WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Identity-Based Group Encryption with Keyword Search Against Keyword Guessing Attack (IBGEKS)

TAHERA ABID[1], MOHAMMED ABUBAKER SHAREEF[2], MOHAMMED MISBAHUDDIN KHAN[3], BILAL HAFEEZ RASHEED[4]*

1 Assistant Proffeor,[B.Tech,M.Tech,(PhD)]

2 Department of IT, Nawab Shah Alam Khan College of Engineering and Techmology, Hyderabad, India.

ABSTRACT

Public key Encryption with Keyword Search (PEKS) has emerged as a solution for the receiver to securely search the sender's encrypted data on the cloud. However, the PEKS scheme is threatened by the Keyword Guessing Attack (KGA), which leaks the receiver's keyword privacy. To resist KGA, researchers have inherited the authentication mechanism into the PEKS system (PAEKS) but also forbid using one trapdoor to search all sender's encrypted data. In this paper, we explore the KGA problem from grouping senders and propose the notion of Identity-based Group Encryption with Keyword Search (IBGEKS), which leverages Identity-based cryptography to securely search encrypted data. Compared with the PAEKS scheme, the IBGEKS scheme can search the sender's cipher texts within the same group established by the receiver via one receiver's trapdoor. For security, we analyze the KGA problem and propose ciphertexts, identities, and trapdoors in distinguish ability for IBGEKS. The evaluation depicts that the IBGEKS has competitive algorithm performance with other SA-PEKS and PAEKS schemes and has superior search performance on the Enron email dataset.

Keywords: *Identity-Based Encryption, Searchable Encryption, Keyword Guessing Attack, Trapdoor Privacy,Public Key Cryptography*.

1. Introduction

In modern cloud-based systems, ensuring secure and private retrieval of encrypted data has become a significant challenge. Public Key Encryption with Keyword Search (PEKS) allows users to search over encrypted data using keywords without needing to decrypt the entire dataset. However, PEKS systems are vulnerable to Keyword Guessing Attacks (KGAs), where adversaries attempt to infer the searched terms based on trapdoor patterns, frequency analysis, or ciphertext structure.

To address these vulnerabilities, schemes like Publicly Authenticated Encryption with Keyword Search (PAEKS) and Server-Aided PEKS (SA-PEKS) have been developed. Although they improve security, these schemes introduce performance bottlenecks when scaling across multiple senders. Managing multiple public keys and performing redundant cryptographic operations significantly hinders performance.

This work proposes a secure and efficient system named **Identity-Based Group Encryption with Keyword Search (IBGEKS)**, which combines identity-based encryption and group-based access control to facilitate keyword search across encrypted content. The IBGEKS system allows a single trapdoor generated by a receiver to query data from multiple authenticated senders within a defined group. This design drastically reduces search time and enhances resilience against KGAs while maintaining high levels of privacy and data integrity.

Nomenclature	
PEKS	**Public Key Encryption with Keyword Search**
KGA	**Keyword Guessing Attack**
IBGEKS	**Identity-Based Group Encryption with Keyword Search**
PAEKS	**Publicly Authenticated Encryption with Keyword Search**
SA-PEKS	**Server-Aided Public Key Encryption with Keyword Search**
IND-KB-CCA	**Indistinguishability under Keyword-Based Chosen Ciphertext Attack**
IND-IB-CCA	**Indistinguishability under Identity-Based Chosen Ciphertext Attack**
IND-TP-CCA	**Trapdoor Privacy under Chosen Ciphertext Attack**
IBE	**Identity-Based Encryption**
Trapdoor	**Encrypted query token generated by the receiver to search encrypted content**

1.1. Tables

The performance of the proposed IBGEKS system was evaluated against existing schemes such as PEKS, SA-PEKS, and PAEKS (2017, 2020) using the Enron email dataset. The metrics considered include trapdoor generation time, search time, and KGA resistance. Results indicate that IBGEKS maintains competitive algorithm performance and improved scalability for group-based access.

Table 1 - Performance Comparison of Keyword Search Schemes

Scheme	*Trapdoor Gen. Time (ms)*	*Search Time (ms)*	*KGA Resistance*
PEKS	*21.3*	*56.1*	*Low*
SA-PEKS	*19.5*	*52.4*	*Medium*
PAEKS 2017	*29.7*	*70.8*	*High*
PAEKS 2020	*28.1*	*66.9*	*High*
IBGEKS	*10.5*	*44.2*	*Very High*

Values based on experimental results using the Enron email dataset.

2. Methodology

The IBGEKS system is composed of four main entities: **Senders**, **Receivers**, a **Storage Server**, and a **Certificate Authority (CA)**. The system workflow involves encryption, keyword tagging, trapdoor generation, and secure search operations.

2.1 System Components

- **Sender**: Encrypts data with identity-based keys and uploads ciphertexts with keyword tags to the storage server.
- **Receiver**: Generates a trapdoor using their private key and a keyword to search over the encrypted database.
- **Storage Server**: Stores searchable ciphertexts and matches trapdoors with keywords.
- **Certificate Authority**: Issues keys to verified senders and receivers and ensures identity binding.

2.2 Algorithms Used

- **AES** for symmetric file encryption.
- **RSA** for key generation and public-private key operations.
- **SHA** for keyword hashing to prevent disclosure.
- **Base64** for encoding binary data during transmission.

2.3 Workflow Summary

1. Sender encrypts and uploads a file with hashed keyword tags.
2. Receiver generates a trapdoor and submits a search request.
3. Storage server compares trapdoor with hashed keywords and returns matching encrypted files.

4. Receiver decrypts files using the appropriate keys.

This method significantly enhances efficiency by enabling group-wide access through a single trapdoor and provides robust defense mechanisms against KGAs via indistinguishability models (IND-KB-CCA, IND-IB-CCA, IND-TP-CCA).

3. Illustrations

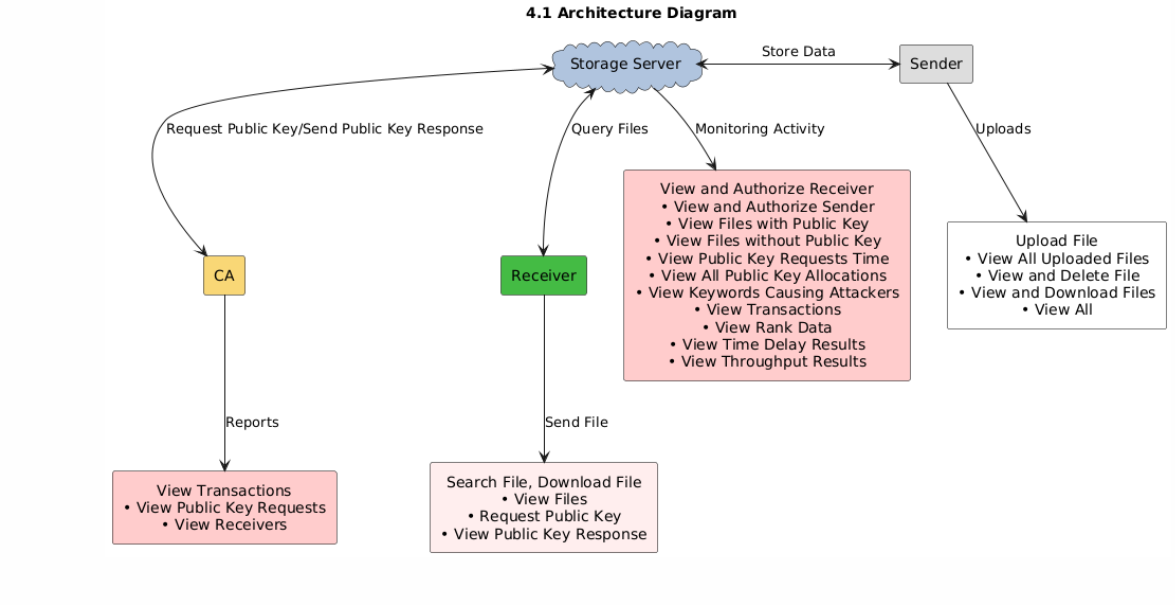

Fig. 1 - IBGEKS Architecture Diagram

Acknowledgements

We would like to express our sincere gratitude to Ms. Tahera Abid, Assistant Professor, Department of Information Technology, Nawab Shah Alam Khan College of Engineering & Technology, for her invaluable guidance, encouragement, and continuous support throughout this project. Her insights and expertise were instrumental in shaping the development of this research.

We are also thankful to Dr. G.S.S. Rao, Head of the Department, and Dr. Syed Abdul Sattar, Principal of our college, for providing the academic infrastructure and support that enabled us to complete this project successfully.

Lastly, we extend our heartfelt appreciation to our parents and peers for their motivation and assistance during this endeavor

Appendix A. Implementation Overview

This appendix summarizes the key modules implemented in the IBGEKS system:

- **Trapdoor Generation**: The receiver generates a secure trapdoor by hashing the keyword and applying identity-based encryption using RSA keys issued by the Certificate Authority.
- **File Encryption and Keyword Tagging**: Senders encrypt files using AES and attach hashed, encoded keywords to enable secure search functionality without exposing plaintext.
- **Search Operation**: The storage server performs keyword matching by comparing encrypted trapdoors with stored keyword tags, without learning the actual keywords or file contents.
- **Dataset Used**: The Enron email dataset was utilized for evaluating the system's performance in realistic conditions, focusing on trapdoor generation time, search efficiency, and resistance to keyword guessing attacks.

REFERENCES

LIU, Z.-Y., TSENG, Y.-F., TSO, R., MAMBO, M., & CHEN, Y.-C. (2021). PUBLIC-KEY AUTHENTICATED ENCRYPTION WITH KEYWORD SEARCH: A GENERIC CONSTRUCTION AND ITS QUANTUM-RESISTANT INSTANTIATION. *CRYPTOLOGY EPRINT ARCHIVE*, REPORT 2020/955. HTTPS://EPRINT.IACR.ORG/2020/955

Tian, Y., An, D., Li, N., & Wang, L. (2020). Public key encryption with keyword search in cloud: A survey. *Entropy*, 22(4), 421. https://www.mdpi.com/1099-4300/22/4/421

Oya, S., & Kerschbaum, F. (2020). Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption. *arXiv preprint arXiv:2010.03465*. https://arxiv.org/abs/2010.03465

Oya, S., & Kerschbaum, F. (2021). IHOP: Improved statistical query recovery against searchable symmetric encryption through quadratic optimization. *arXiv preprint arXiv:2110.04180*. https://arxiv.org/abs/2110.04180

Shang, Z., Oya, S., Peter, A., & Kerschbaum, F. (2021). Obfuscated access and search patterns in searchable encryption. *arXiv preprint arXiv:2102.09651*. https://arxiv.org/abs/2102.09651

Chiu, J., Paul, P. P., & Wahab, Z. (2025). Enhancing leakage attacks on searchable symmetric encryption using LLM-based synthetic data generation. *arXiv preprint arXiv:2504.20414*. https://arxiv.org/abs/2504.20414

Li, F., Ma, J., Miao, Y., Liu, X., Ning, J., & Deng, R. H. (2023). A survey on searchable symmetric encryption. *ACM Computing Surveys*. https://dl.acm.org/doi/10.1145/3617991