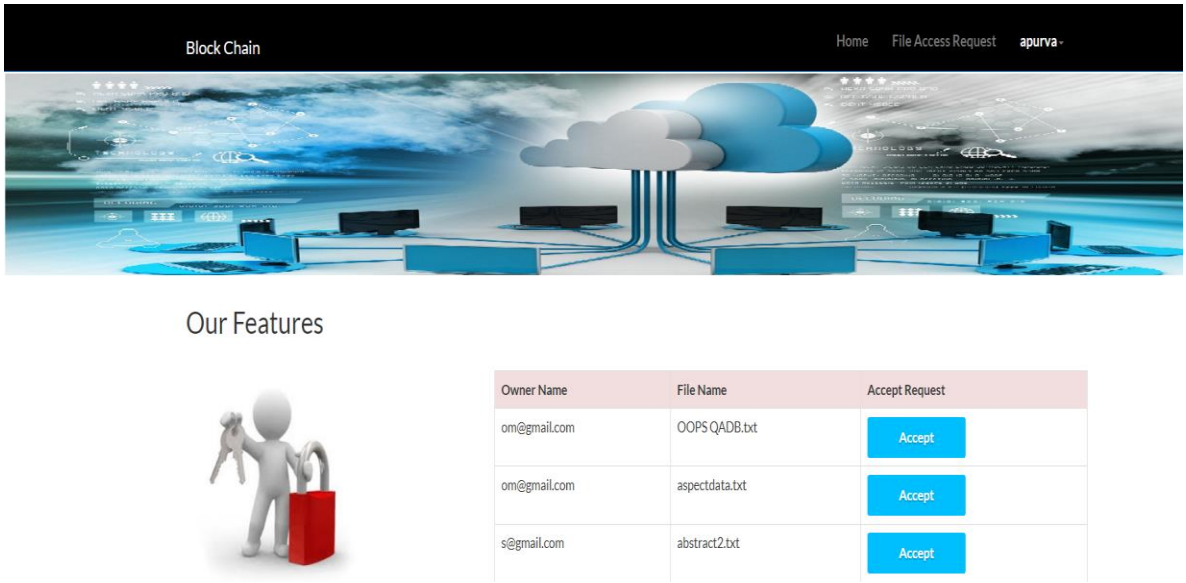


Fig 4: Data user handling file access request

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

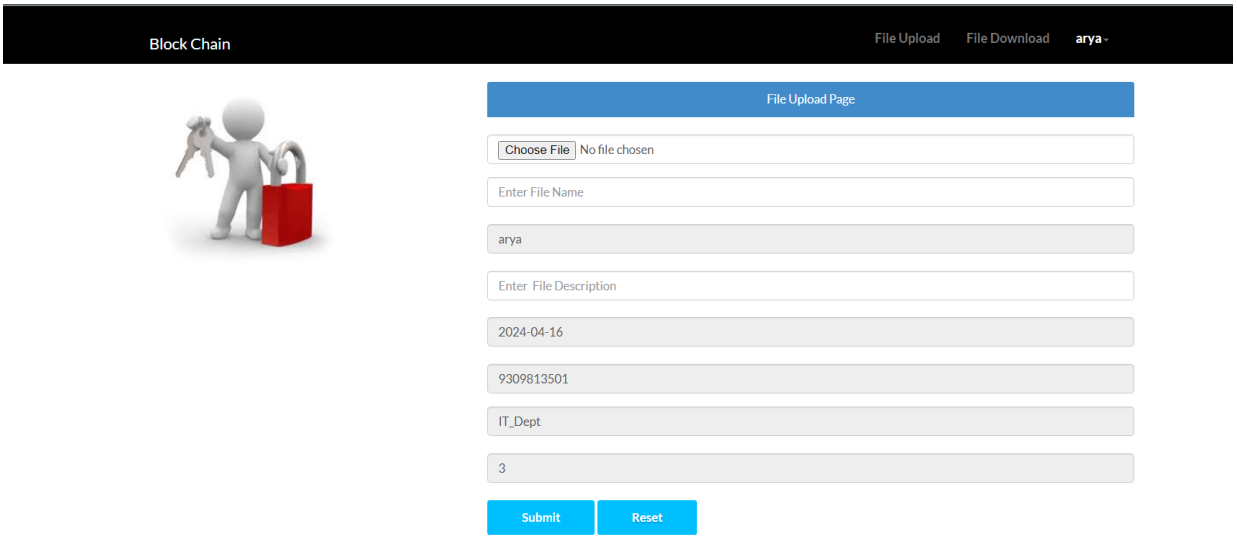


Fig 5: Data owner uploading file

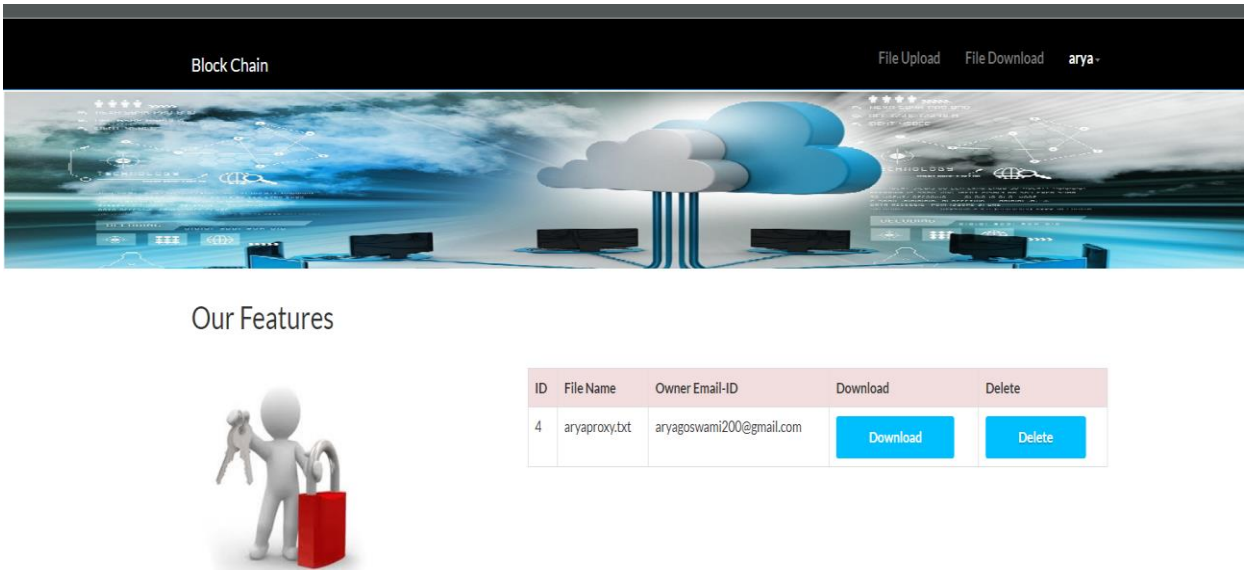


Fig 6: Data owner file download & delete control

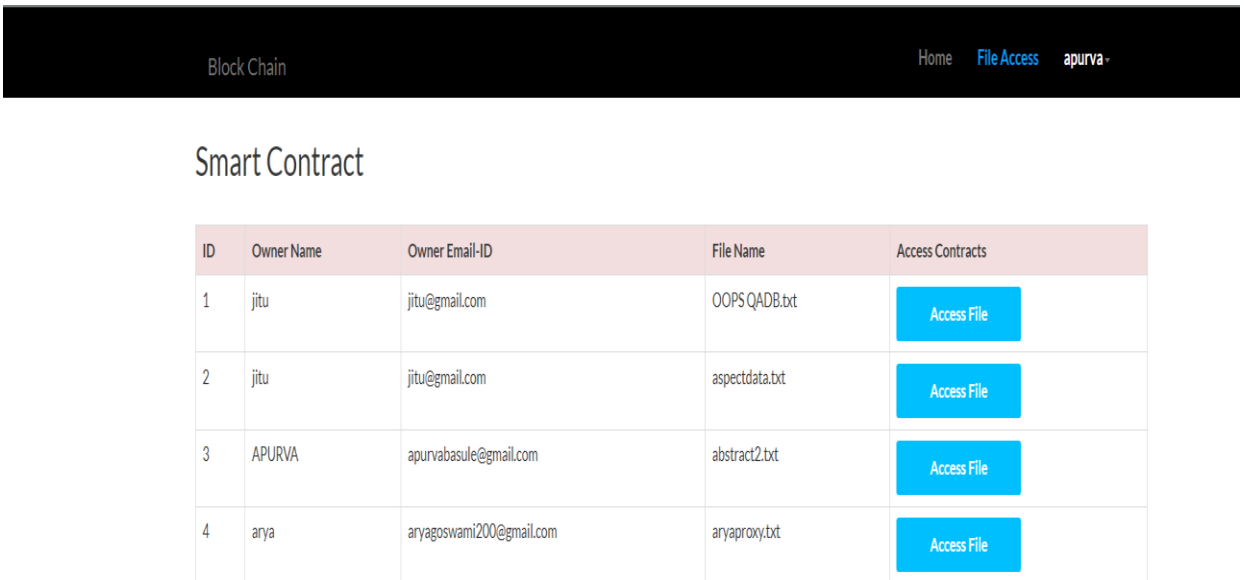


Fig 7: Service provider interface

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

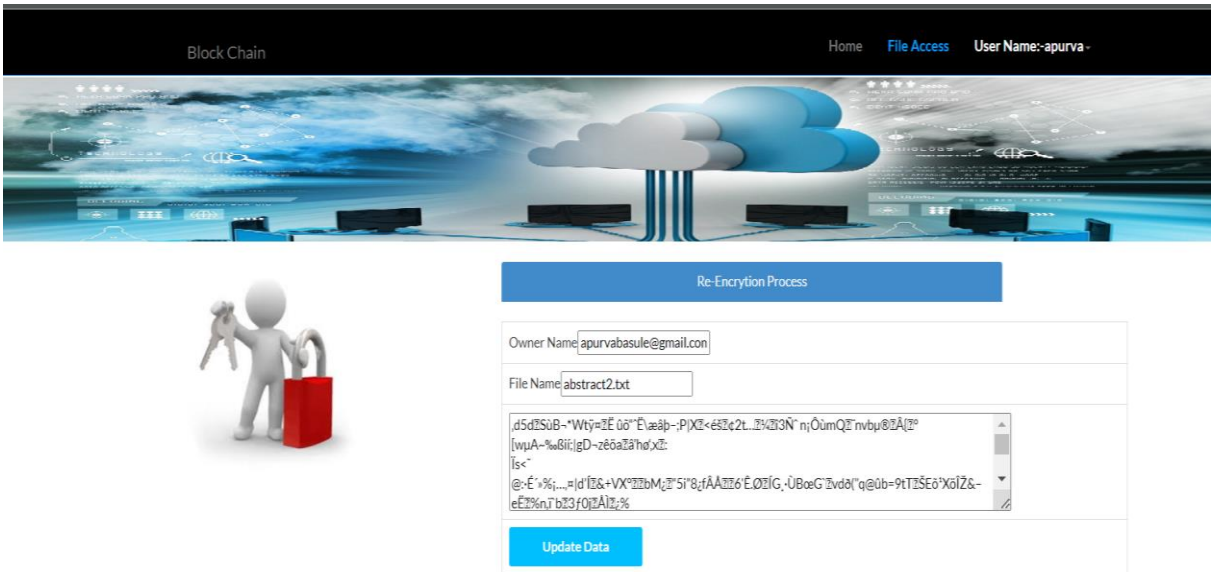


Fig 8: Re-encryption using proxy server

V. TOOLS AND PLATFORMS USED

TOOLS:

1. Eclipse:

Eclipse is an integrated development environment (IDE) used for software development. It provides a platform for writing, editing, and debugging code in various programming languages. Eclipse offers a range of features and plugins that assist developers in creating applications efficiently. It is widely used in the software development community and supports multiple programming languages such as Java, C++, Python, and more. Eclipse is known for its user-friendly interface and extensive customization options, making it a popular choice among developers.

2. JDK:

The Java Development Kit (JDK) is a software package that provides the necessary tools and libraries for developing Java applications. It includes the Java Runtime Environment (JRE), which allows you to run Java programs, as well as the Java compiler, debugger, and other development tools. The JDK is essential for writing, compiling, and running Java code. It also provides various APIs and libraries that developers can use to build robust and scalable Java applications. Overall, the JDK is a crucial component for Java developers as it enables them to create and deploy Java applications effectively.

PLATFORMS USED:

1. Java:

Java is a popular programming language that is widely used for developing a variety of applications, including web and mobile applications, desktop software, and enterprise systems. It was created by Sun Microsystems and is now owned by Oracle Corporation. Java is known for its platform independence, meaning that Java programs can run on different operating systems without the need for recompilation. It is also highly regarded for its robustness, security features, and extensive library of reusable code. Java is used by millions of developers worldwide and has a strong presence in the software industry.

VI. ADVANTAGES AND APPLICATION

6.1 ADVANTAGES:

1. Proxy Re-Encryption allows for secure data sharing while maintaining the privacy of sensitive information.
2. It enables authorized parties to access encrypted data without exposing the original data or decryption keys.
3. Blockchain technology ensures the integrity of shared data by creating an immutable and transparent record of transactions.
4. Proxy Re-Encryption adds an extra layer of security by encrypting data in transit, reducing the risk of unauthorized access or tampering.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

5. Proxy Re-Encryption can facilitate efficient and scalable data sharing in IoT environments. It enables
6. data to be securely shared among multiple parties without the need for each party to hold a copy of the original data, reducing storage and bandwidth requirements.
7. By leveraging blockchain technology, the Proxy Re-Encryption approach provides a decentralized and transparent framework for data sharing.
8. It enhances trust among participants by enabling them to verify the integrity and authenticity of shared data.

6.2 APPLICATIONS:

1. **Healthcare:** Proxy Re-Encryption can be used to securely share patient health data among healthcare providers, ensuring privacy and data integrity while enabling collaborative care and research.
2. **Supply Chain Management:** By implementing Proxy Re-Encryption in the IoT-based supply chain, sensitive data such as product information, shipment details, and transaction records can be securely shared among stakeholders, preventing unauthorized access and ensuring transparency.
3. **Smart Home Systems:** Proxy Re-Encryption can enhance the security and privacy of data exchanged between IoT devices in smart homes. It enables secure sharing of data such as sensor readings, video feeds, and personal information among authorized devices and users.
4. **Energy Grid Management:** Proxy Re-Encryption can be applied to secure data sharing in IoT-based energy grid management systems. It allows for secure exchange of data between smart meters, energy providers, and grid operators, ensuring privacy and preventing unauthorized access to energy consumption data.
5. **Industrial IoT:** Proxy Re-Encryption can be used to secure data sharing in industrial IoT applications, such as remote monitoring and control of industrial processes. It ensures the confidentiality and integrity of sensitive data, protecting against unauthorized access or tampering.

VII. CONCLUSION

In this study, we addressed the challenges of secure data sharing in IoT environments by proposing a solution integrating proxy re-encryption and blockchain technology. Our methodology ensures confidentiality, integrity, and access control in data sharing processes.

Through implementation and testing, we demonstrated the effectiveness of our approach in real-world scenarios. By adopting our solution, stakeholders can enhance the security of their IoT systems and enable trustworthy data sharing practices.

Moving forward, further research can focus on optimizing the proposed methodology and exploring new applications in diverse IoT domains.

ACKNOWLEDGEMENT

The success of any work depends on the efforts of many individuals. We would like to take this opportunity to express our deep gratitude to those who extended their support and have guided us to complete this project work.

We wish to express our sincere and deepest gratitude to our guide Prof. Bharat Dhak for his invaluable and unique guidance. We would also like to thank him for the constant source of help, inspiration and encouragement in the successful completion of the project. It has been our privilege and pleasure to work under her expert guidance.

We are sincerely thankful to Dr. A. M. Shende (Principal, PJLCE) for his valuable assistance and mentorship, which have played a significant role in the successful completion of this project. His dedication to fostering academic excellence has been a constant source of inspiration.

We like to thank Prof. S. S. Bawankule (HOD) for providing us the necessary information about the topic and for providing us the necessary help and facilities we needed.

We would like to express our heartfelt gratitude to the following contributors and projectees who actively participated in the development of the project:

Apurva Basule, Arya Goswami, Mujahid khan, Sahil Armarkar.

VIII. REFERENCES

[1] A. Rajakaruna. P. Porambage. A. Manzoor. M. Liyanage. A. Gurtov, and M. Ylianttila. "Enabling end-to-end secure connectivity for low-power iot devices with uavs." in in 2m1 Workshop on Intelligent Computing and Caching at the Network Edge at IEEE Wireless Communications and Networking Conference (WCNC). 2019.

[2] A. Braeken. M. Liyanage. and A. D. Jurcut. "Anonymous lightweight proxy based key agreement for iot (alpka)." Wireless Personal Communications. pp. 1720. 2019.

[3] S.Niu, L. Chen, J. Wang, and F. Yu, "Electronic health record sharing scheme with searchable attribute based encryption on blockchain," IEEE Access, vol. 8, pp. 7195–7204, 2019.

[4] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.

[5] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicles," Comput. Netw., vol. 145, pp. 219–231, Nov. 2018.

[6] T. Kumar. P. Porarnbage. I. Ahmad. M. Liyanage. E. Harjula. and M. Ylianttila. "Securing gadget-free digital services." Computer. vol. 51. no. 11. pp. 66777. 2018.

[7] M. Singh. A. Singh. and S. Kim. "Blockchain: A game changer for securing iot data." in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE. 2018. pp. 51755.

[8] J. Lin. W. Yu. N. Zhang. X. Yang. H. Zhang. and W. Zhao. "A survey on the internet of things: Architecture. enabling technologies. security and privacy. and applications." IEEE Internet of Things Journal. vol. 4. n0. 5. pp. 112571142. 2017.

[9] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," IEEE Trans. Ind. Inform., vol. 15, no. 9, pp. 5099–5108, Jan. 2019.

[10] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, "A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing," IEEE Access, vol. 7, pp. 62785–62793, 20.