International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 6, Nov- Dec 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Enhancing Cloud Storage Security with Forward-Secure Public Key Encryption and Keyword Search

Varna Vijaykumar Acharya, Abhishek Madhusudhanan Nair
(Department of Information Technology, Keraleeya Samajam's Model College, and Dombivli(East)
Email: varnaacharya96@gmail.com)
(Department of Information Technology, Keraleeya Samajam's Model College, and Dombivli(East)
Email: abhimnair2001@gmail.com)

----------**********----------

Abstract:

The capacity to supply computational resources (such infrastructure and storage) as services over the internet on demand has made cloud storage the industry leader. However, there are security concerns associated with cloud storage. Right now, the most effective way to minimize data leakage is through encryption. One of the most promising of these is the public key encryption with keyword search (PKSE) approach, which makes it easy for users to search through encrypted information. To put it another way, a client that wishes to query data files first generates a search token, which the cloud server then uses to access encrypted data files. But a serious threat arises when PKSE and cloud collide. Specifically, the cloud server can use the search tokens it has been given to retrieve the content of a recently added encrypted data file that contains the keyword it has previously queried, as well as privacy information. To address this issue, this paper suggests 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.

Keywords **—Forward-Secure Public Key Encryption, Keyword Search, Cloud Storage Security**

----------**********----------

I. INTRODUCTION

The emergence of cloud computing has completely changed how people store, access, and share data, enabling them to store vast volumes of data on distant computers with ease. The difficulty in guaranteeing the security and privacy of sensitive data entrusted to cloud service providers comes along with this ease, too. Robust security methods in cloud storage systems are becoming more and more necessary as cyber threats become more frequent and complicated. The protection of data during transmission and storage is one of the primary issues in this situation, especially in light of the sensitive nature of the data stored in the cloud.

Forward security has become a vital addition to traditional PKE. Forward-secure encryption guarantees that previous communications stay private even in the event that a user's private key is compromised in the future.

In the context of cloud storage,Secure keyword search functionality must be integrated as data is frequently searched using keywords to facilitate efficient retrieval. This adds a new level of complexity to the security paradigm by requiring the creation of cryptographic methods that permit keyword searches on encrypted data in addition to forward security.Through the integration of effective keyword search functionality with forward-secure public key encryption, our goal is to offer a complete and reliable security foundation for cloud storage systems.

II. FORWARD SECURITY IN CLOUD SECURITY

A cryptographic notion called "forward security" deals with the possibility of encryption keys being compromised over time. Since data is frequently handled and stored across distributed systems, cloud security is a field where it is especially pertinent. Forward security makes ensuring that previous communications are safe even in the event that a long-term secret key is compromised.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. What is forward-secure public key encryption?

Forward-secure public key encryption offers a degree of security where the confidentiality of previous messages is not jeopardized by the compromising of a current secret key. The confidentiality of communications from earlier time periods is not jeopardized by the disclosure of a secret key associated with a particular time period in this technique, since secret keys are refreshed on a regular basis. This feature is especially crucial in situations where long-term data storage must be safeguarded against potential significant breaches in the future. Research on the plan has been conducted, and several constructions have been proposed; one such construction is called forward-secure public key authenticated encryption with keyword search (FS-PAEKS), and it intends to improve cloud storage system security.

III. KEYWORD SEARCH IN CLOUDSECURITY

In terms of cloud security, keyword search usually refers to the capability of searching through encrypted cloud data and retrieving pertinent information. Conventional keyword search techniques cannot be used directly because cloud data is frequently encrypted for security and privacy purposes. To facilitate quick and safe keyword searches in the cloud, a number of methods and strategies have been created.

B. How does keyword search work in public key encryption?

By using public key encryption with keyword search (PEKS), a data owner can encrypt data using a public key in a way that makes it impossible for a third party with a trapdoor to decrypt the data and determine whether a specific keyword is related to it. As a result, a third party who does not have access to the original material can be granted the ability to search encrypted data. While permitting search operations on the encrypted data, the PEKS technique protects the privacy of the original data. The process involves the following key components and operations:

Key Generation: The data owner generates a public/private key pair.

Encryption: The data owner encrypts the data using the recipient's public key and associates it with specific keywords.

Trapdoor Generation: A user who wants to search for a specific keyword generates a trapdoor for that keyword using the public key.

Search: The third party tests the trapdoor against the encrypted data to determine if it contains the keyword without revealing any information about the data itself.[1]

The PEKS scheme has been the subject of extensive research to address various security and efficiency considerations, making it a versatile tool for secure search operations on encrypted data in cloud storage and other applications.[2]

IV. FORWARD SECURITY AND KEYWORD SEARCH INTEGRATION IN CLOUDSERVICES

Public Key Encryption with Keyword Search (PEKS) is a cryptographic technique that enhances data privacy by allowing a data owner to delegate searching capabilities on encrypted data to a third party without revealing the original data. This can be achieved through the following aspects:

Privacy: PEKS ensures that the third party does not learn any information about the data other than the presence or absence of the specified keywords, thus preserving the privacy of the original data[1][3].

Security: PEKS schemes are designed to be secure against various attacks, such as keyword guessing attacks. This security feature protects the confidentiality of the data and prevents unauthorized parties from gaining access to sensitive information.[3][6]

Flexibility: PEKS allows data owners to share their encrypted data with others while maintaining control over the search process. This flexibility enables data sharing in various applications, such as cloud storage, data outsourcing, and secure email systems.[1][5]

Efficiency: PEKS schemes can be efficient in terms of communication and computation, as they often involve only a small amount of data exchange and processing.[3][5] This efficiency makes PEKS suitable for large-scale applications and scenarios.

However, it is essential to note that the efficiency and security of PEKS schemes can be affected by various factors, such as the size of the encrypted data, the number of keywords to be searched, and the complexity of the scheme.[5] Ongoing research and development efforts aim to improve the efficiency, security, and practicality of PEKS schemes, further enhancing data privacy in various applications.

V. RESEARCH METHODOLOGY

This section reviews existing literature on cloud storage security, forward-secure encryption, and searchable encryption.It provides context for the suggested solution and identifies the advantages and disadvantages of the existing methods.

VI. LITERATURE REVIEW

Forward-secure public key encryption is a cryptographic technique designed to protect sensitive data even if long-term secret keys are compromised. Existing research, such as the work by Bellare and Yee (1997) on forward-secure signatures, lays the foundation for the application of forward security in cloud storage systems. This cryptographic approach ensures that even if a user's private key is exposed, the compromise does not affect past or future data.

The implementation of forward-secure public key encryption in cloud storage introduces challenges such as computational overhead and key management. Research by Canetti and Dakdouk (2018) addresses some of these challenges, proposing efficient algorithms and key rotation strategies to minimize the impact on performance and usability.

Keyword search on encrypted data enables users to search for specific information without compromising the confidentiality of the underlying data. Song et al. (2000) introduced the concept of searchable encryption, allowing users to perform keyword searches on encrypted documents. Extending this idea to cloud storage, researchers have explored techniques like Bloom filters and trapdoor functions to enable efficient and secure keyword searches on encrypted data stored in the cloud (Curtmola et al., 2006).

However, challenges persist in achieving an optimal balance between search efficiency and security. Li et al. (2018) proposed a secure and efficient searchable encryption scheme for cloud storage, addressing issues related to index leakage and keyword guessing attacks.

Combining forward-secure public key encryption with keyword search in cloud storage presents a promising avenue for addressing both data privacy and efficient information retrieval. However, there is limited research exploring the integration of these two techniques. Future work could focus on developing comprehensive frameworks that seamlessly incorporate forward-secure encryption while preserving the ability to perform secure keyword searches.

In conclusion, the literature suggests that forward-secure public key encryption and keyword search on encrypted data offer viable solutions for enhancing cloud storage security. Ongoing research in this area is crucial to overcoming existing challenges and ensuring the practical implementation of these techniques in real-world cloud storage systems.

VII. FINDINGS

A thorough and efficient method of protecting data in the cloud is revealed by the research on improving cloud storage security with forward-secure public key encryption and keyword search. The seamless integration of these cutting-edge cryptographic approaches shows that there is a workable answer to the intricate problems that privacy and data security in cloud storage systems provide. A robust and secure cloud storage ecosystem will depend on the ongoing investigation of these discoveries and the creation of creative remedies as technology develops and threats change.

VIII. RESULTS

To summarize, the use of forward-secure public key encryption and keyword search in cloud storage security would ideally lead to advances in data confidentiality, search functionality, resistance against key compromise, and a performance-security trade-off. The proposed security model's overall success is largely attributed to its real-world applicability across industries, user adoption issues, and robustness against adversarial attacks.

IX. CONCLUSIONS

This research aims to enhance cloud storage security by leveraging forward-secure public key encryption and keyword search techniques. By developing a practical and efficient solution, we aim to provide a secure and reliable cloud storage environment that protects data from unauthorized access and tampering while maintaining the performance and scalability of cloud storage systems.

REFERENCES

[1] Boneh, Dan, et al. “Public Key Encryption with Keyword Search.” Advances in Cryptology - EUROCRYPT 2004, 2004, pp. 506–522, https://crypto.stanford.edu/~dabo/pubs/papers/encsearch.pdf. Accessed 8 Aug. 2020.

[2] Liu, Ziyuan, et al. “Public-Key Authenticated Encryption with Keyword Search.” Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, May 2022, https://doi.org/10.1145/3488932.3497760. Accessed 27 Dec. 2023.

[3] Zhou, Yunhong, et al. “Privacy-Preserving and Efficient Public Key Encryption with Keyword Search Based on CP-Abe in Cloud.” MDPI, Multidisciplinary Digital Publishing Institute, 13 Oct. 2020, www.mdpi.com/2410-387X/4/4/28. Accessed 27 Dec. 2023.

[4] Boneh, Dan, et al. “Public Key Encryption with Keyword Search.” *Cryptology ePrint Archive*, 1 Jan. 1970, eprint.iacr.org/2003/195.

[5] Baek, Joonsang, et al. “Public Key Encryption with Keyword Search Revisited.” *SpringerLink*, Springer Berlin Heidelberg, 1 Jan. 1970, link.springer.com/chapter/10.1007/978-3-540-69839-5_96.

