International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Multi-Authority Attribute Based Keyword Search Over Encrypted Cloud Data

Mr. Madar Bandu, L. Sai Kethana, M. Uday Sai Kiran, N. Meghan Satwik, P. Keerthipriya

Department of Computer Science and Engineering, Anurag University Hyderabad Telangana.

Abstract: To guarantee data security and usability in the cloud simultaneously, Searchable Encryption (SE) is an important technique. Using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control at a time. However, the single attribute authority in existing CP-ABKS schemes is done with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our meticulous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.

Keywords: Searchable encryption, attribute-based encryption, multi-authority, access control, selective-matrix model, selective-attribute model.

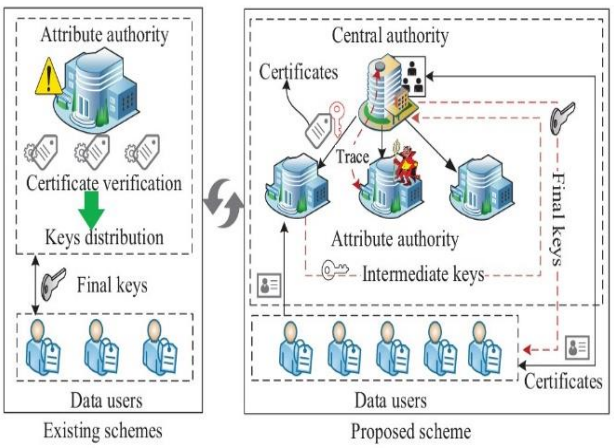
1. Introduction

Cloud computing is a powerful technology that uses the Internet and remote servers to maintain massive-scale data and perform complex computing. An important application of cloud computing is in personal health record systems where individuals can access, manage and share their health information. Each patient is completely in control of his personal health record and can freely share his health information with a wide range of users, such as staff from healthcare providers. In order to minimize storage and operational costs, many large organizations and individual users outsource their personal health records to the cloud. However, in some way, it directly makes patients lose control of their personal health records. In addition, the semi-trust cloud server can smoothly view personal health records and, in some cases, personal health records may even be utilized for unauthorized secondary use or commercial use. In order to ensure the confidentiality of sensitive personal health records, it is necessary for patients (data owners) to encrypt their personal health records (data) before outsourcing them to the cloud. This, however, prevents users from searching outsourced encrypted data as normal search algorithms cannot be executed in the encrypted domain.

Searchable encryption (SE) is a cryptographic technique that allows searching specific information (e.g., keyword) in an encrypted document without learning information about the plaintext data. The key steps are as follows. First, a data owner gets the set of

keywords and encrypts both documents and keywords, and uploads both the encrypted document and the keyword ciphertext to the cloud. Then, when a data user needs to retrieve some document, he generates a keyword token and sends the token to the cloud. Finally, the cloud uses a search algorithm to verify which keyword ciphertext matches the keyword token and sends back the encrypted document with matching keywords to the data user. But, in traditional searchable encryption, the access of a user to the shared data is all or nothing which means one can get the entire access to the data if he gets the secret key; otherwise, he can get nothing. However, in many cases, the data owner may expect to share his data in a more expressive way.

Attribute-based encryption (ABE) addresses the above problem. An ABE scheme is attribute-based encryption where each user is defined by a set of attributes. Sahai and Waters introduce the concept of ABE which enables us to implement access control over encrypted files by utilizing access policies. The ABE scheme, namely Ciphertext-policy ABE (CP-ABE) is proposed. In this scheme, each ciphertext is related to a set of attributes, and each user's private key is associated with an access policy for attributes. A user is able to decrypt a ciphertext if and only if the attribute set related to the ciphertext satisfies the access policy associated with the user's private key. To realize fine-grained access control and keyword search in an e-healthcare cloud computing system, we are using the attribute-based encryption technique.



Prior work did not demonstrate that the existing attribute-based mechanisms could both support keyword search and data sharing in one scheme. Therefore, a secure scheme is desired to fully support keyword searching and data sharing as well as the protection of the privacy of keywords. So, here we are introducing a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The searching and sharing functionality are enabled in the ciphertext-policy setting.

2. Literature Review

D. X. Song, D. Wagner, and A. Perrig et al. proposed a desirable methodology to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proof of security for the resulting cryptosystems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano of Public key encryption with keyword search (PKES) enables senders to send encrypted data to a receiver like traditional public key encryption (PKE) schemes. The difference between PKES and PKE is that the receiver in PKES can search on the encrypted data which is stored on a third-party server (like a cloud storage server). As far as we know, most of the existing PKES schemes are based on a bilinear map, so they are costly in computation and hard to be used in practice. In this paper, we construct a PKES scheme based on factoring, it's computationally efficient and secure. The public parameters in our scheme are also short, we just need a public module and a random element of the set of integers.

Q. Zheng, S. Xu, and G. Ateniese et al implemented a technology that is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VABKS and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

Later and *Waters et al.* described an approach to construct searchable encrypted audit logs and showed that PEKS has a wide application. *Park et al.* defined a security model for PEKS with conjunctive keyword search and proposed two efficient search constructions which partly hide keywords, as the search token reveals the positions of keywords that are needed to query encrypted data.

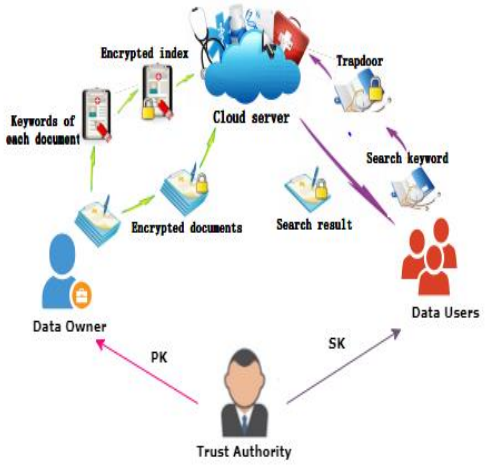
The desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. However, this also implies the necessity of securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data. *Baojiang Cui et al.* is proposed the novel concept of key aggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents.

3. Methodology

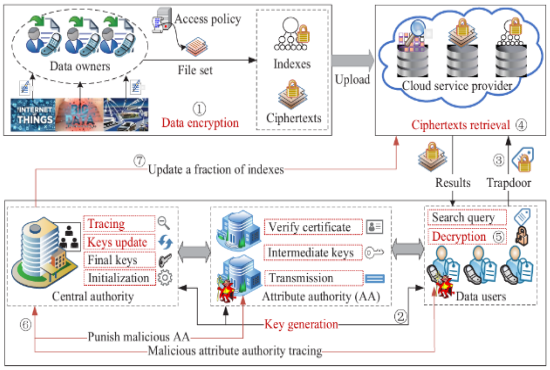
3.1 System Model

Multi-authority attribute-based keyword search over encrypted cloud data (MA-ABKS) is a technique used to securely search for specific keywords within encrypted data stored in a cloud environment, particularly relevant in scenarios where multiple authorities, such as different doctors of different hospitals, need to access and search the patient’s data.

3.2 System Architecture Design



The system architecture typically involves three main components: data owner (patients), cloud server, and data users (authorized personnel within the hospital). The patient owns the data and determines access policies based on attributes (e.g., hospital, specialization) of the users. The cloud server stores the encrypted data and performs search operations on behalf of authorized users. Data users have specific attributes and are granted access to encrypted data based on their attributes.



3.3 Attribute-Based Encryption (ABE)

ABE is a cryptographic technique used to enforce access control policies based on attributes. In this scenario, the patient encrypts the data using ABE before outsourcing it to the cloud. Each user is associated with a set of attributes, and access policies are defined based on these attributes. ABE allows data to be encrypted in such a way that only users possessing specific attributes can decrypt it.

3.4 Multi-Authority Setup

In this scenario, there may be multiple authorities with their own attribute authorities responsible for managing access control policies. Each authority can define its own set of attributes and access policies for its data. Multi-authority setup ensures decentralized management of attributes and access policies, enhancing scalability and flexibility.

3.5 Keyword Searchable Encryption

Traditional ABE schemes do not support keyword search over encrypted data. However, in this scenario, users need to search for specific keywords within encrypted documents. Techniques like searchable encryption are employed to enable keyword search while maintaining data confidentiality. Methods such as attribute-based keyword search (ABKS) allow authorized users to search for keywords based on their attributes without revealing the contents of the documents to the cloud server.

3.6 Secure Index Generation

To enable keyword search over encrypted data, secure indexes are generated for each document based on the keywords it contains. These indexes are encrypted using ABE, ensuring that only users with appropriate attributes can access them. Secure index generation involves techniques such as inverted index construction and encryption using ABE.

3.7 Search Operation

When a user wants to search for a specific keyword, they submit a search query to the cloud server. The cloud server, equipped with the necessary cryptographic keys and access policies, performs the search operation on the encrypted data and returns the relevant results to the user. The search operation is executed in such a way that the cloud server does not learn anything about the plaintext data or the search query.

3.8 Access Control Enforcement

Before granting access to search results, the cloud server verifies that the requesting user's attributes satisfy the access policies associated with the encrypted data. Access control enforcement ensures that only authorized users with relevant attributes can access the search results.

3.9 Security and Privacy Considerations

Throughout the process, various security and privacy considerations must be addressed, including protecting data confidentiality, ensuring data integrity, preventing unauthorized access, and mitigating risks such as insider attacks and collusion.

4. Experiment Results Screenshots

Fig 1. Home page

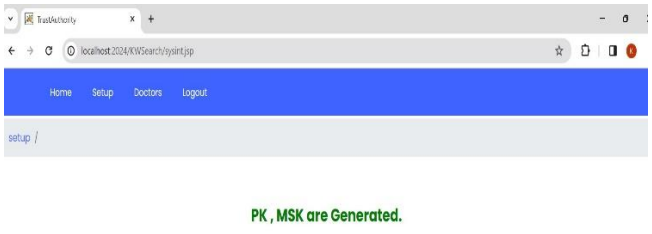


Fig 2. Generation of public and master keys by trusted authority

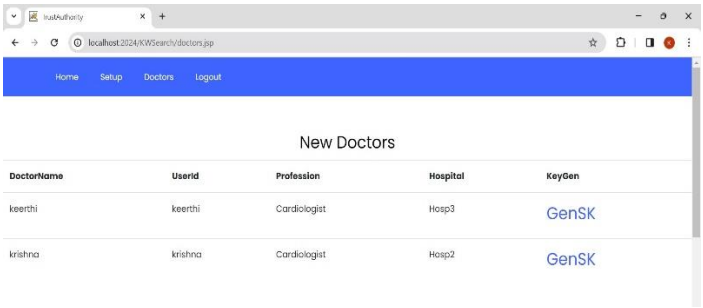


Fig 3. Generation of secret keys for doctors

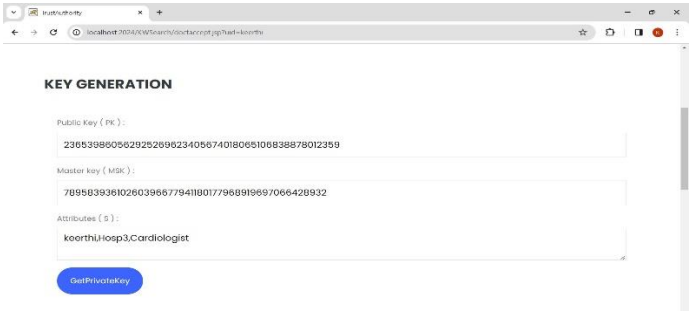


Fig 4. Secret key generation using attributes

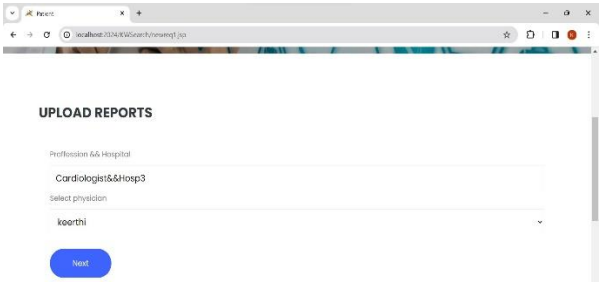


Fig 5. Patient uploads data to specific doctor

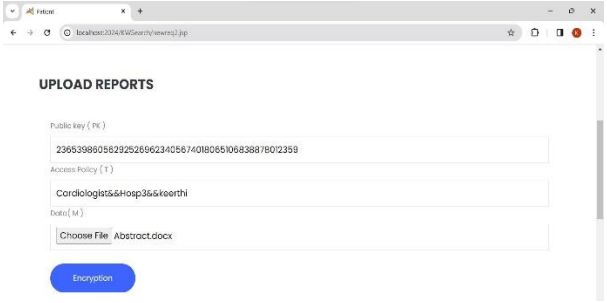


Fig 6. Data files are encrypted using access control policy

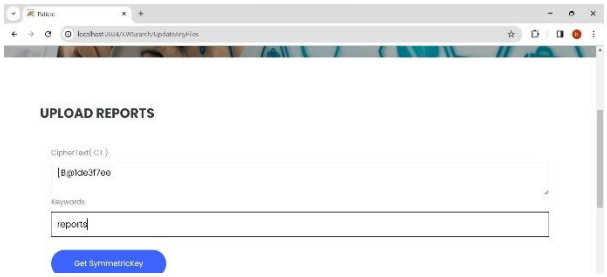


Fig 7. Generating symmetric key using keyword

Fig 8. Encryption of keyword using symmetric key

Fig 9. Patient sharing the data files with the doctor

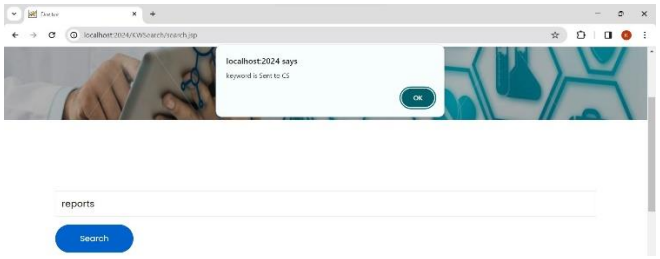


Fig 10. Doctor searches patient's data using keywords

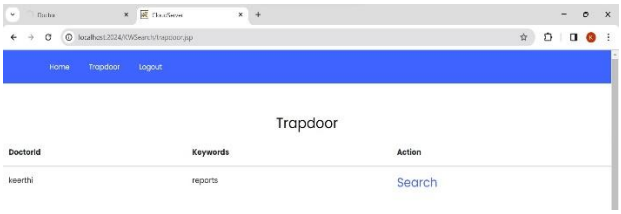


Fig 11. Cloud server search the keyword in the database and return the matched data to the doctor

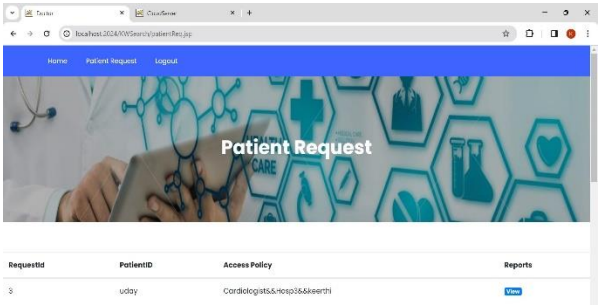


Fig 12. If the access policy satisfies, the doctor can view the encrypted data file

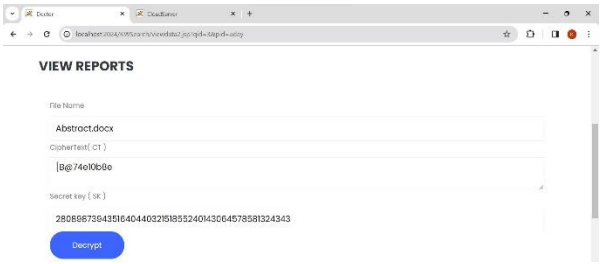


Fig 13. Using secret key doctor can decrypt the encrypted data file

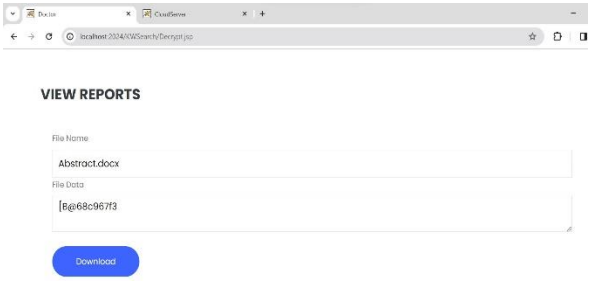


Fig 14. Doctor can download the data file now

5 Results and Discussion

The system is designed to provide a seamless user experience for hospital staff, allowing them to search for patient records efficiently while adhering to access control policies. Before outsourcing the data to the cloud, the patient encrypts the data using attribute-based encryption (ABE). ABE ensures that only users possessing specific attributes can decrypt and access the data. Access policies are defined based on users' attributes, allowing fine-grained control over who can access which patient records.

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

The system employs cryptographic techniques to ensure the confidentiality of patient data and protect against unauthorized access. Strong access control mechanisms enforce fine-grained access policies, minimizing the risk of data breaches and insider threats. Privacy-preserving measures are implemented to prevent the leakage of sensitive information during search operations or access control checks.

6. Conclusion

The system supports multiple authorities, in order to avoid having performance bottleneck at a single point in cloud systems. Furthermore, the presented MABKS system allows us to trace malicious AAs (e.g., to prevent collusion attacks) and support attribute update (e.g., to avoid unauthorized access using outdated secret keys). We then demonstrated the selective security level of the system in selective-matrix and selective-attribute models under decisional q-parallel BDHE and DBDH assumptions, respectively. We also evaluated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes. However, the main flaw is that the MABKS system cannot support expressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. The future work will focus on building an efficient and flexible index construction so that the MABKS system is capable of supporting various search requests.

7. 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] 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.

[3] 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.

[4] 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.

[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] 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.

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