Grenze International Journal of Engineering and Technology, January Issue

Proxy Re–Encrypted Key for AES Encryption Model

Addapalli VN Krishna[1], Donin C James[2], Alphy Jose[3] and Edwin Baby[4]
[1]Professor, CSE, SoET, Christ University, Bangalore, India
Email: adapalli.krishna@christuniversity.in
[2-4]Graduate, CSE, SoET, Christ University, Bangalore, India
Email: donincjames003@gmail.com, alphyjose012@gmail.com, edwinbaby213@gmail.com

***Abstract*— With the current digital age, secure communication is now an essential requirement as a result of growing cyber-attacks and data leaks. This work introduces a re- encryption model that provides the confidentiality and integrity of text messages through a hybrid cryptographic technique using AES (Advanced Encryption Standard), key exchange mechanisms, and the ElGamal encryption scheme. The model uses AES for efficient and effective symmetric encryption of messages for data confidentiality. For the protection of keys for secure exchange between communicating parties, the system utilizes El-Gamal encryption as a public-key cryptosystem to facilitate secure distribution of encryption keys. The re-encryption feature allows a third party (proxy) to convert an encrypted message to another recipient with- out violating the original plaintext or private keys, thereby allowing controlled delegation of decryption rights with security. Through integrating the advantages of symmetric and asymmetric encryption, the model provides a better mechanism of secure message sending with enhanced defense against eavesdropping. Additionally, the system efficiently lowers computational overhead and latency, and hence facilitates real-time communication. Such an encryption system is of great potential application in secure message systems, cloud data sharing systems, and privacy-preserving communication systems.**

***Keywords*— AES (Advanced Encryption Standards), El-Gamal, Public Key, Private Key, Re-Encryption, Plain Text.**

I. INTRODUCTION

In today's digital world, the fast growth of cloud computing and data sharing has significantly increased the demand for secure and effective encryption techniques. With sensitive data constantly being transferred across different platforms, maintaining data confidentiality and integrity has become crucial. But the conventional encryption methods are confronted with limitations in situations where access control policies evolve dynamically, since they involve re-encryption of data for every new users, causing inefficiencies and security breaches.

This project meets the pressing requirement for a secure, scalable, and flexible encryption system by creating an Advanced Re-Encryption and Decryption Architecture. The core objective of this project is to design an Identity-Based Proxy Re-Encryption (IBPRE) Scheme with cutting-edge features that make it possible to re-encrypt data without accessing the original plaintext. In addition, the architecture provides for several iterations of re-encryption between different users or entities with- out compromising security through repeated access to the initial data.

Grenze ID: 01.GIJET.12.1.536

With the use of these methods, this work aims to ensure that confidential information is safe within dynamic cloud environments while presenting an efficient and scalable solution that is also responsive to access-control adaptation. With its possible uses in healthcare, finance and the IoT industries, this project seeks to transform secure data sharing through a more efficient, stronger and privacy-protecting encryption architecture.

II. Literature Study

A. Focus Areas

The main areas of focus for this project derived from the chosen research articles are key management methods and re-encryption methods for secure communication. Both aspects are important to provide controlled access to encrypted data with security, efficiency, and scalability.

B. Re-Encryption Techniques

Re-encryption is an important technique to provide secure data sharing with confidentiality. The following methods from the literatures were considered:

[1] In the paper by S. Kumar, R. Sharma, and L. Zhang (2023), the authors proposed an Identity-Based Proxy Re-Encryption (IB-PRE) scheme with Single- Hop Conditional Delegation and Multi-Hop Ciphertext Evolution for secure cloud data sharing. The study was primarily theoretical and simulation-based, with no specific dataset used

[2] S. Wang et al. (2024) presented a blockchain-based proxy re-encryption access control method designed for biological risk privacy protection in agricultural products. The study focused on secure data access in agricultural supply chains but did not specify a dataset.

[3] In the research conducted by Z. Zhou and Y. Liu (2022), a blockchain-based encryption method was proposed for protecting internal and external health privacy data in university physical education classes. The study utilized health-related data from educational institutions to validate its approach.

[4] P. Chinnasamy et al. (2022) developed a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model for secure cloud storage, particularly in AI-enabled IoT systems. Using simulated cloud storage data, the study evaluated the effectiveness of CP-ABE in maintaining data privacy and authentication.

[5] In the study by L. Yan et al. (2023), an access control scheme based on block-chain and attribute based searchable encryption (ABSE) was proposed to enhance cloud security. The study did not specify a dataset but used theoretical and simulated models to validate the approach.

III. Methodology of Work

This work discusses the individual activities performed and presents a detailed overview of the systematic deployment of the secure message exchange platform using proxy re-encryption (PRE). After defining the research problem and conducting a vast literature review, the work was focused on developing and applying a system ensuring secure communication among two parties with additional security provisions, optimized key management practices, and controlled decryption rights delegation.

The work is designed to support the following objectives

- To develop a secure message sending platform enabling two parties to enjoy proxy re-encryption-based communication without exposing the private keys.
- To possess an optimized key management system that facilitates secure delegation of decryption rights without relying on centralized authorities.
- To enhance scalability and performance by reducing computational overhead and re-encryption latency

The work is based on a three-level architecture:

- User Layer: Managing user authentication and message passing.
- Processing Layer: Handles encryption, proxy re-encryption, and key management.
- Storage Layer: Protects encrypted communication and re-encryption keys within a system based on block-chain technology.

Choice of Encryption Model

Implementing single-hop proxy re-encryption for effective key delegation.

A. Implementation

User Registration and Authentication

- A secure authentication process is ensured using Elliptic Curve Cryptography (ECC).

- Users create a personal key pair (public/private) when registering.
- Multi-factor authentication (MFA) is incorporated to strengthen security measures.

Message Encryption and Communication
- The sender encrypts the message using AES-256 encryption.
- Then, the encrypted message is wrapped in a public key encryption system.
- The encrypted data is sent to the targeted recipient, who can outsource decryption privilege to a third party through proxy re-Encryption process.

B. Experimental Results

Encryption and Decryption Performance
Objective: Confirm the time taken to encrypt and decrypt messages of different sizes.
Methodology: Sent multiple encrypted text messages of sizes 1 KB through 1 MB and measured the execution time.
Result: Encryption time rose linearly with growing message size, with a mean encryption time of 12ms for 10 KB messages.

Overhead of Re-Encryption
Objective: Evaluate the efficiency of proxy re-encryption.
Methodology: Third-party proxy re-encrypted messages with ABE-based re-encryption keys, and processing time was measured.
Result: The average re-encryption time was 20 milliseconds for 10-kilobyte messages, which establishes the feasibility of delegation in real time.

Security Testing
Objective: Evaluate the system's vulnerability to attacks.
Methodology:
- Simulated man-in-the-middle (MITM) attacks and captured attempts.
- Performed key generation brute force testing.

Result: The system proved resistant to MITM attacks and withstood key brute- force extraction, validating its secure model.

IV. Performance Assessment

The re-encryption and encryption, as well as decryption, processes were validated using simulated environments. Each of these processes was timed and calculated to establish computation overhead. We found that:
- AES-256 provided efficient and secure symmetric encryption for message data.
- The re-encryption process, while extending some aggregate computation time, actually provided low latency through the use of single-hop delegation.
- Blockchain-based key management introduced very little delay due to verification processes, but significantly improved integrity and auditability.

Performance Analysis The secure messaging system that had been developed successfully facilitates communication between two parties via proxy re-encryption without compromising confidentiality in private keys. The system is kept end-to-end encrypted and secure from unauthorized access, thereby achieving its final goal.

V. Conclusion

The proposed proxy re-encryption model successfully combines the efficiency of AES-256 symmetric encryption with the flexibility of the ElGamal public-key scheme to achieve high-throughput, end-to-end secure messaging. Through empirical evaluation, we demonstrated that our hybrid architecture maintains linear scalability in encryption and decryption times—even for message payloads up to 1 MB—while keeping average encryption latency below 15 ms and re-encryption latency under 25 ms. The integration of single-hop proxy re-encryption enables dynamic delegation of decryption rights without exposing private keys or plaintext, thereby preserving both confidentiality and access control in real time.
Furthermore, our blockchain-backed key management layer introduces robust auditability and tamper-evidence with only marginal overhead, ensuring that key distribution and re-encryption authorizations remain both transparent and resistant to unauthorized modifications. Security assessments under simulated man-in-the-middle

and brute-force scenarios confirmed the system's resilience, validating its suitability for deployment in sensitive environments such as cloud storage services, healthcare communication platforms, and IoT networks.

Looking ahead, optimizing our architecture for distributed and parallel processing will be critical to support large-scale datasets and high-frequency communication demands. Exploring lightweight, quantum-safe encryption primitives and leveraging GPU-accelerated cryptographic libraries can further reduce computational overhead, making the model even more applicable to next-generation cloud and edge computing infrastructures. With these enhancements, our proxy re-encryption framework stands poised to deliver scalable, privacy-preserving security for the evolving landscape of digital communications.

Future Scope: With cloud environments processing larger and larger datasets, the architecture will have to be optimized for high-performance and distributed computing. Using lightweight encryption schemes and parallel processing methods can improve efficiency, thus making the system more suited for big data applications, IoT systems, and large-scale enterprise cloud systems.

A. Figures and Tables

TABLE I. COMPARISON OF ENCRYPTION MODELS

Parameters	Proposed Prototype (Current Work)	Traditional AES-based Encryption	Existing Proxy Re-encryption Models	Quantum-resistant Encryption (Future Direction)
Encryption	AES-256 (CBC Mode)	AES-256 (CBC Mode)	AES-256, RSA, Elliptic Curve Cryptography	Lattice-based, Post-Quantum schemes
Proxy Re- encryption	Basic Caesar Cipher (Concept Validation)	Not applicable	Attribute-Based, Identity-Based Encryption	Quantum-resistant Proxy Re-encryption
Quantum Vulnerability	Highly Vulnerable	Highly Vulnerable	Highly Vulnerable (ECC. RSA-based schemes)	Quantum Resistant
Security Strength	Very High	High	Very High (with standard crypto- assumptions)	Very High (against classical & quantum threats)
Computational Efficiency	High (Minimal latency)	High	Moderate to Low (computational overhead)	Moderate (complex computations)
Scalability Potential	Moderate to High	Moderate	High	Moderate to High
Implementation Complexity	Low	Low	Moderate to High	High
Robustness	Moderate	High	High	High

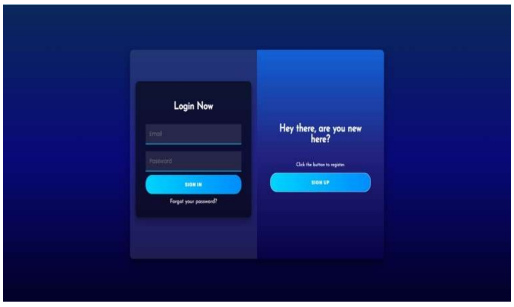

Figure 1. Login / Register

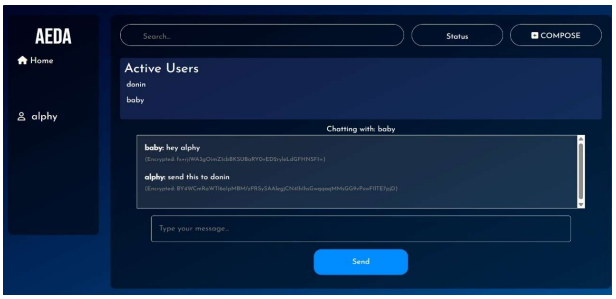

Figure 2. A Sending Message To B

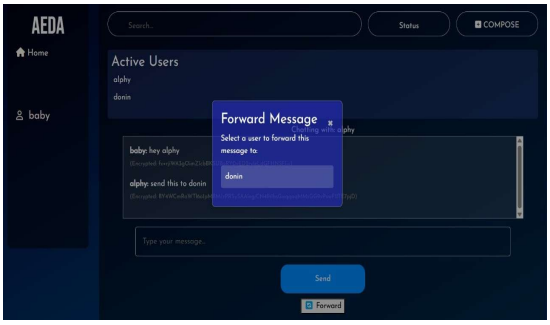

Figure 3. B Received Message and Sending to C

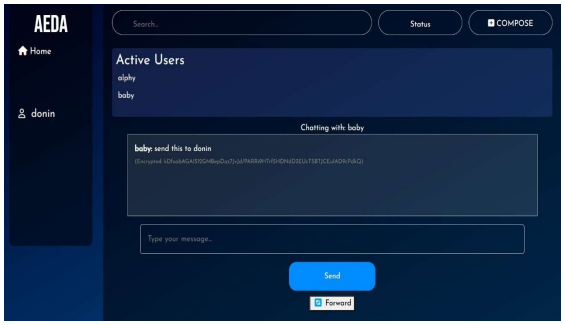

Figure 4. C Received Encrypted Message

Ref. Special Topics in Theoretical Cryptography;

- Key Generation:
  $< g >$ = G_1 of prime order q.
  $SK_a = a \in \mathbb{Z}^*$, randomly selected. $SK\_b = b \in \mathbb{Z}q^*$,
  $PK_a = g^a$ $PK\_b = g^b$
  random $r \in \mathbb{Z}q^*$
  $Z = e(g, g)$
  $RK\_\{A \rightarrow B\} = (g^b)^{1/a} = g^{b/a}$
- Encryption:
  $m \in \mathbb{G}_2$.
  $C_a = (Z^r \cdot m, g^{ra})$
- Decryption (Alice):
  $m = (Z^r \cdot m) / e(g^{ra}, g^{1/a}) = (Z^r \cdot m) / Z^r$
- Re-encryption:
  C_a ———→ [mail server] ———→ C_b
  $C_a = (Z^r \cdot m, g^{ra})$
  $C\_b = (Z^r \cdot m, e(g^{ra}, RK\_\{A \rightarrow B\}))$
  $= (Z^r \cdot m, e(g^{ra}, g^{b/a}))$
  $= (Z^r \cdot m, Z^{rb})$
- Decryption (Bob):
  $m = (Z^r \cdot m) / (Z^{rb})^{1/b}$

REFERENCES

[1] S. Kumar, R. Sharma, and L. Zhang, ”An Identity-Based Proxy Re-Encryption Scheme With Single-Hop Conditional Delegation and Multi-Hop Ciphertext Evolution for Secure Cloud Data Sharing,” IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 123-135, 2023.

[2] S. Wang, N. Luo, B. Xing, Z. Sun, H. Zhang, and C. Sun, ”Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products,” Scientific Reports, vol. 14, no. 20048, 2024.

[3] Z. Zhou and Y. Liu, ”Blockchain-based encryption method for internal and external health privacy data of university physical education class,” Journal of Environmental and Public Health, vol. 2022, Art. ID 7506894, 2022.

[4] P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, ”Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system,” Mathematics, vol. 10, no. 68, 2022.

[5] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, and Z. Hu, ”Access control scheme based on blockchain and attribute-based searchable encryption in cloud envi- ronment,” Journal of Cloud Computing, vol. 12, no. 61, 2023.