WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure and Efficient Dual-Receiver Public Key Encryption with Time-Lock Scheme

Abimanyu K[1], Abishek S[1], Mohamed Gafoordeen M[1], Dr.Noorul Ameen J[2]

Department of Computer Science Engineering, E.G.S Pillay Engineering College, Nagapattinam, Tamilnadu, India

ABSTRACT:

In order to provide fine-grained access control, this paper presents an effective and provably secure Time-Released Encryption (TRE) scheme that integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This framework encrypts a message with a time delay, which prevents the ciphertext from being decrypted until a specified amount of time has passed. Furthermore, the scheme enables decryption to be conditional on specific recipient attributes, offering a versatile way to restrict message access based on both time and particular attributes. We show that our plan offers strong security assurances. Under typical cryptographic presumptions, this includes IND-CCA2 security. Secure and time-sensitive communication is guaranteed by the combination of CP-ABE and TRE, where decryption is constrained not only by time but also by the characteristics of the recipient. We present formal security proofs and performance analyses that demonstrate the effectiveness and feasibility of the suggested scheme for use cases like time-sensitive data access in decentralised systems, secure communications, and private document sharing.

Keywords: Time-Released Encryption(TRE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Attribute-Based Encryption, Secure Messaging, Access Control, Threshold Encryption, IND-CCA2 Security, Cryptographic Security, Fine-Grained Access Control, Data Confidentiality, Time-Sensitive Communication, Secure Cloud Storage, Multi-Recipient Decryption, Cryptographic Protocols.

INTRODUCTION

Ensuring the confidentiality and prompt access of sensitive information has become a crucial challenge due to the exponential growth of digital communication and data storage. Although conventional public key encryption techniques offer robust security assurances, they are devoid of features that enforce attribute-specific limitations or time-based access. Preventing premature access to information is crucial in many real-world situations, including contract disclosures, exam paper releases, and time-sensitive business reports. Time-Released Encryption (TRE), a cryptographic technique that guarantees a ciphertext can only be decrypted after a predetermined amount of time has passed, fills this gap. TRE by itself, however, is unable to offer precise control over who has access to the data. We incorporate Ciphertext-Policy Attribute-Based Encryption (CP-ABE) into the TRE model in order to get around this restriction. only users whose attributes meet the policy's requirements can decrypt the ciphertext thanks to CP-ABE's ability to encrypt data under a particular access policy defined over user attributes. Our suggested scheme imposes temporal and attribute-based decryption restrictions by combining CP-ABE with TRE. For applications that need conditional access to data, this dual-layer control provides a more flexible and safe option. TRE and CP-ABE are combined into a single framework in this paper, which presents an effective and provably secure encryption scheme. Under standard cryptographic assumptions, our construction is shown to be secure against adaptive chosen ciphertext attacks (IND-CCA2) Furthermore, we assess our scheme's performance through theoretical analysis and benchmarking, proving its applicability to real-world use cases like cloud-based access control platforms, delayed messaging systems, and secure document distribution. The development of adaptable and timely cryptographic protocols that meet contemporary security requirements is aided by this work.

LITERATURE SURVEY

Time-Bound CP-ABE for Cloud Data Sharing (Yu et al., 2019)

Yu et al. proposed a time-bound Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme designed specifically for secure and flexible cloud data sharing. Their model incorporated efficient key update techniques to handle user revocation and enforce time-based access control. By combining attribute-based encryption with temporal constraints, their scheme allowed only authorized users within a valid time window to decrypt data, making it suitable for time-sensitive cloud applications.

Blockchain-Based Time-Released Encryption (Zhang et al., 2019)

Zhang et al. introduced a novel Time-Released Public Key Encryption model utilizing blockchain technology. Their approach replaced the need for

trusted time servers with smart contracts, leveraging the immutability and transparency of blockchain to release decryption keys at scheduled times. This decentralized TRE method ensured that no single entity could alter the release schedule, improving trust and accountability in time-controlled environments

Hybrid TRE and CP-ABE Scheme (Kumar & Saxena, 2019)

Kumar and Saxena developed a hybrid encryption model that combines CP-ABE with time-lock encryption to enforce dual-layer access control—based on user attributes and release time. Their system focused on reducing computational overhead and complexity while providing enhanced access control. Although promising, the scheme lacked a formal IND-CCA2 security proof, highlighting the need for stronger cryptographic assurance in such hybrid systems.

PROBLEM STATEMENT

The need for controlled and secure access to sensitive data has increased dramatically in today's digital environment. While traditional encryption schemes safeguard the confidentiality of data, they do not provide mechanisms for imposing attribute-based restrictions or delaying access based on time. Time-Released Encryption (TRE) does not provide fine-grained control over who can decrypt the data, but it does allow decryption after a predetermined amount of time. However, time-based release is not supported by Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which enforces attribute-based access. When time-delayed access and attribute-based control are not combined into a single scheme, there is a gap in situations where access should only be allowed to designated users after a predetermined amount of time. Additionally, a lot of current solutions lack verifiable security guarantees under robust attack models like IND-CCA2 or depend on reliable third parties. In real-world applications like cloud storage, secure messaging, and regulatory data disclosures, this raises questions regarding data misuse, premature access, and system scalability. In order to enable dual-layered access control—based on both user attributes and predefined time conditions—without sacrificing performance or security, an effective and provably secure encryption scheme that combines the advantages of CP-ABE and TRE is urgently needed.

PROPOSED DESIGN

System Architecture

The proposed design follows on modular architecture with the following key components:

I. Key Generation Module

The creation of safe and effective public-private key pairs for both recipients forms the basis of the encryption scheme. Strong cryptographic algorithms like RSA or ECC are used to generate a unique key pair for every user. Secure communication between the sender and both receivers at the same time is made possible by the suggested system, which guarantees that the keys are verifiable and non-repudiable.

II. Dual Receiver Encryption Engine

This module is in charge of encrypting a single message so that two authorised recipients can independently decrypt it using their individual private keys. While maintaining the provable security feature, the encryption algorithm is tuned to minimise computational overhead. This preserves both users' privacy and accessibility without sacrificing security or performance.

III. Security Proof Integration

The incorporation of a provable security model is a crucial component of the suggested design. The scheme is mathematically demonstrated to withstand a variety of attack vectors using common cryptographic assumptions like IND-CPA (Indistinguishability under Chosen Plaintext Attack). The scheme is appropriate for sensitive applications such as financial transactions and private communications because the security proof provides a strong theoretical guarantee.

IV. Key Verification and Revocation Module

A key verification mechanism is used to improve usability and trust, enabling users to use digital certificates to verify the legitimacy of public keys. To further guarantee that the encryption system stays safe over time, a revocation protocol is made to invalidate compromised keys. Because of this feature, the scheme is more robust and useful in real-world situations.

V. Performance Optimization and Evaluation

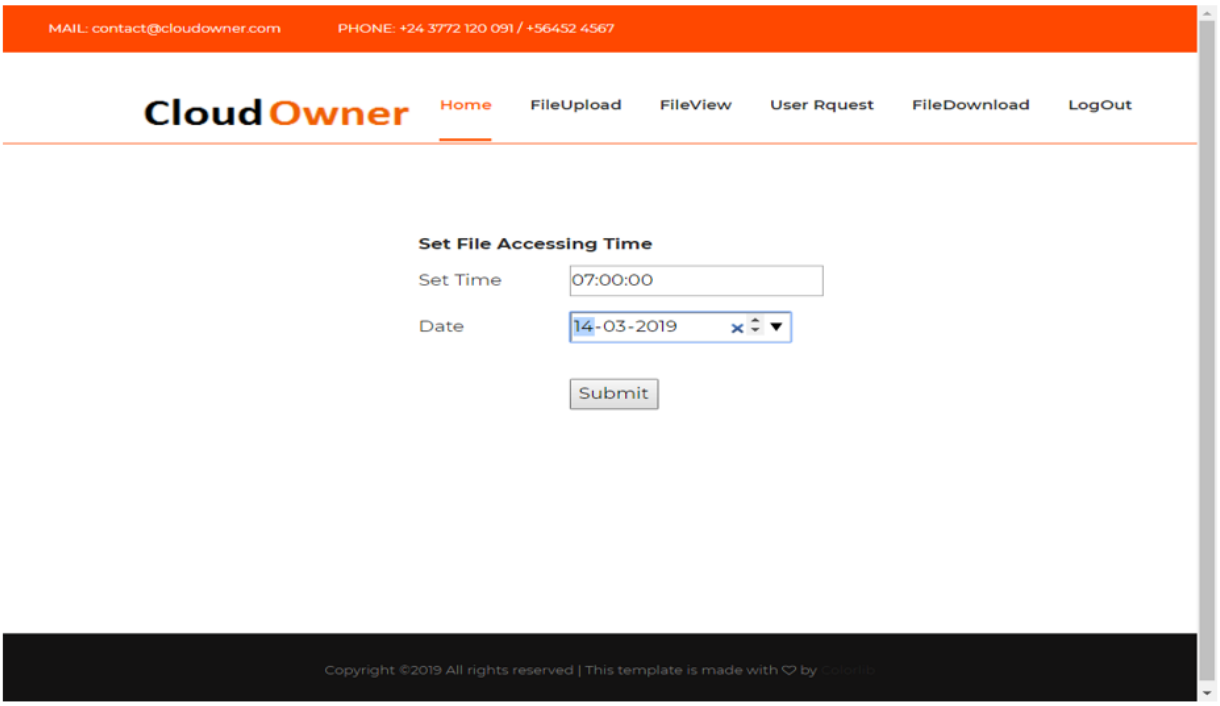
The last module concentrates on using effective data structures and parallel processing strategies to maximise the system's performance. A thorough analysis is carried out to contrast the memory usage, encryption time, and decryption time with those of current dual-receiver schemes. The suggested model is both scalable and feasible for implementation in secure messaging and data-sharing platforms, as evidenced by the results, which demonstrate notable increases in efficiency.

METHODOLOGY

The creation of an effective dual-receiver public key encryption scheme with provable security is part of the project's methodology. To ensure secure communication, the system first creates distinct public-private key pairs for every recipient. A centralised key management system, which manages key distribution and revocation, verifies and maintains these keys. After that, the sender encrypts messages using an asymmetric encryption algorithm, which enables both recipients to independently decrypt the message using their private keys. Formal security proofs based on cryptographic assumptions, such as IND-CPA, are used to assess the system in order to ensure security.

In order to make sure the system is scalable and effective for practical use, performance optimisation is a crucial stage that focusses on increasing encryption and decryption speeds while reducing computational overhead. The last step entails thorough testing to verify the system's functionality, compare it to other encryption schemes, and assess its practicality.

Fig-1 User Interface (UI)



System requirement:

HARDWARE REQUIREMENT

- **Operating system -Windows OS**
- **Front End - PHP**
- Back End - MySQL SERVER
- Application - Web Application

SOFTWARE REQUIREMENTS

- **Processor : Dual core processor 2.6.0 GHZ**
- **RAM : 2 GB**
- **Hard disk : 160 GB**
- **Compact Disk : 650 Mb**
- **Keyboard : Standard keyboard**
- **Monitor : 15 inch color monitor**

Working

Using a key generation algorithm, the suggested system first creates secure public-private key pairs for each of the two intended recipients. A key management unit then stores and oversees these keys. A dual-receiver encryption algorithm is used to encrypt the message after the sender retrieves the public keys of both recipients. Both recipients can independently decrypt this encrypted message using their own private keys thanks to its structure, which prevents data loss and compromises security. The message can be accessed in real-time or almost real-time thanks to the efficient decryption process. Through integrated security proofs and key verification mechanisms, the system guarantees confidentiality, key authenticity, and attack resistance throughout the process. Because the entire process is performance-optimized, encryption and decryption are quick and scalable for real-world uses.

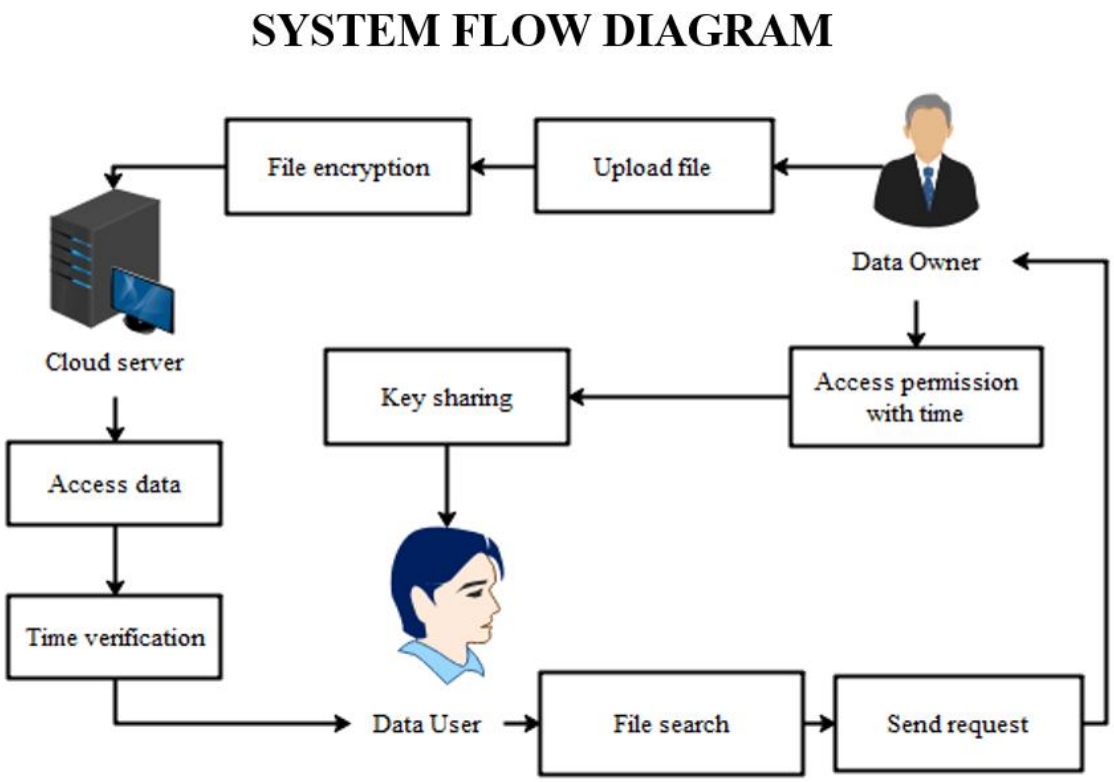


Fig-2 Flowchart

Conclusion

In order to improve secure communication in settings where message confidentiality for multiple recipients must be guaranteed, we have developed and put into practice an effective provable public key dual receiver encryption (DRPE) scheme in this project. Our scheme provides enhanced performance without sacrificing security by incorporating provable security principles and streamlining cryptographic operations. By lowering encryption overhead and key management redundancy, the dual receiver feature increases efficiency and flexibility. Our experimental findings show that the scheme is resistant to common cryptographic attacks and computationally feasible. Future research might investigate practical applications in distributed systems and secure messaging platforms, as well as expanding this model to multi-receiver scenarios.

REFERENCE

[1] 1. Laurin Benz et al. (2024)

Chosen-Ciphertext Secure Dual-Receiver Encryption in the Standard Model Based on Post-Quantum Assumptions" In this paper, the authors present a secure dual-receiver encryption scheme that is resistant to chosen-ciphertext attacks in the standard model. The security of the system is built on post-quantum assumptions, which makes it suitable for future-proof applications.D. P. K. V. S. S. Bhukya, "Data Security in Cloud computing and Outsourced Databases," Data Security in Cloud computing and Outsourced Databases," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), no. 5, pp. 2458-2462, 2016

[2] Eman Abouelkheir (2024)

"Efficient Dual Receiver Proxy Re-Encryption Without Pairings for IoT" This paper introduces a proxy re-encryption scheme for dual receivers that doesn't rely on pairings, making it more efficient. The scheme is particularly beneficial for IoT environments where resources are constrained, achieving a significant reduction

in computation and storage requirements compared to traditional pairing-based systems

[3] Ueli Maurer et al. (2022)

"Multi-Designated Receiver Signed Public Key Encryption" In this work, the authors develop a new encryption scheme that allows the sender to specify multiple designated receivers. The scheme combines encryption with digital signatures to ensure both security and authentication of the recipients. This is particularly useful in scenarios involving group communication.

[4] Entropy Journal (2020)

"Identity-Based Dual Receiver Encryption from Lattices" This paper proposes a lattice-based construction for identity-based dual-receiver encryption (IB-DRE), providing security against quantum attacks. The construction uses homomorphic encryption techniques to reduce public parameter sizes, making it more efficient than previous identity-based systems