IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13385

ASYMMETRIC UPDATABLE ENCRYPTION USING ELGAMAL FOR INFINITE CIPHERTEXT REVISIONS

Mr.Mohd Irfan [1], Bolligorla Shiva Kumar[2] , Chikkonda Anand Kumar [3], Boddupally Naveen[4]

Assistant Professor, Department of Computer Science and Engineering Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[1]

UG Scholars, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, Telangana, India[2,3,4]

Abstract: This paper presents an ElGamal-based asymmetric updatable encryption scheme designed to tackle the challenges associated with secure key rotation in cryptographic systems. The proposed method allows ciphertexts encrypted under a previous key to be securely and efficiently transitioned to a new key without the need for decryption, thereby preserving data confidentiality and integrity. By exploiting the mathematical characteristics inherent in ElGamal encryption, the scheme supports unlimited key update iterations, asymmetric encryption functionality, and is independent of specific ciphertext formats. Lightweight pseudorandom generators (PRGs) are employed to ensure secure and efficient handling of the random values necessary during encryption and re-encryption operations. The approach guarantees strong forward and backward security, protecting against data leakage even if keys are compromised. Extensive performance assessments demonstrate its efficiency, showing minimal computational and communication overhead, making it well-suited for both large-scale infrastructures and environments with limited resources. Additionally, comparative studies confirm its advantages over existing methods in terms of encryption speed, ciphertext update duration, and scalability. Overall, this work offers a practical and secure solution for frequent key management across various applications, including cloud storage, Internet of Things (IoT) devices, and secure communication networks.

Keywords: Blockchain, Differential Privacy, E-Voting, Ethereum, Smart Contracts, Voter Authentication

1.INTRODUCTION

In today's digital landscape, the rapid exchange of sensitive data over networks demonstrates the critical need for robust encryption mechanisms [1]. Cryptographic schemes are the foundation of secure communication, protecting information from unauthorized access and ensuring data integrity. Among these schemes, the ElGamal cryptosystem demonstrated re markable resilience and adaptability, due to its mathematical design and widespread use in securing digital communica tions [2], [3]. As computational capabilities continue to advance and new security threats emerge, the demand for dynamic security measures increases**.**

A key area of concern is the manage ment and rotation of cryptographic keys, which is vital for maintaining security over time, especially in scenarios in volving long-term data storage and transmission. Traditional methods of key rotation often necessitate decrypting data en crypted with an old key and subsequently re-encrypting it with a new key. This process not only consumes significant time but also exposes sensitive data to potential risks during the transition.

Updatable Encryption (UE) schemes present a suitable so lution to key rotation [4]. It allows ciphertexts encrypted under an old key to be transformed into ciphertexts under a new key without revealing the plaintext, thereby maintaining data confidentiality throughout the key rotation process [5]. While several updatable encryption schemes were proposed, many rely on symmetric key cryptography or intricate constructions which may not be practical for every application.

2. LITERATURE SURVEY

The security concepts of updatable encryption evolved sig nificantly since their initial introduction in [10]. The authors of [11] introduced two security notions within the chosen plaintext attack (CPA) model, allowing an adversary to adjust corrupt keys and tokens. Their IND-ENC notion mandates that fresh encryptions remain indistinguishable, while the IND-UPD notion extends this indistinguishability require ment to updated ciphertexts.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13385

Building on their work, Kloob et al. [12] expanded these notions to include security against chosen ciphertext attacks (CCA) and integrity safekeeping. Subsequently, Boyd et al. [13] introduced an enhanced secu rity notion called IND-UE, that requires the fresh encryptions to be indistinguishable from updated ciphertexts. The authors demonstrated that a CPA-secure updatable encryption scheme with ciphertext integrity (CTXT) can achieve CCA secu rity. The introduced permutation is based on SHINE method, achieving its detIND-UE-CCA security concept within the ideal cipher model and relying on the DDH assumption.

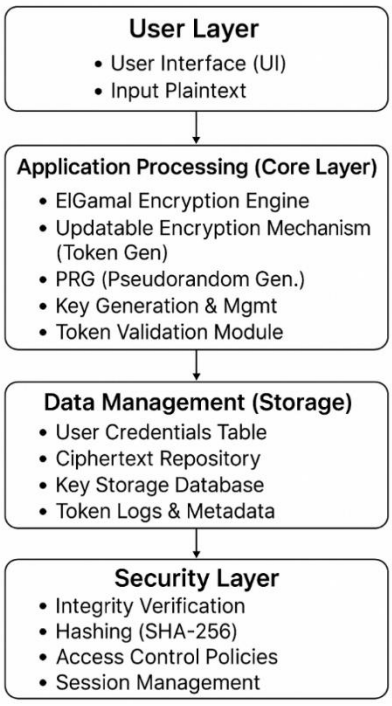
3. PROPOSED SYSTEM

- The proposed system is an ElGamal-based updatable encryption scheme designed to securely transform ciphertexts encrypted under an old key into ciphertexts under a new key without decrypting the underlying plaintext.
- This transformation is achieved through an update token generated using both the old and new keys, enabling secure key rotation without exposing sensitive data.
- Key features of this approach include seamless key updates that maintain data confidentiality throughout the process, as there is no need for decryption and re-encryption. The scheme also guarantees strong forward and backward security.

PROPOSED SYSTEM ADVANTAGES:

- Enables secure key updates without decrypting data, keeping it confidential at all times.
- Supports unlimited key rotations without performance loss.
- Works independently of ciphertext structure, increasing flexibility.
- Provides strong forward and backward security to protect data even if keys are leaked.

4. SYSTEM ARCHITECTURE



Updatable encryption schemes are illustrated in two forms depending on their reliance on ciphertext. The first form is ciphertext-dependent protocols, where clients pre-store or download the ciphertext, or part of it, from the cloud to com pute tokens. The second form is the ciphertext-independent protocol, where clients generate tokens without accessing the ciphertext.

ElGUE focuses on the ciphertext-independent method, which offers greater efficiency compared to the first category. Additionally, updatable encryption schemes are categorized based on how they handle ciphertext updates. One category employs deterministic update methods, where the ciphertext update algorithm consistently transforms the same original ciphertext into the same updated ciphertext using a given token.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13385

5. RESULTS AND DISCUSSION

Java offers several features that make it well-suited for interacting with databases. One of its key strengths is the Java Database Connectivity (JDBC) API, which provides a standard interface for connecting to relational databases. JDBC enables Java applications to execute SQL queries, update data, and manage database connections, allowing developers to work with databases in a consistent and platform-independent way.

Java also supports Object-Relational Mapping (ORM) frameworks like Hibernate, which simplify the interaction between Java objects and relational database tables, reducing the need for boilerplate SQL code. Additionally, Java's portability and scalability make it ideal for large-scale enterprise applications that need to interact with databases, whether running on a local server or in the cloud. Its strong exception handling, multi-threading capabilities, and robust security features also ensure reliable, efficient, and secure database management. Overall, Java's rich set of libraries and frameworks, along with its ability to seamlessly integrate with databases, makes it a powerful choice for developing database-driven applications.

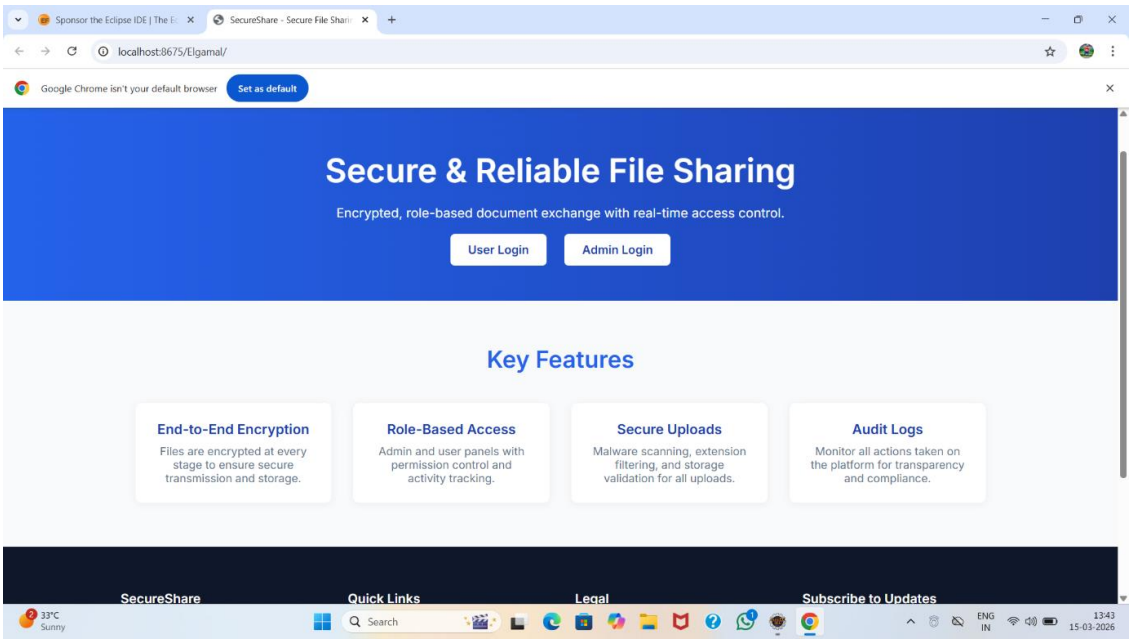


Figure 1: HOME PAGE

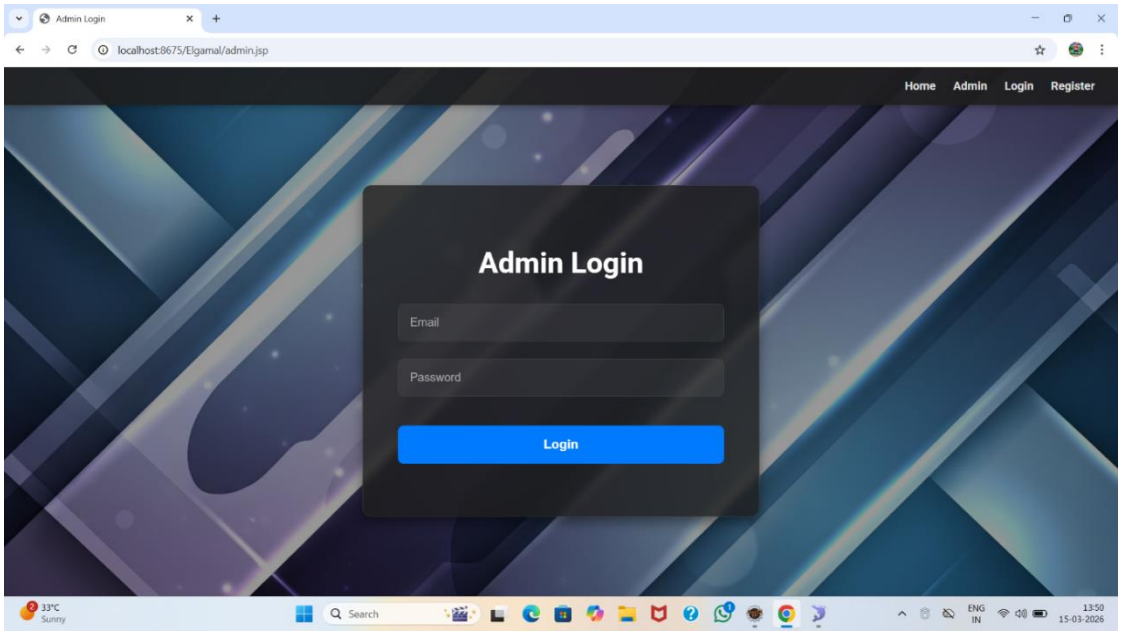


Figure 2: ADMIN LOGIN

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13385

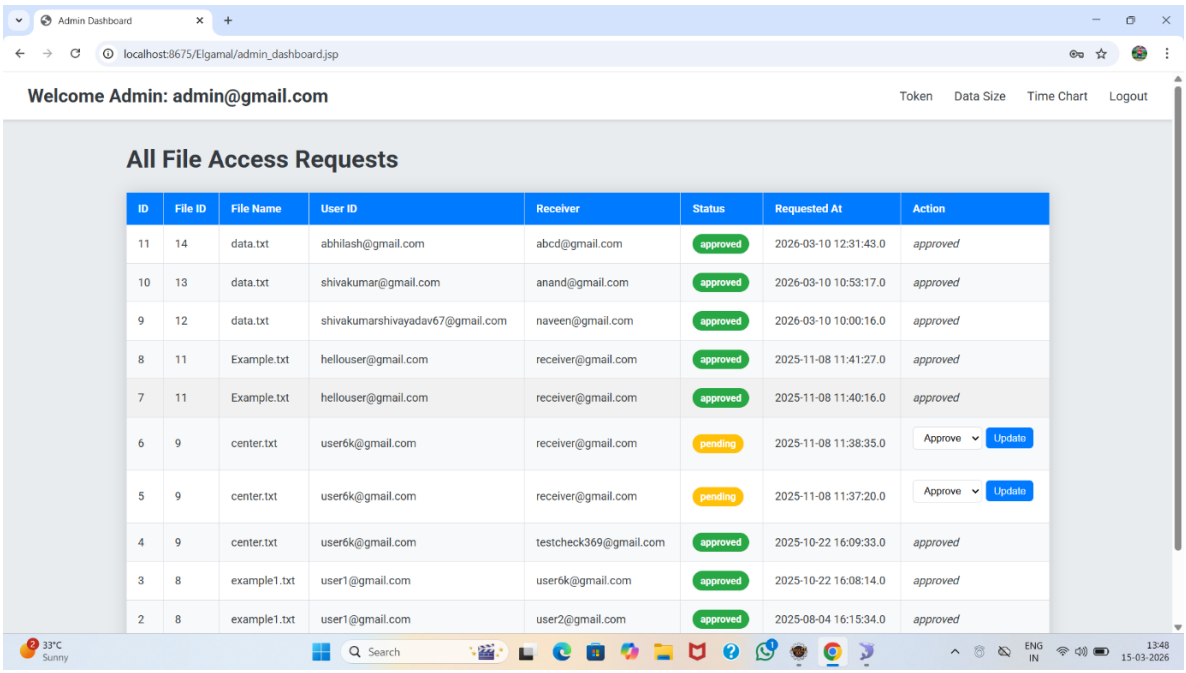


Figure 3:ADMIN APPROVAL

Figure 4:USER DASHBOARD

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13385

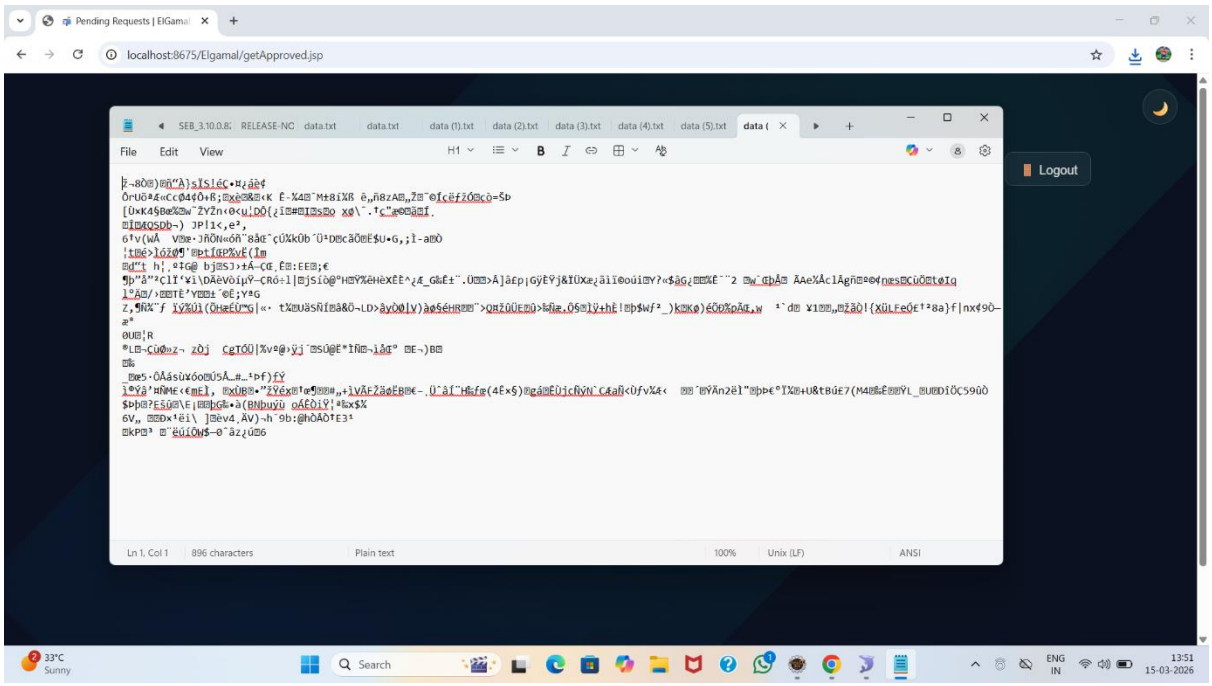


Figure 5: RESULTS

6. CONCLUSION

The ElGamal-Based Updatable Encryption (ElGUE) system successfully demonstrates an efficient and secure method for managing key rotations within encryption frameworks. By allowing ciphertexts to be updated directly from an old key to a new key without decrypting the underlying plaintext, the scheme ensures both forward and backward security. This approach minimizes data exposure risks while maintaining strong cryptographic integrity. The integration of ElGamal's mathematical foundation guarantees robustness against unauthorized access and data leakage, making it highly suitable for secure communication systems and data storage platforms. The overall performance analysis indicates that the system achieves high security with minimal computational overhead, proving its practicality for large-scale implementations.

REFERENCES

[1] B. Pahlevanzadeh, S. Koleini, and S. I. Fadilah, "Security in IoT: Threats and vulnerabilities, layered architecture, encryption mecha nisms, challenges and solutions," in Proc. Int. Conf. Adv. Cyber Secur., Springer, 2020, pp. 267–283.

[2] C. Zhang, Y. Liang, A. Tavares, L. Wang, T. Gomes, and S. Pinto, "An improved public key cryptographic algorithm based on chebyshev polynomials and RSA," Symmetry, vol. 16, no. 3, 2024, Art. no. 263.

[3] S. Medileh, M. Kara, A. Laouid, A. Bounceur, and I. Kertiou, "A secure clock synchronization scheme in WSNS adapted for IoT-based applications," in Proc. 7th Int. Conf. Future Netw. Distrib. Syst., 2023, pp. 674–681.

[4] X.Wang,K.Zhang,J. Gong, S.-F. Sun, and J. Ning, "Updatable search able symmetric encryption: Definitions and constructions," Theor. Comput. Sci., vol. 983, 2024, Art. no. 114304.

[5] A.Leroux and M.Roméas, "Updatable encryption from group actions," in Proc. Int. Conf. Post-Quantum Cryptogr., Springer, 2024, pp. 20–53.

[6] M. Kara et al., "A fully homomorphic encryption based on magic number fragmentation and EL-Gamal encryption: Smart healthcare use case," Expert Syst., vol. 39, no. 5, 2022, Art. no. e12767.

[7] H. Gupta and A. Nayak, "Publish subscribe system security require ment: A case study for V2V communication," IEEE Open J. Comput. Soc., vol. 5, pp. 389–405, 2024.

[8] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," IEEE Open J. Comput. Soc.,vol.3, pp. 23–38, 2022.

[9] P. Tandel and J. Nasriwala, "Secure authentication framework for IoT applications using a hash-based post-quantum signature scheme," in Service Oriented Computing and Applications. Berlin, Germany: Springer, 2024, pp. 1–12.