Advanced International Journal for Research
E-ISSN: XXXX-XXXX editor@aijfr.com
Volume 2, Issue 4, July – August 2024

Security Measures for Dynamic Encrypted Search Data

C. Vishwas[1], J. Kumara Gaurav[2], Prof. D. Swaminathan[3]

[1,2]Undergraduate Students, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology, Hyderabad
[3]Associate Professor, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology, Hyderabad

Abstract
In the field of cloud security, Verifiable Searchable Symmetric Encryption (VSSE) is crucial, allowing users to retrieve encrypted cloud data through keywords while preserving the integrity of the results. However, current VSSE methods struggle with dynamic updates to cloud data because verifying these updates using asymmetric-key cryptography is time-consuming, especially with large data volumes. To address this issue, we propose a novel approach for efficient keyword searches on dynamically encrypted cloud data using symmetric-key-based verification. Our method introduces Accumulative Authentication Tags (AATs), which utilize symmetric-key cryptography to create authentication tags for each keyword. AATs are designed to accumulate updates, facilitating easy authentication tag adjustments during dynamic data changes. Additionally, we propose a secure indexing system that includes a search table (ST) with orthogonal lists and a verification list (VL) with AATs. Through extensive security analysis and performance testing, we show that our approach is both effective and efficient. This solution not only meets the challenge of managing dynamic updates for encrypted cloud data but also provides strong security, representing a significant advancement in cloud security technology.

Keywords
Verifiable Searchable Symmetric Encryption (VSSE), Cloud Security, Dynamic Encrypted Cloud Data, Keyword Search, Efficient Verification, Symmetric-Key Cryptography, Accumulative Authentication Tags (AATs), Secure Indexing, Orthogonal Lists, Performance Evaluation.

Introduction

Searchable Symmetric Encryption (SSE) has become increasingly important in cloud computing security, allowing users to securely retrieve specific encrypted data from cloud storage using keywords. However, despite progress in SSE technology, most existing solutions are designed for static encrypted data, neglecting the dynamic nature of real-world cloud environments. As cloud data frequently changes, there is a pressing need for schemes that can handle additions, deletions, and modifications. While dynamic SSE schemes have been developed, ensuring the integrity of search results from cloud servers remains a critical and underexplored issue.

Traditional verifiable dynamic SSE schemes use asymmetric-key cryptography, which introduces computational overhead that can hinder efficiency, especially for devices with limited resources. To address this, our research presents a novel approach that enables keyword searching over dynamically encrypted cloud data using symmetric-key-based verification.

Our contributions include

1. Symmetric-Key Based Accumulative Authentication Tag (AAT): We introduce a new AAT scheme based on symmetric-key cryptography, which facilitates seamless updates of authentication tags during dynamic data operations. This AAT scheme is designed to be collision-resistant and resistant to replay attacks, thereby enhancing data integrity.
2. Efficient Data Update with Secure Indexing: Our solution features a secure indexing system that includes a search table (ST) and a verification list (VL), designed to improve data update efficiency. The ST, utilizing orthogonal lists, and the VL enable quick identification of index nodes related to modified files, thereby streamlining the update process.
3. Proposed Keyword Search Scheme: We offer a keyword search scheme specifically designed for dynamic encrypted cloud data, leveraging symmetric-key-based verification. Our security analysis confirms the scheme's robustness, and performance comparisons highlight its efficiency.

Problem Statement

Ensuring the accuracy of search results in cloud environments is critical for maintaining data security. Kurosawa et al. proposed two verifiable dynamic SSE schemes to address this need. The first scheme uses a Message Authentication Code (MAC) for result validation but is vulnerable to replay attacks during data updates. While suitable for static cloud data, this MAC-based scheme fails to adequately verify updated data, making it prone to such attacks. The second scheme improves upon this by incorporating timestamp functionality from the RSA accumulator, allowing users to identify outdated results by comparing them with the latest accumulators maintained by the data owner. Subsequent schemes have extended this concept by using RSA or bilinear-map accumulators for result validation and dynamic data updates. However, both RSA and bilinear-map accumulators rely on asymmetric-key cryptography, which can be computationally intensive and problematic for devices with limited resources. Thus, improving the efficiency of verification processes in dynamic SSE schemes remains a crucial challenge, particularly in resource-constrained environments.

System Analysis

Existing System

The initial scheme, which uses MACs for result verification, works well for static data but struggles with dynamic updates. The improved scheme incorporates RSA accumulators to verify search results and manage dynamic updates, allowing data owners to detect non-updated results through the latest accumulators. Despite these advancements, the existing system has several limitations:

- Difficulty in implementation on low-performance devices for receiving and uploading patient data.
- Inefficiencies in handling dynamic data updates.
- Inadequate privacy protection measures.

Proposed System

This paper proposes a new approach for enabling keyword searches over dynamically encrypted cloud data using symmetric-key-based validation. The key contributions of this study are:

1. Symmetric-Key Based Accumulative Authentication Tag (AAT): We introduce a novel AAT scheme based on symmetric-key cryptography, which facilitates efficient verification and update of authentication tags during dynamic cloud data operations. The AAT scheme ensures collision resistance and is resilient to replay attacks, preventing the cloud server from providing outdated data.
2. Efficient Data Update with Secure Indexing: Our approach includes a secure index system comprising a search table (ST) with orthogonal lists and a verification list (VL) structured as a singly linked list. Each keyword is associated with a linked list of uniform length to obscure keyword frequencies. This design enables rapid identification of modified file index nodes, improving update efficiency. Additionally, the secure index supports flexible resizing for adding or removing files, enhancing overall efficiency.
3. Innovative Keyword Search Scheme: We present a keyword search scheme specifically designed for dynamic encrypted cloud data using symmetric-key-based validation. Our comprehensive security analysis and performance comparisons with existing methods demonstrate the scheme's robustness and efficiency, focusing on search token generation, verification, and update efficiency.

System Components

1. Interface Design: This module creates secure login pages for users. Users enter their credentials to access the server, either by logging in or registering with required details such as username, password, and email ID. Successful authentication grants access to the appropriate pages.
2. Data Ownership Management: This module handles tasks for data owners (DO), including publishing encrypted documents and secure indexes to the cloud server. DOs can delegate trapdoor generation to a Trusted Authority (TA) to reduce their computational load. They can also upload files, view file details, and transmit keys to the TA. During file updates, DOs generate update tokens locally and send them to the server.
3. Cloud Server Operations: This critical component stores encrypted data from data owners and executes search algorithms using trapdoors on secure indexes. It responds to search requests by retrieving relevant documents and manages updates to secure indexes and ciphertexts based on instructions from data owners.
4. Trusted Authority (TA) Functionality: The TA module handles authorization and trapdoor generation. No registration is required; only login credentials are needed. The TA manages user accounts, grants access, and generates trapdoors for keyword searches.
5. User Operations: This module covers tasks for users, including registration and account activation. Once registered, users' accounts are activated by the TA. Activated users can log in, conduct searches using keywords, filenames, or file contents, and receive trapdoors from the TA. They then submit these trapdoors to the cloud server to retrieve files and can download and decrypt data shared by data owners.

System Architecture

The cloud server is believed to be an untrusted entity. While it is allowed to discover which encrypted files includes the queried keyword during the search process, it may endeavor to dig out extra effective knowledge from the encrypted files, secure index, and search trapdoors. For example, it could try to establish which files include multiple queried keywords or discover changes in keywords within modified files.

Fig. 1. System Architecture

Algorithms and Techniques Used

Search Encryption Technique

Searchable Symmetric Encryption (SSE) facilitates the outsourcing of data to a third-party while allowing selective keyword searches on encrypted data without exposing sensitive information. This technique has received significant research attention, with various security definitions and implementations proposed.

Verifiable and Dynamic SSE (VDSSE) Scheme

The VDSSE scheme comprises eight polynomial-time algorithms:

1. Key Generation (K Setup): Creates a private key set K for the data owner.
2. Index Building (I; C IndexBuild): Constructs a secure index I and a ciphertext collection C based on the private key set K, the file set F, and the keyword set W.
3. Trapdoor Generation (Tw GenToken): Generates a trapdoor Tw from the private key set K and the queried keyword w.
4. Search (C(w) Search): Performs a search on the cloud server using the trapdoor Tw, secure index I, and ciphertext set C, resulting in a ciphertext set C(w) and an authentication tag AATS.
5. Verification (Verify): Verifies the authenticity of the returned ciphertext set C(w) and authentication tag AATS using the private key set K and trapdoor Tw.

6. Decryption (F(w) Dec): Decrypts the ciphertext set C(w) using the private key set K to yield a plaintext set F(w).
7. Update Tokens Generation (T UpToken): Creates update tokens Tm or Ta for modifying or adding files, respectively, based on the original and new files and the private key set K.
8. Update (I', C' Update): Updates the secure index I' and ciphertext collection C' on the cloud server using the update token T, secure index I, and ciphertext collection C.

In this project, two key cryptographic techniques are utilized: Searchable Symmetric Encryption (SSE) and Advanced Encryption Standard (AES).

Searchable Symmetric Encryption (SSE)
SSE allows encrypted data to be stored on a third-party server while maintaining the ability to perform selective keyword searches without revealing sensitive information. It enables data owners to create an encrypted index of their data and send it to the server. When a user needs to search for a specific keyword, they generate a trapdoor for that keyword and send it to the server, which then searches the encrypted index and returns relevant results.

Security
Securing data in the cloud involves various mechanisms, including Trusted Authorities (TAs), user activation processes, and encryption methods.

User Activation Procedure
The user activation procedure validates and activates user accounts after registration to ensure authenticity and prevent unauthorized access. This process includes verifying the user's identity and the accuracy of the provided information. Once validation is complete, the user's account is activated, granting access to system functionalities and resources. Activation may involve sending a confirmation email or SMS with a unique activation link or code for user verification. This procedure protects against unauthorized access and ensures that only legitimate users can interact with sensitive cloud data.

Trusted Authority (TA)
TAs are crucial for maintaining data security and integrity within the cloud environment. They oversee access control, authentication, and encryption key distribution. TAs generate and distribute cryptographic keys, such as symmetric keys, for encryption and decryption operations. They also manage user authentication processes and restrict access to authorized users. Operating in secure environments, TAs implement strong security measures to protect cryptographic materials and sensitive information.

Storage of Encrypted Files with Symmetric Keys
Encrypted file storage involves encrypting each file with a unique symmetric encryption key. Symmetric keys are generated through secure processes managed by TAs or trusted entities. Upon upload, files are encrypted using these symmetric keys. Encrypted files, along with metadata and encryption parameters, are stored securely in the cloud. Authorized users obtain the necessary symmetric keys from TAs or secure key management systems to decrypt files. Each file is encrypted with a distinct symmetric key, reducing the impact of potential key compromises. By leveraging Trusted Authorities, robust user activation procedures, and secure

storage practices, organizations enhance the security and privacy of cloud-stored data, mitigating risks related to unauthorized access, data breaches, and cryptographic vulnerabilities.

Conclusion

In summary, the development of a keyword search method for dynamic encrypted cloud data using symmetric-key-based verification has produced promising results. The introduction of Accumulative Authentication Tags (AAT) has led to an efficient approach for generating authentication tags for each keyword using symmetric-key cryptography. This advancement enhances data integrity and simplifies the verification of dynamic data updates. Additionally, our scheme features a novel secure index structure based on orthogonal lists and singly linked lists, which significantly improves data update efficiency. Our comprehensive security analysis and performance evaluations demonstrate that our proposed scheme excels in both security and efficiency, offering strong protection against unauthorized access while maintaining high performance for keyword searches and data updates. Overall, this scheme represents a viable solution for improving the security and efficiency of keyword searches in dynamic encrypted cloud data environments.

References

1. C. Guo, X. Chen, Y. M. Jie, Z. J. Fu, M. C. Li and B. Feng, “Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption,” in IEEE Transitions on Services Computing, vol. 99.
2. S. Kamara and C. Papamanthou, “Parallel and Dynamic Searchable Symmetric Encryption,” presented at the International Conference on Financial Cryptography and Data Security.
3. J. B. Yan, Y. Q. Zhang and X. F. Liu, “Secure multikeyword search supporting dynamic update and ranked retrieval,” in China Communication, vol. 13.
4. K. Kurosawa and Y. Ohtaki, “How to Update Documents Verifiably in Searchable Symmetric Encryption,” presented at International Conference on Cryptology and Network Security.
5. Q. Liu, X. H. Nie, X. H. Liu, T. Peng and J. Wu, “Verifiable Ranked Search over dynamic encrypted data in cloud computing,” presented at the IEEE/ACM International Symposium on Quality of Service.
6. X. H. Nie, Q. Liu, X. H. Liu, T. Peng and Y. P. Lin, “Dynamic Verifiable Search Over Encrypted Data in Untrusted Clouds,” presented at the International Conference Algorithm and Architectures for Parallel Processing.
7. X. Y. Zhu, Q. Liu and G. J. Wang, “A Novel Verifiable and Dynamic Fuzzy Keyword Search Scheme over Encrypted Data in Cloud Computing,” presented at the IEEE Trustcom/BigData SE/ISPA.