Alinteri J. of Agr. Sci. (2021) 39(2): 62-66
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

Multi-authority Attribute Based Keyword Search Over Encrypted Cloud Data

Mr. Madar Bandu[1], P. Keerthipriya[1], L. Sai Kethana[1], M. Uday Sai Kiran[1], N. Meghan satwik[1]
[1]*Department of Computer Science and Engineering,*
Anurag University, Hyderabad, India

***Abstract*— To ensure both data security and usability in cloud environments simultaneously, Searchable Encryption (SE) emerges as a crucial technique. Through the utilization of Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme accomplishes keyword-based retrieval and fine-grained access control concurrently. However, existing CP-ABKS schemes with a single attribute authority entail costly user certificate verification and secret key distribution, leading to a performance bottleneck in distributed cloud systems. Thus, this study introduces a secure Multi-authority CP-ABKS (MABKS) system to overcome these challenges and alleviate the computation and storage burden on resource-limited devices within cloud systems. Furthermore, the MABKS system extends its functionality to support malicious attribute authority tracing and attribute updates.**

***Index Terms* – Multi-authority, Searchable Encryption, Attribute-based Encryption, Access Control, Keyword Search**

I. Introduction

Cloud computing, a potent technology leveraging the Internet and remote servers, handles vast-scale data maintenance and intricate computations. One significant application lies in personal health record systems, granting individuals access to, management of, and sharing of their health information. Each patient retains full control over their personal health record, enabling sharing with various users, including healthcare providers' staff. To curb storage and operational expenses, numerous large organizations and individual users entrust their personal health records to the cloud, albeit relinquishing some control in the process. However, this reliance on semi-trusted cloud servers exposes personal health records to potential unauthorized access or commercial exploitation. Encrypting personal health records before cloud outsourcing becomes imperative to safeguard confidentiality, yet this hinders conventional search algorithms from operating in the encrypted domain.

Searchable encryption (SE) emerges as a cryptographic solution facilitating specific information retrieval, such as keywords, from encrypted documents without revealing plaintext details. The process involves the data owner encrypting both documents and keywords, then uploading the encrypted data and keyword ciphertext to the cloud. When a data user seeks document retrieval, they generate a keyword token sent to the cloud, which employs a search algorithm to match the keyword token with corresponding keyword ciphertext, returning encrypted documents with matching keywords. Traditional searchable encryption models grant either complete or no access to shared data based on possession of the secret key. However, many data owners desire more nuanced sharing capabilities for their data.

Attribute-based encryption (ABE) provides a solution to the aforementioned issue. ABE involves encrypting files based on attributes associated with each user. Sahai and Waters introduced ABE, which allows for access control over encrypted files through the use of access policies. Specifically, Ciphertext-policy ABE (CP-ABE) is proposed within this framework. In CP-ABE, each ciphertext is linked to a set of attributes, and each user's private key corresponds to an access policy for attributes. Users can decrypt a ciphertext only if the attributes associated with it meet the access policy defined by their private key. To enable fine-grained access control and keyword search within an e-healthcare cloud computing system, we leverage attribute-based encryption techniques.

Previous research failed to show that current attribute-based methods could simultaneously facilitate keyword search and data sharing within a single scheme. Consequently, there's a need for a secure solution capable of fully supporting both keyword searching and data sharing while ensuring the privacy of keywords. Thus, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. This mechanism enables searching and sharing functionalities within a ciphertext-policy framework.

II. Literature Survey

D. X. Song, *D. Wagner*, and *A. Perrig et al.* [1] proposed an effective approach for storing data on servers, such as mail and file servers, in encrypted form to mitigate security and privacy risks. However, this often entails compromising functionality for security.

D. Boneh, *G. D. Crescenzo*, *R. Ostrovsky*, and *G. Persiano* [2] introduced Public Key Encryption with Keyword Search (PKES), which enables senders to transmit encrypted data to a receiver, akin to traditional public key encryption (PKE) schemes. The distinction lies in PKES allowing the receiver to conduct searches on encrypted data stored on a third-party server, such as a cloud storage server. Most existing PKES schemes rely on bilinear maps, resulting in high computational costs and impracticality.

Q. Zheng, S. Xu, and *G. Ateniese*, among others, [3] have addressed the prevalent practice of data owners outsourcing their data to the cloud, necessitating encryption due to the cloud's lack of full trustworthiness. However, this introduces several challenges: How can a data owner grant search capabilities to data users? How can authorized data users search over a data owner's outsourced encrypted data? How can data users verify the cloud's faithful execution of search operations? Addressing these concerns, they propose a novel cryptographic solution termed Verifiable Attribute-Based Keyword Search (VABKS). This solution enables data users, whose credentials satisfy a data owner's access control policy, to (i) search over outsourced encrypted data, (ii) delegate search operations to the cloud, and (iii) verify the cloud's execution of search operations.

Later, *Waters et al.* [4] presented an approach for constructing searchable encrypted audit logs and highlighted the broad applicability of PEKS.

Park et al. introduced a security model for PEKS with conjunctive keyword search and proposed two efficient search constructions that partially conceal keywords. The desire for flexible sharing of selected documents among various user groups necessitates the use of different encryption keys for different documents. However, this also entails securely distributing a large number of keys to users for both encryption and search, requiring users to securely store received keys and submit a considerable number of keyword trapdoors to the cloud for querying shared data.

Baojiang Cui, Zheli Liu et al. [6] proposed the novel concept of Key Aggregate Searchable Encryption (KASE) and instantiated it through a concrete KASE scheme. In this scheme, a data owner only needs to distribute a single key to a user for sharing numerous documents, and the user only needs to submit a single trapdoor to the cloud for querying shared documents.

III. Problem Statement

In the current landscape of cloud computing, both organizations and individuals are increasingly reliant on remote storage solutions to handle extensive volumes of sensitive data. However, ensuring the privacy and confidentiality of this data presents notable hurdles, particularly when striving to achieve efficient search capabilities over encrypted data, all while adhering to multi-authority access control policies.

The principal challenge tackled by this project involves creating a resilient system capable of facilitating secure keyword searches over encrypted cloud data while accommodating the demands of multi-authority attribute-based access control. This entails the development of mechanisms that empower authorized users to search for specific information based on keywords or attributes, while concurrently preventing unauthorized access attempts to sensitive cloud-stored data.

IV. Proposed Model

The proposed system model consists of four components namely Data Owner (patients), Data User (doctors belonging to different hospitals), Trusted Authority and Cloud Service Provider.

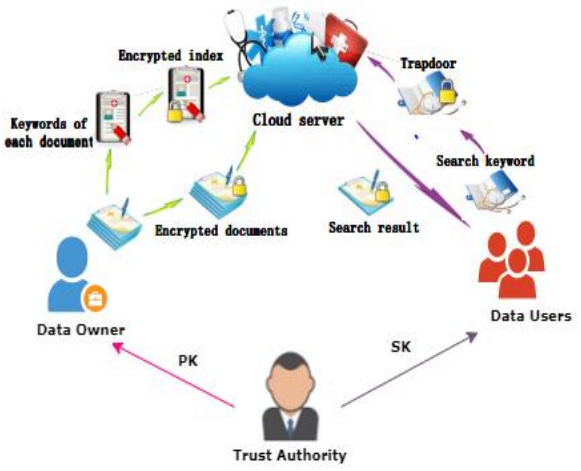

Fig 1. The system architecture design

Data Owners:
Data owners are entities or individuals who possess ownership rights over the data stored in the cloud. They are responsible for determining access control policies, defining attributes, and specifying which users or authorities have permission to access specific data based on their attributes.

Data owners collaborate with trusted authorities to establish and enforce access control policies that govern data access within the cloud environment. They may also interact with data users to grant access to relevant data based on predefined attributes and search criteria.

Data Users:
Data users are individuals or entities who require access to specific data stored in the cloud for various purposes, such as information retrieval, analysis, or decision-making.

Data users submit search queries containing keywords or attributes to retrieve relevant encrypted data from the cloud storage while preserving data privacy. They rely on the mechanisms established by the trusted authorities and data owners to access encrypted data securely and efficiently based on their authorization levels and attributes.

Trusted Authority:
Trusted authorities are entities responsible for managing

and enforcing access control policies in the multi-authority attribute-based system. They collaborate with data owners to define attribute-based access control policies and ensure that these policies are enforced consistently across the cloud environment.

Trusted authorities authenticate users, validate their access rights based on attributes, and facilitate secure keyword search operations over encrypted data. They play a central role in mediating interactions between data owners, data users, and the cloud service provider to ensure secure and efficient data access and retrieval.

Cloud Service Provider:
The cloud service provider hosts and manages the infrastructure and resources required for storing and processing encrypted data on behalf of data owners and users. The provider ensures the confidentiality, integrity, and availability of the data stored in the cloud environment and adheres to service-level agreements (SLAs) regarding data security and privacy.

While the cloud service provider does not have access to the plaintext data, it facilitates encrypted data storage, retrieval, and processing operations as per the instructions and policies defined by data owners, users, and trusted authorities.

The main contributions of the system are as follows:

- ***Attribute-Based Encryption (ABE)***
  Attribute-based encryption (ABE) is a cryptographic method utilized for enforcing access control policies reliant on attributes. In this context, the patient employs ABE to encrypt data before transferring it to the cloud. Each user is linked to a set of attributes, and access policies are formulated accordingly. ABE ensures that data is encrypted to allow decryption solely by users possessing specific attributes.

- ***Multi-Authority Setup***
  In this scenario, multiple authorities may exist, each having its own attribute authorities tasked with overseeing access control policies. Every authority has the autonomy to establish its unique set of attributes and access policies for its data. The implementation of a multi-authority setup guarantees decentralized management of attributes and access policies, thereby improving scalability and flexibility.

- ***Keyword Searchable Encryption***
  Conventional ABE schemes lack the capability for keyword search within encrypted data. Nonetheless, in this context, users require the ability to search for particular keywords within encrypted documents. To achieve this, techniques like searchable encryption are utilized, preserving data confidentiality while enabling keyword searches. Approaches such as attribute-based keyword search (ABKS) empower authorized users to search for keywords based on their attributes, all without disclosing document contents to the cloud server.

- ***Secure Index Generation***
  To facilitate keyword search within encrypted data, secure indexes are created for individual documents based on their contained keywords. These indexes undergo encryption using ABE, guaranteeing access solely to users possessing relevant attributes. The generation of secure indexes encompasses methods like constructing inverted indexes and employing ABE for encryption.

- ***Fine-grained Keyword Search Operation***
  When a user intends to search for a particular keyword, they send a search query to the cloud server. Equipped with the requisite cryptographic keys and access policies, the cloud server conducts the search operation on the encrypted data and provides the relevant results to the user. The search process is structured to ensure that the cloud server gains no knowledge of the plaintext data or the search query.

- ***Access Control Mechanism***
  Prior to allowing access to search outcomes, the cloud server confirms that the attributes of the requesting user align with the access policies linked to the encrypted data. Through access control enforcement, only authorized users possessing pertinent attributes are permitted to access the search results.

- ***Privacy and Security Considerations***
  Throughout the procedure, several security and privacy concerns need attention, encompassing safeguarding data confidentiality, guaranteeing data integrity, thwarting unauthorized access, and managing risks like insider attacks and collusion.

V. Working

Initially, the Data Owners and Data Users will register with the system. Trusted Authority will generate public key and master key. Then, by using public key, master key and user attributes (user id, hospital name, specialization) it will also generate private keys (secret key) for each data user i.e., doctors.

Now, the data owners will encrypt the data records using their public key, user attributes and keyword before outsourcing the them. The keyword is also encrypted by using a random symmetric key and will be shared to the specific data owner only. Thus, the data owner will share or upload the encrypted data records to the cloud server ensuring that data remains encrypted even during search operations. This prevents unauthorized access to plaintext data by the cloud service provider or any unauthorized entities.

If the data owner i.e., a particular doctor wants to view the data records, he can only able to access the encrypted data records shared to him. Using the keywords which are shared by the data owners, the data user can search for the data records. This moment the Cloud Server searches for the encrypted data records matching the keyword and results the relevant data records only. Thus, efficient search functionality is achieved as the users can retrieve relevant information promptly without compromising data privacy.

Here the encrypted data records can be decrypted and downloaded by the data user using their secret key. If the user's attributes satisfy the access policy, then only they can decrypt and download those encrypted data records with a private key. Otherwise, they are denied to access those data records.

VI. Results and discussion

The primary objective of the system is to furnish an optimal user experience for hospital personnel, enabling efficient searching of patient records while adhering to access control policies. Before transferring data to the cloud, the patient encrypts it using attribute-based encryption (ABE), ensuring that only users who are equipped with specific attributes can decrypt and access it. Access policies, based on users' attributes, provide precise control over access to patient records.

Authorized users can send search queries to the cloud server, specifying keywords related to patient conditions, treatments, or demographics. The cloud server conducts search operations on the encrypted indexes, identifying relevant documents based on the search criteria. Only documents meeting the access control policies of the querying user are returned as search results, ensuring data confidentiality and compliance with privacy regulations.

The system employs cryptographic methods to safeguard patient data confidentiality and prevent unauthorized access. Robust access control mechanisms enforce granular access policies, reducing the risk of data breaches and insider threats. Measures to preserve privacy are implemented to prevent the disclosure of sensitive information during search operations or access control verifications.

VII. Conclusion

The system is designed to accommodate multiple authorities, thereby avoiding performance bottlenecks typically associated with centralized systems in cloud environments. As the data will be encrypted before it is outsourced, integrity and confidentiality of the data is maintained. Also, only relevant search results are retrieved using keywords which significantly boosts the systems overall performance. They are provably secure, ensuring that the untrusted server gains no insight into plaintext from ciphertext alone. They uphold query isolation, preventing the server from extracting additional information beyond search results. Controlled searching restricts the server from querying arbitrary words without user authorization.

Additionally, the introduced MABKS system enables the tracing of malicious Attribute Authorities (AAs) to mitigate collusion attacks and supports attribute updates to prevent unauthorized access using outdated secret keys.

However, a notable limitation is that the MABKS system does not support advanced search queries such as conjunctive keyword search, fuzzy search, or subset search. Future efforts will concentrate on developing an efficient and adaptable index construction method to enable the MABKS system to handle a variety of search requests effectively.

References

[1] 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.

[2] 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.

[3] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in Proc. IEEE Conference on Computer Communications (INFOCOM'14), 2014, pp. 522–530.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An ex pressive, efficient, and provably secure realization." in Proc. International Conference on Practice and Theory in Public Key Cryptography (PKC'11), vol. 6571, 2011, pp. 53–70.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.

[6] Baojiang Cui, Zheli Liu, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on Computers, January 2015.

[7] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp. 127–138, 2015.

[8] Yinbin Miao, Robert H. Deng, Fellow, IEEE, Ximeng Liu, Kim-Kwang Raymond Choo, Senior Member, IEEE, Hongjun Wu, and Hongwei Li "Multi-authority Attribute-Based Keyword Search over Encrypted Cloud Data" IEEE Transactions on Dependable and Secure Computing (Volume: 18, Issue: 4 01 July-Aug. 2021)

[9] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. In Annu. Int. Conf. the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, pp. 457–473, Springer, Berlin.

[10] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, “Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 5, pp. 533–546, 2016.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM conference on Computer and communications security (CCS’06), 2006, pp. 89–98.

[12] J. Li, X. Lin, Y. Zhang, and J. Han, “Ksf-oabe: outsourced attribute-based encryption with keyword search function for cloud stor age,” IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715–725, 2017.

[13] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, “Privacy-preserving attribute-based keyword search in shared multi-owner setting,” IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–15, 2019.