IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

Multi-keyword Searchable Encryption System against Insider Keyword-Guessing Attack in Cloud Computing

Mr.Ghadage Rohit, Prof.Joshi S.G.

Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India

ABSTRACT: Searchable Encryption (SE) is a type of encryption that lets cloud tenants search for encrypted data while keeping their data safe. Insider Keyword-Guessing Attacks are still a problem for a lot of search engine solutions. This means that the internal hackers can figure out the candidate keywords off-line and use them to search for them. Also in existing SE solutions, asemi-honest- but-curious cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly. This system can withstand the inside KGA and achieve verifiable search ability. After introducing the basic version of VSEF, we then show how the enhanced version of VSEF can search for multiple keywords, encrypt multiple keys, and make dynamic changes to data at the same time. This shows how important it is for SE to be practical and scalable in real-world applications using advanced encryption techniques.

KEYWORDS: Advanced encryption, insider keyword- guessing attack, multi-keyword search, multi-key encryption

I. INTRODUCTION

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also provides convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern. As the data shared on the cloud is valuable, various security methods are provided by cloud.

In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology. In existing system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack. Another gap is that a user is not allowed to upload multiple files of same name.

A. Problem Statement

To build and implement Multi-keyword Searchable En-cryption System against Insider Keyword-Guessing Attack in Cloud computing.

B. Objectives

- To do an extensive study by insider guessing attacks in cloud.
- To work on Verifiable Searchable Encryption.
- To Design of an enhanced VSEF, we use system model, thread model and security model.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

- To implement enhanced VSEF technique to improve efficiency and security.

- The main goals of the proposed scheme include access control, data confidentiality, data security, data sharing, efficiency and keyword search

C. Motivation

- Searching and sharing the cipher text data, it is challeng-ing to search and share the data.
- In Cloud based group sharing to maintain the data secu-rity the private keys of co members of group need to be updated after the revocation of any group member.
- Also to restrict the malicious members from accessing the data in group file upload constraints will be introduced.
- Data confidentiality will be maintained using encryption when uploading data on cloud.

II. REVIEW OF LITERATURE

In this paper[1], author introduces a new method called linear secret sharing with multiple values, which can greatly improve the expression of access policy. Moreover, each attribute is divided into two parts, namely the attribute name and its value. Therefore, the most obvious advantage of the proposed scheme is that sensitive attribute values can be hidden. And it can protect users' privacy well in PHR.

Authors formulated [2] the security model of IB-CPRE-FG and proved its IND-CCA security. In this scheme, the access policy is decscribed by an access structure. First, it is interesting to construct an IB-CPRE scheme supporting AND or OR gates directly. Second, as many proxy re-encryption schemes [36, 37] have been proposed to capture the key-private property.

In this paper[3], author introduced a new notion of key-policy attribute-based proxy re-encryption and presents an adaptively CCA-secure KP-ABPRE scheme. this scheme extends the notion of proxy re-encryption to key-policy attribute-based encryption setting.

This scheme[4] allows the data owner to conduct a fine-grained search authorization for a data user. The main idea is that a data owner encrypts an index keyword under a specified access policy, if and only if, a data user's attributes satisfy the access policy, the data user can perform search over the encrypted index keyword.

In the paper[5], author presented a practical attribute-based keyword search scheme supporting hidden access policy in the shared multi-owner setting. Furthermore, they demonstrated how the basic ABKS-SM system can be extended to support traceability (i.e., tracing of malicious DUs) in the modified ABKS-SM system, if desired.

In this paper[6], authors propose a privacy-preserving PHR, which supports fine-grained access control and efficient revocation. When encrypting PHRs, patient can associate an expressive access tree structure with the cipher text, thus achieving fine-grained access control. Authors also achieve privacy-preserving by using anonymous key issuing protocol.

In this paper [7], Author solve the problem left by Fang, Susilo, Ge and Wang by proposing a KP-ABPRE scheme without random oracles. this scheme enhances the security model by making some improvements of the re-encryption key query and reencryption query

In this paper [8] for the first time author defined the notion of DFA-based FPRE, and meanwhile proposed a concrete scheme satisfying the new notion. Furthermore author proved the scheme, which is the first of its type, to be adaptively CCA secure in the standard model by employing Lewko et al.'s dual encryption technology.

In this paper [9], author tackled the challenging multi-keyword fuzzy search problem over the encrypted data. Author proposed and integrated several innovative designs to solve the multiple keywords search and the fuzzy search problems.

Author introduced [10] a novel crypto graphic primitive called verifiable attribute-based keyword search for secure cloud computing over outsourced encrypted data. This primitive allows a data owner to control the search of its

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

outsourced encrypted data according to an access control policy, while the authorized data users can outsource the search operations to the cloud and force the cloud to faithfully execute the search (as a cheating cloud can be held accountable).

III. GAP ANALYSIS

- In previous technology in which Searchable Encryp-tion(SE) is used to preventing data confidentially and securely but most of them are still susceptible to insider Keyword-Guessing Attacks (KGA), which implies that the internal attackers can guess the candidate keywords successfully in an off-line manner.

- In SE, cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly (e.g., to save storage space).

IV. PROPOSED METHODOLOGY

We propose a Verifiable SE Framework against insider KGA by extending the public auditing technique to SE scheme and achieve verifiable searchability detection. In the basic VSEF, the costly correctness verification tasks are assigned to a fully-trusted third-party auditor, and in turn, the auditor honestly reports the auditing results to cloud clients. The VSEF support other features like multi-keyword search, multi- key encryption, file sharing. A. Data user

1) In the proposed scheme, members are people with interests (e.g., bidder, doctors, and businessmen)and want to share data in the cloud.

2) The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data.

3) 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.

4) Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the key.

5) Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.

6) Data user search files using multi-keyword search.

B. Data Owner

1) data owner 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.

2) The data owner in our scheme is a fully trusted third party to both the cloud and group members.

3) 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.

C. Cloud Service Provider (CSP)

1) CSP provides users with seemingly unlimited storage services.
2) In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services.

3) However, the cloud has the characteristic of honest but curious.
4) 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

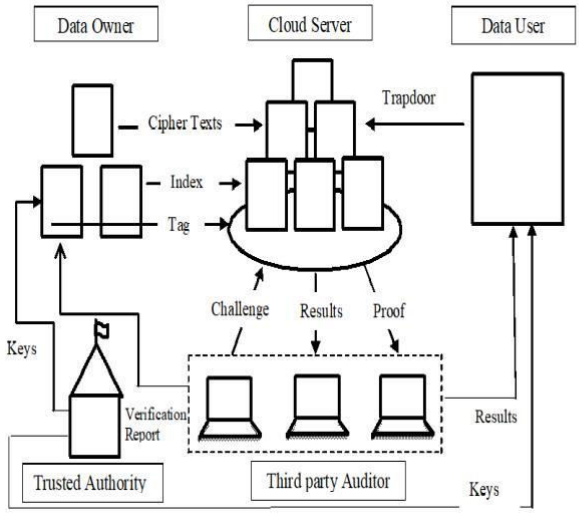
|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

A. Advantages of Proposed System

- It improves efficiency and security.
- This model controlled searching and hidden query.
- It has high key management overhead in symmetric setting.

B. Architecture



Algorithms

1. ECC (elliptic curve cryptography)Encryption Algorithm

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography, based on the algebraic structure of elliptic curves over finite fields. ECC requires a smaller key as compared to non-ECC cryptography to provide equivalent security (a 256-bit ECC security have an equivalent security attained by 3072-bit RSA cryptography). For a better understanding of Elliptic Curve Cryptography, it is very important to understand the basics of Elliptic Curve. An elliptic curve is a planar algebraic curve defined by an equation of the form.

2. TFIDF Algorithm: Terminology:

1. t — term (word)
2. d — document (set of words)
3. N — count of corpus
4. corpus — the total document set

• TF: Term Frequency, which measures how frequently a term occurs in a document. Since every document is different in length, it is possible that a term would appear much more times in long documents than shorter ones. Thus, the term frequency is often divided by the document length (aka. the total number of terms in the document) as a way of normalization:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

tf(t, d) = countoftind/numberofwordsind

• IDF: Inverse Document Frequency, which measures how important a term is. While computing TF, all terms are considered equally important. However it is known that certain terms, such as ”is”, ”of”, and ”that”, may appear a lot of times but have little importance. Thus we need to weigh down the frequent terms while scale up the rare ones, by computing the following:

$$idf(t) = log(N/(df + 1))$$

$$tf - idf(l_i^j)log(tf(l_i^j, d_j) + 1) * log(D/1 + df(l_i^j, D))$$

V. RESULT AND ANALYSIS

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel processor 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as ECC (yellow), AES (Blue).

Fig. 1. System Architecture

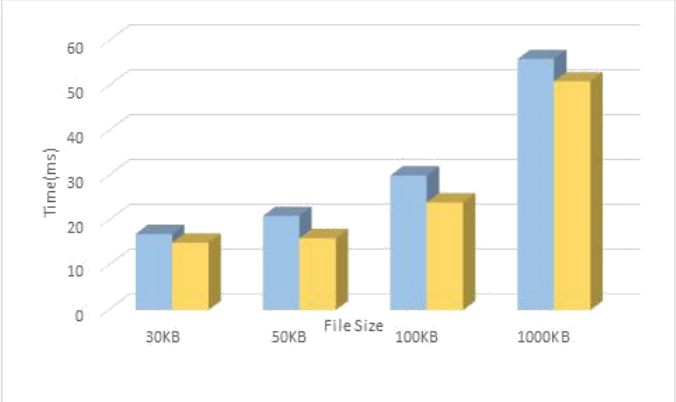


Fig. 2. Encryption and Searching time

Index Number	Image size (KB)	AES Encryption Time	ECC Encryption Time
1	30	31	28
2	50	36	31
3	100	63	58
4	1000	102	93

Fig. 3. Encryption and Searching time

In this paper,we compare system execution time with Hua Deng [1].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005270 |

Fig. 4. overall system execution

VI. CONCLUSION

It was first proposed in this system that a basic VSEF could be used to prevent the malicious CS from giving out bad search results. It could also be used to protect against insider KGA attacks. Then, the basic VSEF was made better to be able to search for multiple keywords, encrypt multiple keys, and update dynamically at the same time in the enhanced VKSF. We showed that basic or enhanced VSEF is safe against the insider KGA, and that it is both correct and sound.

REFERENCES

1. Hua Deng, Jixin Zhang, Zheng Qin, Qianhong Wu, Hui Yin, Aniello Castiglione 2021 " Policy-based Broadcast Access Authorization for Flexible Data Sharing in Clouds"
2. Yinbin Miao, Qiuyun Tong, Robert H. Deng, Fellow, IEEE, Kim-Kwang Raymond Choo, Senior Member, IEEE,Ximeng Liu, and Hongwei Li "Verifiable Searchable Encryption Framework against Insider Keyword-Guessing Attack in Cloud Storage"
3. L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," IEEE Access, vol. 7, pp. 33202–33213, 2019.
4. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy," Computer Standards Interfaces, vol. 52, pp. 1–9, 2017.
5. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," Designs, Codes and Cryptography, pp. 1–17, 2018.
6. H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme," IEEE Access, vol. 7, pp. 5682–5694, 2019
7. 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, 2019.
8. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," The Computer Journal, vol. 59, no. 7, pp. 970–982, 2016.
9. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T.
10. V. X.Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.
11. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE INFO COM 2014-IEEE Conference on Computer Communications, pp. 2112-2120, IEEE, 2014.
12. Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in Infocom, 2014 proceedings IEEE, pp. 522–530, IEEE, 2014.
13. K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1981–1992, 2015.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details