https://doi.org/10.48047/AFJBS.6.Si4.2024.5733-5743

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Multi-authority attribute-keyword search over encrypted cloud data

[1]Dr.S.Selvakumar Raja, [2]M.Nagarani,

Principal & Professor Electronics and communication Engineering.
Kakatiya institute of technology and science for women, Manikbhandar,NIzambad,Telangana,India
Mail Id: kitswnzb@gmail.com
Head of Department Computer science Engineering.
Kakatiya institute of technology and science for women, Manikbhandar,NIzambad,Telangana,India

Volume 6, Issue Si4, Aug 2024

Received: 09 Jun 2024

Accepted: 19 July 2024

Published: 08 Aug 2024

doi: 10.48047/AFJBS.6.Si4.2024.1933-1945

ABSTRACT
Searchable Encryption (SE) ensures cloud data security and usability. The Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) technique uses CP-ABE to provide keyword-based retrieval and fine-grained access control. The single attribute authority in conventional CP-ABKS systems verifies user certificates and distributes secret keys, which is expensive. This causes a distributed cloud system single-point performance bottleneck. We introduce a secure Multi-authority CP-ABKS (MABKS) system in this study to alleviate such restrictions and reduce computation and storage load on resource-limited cloud devices. Malicious attribute authority tracing and updating are added to MABKS. Our comprehensive security study indicates that MABKS is selectively secure in selective-matrix and selective-attribute models. The MABKS system is efficient and useful in practical applications, as shown by our real-world dataset experiments.

INDEX TERMS: — —Searchable encryption, attribute-based encryption, multi-authority, selective-matrix model, selective-attribute model.

I.INTRODUCTION

Cloud-assisted services are becoming more common as cloud computing and the IoT evolve. Benefits of outsourcing large amounts of data to third-party cloud services including reduced local storage and Cloud-assisted services are becoming more common as cloud computing and the IoT evolve. Benefits of outsourcing large amounts of data to third-party cloud services. This outsourcing facilitates data sharing among users, for example, sharing health records in a healthcare context. However, privacy leakage remains a significant risk in data outsourcing environments.

To mitigate privacy concerns, encryption-before-outsourcing mechanisms are typically deployed, providing data protection and privacy in semi-trusted or hacked cloud settings.While these mechanisms effectively protect data, they also introduce challenges in data retrieval and search functionality. Encrypted data, although secure, becomes difficult to search and retrieve efficiently, which hampers the usability of cloud systems.

Searchable Encryption (SE) schemes have emerged as a solution to address these challenges. SE schemes enable secure searching over encrypted data, allowing users to retrieve relevant information based on specific keywords without compromising data security. Despite their utility, existing SE schemes often suffer from limitations in terms of efficiency and scalability, particularly in distributed cloud environments where single-authority systems become bottlenecks.

We propose an MABKS system to address these issues. MABKS provides keyword-based information retrieval and fine-grained access control over encrypted cloud data using CP-ABE and SE methods. The MABKS method eliminates single-point performance bottlenecks and Central Authority computing burdens by dispersing user certificate verification and secret key creation among many Attribute Authorities (AAs).

Our MABKS system introduces a hierarchical structure that enhances system efficiency and security. Each AA independently handles specific tasks, such as user authentication and key distribution,

which significantly reduces the workload on any single authority. This multi-authority architecture not only improves the system's scalability but also enhances its resilience against potential attacks or failures of individual authorities.

In this paper, we detail the design and implementation of the MABKS system. We describe the setup process, including key generation and distribution, encryption and decryption mechanisms, and the generation and use of trapdoors for keyword searches. Our security research shows that the MABKS system protects sensitive data under both selective-matrix and selective-attribute models.

To evaluate the performance of the MABKS system, we conducted experiments using real-world datasets, including the Enron, NSF, and RFC datasets. The results show that the MABKS system performs efficiently in key generation, trapdoor generation, and search processes, outperforming other existing schemes while maintaining reasonable encryption times. These findings underscore the practical applicability and scalability of the MABKS system in real-world cloud environments.

Overall, the MABKS system represents a significant advancement in secure cloud data retrieval, combining the strengths of CP-ABE and SE schemes to address the limitations of existing solutions. By leveraging a multi-authority architecture, the MABKS system ensures efficient, secure, and scalable keyword-based searches over encrypted cloud data, paving the way for more secure and user-friendly cloud storage solutions. Future work will focus on further optimizing the system's performance and exploring additional security enhancements to maintain its robustness against emerging threats.

II.LITERATURE SURVEY

Searchable Encryption (SE) has emerged as a pivotal technique in ensuring the usability and security of data stored in the cloud. The landscape of SE research encompasses various approaches, each aimed at optimizing specific aspects of secure data retrieval and access control. This literature survey delves into the key developments and methodologies in SE, highlighting their

contributions and limitations in the context of cloud storage systems.

1. Public-key Encryption with Keyword Search (PEKS):

Boneh et al. introduced PEKS, which allows a user to encrypt a document in such a way that it can later be searched using a keyword. The core idea is to use a public key for encryption and a trapdoor mechanism for search, enabling a secure and privacy-preserving search over encrypted data. However, PEKS schemes often suffer from inefficiencies in handling large datasets and complex queries.

2. Conjunctive Keyword Search:

Advances in PEKS have led to the development of schemes supporting conjunctive keyword search, where multiple keywords can be queried simultaneously. These schemes enhance the flexibility of keyword searches but introduce significant computation and communication overhead, particularly in environments with limited resources.

3. Ranked Keyword Search:

Ranked keyword search schemes aim to return search results based on their relevance to the query, often using ranking algorithms to prioritize the most pertinent documents. Cao et al. proposed one of the seminal works in this area, which leverages a ranking function to improve the efficiency and effectiveness of search results. Despite their advantages, ranked keyword search schemes may compromise privacy by revealing partial information about the relevance scores.

4. Verifiable Keyword Search:

Verifiable keyword search schemes add an extra layer of security by enabling users to verify the correctness of search results. These schemes employ cryptographic proofs to ensure that the cloud server has not tampered with the results. While verifiable keyword search enhances trust in the cloud service provider, it typically incurs additional computational costs and requires sophisticated cryptographic operations.

5. Ciphertext-Policy Attribute-Based Encryption (CP-ABE):

A popular fine-grained access control method is CP-ABE. It lets data owners set attribute-based access controls to restrict data decryption to matched users. Bethencourt et al. pioneered CP-ABE, enabling more flexible and dynamic access

control in cloud environments. However, traditional CP-ABE schemes face scalability issues and performance bottlenecks when applied to large-scale cloud systems.

6. Multi-authority Attribute-Based Encryption (MA-ABE):

To address the limitations of single-authority CP-ABE, multi-authority ABE (MA-ABE) schemes were introduced. MA-ABE distributes the responsibility of attribute management and key distribution across multiple authorities, reducing the risk of a single point of failure. Li et al. proposed one such scheme, demonstrating improved scalability and resilience. However, MA-ABE schemes often involve complex coordination among authorities, increasing the overall system complexity.

7. Attribute-Based Keyword Search (ABKS):

ABKS combines the principles of ABE and SE to support secure and efficient keyword-based searches over encrypted data. Data owners may restrict keyword search access in ABKS systems to authorised users. This integration allows fine-grained access control and secure search. though it may introduce challenges in key management and policy enforcement.

8. Verifiable Attribute-Based Keyword Search (VABKS):

VABKS extends ABKS by incorporating verifiability, allowing users to verify the authenticity and correctness of search results. By using cryptographic proofs, VABKS ensures that the cloud server cannot tamper with the search process or results. While this approach enhances trust and security, it can also increase computational overhead and complexity.

.III. EXISTING SYSTEM

The traditional single-authority CP-ABE schemes and multi-authority CP-ABE schemes face limitations in avoiding single-point performance bottlenecks and ensuring efficient keyword search functionalities. These existing systems also struggle with the high computation and communication overhead associated with secure data retrieval and key management

DISADVANTAGES OF EXISTING SYSTEM:

1. Detecting abusive words is not possible with the existing system.
2. The existing system cannot predict the person who has tweeted the message.

3. Single-point performance bottlenecks hinder the efficiency of the system.

4. High computation and communication overheads reduce system performance.

IV PRPSED SYSTEM:

The MABKS system introduces a multi-authority architecture where multiple AAs independently perform time-consuming tasks such as user certificate verification and intermediate secret key generation. This architecture significantly reduces the computation burden on the CA. The proposed system includes steps for setup, key generation, encryption, trapdoor generation, search, and decryption, ensuring efficient and secure keyword-based data retrieval

ADVANTAGES F PRPSED SYSTEM

1. The proposed system efficiently predicts and detects abusive words.
2. Identifies the person who tweeted abusive words.
3. Eliminates the need for manual analysis.

V.SYSTEM DESIGN

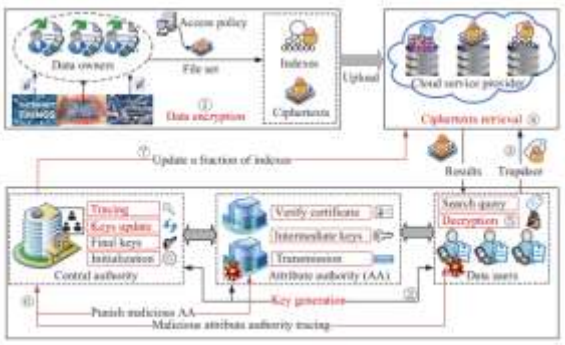

Fig1: Architecture f system.

The Multi-authority Attribute-Based Keyword Search (MABKS) system is designed to enhance the security, efficiency, and functionality of keyword-based data retrieval in cloud storage systems. This section details the architecture, modules, and workflow of the MABKS system.

1. System Architecture

The MABKS system architecture comprises several key components, including data owners, attribute authorities (AAs), a central authority (CA), cloud service providers (CSPs), and data users. The architecture is designed to distribute computational tasks across multiple authorities to avoid single-point performance bottlenecks and enhance system scalability.

Data Owners: Responsible for generating and encrypting data before outsourcing it to the CSP. Data owners also create encrypted keyword indexes for their data.

Attribute Authorities (AAs): Multiple AAs are responsible for managing user attributes, issuing attribute-based keys, and handling user authentication and authorization.

Central Authority (CA): Data owners may restrict keyword search access in ABKS systems to authorised users. This integration allows fine-grained access control and secure search.

Cloud Service Providers (CSPs): Store the encrypted data and indexes provided by data owners. CSPs perform search operations on the encrypted indexes using trapdoors generated by data users.

Data Users: Authorized users who possess the necessary attribute-based keys to generate trapdoors for searching encrypted data on the CSP.

2. Modules of the MABKS System

The system consists of several modules that work together to ensure secure and efficient data retrieval:

Setup Module: Generates public parameters and master keys to start the system. This module requires CA and AA collaboration to build up cryptographic infrastructure.

Key Generation Module: Divided into two phases

AA Phase: Each AA independently verifies user credentials and generates intermediate attribute-based keys.

CA Phase: The CA combines intermediate keys from multiple AAs to generate the final secret keys for users.

Encryption Module: Data owners use the public parameters and their secret keys to encrypt data and create encrypted keyword indexes. Encrypted data and indexes are then outsourced to the CSP.

Trapdoor Generation Module: Authorized data users use their attribute-based secret keys to generate trapdoors (encrypted search queries) based on the keywords they wish to search.

Search Module: The trapdoors allow the CSP to search encrypted indexes. Data users get matching encrypted data from the CSP.

Decryption Module: Data users decrypt the retrieved encrypted data using their attribute-based secret keys.

3. Workflow of the MABKS System

The workflow of the MABKS system involves several key steps:

System Initialization:

The CA generates public parameters and master keys.

AAs are registered with the CA and receive a share of the master key.

User Registration and Key Generation:

Users register with the AAs, providing necessary credentials.

AAs verify user credentials and issue intermediate attribute-based keys.

The CA combines intermediate keys from multiple AAs to generate final secret keys for users.

Data Encryption and Indexing:

Data owners encrypt their data using CP-ABE and generate encrypted keyword indexes.

Encrypted data and indexes are outsourced to the CSP.

Trapdoor Generation and Search:

Data users generate trapdoors using their attribute-based secret keys.

CSP uses the trapdoors to search the encrypted indexes and retrieve matched data.

Data Decryption:

Data users decrypt the retrieved encrypted data using their secret keys.

4. Detailed Design of Each Module

Setup Module:

Public Parameter Generation: The CA generates global public parameters accessible to all entities in the system.

Master Key Distribution: The CA distributes portions of the master key to multiple AAs to enable decentralized key generation.

Key Generation Module:

Attribute Verification: AAs verify user attributes and credentials during registration.

Intermediate Key Generation: AAs generate intermediate keys based on verified attributes.

Final Key Generation: The CA combines intermediate keys to produce final attribute-based secret keys for users.

Encryption Module:

Data Encryption: Data owners use public parameters and their secret keys to encrypt data files.

Keyword Index Creation: Data owners generate encrypted keyword indexes for their data files.

Trapdoor Generation Module:

Trapdoor Creation: Data users use their attribute-based secret keys to create trapdoors corresponding to search keywords.

Search Module:

Search Execution: The CSP uses trapdoors to perform search operations on the encrypted indexes.

Result Retrieval: The CSP returns matched encrypted data to the data users.

Decryption Module:

Data Decryption: Data users decrypt the retrieved encrypted data using their attribute-based secret keys.

5. Security and Performance Considerations

The MABKS system is designed to provide robust security and high performance:

Security: Ensures data confidentiality, integrity, and access control through CP-ABE and multi-authority architecture.

Performance: Distributes computational tasks across multiple authorities to enhance system efficiency and scalability.

By leveraging a multi-authority architecture and integrating advanced cryptographic techniques, the MABKS system addresses the limitations of existing CP-ABE schemes and provides a scalable, secure solution for keyword-based data retrieval in cloud environments.

VI. RESULT:

Home page

Fig: Home page

Registration Page

Fig : Registration page

Admin

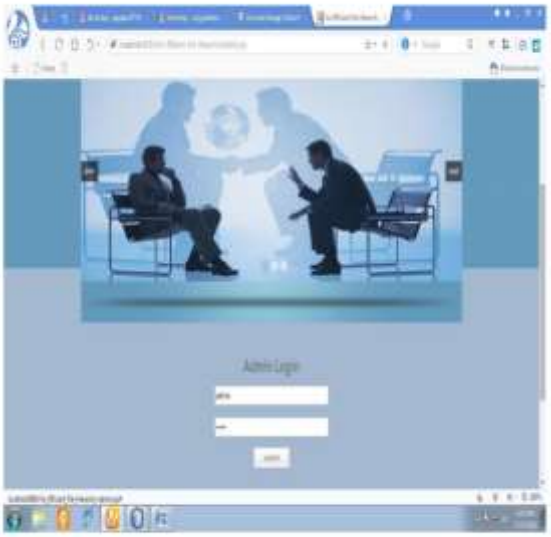

Fig: Admin Login Page

Admin Home

Fig: Admin home

User details

Owner details

Researcher details

User requests

Downloaded file

Owner login

Owner home

Medical record

Patient details

User login

Search details

Download records

Researcher

VII. CNCLUSION

The MABKS system provides a robust solution for secure and efficient keyword-based data retrieval in cloud storage systems. By leveraging a multi-authority architecture, the system addresses the limitations of traditional single-authority and multi-authority schemes, reducing computation burdens and avoiding performance bottlenecks. Future work will explore further enhancements to the MABKS system to improve its security and performance.

VIII. REFERENCES

[1] Y. T. Demey and M. Wolff, “Simiss: A model-based searching strategy for inventory management systems,” IEEE Internet of Things Journal, vol. 4, no. 1, pp. 172–182, 2017.

[2] C. Huang, R. Lu, H. Zhu, J. Shao, and X. Lin, “Fssr: Finegrained ehrs sharing via similarity-based recommendation in cloud-assisted ehealthcare system,” in Proc. ACM on Asia Conference on Computer and Communications Security (AsiaCCS’16), 2016, pp. 95–106.

[3] Y. Miao, J. Weng, X. Liu, K.-K. R. Choo, Z. Liu, and H. Li, “Enabling verifiable multiple keywords search over encrypted cloud data,” Information Sciences, vol. 465, pp. 21–37, 2018.

[4] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine-grained search over encrypted data in fog computing,” IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2018.

[5] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attributebased keyword search over hierarchical data in cloud computing,” IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2017.

[6] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symposium on Security and Privacy (SP’00), 2000, pp. 44–55.

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT’04), vol. 3027, 2004, pp. 506–522.

[8] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, “Personalized search over encrypted data with efficient and secure updates in mobile clouds,” IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 97–109, 2018.

[9] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, “Passive attacks against searchable encryption,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 789–802, 2019.

[10] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, “Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage,” Information Sciences, vol. PP, pp. 1–15, 2019.

[11] J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, and W. Lou, “Searchable symmetric encryption with forward search privacy,” IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–15, 2019.

[12] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, “Practical attributebased multi-keyword search scheme in mobile crowdsourcing,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3008–3018, 2018.

[13] Q. Zheng, S. Xu, and G. Ateniese, “Vabks: verifiable attributebased keyword search over outsourced encrypted data,” in Proc. IEEE Conference on Computer Communications (INFOCOM’14), 2014, pp. 522–530.

[14] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187–1198, 2016.

[15] L. Harn and J. Ren, “Generalized digital certificate for user authentication and key establishment for secure communications,” IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.