www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1856-1858

e-ISSN : 2583-1062
Impact Factor : 7.001

FORWARD SECURE PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH FOR OUTSOURCED CLOUD STORAGE

Bhuvaneswara Boopathy. G[1], Malini. S[2]

[1]Student, Master of Computer Application, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India.

[2]Professor, Master of Computer Application, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India.

ABSTRACT

Cloud storage has become a primary industry in remote data management service but also attracts security concerns, where the best available approach for preventing data disclosure is encryption. Among them the public key encryption with keyword search (PKSE) is considered to be a promising technique, since clients can efficiently search over encrypted data files. That is, a client first generates a search token when to query data files, the cloud server uses the search token to proceed the query over encrypted data files. However, a serious attack is raised when PKSE meets cloud. Formally speaking, the cloud server can learn the information of a newly added encrypted data file containing the keyword that previously queried by using the search tokens it has received, and can further discover the privacy information. To address this issue, we propose a forward secure public key searchable encryption scheme, in which a cloud server cannot learn any information about a newly added encrypted data file containing the keyword that previously queried. To better understand the design principle, we introduce a framework for constructing forward secure public key searchable encryption schemes based on attribute-based searchable encryption. Finally, the experiments show our scheme is efficient.

Keywords: Cloud Storage, Encryption, Public Key Encryption, Cloud Server, Data Privacy, Efficiency

1. INTRODUCTION

In recent years, with the widespread development of cloud computing technology, the application of cloud storage has become increasingly popular. With the support of cloud storage, users and enterprises can easily reduce the cost of local maintenance and storage. In addition, combined with the Internet of Things devices, cloud storage systems can provide more meta-services and applications. However, as the uploaded data are usually critical and sensitive, ensuring that service providers can properly protect the privacy of data becomes an important issue. Therefore, to avoid privacy leakage, users need to encrypt data before outsourcing them to the cloud. Unfortunately, the encrypted data will lose the flexibility of use, such as search or modification. As the search function can considerably reduce the transmission demand, this function is extremely important for cloud storage. In these primitives, encrypted data are uploaded along with multiple encrypted keywords by the sender, while the receiver can generate trapdoors for specific keywords. With the trapdoor, the cloud server can perform a search to find the matched encrypted keywords, i.e., they are associated with the same keyword, and return the corresponding encrypted data to the receiver. With the distinction of whether the generation of encrypted keywords and trapdoors is symmetric or asymmetric, searchable encryption can be further divided into symmetric search encryption (SSE) and public-key encryption with keyword search (PEKS).

2. METHODOLOGY

1.1 Searchable Encryption Module

Implements Public Key Encryption with Keyword Search (PKSE) to ensure secure data storage and retrieval. The client generates a search token using their private key for querying encrypted data. The cloud server uses the token to search encrypted data without decrypting it.

1.2 Forward Security Module

This module prevents the cloud server from learning information about newly added encrypted files, even if they contain previously queried keywords. It uses forward secure encryption by frequently updating keys, making old search tokens ineffective for identifying new data. This ensures robust protection against keyword-based attacks.

1.3 Attribute-Based Searchable Encryption (ABSE) Module:

ABSE provides fine-grained access control by encrypting data with attribute-based policies. Only users with matching attributes can generate valid search tokens and access files. This ensures secure, authorized access while maintaining data confidentiality in a multi-user cloud environment.

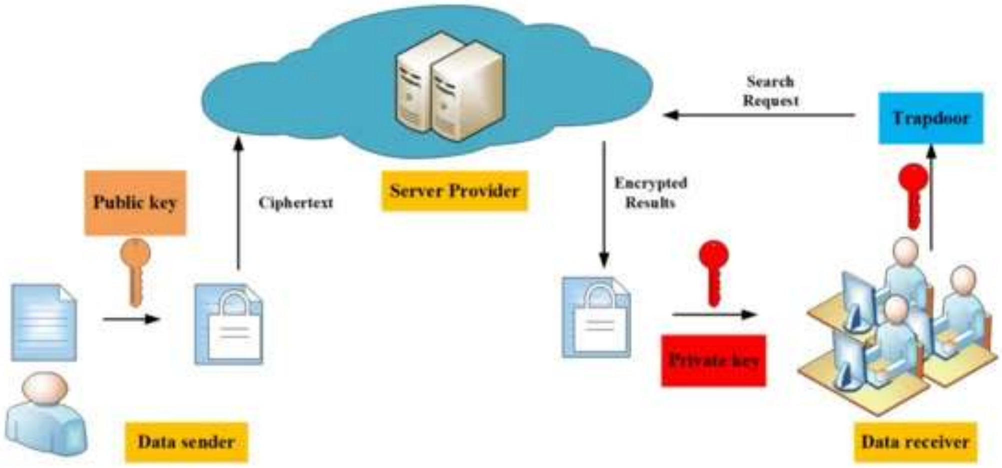
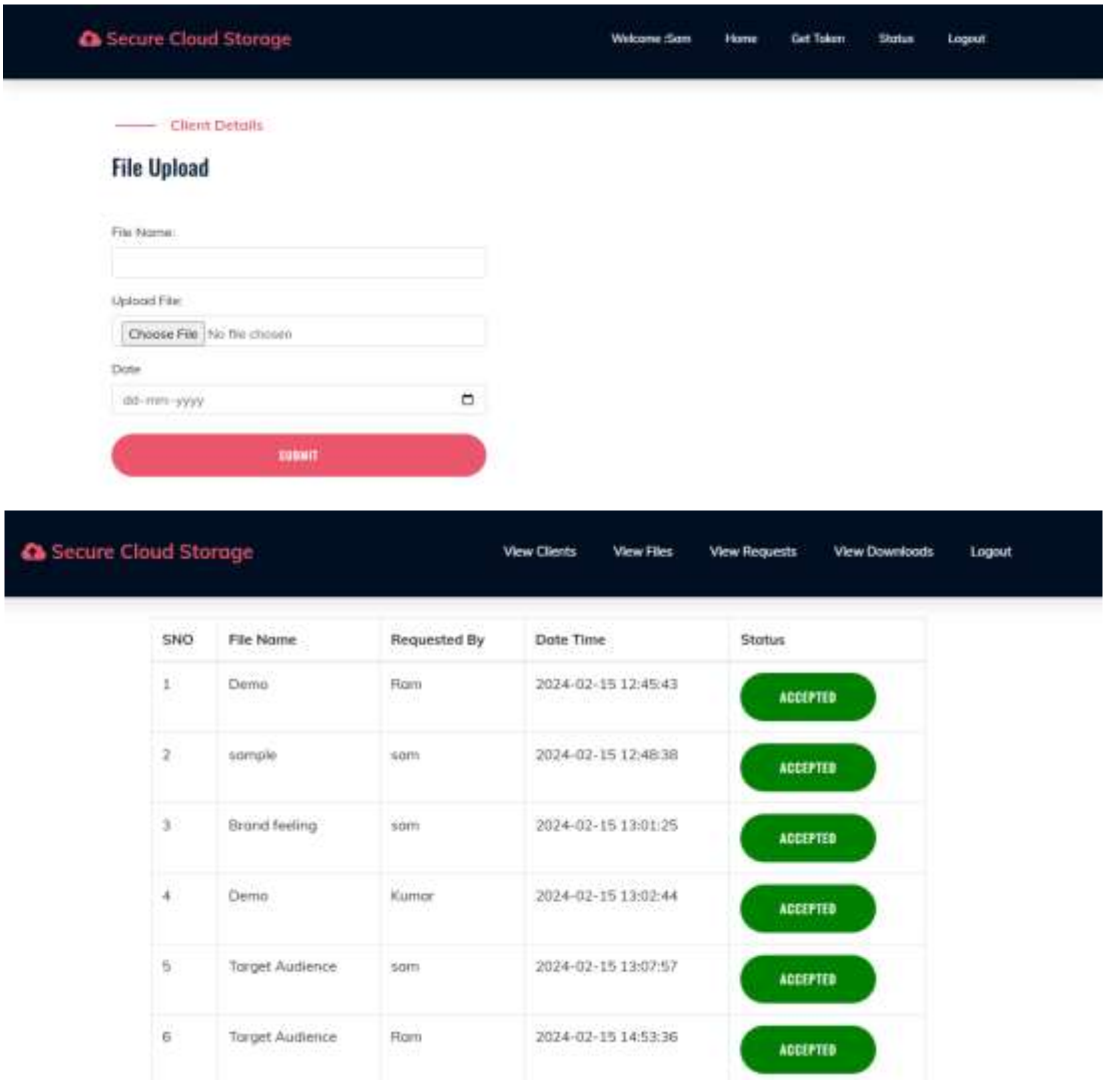


Figure 1: ERP Flow

3. RESULT

The **result** of the proposed forward secure public key searchable encryption (PKSE) scheme, as mentioned in the abstract, demonstrates its **efficiency** and **effectiveness** in securing data privacy. The experiments validate that the scheme successfully prevents the cloud server from gaining information about newly added encrypted files containing previously queried keywords. Additionally, the implementation ensures secure data searches using attribute-based encryption, maintaining both **data confidentiality** and **access control**. Overall, the scheme provides a robust solution to mitigate keyword-based attacks in cloud storage systems.



Client Details

File Upload

File Name:

Upload File:

Choose File No file chosen

Date

dd-mm-yyyy

SUBMIT

SNO	File Name	Requested By	Date Time	Status
1	Demo	Ram	2024-02-15 12:45:43	ACCEPTED
2	sample	sam	2024-02-15 12:48:38	ACCEPTED
3	Brand feeling	sam	2024-02-15 13:01:25	ACCEPTED
4	Demo	Kumar	2024-02-15 13:02:44	ACCEPTED
5	Target Audience	sam	2024-02-15 13:07:57	ACCEPTED
6	Target Audience	Ram	2024-02-15 14:53:36	ACCEPTED

Figure 2: Expected Outcome

4. CONCLUSION

The proposed forward secure public key searchable encryption (PKSE) scheme effectively addresses the privacy concerns in cloud storage by preventing keyword-based attacks. By ensuring that the cloud server cannot learn information about newly added encrypted files containing previously queried keywords, the scheme enhances data confidentiality. Additionally, the integration of attribute-based searchable encryption (ABSE) ensures secure and authorized data access. Experimental results demonstrate the efficiency and practicality of the scheme, making it a reliable solution for secure data management in cloud environments.

ACKNOWLEDGEMENTS

This journal paper was truly prepared by my itself I agree the terms and conditions.

5. REFERENCES

[1] D. Song, D. Wagner and A. Perrig, “Practical techniques for searches on encrypted data”, 2000.

[2] D. Boneh, G. D. Crescenzo, R. Ostrovsky and G. Persiano, “Public key encryption with keyword search”,2004.

[3] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data”, 2004.