A Multi-Client Secure Cloud Framework with Enhanced Storage Efficiency and Latency Reduction

Mr.Kothakota Yatheesh [1], Mrs.T. RajyaLakshmi[2]
[1]*PG Scholar, Vemu Institute of Technology*
[2]*Assistant Professor, Department of CSE, Vemu institute of Technology*

***Abstract*- Cloud servers provide storage and computational resources at lower costs but face challenges regarding data security and efficiency. This project employs a multi-client Distributed Point Function (DPF)-based keyword search scheme with algorithms like Garbled Bloom Filter and Cuckoo Hash to address these challenges. The segmentation technique optimizes search latency, while Wegman authentication ensures data integrity. To enhance storage efficiency, a data compression algorithm is introduced, and to reduce repeated computation, a caching mechanism is implemented for encrypted search results. These extensions significantly minimize latency, computational costs, and storage requirements, enabling secure and efficient cloud-based keyword searches. The proposed system demonstrates a comprehensive solution for secure cloud storage with real-world applicability.**

Keywods: Cloud computing, Distributed Point Function (DPF), Keyword search, Garbled Bloom Filter, Cuckoo Hash, Segmentation technique, Wegman authentication, Data integrity, Data compression algorithm.

INTRODUCTION

The rise of cloud computing has transformed data storage by providing affordable and scalable solutions for individuals and organizations. Despite these advantages, concerns over data security and search efficiency hinder widespread adoption. Cloud servers often store encrypted data to maintain confidentiality, but this approach complicates operations like keyword searches. Distributed Point Function (DPF)-based schemes offer a promising solution, enabling secure keyword searches without compromising encryption. This project builds on state-of-the-art methods by incorporating Garbled Bloom Filters, Cuckoo Hashing, and segmentation techniques to enhance performance. Additionally, extensions like data compression and caching algorithms address storage and latency issues. The methodology employs multi-client authorization, ensuring fine-grained access control and robust security against malicious servers. By balancing computational efficiency with privacy, the system provides an innovative approach to overcoming the challenges associated with secure cloud storage and keyword search.

LITERATURE SURVEY

1. X. Shen et al. (2021) - Data Management for Future Wireless Networks
   - This study examines data management in wireless networks, focusing on architecture, privacy preservation, and regulatory challenges. The research highlights the necessity of integrating encryption and security frameworks into cloud-based data management.
2. H. Cui et al. (2017) - Encrypted Data for Secure Mobile Image Sharing
   - The authors propose an encrypted data-sharing model that ensures security in mobile image-sharing platforms. The framework integrates cryptographic methods to prevent unauthorized data access.
3. S.-F. Sun et al. (2022) - Multi-Client Searchable Encryption
   - This paper introduces a multi-client searchable encryption system that supports non-interactive retrievals. The framework is based on homomorphic encryption and differential privacy principles to enhance data protection.
4. Y. Miao et al. (2021) - Attribute-Based Keyword Search Over Encrypted Cloud Data
   - The research presents a multi-authority attribute-based keyword search mechanism for cloud environments. The model integrates fine-grained access control to manage multi-user searches securely.

5. S. G. Choi et al. (2021) - Oblivious Encoding for Encrypted Search
    - The authors develop a compressed oblivious encoding technique that improves the efficiency of homomorphic encrypted searches. The study emphasizes reducing computational overhead while ensuring data privacy.

PROBLEM STATEMENT

Existing encrypted keyword search mechanisms struggle with high storage costs, search latency, and computational overhead. A robust solution is required to address these inefficiencies while maintaining data security and ensuring seamless, multi-client access to cloud-stored information.

PROPOSED METHOD

The proposed system introduces an optimized multi-client keyword search framework using Distributed Point Function-based algorithms. It employs Garbled Bloom Filters and Cuckoo Hashing for secure and accurate searches, while a segmentation technique minimizes latency. Additionally, data compression reduces storage costs, and a caching mechanism stores encrypted results for frequent queries, decreasing computation overhead. Wegman authentication ensures the integrity of search results. The system's modular design supports fine-grained access control, enabling secure and scalable keyword search operations. These enhancements collectively address the limitations of existing methods, offering a practical and efficient solution for modern cloud storage challenges.

METHODOLOGY

1. User Registration Module
Objective: Enable secure onboarding of data owners and users.
Features:
User-friendly interface for registration.
Validation for secure input data.
Storage of user credentials in a secure database.
Process: Users register by entering their details, including username and password. The system validates and securely stores the information, allowing users to access the platform.
Outcome: The module ensures safe and efficient registration for data owners and users.

2. User Login Module
Objective: Authenticate users to grant secure access to the system.
Features:
Secure login through encrypted credentials.
Error handling for failed login attempts.
Process: Registered users enter their login credentials. These are authenticated against the database, allowing access upon successful verification.
Outcome: This module guarantees secure access to the platform for legitimate users.

3. Data Owner Upload File Module
Objective: Enable data owners to securely upload files to the cloud.
Process:
The data owner selects a file to upload.
The file is encrypted using ECC and AES algorithms.
Search indexes are generated using Garbled Bloom Filter and Cuckoo Hash and then encrypted.
Compressed encrypted data is uploaded to the cloud.
Outcome: Secure file storage with optimized storage costs.

4. Keyword Search Module
Objective: Allow data users to search for files securely using keywords.
Process:
The user enters keywords for the search.
The system hashes keywords and divides the search into segments.
Parallel searches are performed using Distributed Point Function (DPF).
Results are authenticated with Wegman hash codes.
Verified results are displayed, enabling file downloads.
Outcome: Efficient and secure keyword search with minimized latency.

6. Model Training
KNNI Imputation:
Apply KNN-based imputation, which replaces missing values with those from the most similar records in the dataset.
Model Training and Testing:
Train machine learning models, including SVM, on both KNNI and other imputed datasets to evaluate model accuracy in predicting JIF.
Hyperparameter Optimization of SVM:

Extend the SVM model through parameter tuning to achieve the lowest RMSE and MAE, indicating the best forecast accuracy.

CONCLUSION

We have proposed a multi-client secure and efficient keyword search scheme for cloud storage services. In our scheme, with encoding methods derived from garbled bloom filter and cuckoo filer, novel keyword indexes have been constructed to offer high search efficiency in terms of computation and communication overheads. To enable high security guarantees in multi-client environments, we have designed a double encryption method, put forward an authorization algorithm based on SCPRF, and applied WCMAC with cover-free systems. In addition, we have implemented a proof-of-concept prototype to demonstrate our scheme's practicality. For the future work, we will further explore DPF-based expressive keyword search such as ranked search, and investigate the opportunity to achieve multi-client efficient and leakage-free keyword search based on single-server PIR.

REFERENCE

[1] X. Shen et al., "Data management for future wireless networks: Architecture, privacy preservation, and regulation," IEEE Netw., vol. 35, no. 1, pp. 8–15, Jan./Feb. 2021.

[2] H. Cui, X. Yuan, and C. Wang, "Harnessing encrypted data in cloud for secure and efficient mobile image sharing," IEEE Trans. Mobile Comput., vol. 16, no. 5, pp. 1315–1329, May 2017.

[3] S.-F. Sun et al., "Non-interactive multi-client searchable encryption: Realization and implementation," IEEE Trans. Dependable Secure Comput., vol. 19, no. 1, pp. 452–467, Jan./Feb. 2022.

[4] Y. Miao, R. H. Deng, X. Liu, K.-K. R. Choo, H. Wu, and H. Li, "Multiauthority attribute-based keyword search over encrypted cloud data," IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1667–1680, Jul./Aug. 2021.

[5] S. G. Choi, D. Dachman-Soled, S. D. Gordon, L. Liu, and A. Yerukhimovich, "Compressed oblivious encoding for homomorphically encrypted search," in Proc. ACM Conf. Comput. Commun. Secur., 2021, pp. 2277–2291.

[6] E. Stefanov et al., "Path ORAM: An extremely simple oblivious RAM protocol," J. ACM, vol. 65, no. 4, pp. 1–26, 2018.

[7] S. Oya and F. Kerschbaum, "Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption," in Proc. USENIX Secur. Symp., 2021, pp. 127–142.

[8] Z. Gui, K. G. Paterson, and S. Patranabis, "Rethinking searchable symmetric encryption," Proc. IEEE Secur. Privacy, May 22/25, 2023.

[9] E. Boyle, N. Gilboa, and Y. Ishai, "Function secret sharing: Improvements and extensions," in Proc. ACM Conf. Comput. Commun. Secur., 2016, pp. 1292–1303.

[10] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998. 22.3205670.