IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003031

# Traceable Authorization Secure Keyword Search System for Cloud Storage

**Sajjada Zeba Mojez[1], Dr. A ADandavate[2], Mr. M D Ingle[3]**

PG Student, Department of Computer Engineering, JSPM's Jayawantrao Sawant College of Engineering, Hadapsar, India[1]

Professor, Department of Computer Engineering, JSPM's Jayawantrao Sawant College of Engineering, Hadapsar, India [2]

**ABSTRACT:** A large number of data owners have transferred their data to cloud storage for multiprocessing ease, but confidential and sensitive data must first be encrypted before being processed in the cloud. In cloud computing, keyword search over encrypted data is important. In a multi-owner scheme, fine-grained access control is needed to prevent unauthorized data access. Registered owners sometimes misplace the secret key for a fee. As a result, tracing and revoking the malicious user who is abusing the secret key must be resolved as soon as possible. We present a free traceable attribute-based multiple keywords subset search method with verifiable outsourced decryption in this paper. When users' searching inputs exactly match the predefined keywords, keyword search significantly improves device usability by returning matching files. We extract the keywords from the file, encrypt them, and then add them to the index in our solution. Instead of storing the file and searchable index in the cloud, the proposed method would store the file on a private server and the searchable index in the cloud. This greatly eliminates network congestion and overheads, as well as file retrieval speed and storage by using file compression. We demonstrate that our proposed solution is safe and privacy-preserving with enhanced protection using encryption techniques and permission to access the data, as well as accurate security analysis.

**KEYWORDS:** authorized searchable encryption, traceability, verifiable outsourced decryption, key escrow free, multiple keywords subset search.

## I. INTRODUCTION

Many companies find that outsourcing data to the public cloud is an appealing business practice because of the need for data and services at lower costs. Data protection and privacy, on the other hand, have become crucial. Concern for the service provider and service users by adopting cloud services, especially for the public cloud, for commercial purposes. Outsourced data can contain sensitive information, such as a person's or organization's financial records, tender information, personal medical records (PHR), and so on, where the data may give the cloud server or unauthorized users access to and/or infer sensitive information. A feasible approach to the issue of data protection and access control is to encrypt documents before sending them to a cloud storage server [1]. Consider the following scenarios: most data owners use public cloud storage services to upload encrypted information, and multiple users can access documents stored on the cloud storage server. Applying fine-grained access control policies to such applications enables the security check offered when accessing documents. Searchable Encryption is a process that allows you to search for keywords in encrypted data [2].

Searchable encryption can assist a receiver in retrieving data from public cloud storage that is of interest to the user and is available to the user in a safe and selective manner. For example, a doctor may want to look up all of his patients' medical records that have been diagnosed with chronic kidney disease and for whom the doctor has been granted access to the patient's medical records, where each report is encrypted and submitted by the patient. In this case, single-user searchable symmetric encryption schemes are ineffective since the patient must encrypt his medical records with his secret key and then share this secret key with the doctor. As a result, multi-user searchable symmetric encryption schemes [6–8] are the most powerful for implementing access control policies and searching over encrypted data, where a data owner, such as a patient, may generate the shared secret key or search token from his master secret key and issue it

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003031

to approved users (e.g., doctor in our example) for searching over encrypted data. While these schemes can be used in a single-sender multi-receiver scenario, they cannot be used in a multi-sender multi-receiver scenario because each data sender must communicate with each data receiver in a safe manner in order to issue the secret key or search token, which incurs a significant communication overhead [9].

The allowed entities can benefit from illegally disclosing their secret key to a third party. Assume a patient learns one day that a hidden key relating to his electronic medical data is being sold on e-Bay. Such heinous action puts the patient's data privacy at risk. Much worse, whether the insurance provider or the patient's employer misuses private electronic health data containing severe health diseases, the patient's medical insurance or labour contracts will be terminated. The deliberate disclosure of hidden key, foundations of permitted access control and data privacy security. As a result, identifying the malicious user, or even proving it in court, is critical [4]. The secret key of a user is associated with a collection of attributes rather than the individual's identity in an attribute-based access control scheme. It's difficult to track down the original key owner since the search and decryption authority can be shared by a group of users who share the same collection of attributes. It's important to have traceability to a fine-grained search authorization scheme, which hasn't been taken into account in previous searchable encryption schemes [5].

## II. RELATED WORK

1. “Keyword quest with public key encryption” We look at the problem of searching for data encoded with an open key scheme. Consider the case of customer Bob, who sends email to customer Alice while Alice's key is open. With the aim of properly routing the email, an email entryway must verify whether the email contains the catchphrase "sincere." Consider a mail server that holds numerous messages that have been plainly encoded for Alice by others. Using our tool, Alice can send a key to the mail server that will allow the server to see all messages containing a specific catch, but nothing else. We show open key encryption with password demand and suggest two or three improvements [1].

2. “Vabks: Verifiable attribute-based keyword search over encrypted data outsourced” Nowadays, it is common for data owners to re-appropriate their data to the cloud. Since the cloud can't be trusted fully, re-appropriated data should be encrypted. This, however, raises a slew of questions, such as how does a data owner provide data customers with look capabilities? What advantages do endorsed data consumers have over re-appropriated mixed data from a data owner? How can data consumers be confident that the cloud can reliably carry out their interest assignments for their own good? We suggest a novel cryptographic course of action, known as obvious trademark based grab look, in response to these requests (VABKS). A data customer whose credentials satisfy a data proprietor's passageway control system may use the game plan to (I) examine the data proprietor's re-appropriated encoded data, (ii) redistribute the grim interest errands to the cloud, and (iii) confirm whether the cloud has consistently performed the request exercises. We formally define the VABKS security requirements and depict a solution that meets them. The proposed proposals are realistic and deployable, according to the execution assessment [2].

3. Encryption based on fluffy characters. We present Fuzzy Identity-Based Encryption, a new type of Identity-Based Encryption (IBE) storey. We see a way of life as a collection of illuminating properties in Fuzzy IBE. If and only if the characters and 0 are close to each other as measured by the "fixed cover" simple calculation, a Fuzzy IBE invention considers a private key for a character,, to unravel a figure content encoded with a personality, 0. A Fuzzy IBE plot can be used to allow encryption using biometric identities as identities; the error prevention property of a Fuzzy IBE plot is entirely what considers the use of biometric characters, which normally cause some commotion when dismembered. Similarly, we show that Fuzzy-IBE can be used for a form of application that we call "trademark based encryption." We display two Fuzzy IBE plan headways in this article. Our headways can be viewed as an Identity-Based Encryption of a message that is formed by many properties that form a (padded) character. Our IBE structures are both blunder-resistant and protected against ambush intrusion. Furthermore, we do not rely on sporadic prophets to make significant progress. We use the Selective-ID protection display to demonstrate the security of our plans [3].

4. “Revisiting searchable encryption: Consistency properties, anonymous IBE, and extensions” With a watchword search for open key encryption, we see and fill two or three gaps in terms of consistency (how many false positives are generated) (PEKS). We show computational and authentic relaxations of the current idea of perfect continuity, show that the game plan is computationally constant, and propose another course of action that is quantifiably reliable. We also make a distinction in a strange IBE plan between an anchored PEKS plot that, unlike the previous one, ensures continuity. Finally, we suggest three enhancements to the main ideas discussed here: clearly amazing HIBE, open key encryption with brief catchphrase demand, and character-based encryption with watchword look [4].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003031

"Anonymous hierarchical identity-based encryption (without random oracles)" is number five. We demonstrate a character-based cryptosystem with completely cloud figure writings and a unique levelled key mission. In view of the fragile Decision Linear multifaceted existence supposition in bilinear social gatherings, we include a proof of protection in the standard model. The structure is incredible and welcoming, with small figure writings of varying sizes directing attention to the hugeness of the chain. Applications combine interest in encrypted data, completely private communications, and so on. Our findings resolve two open issues in the field of darken character-based encryption, with our strategy being the first to include a provable puzzle in the standard model, despite being the first to detect completely unique HIBE at all measurements in the chain of significance [5].

6. "Revocable keyword search with efficient public key encryption" Open key encryption with explicit watchword look is a novel cryptographic rough engaging one to specifically look for on encoded data. According to the known plans, once a trapdoor is obtained, the server can search for related data without restriction. In any case, in light of the fact that the server isn't completely trusted, it's sometimes necessary to keep the server from constantly scanning the data. To fix the issue, we propose open key encryption with revocable watchword chase in this paper. Similarly, we develop a strong change by splitting the whole system's presence into discrete events in order to achieve our goals. Under the co-decisional bilinear Diffie– Hellman assumption in our security demonstrate, the proposed plot achieves the properties of the caprice of cypher texts against a versatile picked watchwords ambush security. Our own, which is differentiated and two somewhat plots, provides much better execution in terms of computational cost [6].

7. "Practical methods for encrypted data searches" To reduce security and privacy risks, it is appealing to store information in encrypted form on information storage servers, such as mail servers and record servers. However, this usually implies that utility must be sacrificed in the name of protection. For example, if a customer wants to recover only archives containing specific terms, it wasn't clear how to let the information storage server carry out the inquiry and respond without losing information classification [7].

## III. OPEN ISSUES

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the techniques for Traceable search systems [3].

**Authorized keyword search is inflexible -** Several documents are held in encrypted form in the safe cloud storage system. To make document searching easier, a versatile safe keyword query feature is needed. Furthermore, the cloud files should be shared among various data users through a flexible authorization mechanism.

**Inflexible system extension -** If a new attribute is applied to the system, it must be rebuilt from the ground up, with all encrypted files re-encrypted. The cloud storage infrastructure will be destroyed [2].

**Abuse of the attribute secret key** - Approved entities can sell their secret key to a third party illegally for profit.

**Ineffective user revocation** - In a multi-user cloud storage environment, the ability to revoke access is critical [4].

**Escrow's most serious problem** - In conventional searchable encryption systems, the key generation centre generates all of the users' secret keys (KGC). As a result, all confidential keys are escrowed to KGC, and the data user's secret key is revealed to both KGC and the user, a process known as "key escrow."

**Data Security** – The primary concern is data protection.

## IV. PROPOSED SYSTEM ARCHITECTURE

**Group Member**

- In the proposed scheme, members are people with the same interests (e.g., bidder, doctors, and businessmen) and want to share data in the cloud.
- The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003031

- In this system, users of the same group conduct a key agreement. Subsequently, a common conference key can be used to encrypt the data that will be uploaded to the cloud to ensure the confidentiality of the outsourced data.
- Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.

**Group Manager:**

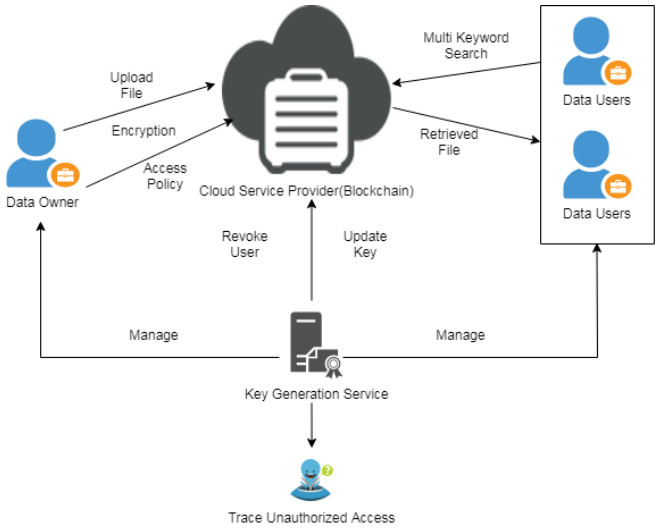
- Group Manager is responsible for generating system parameters, managing group members (i.e., uploading member's encrypted data, authorizing group members) and for the fault tolerance detection.
- The group manager in our scheme is a fully trusted third party to both the cloud and group members.
- If an external user tries to access files from a different group more than three times then the manager will remove that particular user from the applications.

**Cloud Service Provider (CSP):**

- CSP provides users with seemingly unlimited storage services.
- In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services.
- However, the cloud has the characteristic of honest but curious.
- In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user's identity.

**Key Generation Center**

- KGC is responsible to generate the public parameter for the system and the public/secret key pairs for the users.
- Once the user's secret key is leaked for profits or other purposes, KGC runs trace algorithm to find the malicious user.
- After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user's search privilege.




**1.1 Proposed System Architecture**

## V. CONCLUSION

Implementing multikeyword search on encrypted files, enforcing access control, and supporting keyword search are all important issues in this proposed secure cloud storage framework. We proposed a concrete construction and described a new architecture for searchable encryption systems in this paper. It allows for versatile multiple keyword subset searches

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003031

and eliminates the problem of key escrow during the key generation process. Malicious users who sell hidden keys for profit can be tracked and their data stored in the cloud in encrypted form.

## REFERENCES

[1] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.
[2] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Trans. Depend. Sec. Comput., to be published
[3] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," IEEE Trans. Knowl.Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.
[4] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Trans. Comput., vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
[5] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Trans. Depend. Sec. Comput., to be published.
[6] H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," IEEE Trans. Serv. Comput., to be published.
[7] Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.
[8] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.
[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343- 1354.
[10] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.
[11] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in: EUROCRYPT, 2004, pp. 506-522.
[12] Z. Liu, Z. Cao, D.S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 1, pp. 76-88.
[13] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 6, pp. 1274-1288.
[14] Z. Liu, Z. Cao, D.S. Wong, "Traceable CP-ABE: how to trace decryption devices found in the wild," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details