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 6, June 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 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006166|

Review on Traceable Authorization Multi-Keyword Search System in Cloud Computing

Mansi Vijay Nawale[1], Kaveri Jagannath Ugale[2], Akanksha Kashinathkadam[3], Amruta Narendra Deshmukh[4], Dr. H.B.Jadhav[5]

Students, Department of Computer Engineering, S.C.S.M.C.O.E, Nepti, Maharashtra, India[1, 2, 3, 4]

Professor, Department of Computer Engineering, S.C.S.M.C.O.E, Nepti, Maharashtra, India[5]

ABSTRACT: While several data owners have moved their data to cloud storage to facilitate multiprocessing, confidential and sensitive data must first be encrypted before being processed in the cloud. Keyword search over encrypted data is critical in cloud computing. To prevent unauthorised data access in a multi-owner scheme, fine-grained access control is required. The hidden key is sometimes misplaced by registered owners for a fee. As a result, locating and revoking the malicious user who is exploiting the secret key must be completed as quickly as possible. In this article, we present a search method with a free and verifiable outsourced decryption based on multiple keywords. Keyword search increases system effectiveness when files are returned if the user's search input matches the predefined keywords precisely. Our solution is to extract the keywords, encrypt them and add them to the index. Instead of store a file and the searchable index into the cloud, the proposed approach would save the file to a private server. This reduces network congestion and overheads, and speed of recovery and storage by using file compression.

KEYWORDS*:* authorized searchable cryptography, traceability, verifiable outsourced decryption, free key escrow, multiple sub-set search keywords.

I. INTRODUCTION

Because of the need for data and resources at lower prices, many businesses find that outsourcing data to the public cloud is an attractive business practice. On the other hand, data security and privacy have become critical. For the service provider and service users, cloud services, in particular the public cloud, are used for business purposes. Outsourced data could contain confidential information that the cloud-based cloud server or unauthorized users may access and/or infer, such as a person or organization's financial record, tender data, personal medical records (PHRs), etc.Encrypting documents before sending them to a cloud storage server is a viable solution to the problem of data security and access control. Consider the scenarios below: Most data holders use public cloud storage services for the uploading of encrypted data, and multiple people can access records which are stored in the cloud storage system. If a thorough access control policy is applied to these applications, a safety check is provided when documents are accessed. The searchable encryption method helps to search for encrypted data with keywords.

Searchable encryption can aid a recipient in the retrieval of data from the user-interesting public cloud storage, which is secure and selectively available to the user. A doctor may, for example, want to review all of the medical records of his patients that have been diagnosed with chronic kidney disease and for whom the medical records of the patient have been given to the doctor, where each report is encrypted and provided by the patients. In this situation, single-user symmetric coding systems are ineffective because patients need the secret key to encrypt their medical records and then share this secret key with the physician.As a result, multifunctional symmetrically searchable encryption systems are the most powerful to implement access control policies or to search encrypted data when a database owner such as a patient, from his master secret key, can generate the secret shared key or token and send it to authorised users (e.g. a physician, in our example). Whilst the schemes are usable in a single sent multi-receiver scenario, they cannot be used in a multi-sender multi-receiver scenario because every sender of data must communicate securely with each receiver so that the secret key or search token can be issued, which is a significant overhead communication.

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

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

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006166|

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 labor contracts will be terminated. The deliberate disclosure of a hidden key jeopardizes the foundations of permitted access control and data privacy security. As a result, identifying the malicious user, or even proving it in court, is critical. 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.

II. RELATED WORK

We[1] examine the problem of data search with an open key system. Consider Bob, who sends an email to Alice when the key of Alice is open. An eMail entry must check if the email contains a 'sincere' catchphrase, in order to properly route the eMail. Consider a mail server containing numerous messages that others have encoded for Alice. Alice can use our tool to send a key to the server so that it can see all the messages with a certain catch, but nothing more. We show open password-required key encryption and propose two or three improvements.

It is common for data owners to reuse their data into the cloud nowadays[2]. Since cloud cannot be fully trusted, it is important to encrypt re-appropriated data. That however raises a number of questions such as how can a data owner offer data customers the ability to look? What are the benefits for endorsed data consumers over a re-appropriated data owner's mixed data? How can data consumers be sure of the cloud being able to reliably fulfil its own interests? In response to these requests, we propose a new cryptographic path, known as a clear mark based grab look (VABKS).A data client whose credentials meet the passageway system of a data proprietor can use a game plan, to I review the re-appropriated encoded data of the data proprietor, (ii) redistribute the grim cloud interest orders, and (iii) to verify if the cloud has consistently exercised the request. We define formally and present a solution that meets VABKS security requirements. According to the implementation evaluation, the suggestions are realistic and deployable.

We [3] see a way of life in Fuzzy IBE as an illuminating collection. Only when the features and zero are close together by the calculation of the "simple fixed cover," a Fuzzy IBE invention, in order to uncover the figurative contents with a personality, considers a private key to a particular character. 0. A Fuzzy IBE plot may be used to encode biometrical identities as identities; the Fuzzy IBE plot is a mispronouncement property completely deemed to be the use of biometric characters which, if dismembered, normally cause some turmoil.Similarly, we show that Fuzzy-IBE may be used as a "trademary-based encryption" application. This article shows two progressive Fuzzy IBE plans. Our progress can be seen as an ID-based encryption of a message formed of several (padded) properties. Our IBE structures are both stupid and safe from embushments. Moreover, in order to achieve significant progress we do not rely on sporadic prophets. We use the Selective-ID protection display to show our plans' safety.

We[4] see two or three consistency gaps (how many false positives are generated) in the search for open key encryption by watchword (PEKS). We show the current idea of perfect continuity computational and genuine relaxation, prove that the plan is computationally consistent, and propose another measurably reliable course of action. In a strange IBE plan, we distinguish between a plot of anchored PEKS which guarantees continuity, unlike the previous. Finally, three enhancements are proposed to the main ideas discussed: clearly incredible HIBE, open key encryption with a short catchphrase requirement and watchword-style encryption.

We show a character-based crypto-system with entire cloud scripts and a unique levelled key task. Given the fragile linear multifaceted assumption of existence in bilinear social gatherings, the standard model includes evidence of protection. The structure is unbelievable and welcoming. Small pieces of various sizes focus on the hardness of the chain. Applications bring together interest in encrypted data, entirely private communications etc.Our findings solve two open problems in the field of dark character-based encryption, with our strategy as the first in the standard model to include a proven puzzle although the first one in all measures in the chain of importance to find completely unique HIBE [5].

Open key [6] encryption with an explicit look at the watchword is a new encrypting rough that specially searches for encoded information. The known plans allow the server to search for the data without restriction once a trapdoor has been obtained. In any case it is sometimes necessary to prevent the server from constantly scanning the data because the

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

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006166|

server is not entirely trusted. In order to solve the problem, we propose in the paper open key encryption with revoked motto chase. Similarly, to achieve our objectives, we are making strong changes by dividing the presence of the entire system into discrete events.Assumption in our security demonstrates, 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.

It is useful [7] to store in encrypted form information on information storage servers, such as mail servers and recording servers, in order to reduce security and privacy risks. But this usually means that utility in the name of protection must be sacrificed. For example, if a customer only wishes to recover archives with specific terms, it was not clear how the server can perform the inquiry and reply without losing information classification.

III. EXISTING SYSTEM

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.
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.
Escrow's most serious problem - The key generation center generates all the secret user keys in conventional searchable encryption systems (KGC). As a result, all confidential keys will be escorted to KGC and both KGC and the user, a process known as "key escrow," will receive a secret key from the user.
Data Security – The primary concern is data protection.

IV. PROPOSED SYSTEM

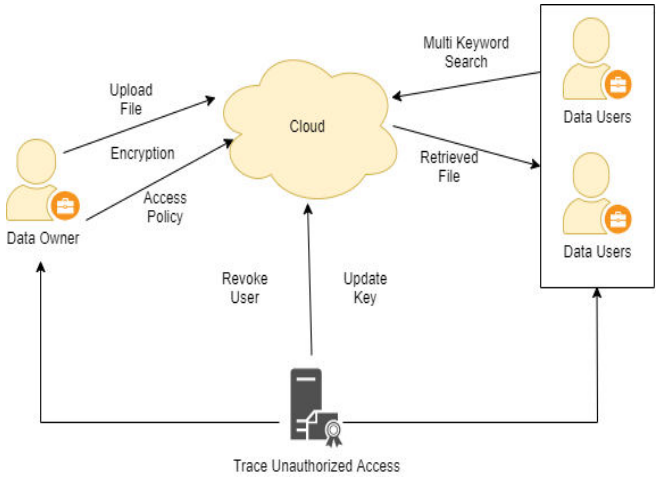

Figure. System Architecture

- **Flexible authorized keyword search** –This proposed system obtains fine-grained authorization to access the data and supports multiple keyword subset searches for encrypted information.
- **Flexible System Extension -**In the system initialization stage, attributes are not fixed and the size of a set of attribute is not limited to polynomials and can be added to the system at any time.
- **Traceability of Abused Secret Key -**Approved users leak or sell their secret key, traceability of a white-box is able to identify who is leaking a key.
- **Efficient revocation from group -**Once a user is tracked by an algorithm, the system proposed cancels this malicious user off the authorized group.
- **Key Escrow Free -** lightweight holomorphic encryption algorithm is utilized for key escrow problem.

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

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006166|

- **Data Security** –Crypto data on block chain technology is stored in the proposed system. Data distribution is less the result of block chain data stored on nodes and potential data loss.

V. CONCLUSION

Implementing multi-keyword 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 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