Secure File Sharing System

*PROJECT PROPOSAL

Sameer Khan
Dept. of computer science
BGSU
Bowling Green, OHIO, USA
Sameerk@bgsu.edu

Abstract—**This project proposes a Secure File Sharing System leveraging Proxy Re-Encryption (PRE) to address the inefficiencies and security concerns of traditional encryption methods in data sharing. PRE enables the secure sharing of encrypted data without revealing encryption keys or requiring a trusted third party, by allowing a third-party service to re-encrypt data for specific recipients based on public re-encryption keys. This approach significantly streamlines the sharing process, reduces resource consumption, and maintains high levels of security and privacy. The system aims to provide an innovative solution to the challenges of secure digital communication and data exchange, emphasizing efficiency, security, and user privacy.**

I. Introduction

Sharing files securely in today's digital world can be challenging. Traditional encryption methods offer robust security but often fall short in terms of usability and flexibility, particularly when it comes to sharing encrypted data with multiple recipients. This proposal introduces a Secure File Sharing System that leverages Proxy Re-Encryption (PRE) and cloud storage to address these challenges. By combining the security benefits of encryption with the convenience of cloud-based storage, the system provides a solution that is both secure and user-friendly.

The proposed system utilizes PRE to facilitate the secure sharing of encrypted files without the need for direct key exchange or exposing sensitive data. Files encrypted by the data owner are uploaded to a cloud storage platform, from where they can be securely shared with designated recipients through re-encryption keys. This approach not only enhances security by minimizing the risk of key compromise but also simplifies the process of file sharing, making it more efficient and accessible. The integration of PRE with cloud storage presents a novel solution to the longstanding problems of digital data exchange, offering a practical pathway to secure, private, and convenient file sharing in the digital age.

II. Related Work

New technologies in cryptography have made it easier to securely share data, specifically in the context of the Internet of Things (IoT) and cloud computing. The proposed Secure File Sharing System using Proxy Re-Encryption (PRE) is built upon three significant contributions in this domain, which serve as its foundation.

- **Opuni-Boachie et al.** introduced a proxy re-encryption approach to secure data sharing in IoT environments, they used identity-based encryption and blockchain technology to encrypt the data and store it in the cloud. A proxy server acts as an intermediary to grant access only to authorized users. By using blockchain, the method ensures decentralized access control and enhances data confidentiality, integrity, and security. [1]
- **Pareek and Purushothama B.R.** presented a key-aggregate proxy re-encryption (KAPRE) system that emphasizes the efficiency of predefined access control policies for outsourced data. Their work introduces a novel cryptographic primitive that allows someone to decrypt the data without the need for secure transmissions, addressing the dynamic environment challenges like the non-revocability of aggregate keys. [2]
- **Manzoor et al.** developed a blockchain-based marketplace for IoT data sharing that employs an efficient PRE scheme for secure and anonymous data transfer. This approach eliminates the need for a trusted third party by establishing dynamic smart contracts directly between data producers and consumers. The system's efficiency is further enhanced by a highly effective PRE scheme, ensuring data visibility only to the owner and authorized users specified in the smart contract. The performance of this hybrid system was analyzed using both permissionless and permissioned blockchain technologies, highlighting its practical applicability and security. [3]

III. Proposed Approach

The Secure File Sharing System aims to address the inefficiencies and security concerns associated with traditional encryption methods for data sharing, specifically targeting the challenges of key management and the risk of data exposure. By leveraging Proxy Re-Encryption (PRE) and integrating it with cloud storage, the proposed system introduces an innovative, secure, and efficient solution for sharing encrypted files.

A. System Architecture

The system architecture is built on two core technologies: Proxy Re-Encryption (PRE) and cloud storage. The process begins when a data owner encrypts a file using their private

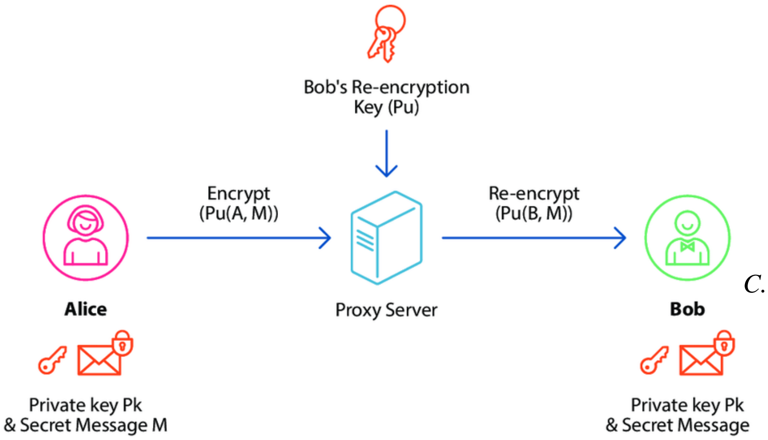
Bob's Re-encryption Key (Pu)
Encrypt (Pu(A, M))
Re-encrypt (Pu(B, M))
Alice
Proxy Server
Bob
Private key Pk & Secret Message M
Private key Pk & Secret Message

Fig. 1. Overview of proxy re-encryption scheme. [4]

key and uploads this encrypted file to a cloud storage service. When sharing the file with a recipient, instead of sharing the decryption key or re-encrypting the file for each recipient, the data owner generates a re-encryption key. This key enables a third-party service (the proxy) to convert the encrypted file from being decryptable by the data owner's key to being decryptable by the recipient's public key, without the proxy ever knowing the content of the file.

Example (shown in Fig.1)
The system architecture incorporates three principal entities:

- **Data Owner (Alice):** Initially, Alice encrypts her file using her private key (Pk) and a secret message (M). The encrypted file is denoted as Enc(Pu(A),M), where Pu(A) is Alice's public key, and M is the message or file content.
- **Proxy Server:** Once the file is encrypted, it is uploaded to a cloud-based proxy server. The proxy server is the pivotal component that facilitates the PRE process without ever decrypting the file.
- **Recipient (Bob):** To share the encrypted file with Bob, Alice provides the proxy server with Bob's re-encryption key (Pu). The proxy server uses this key to re-encrypt the file for Bob, transforming it into Re-Enc(Pu(B),M), which Bob can decrypt using his private key.

B. Key Features

- **Secure Encryption and Re-Encryption:** The initial encryption and subsequent re-encryption ensure that at no point is the file decrypted in transit or at rest on the proxy server, maintaining the integrity and confidentiality of the data.
- **No Trusted Third Party Required:** Unlike traditional systems that rely on a trusted third party to facilitate key exchange or data sharing, our system ensures that the encrypted data can be re-encrypted and shared without exposing sensitive information to any intermediary.
- **Efficient Key Management:** By using PRE (Proxy Re-Encryption), there is no longer a need for using multiple encryption keys for different recipients. A single instance of encrypted data can be securely shared with multiple recipients, simplifying key management.
- **User Privacy:** The system is designed to safeguard user privacy by ensuring that data owners have complete control over who has access to their data. The re-encryption keys can be generated and revoked as needed, providing dynamic access control.

C. Timeline

- **Project Initialization:** March 5 - March 9, 2024
Project kickoff, initial setup, and resource allocation.
- **System Design and Planning:** March 10 - March 19, 2024
Detailed system architecture design and planning phase, including selection of cryptographic libraries and cloud storage providers.
- **Development of Encryption Mechanisms:** March 20 - March 30, 2024
Implementation of encryption and proxy re-encryption algorithms.
- **Integration with Cloud Storage:** March 31 - April 6, 2024
Integration of the encryption mechanisms with the chosen cloud storage solution.
- **User Interface Development:** April 7 - April 11, 2024
Development of the front-end interface for user interaction with the system.
- **Testing and Security Evaluation:** April 12 - April 18, 2024
Comprehensive testing of the system for security vulnerabilities and performance issues.
- **Final Review and Documentation:** April 19 - April 21, 2024
Final review of the project to ensure all requirements are met and completion of project documentation.

TABLE I
PROJECT TIMELINE

Milestone	**Date**
Project Initialization	March 5 - March 9, 2024
System Design and Planning	March 10 - March 19, 2024
Development of Encryption Mechanisms	March 20 - March 30, 2024
Integration with Cloud Storage	March 31 - April 6, 2024
User Interface Development	April 7 - April 11, 2024
Testing and Security Evaluation	April 12 - April 18, 2024
Final Review and Documentation	April 19 - April 21, 2024

References

[1] K. O. -B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, ”A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain,” in IEEE Systems Journal, vol. 16, no. 1, pp. 1685-1696, March 2022, doi: 10.1109/JSYST.2021.3076759.

[2] Gaurav Pareek, Purushothama B.R., KAPRE: Key-aggregate proxy re encryption for secure and flexible data sharing in cloud storage, Journal of Information Security and Applications, Volume 63, 2021, 103009, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2021.103009.

[3] Ahsan Manzoor, An Braeken, Salil S. Kanhere, Mika Ylianttila, Madhsanka Liyanage, Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain, Journal of Network and Computer Applications, Volume 176, 2021, 102917, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102917.

[4] Towards Secure Searchable Electronic Health Records Using Consortium Blockchain - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Overview-of-proxy-re-encryption-scheme-fig2-360118293, accessed 3 Mar 2024.