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

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

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: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008009 |

Survey on Secure and Accurate Multi-Keyword Retrieval With Privacy Protection for Multiple Data Owners in Cloud Computing

Supriya Ramdas Shete[1], Prof.Nagaraju Bogiri[2]

Student, KJ College of Engineering and Management Research, Pune, India[1]

Professor, KJ College of Engineering and Management Research, Pune, India [2]

ABSTRACT: Demand for endless storage and high quality retrieval services has increased rapidly, cloud computing is an outstanding technology. A variety of keyword searches have been carried out in numerous research studies into privacy problems. In compliance with the multiple data owners definition, cloud storage is encrypted. However, most of these systems are vulnerable to keyword threats and assaults. In addition, from the individual data owners, the best search results can be returned correctly. Obviously, those disadvantages will lead to an intimate leak. Returned keywords and imprecise search results. The recovery system in this paper contains several confidentiality data holders which allow the cloud server to scan the cloud in a few words and then return the relevant files without a keyword leakage in the data customer search results. We also prove that our system is secure against attacks initiated by indoor and outdoor assailants by rigorous safety analysis. Finally, the performance evaluation shows that our system is more efficient than the current system of graded search keywords.

KEYWORDS: Cloud computing, Encryption, multi-keyword retrieval, multiple data owner model, privacy protection.

I. INTRODUCTION

In Cloud Computing, people and companies will benefit from a high-quality storage facility through the movement and provision of a cloud server service and local data processing and maintenance responsibilities. However, because data owners cannot completely complete their data outsourcing in real-time, extensive use of cloud computing represents the main challenges of data protection and privacy. Confidential data is sent by ciphertext to the server the most common means of protecting data privacy. Data security does not enable data users to effectively decrypt encrypted server information. A naive solution like copying and local decryption of all encrypted search data would considerably reduce cloud usefulness. As a result, a key question to be resolved immediately is how to research encrypted target data quickly and cost-effectively.

We propose a new, classified multi-keyword retrieval with confidentiality for multiple data owners. The linear splitting technique is used to hide the randomization keyword, so that a keyword does not devise server cloud attacks. As a result, both ciphertext and Trapdoor information that is vulnerable to privacy cannot be obtained from the cloud service. The cloud server can also avoid this splitting strategy by evaluating whether both trapdoors have the same keyword gathering. An updated KBB-Tree keyword is created to enable the cloud server to search for encrypted data from different systems of data owner and to make the data user seek relevant data.

II.LITERATURE REVIEW

Sr No	Paper Details	Advantages	Disadvantages	Conclusion
1	L. Zhang, G. Hu, Y. Mu,	This paper	This scheme only	In this paper, the author introduces a new

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008009 |

	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.	implements access structure, fast decryption, data verifiability.	achieves partly hidding policy. It is an interesting problem that achieves fully hidding policy with fast encryption.	method called linear secrecy sharing, which can improve the way the access policy is expressed. In addition, the name of each attribute and its value are divided into two parts. Consequently, the most obvious benefit of the scheme is that it is possible to hide sensitive attribute values. And in PHR it can well protect the privacy of users.
2	C. 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.	This work, for the first time, answers the aforementioned open problems affirmatively by presenting an identity-based proxy re-encryption with fine grain policy.	open problem to construct a key-private IB-CPRE scheme	The authors developed the IB-CPRE-FG safety model and demonstrated the security of the IND-CCA. The access policy is defined in this scheme by an access structure. Firstly, an IB-CPRE system supporting AND or OR gates can be developed directly at all interesting. Second, as many proxies are proposed for re-encrypting the key-private property is captured
3	C. 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.	Author propose the notion of key-policy attribute-based proxy re-encryption, which supports any monotonic access structures on users' keys. This scheme is proved against chosen-ciphertext attack secure in the adaptive model	How to construct a multi-hop attribute-based proxy re-encryption scheme remains to be an interesting problem	This paper presents an adaptively CCA-secure scheme for the KP-ABPRE system and introduces a new notion about key policy attribute-based proxy re-encryption. This scheme extends to key-policy-based encryption setting the notion of re-encryption of proxies.
4	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.	Author propose an attribute-based searchable encryption scheme by leveraging the ciphertext-policy attribute-based encryption technique	Not support dynamic, forward secure, and anonymous attributed-based searchable encryption scheme	This scheme allows the data owner to perform a fine-grained data user search authorisation. The main idea is to encrypt an index keyword in the context of a specified access policy, provided the data User is able to search over the encrypted index keyword only when the data User's attributes comply with the access policy.
5	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.	1. Author Propose Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access control over encrypted data in	1. limitation of the proposed ABKS-SM systems is that as the number of system attributes increases, so does the computational and storage costs 2. Not focus on expressive search	The author presented in the paper a practical keyword search scheme which supports hidden access policy in common multi-owner environments. In addition, it showed how the basic ABKS-SM system can be extended in the amended ABKS-SM system to support traceability (that is, tracking malicious DUs) if required.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008009 |

		the cloud. 2. CP-ABKS schemes were designed to support unshared multi-owner setting, and cannot be directly applied in the shared multi-owner setting (where each record is accredited by a fixed number of data owners), without incurring high computational and storage costs		
6	C. 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.	1. This scheme achieves the goals (1) scalable and finegrained access control for PHRs by using multi-authority ABE scheme, and (2) efficient on-demand user/attribute revocation and dynamic policy update. 2. This scheme supports efficient and on-demand lazy user revocation, which reduce the overhead a lot	Security is less	Authors propose a privacy-preserving PHR in this paper, which supports a thorough control of access and effective cancellation. Patients can combine an expressive access tree structure with the ciphertext when encrypting PHRs to achieve a thin grain access control. Authors also ensure confidentiality through the anonymous protocol issuing key.
7	K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X.Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing,"	Author propose a KP-ABPRE scheme which is CCAsecure under the 3-weak decisional bilinear Diffie–Hellman inversion assumption without random	Not designed non-interactive KP-ABPRE schemes, and KP-ABPRE schemes without pairings	In this paper, the author addresses the problem that Fang, Susilo, Ge, and Wang have left by proposing a randomly oracled KP-ABPRE system. By improving the reencryption key query and reencryption query this scheme enhances the security model.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008009 |

	IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.	oracles.		
8	B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFO COM 2014-IEEE Conference on Computer Communications, pp. 2112-2120, IEEE, 2014.	1. In this scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. 2. the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given	Not support DFA-based FPRE in the prime order bilinear group	In this paper 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
9	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.	1. Author proposes a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. 2. proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file	Not efficient	In this paper, 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.
10	K. Liang and W. Susilo, "Searchable attribute-	(i) search over the data owner's	This system focus on static data.Not support	Author introduced a novel cryptographic primitive called verifiable attribute-based

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008009 |

	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.	outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations.	accommodate dynamic data	keyword search for secure cloud computing over outsourced encrypted data. This primitive allows a data owner to control the search of its 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. CONCLUSION

We propose an extension of multi-keyword search and recall to search for multi-keyword queries to recover top-cloud data. The updated similarity scoring system is used for the calculation and extraction of associated data from outsourced cloud data to increase scan accuracy.

The proposed procedure improves efficient access to data, reducing the search and recovery time in relation to other processes. By examining the findings we prove that the proposed device guarantees high safety and an efficient recovery at high speed.

REFERENCES

[1] 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.

[2] C. 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.

[3] C. 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.

[4] 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.

[5] 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.

[6] C. 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.

[7] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. 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.

[8] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFO COM 2014-IEEE Conference on Computer Communications, pp. 2112-2120, IEEE, 2014.

[9] 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.

[10] 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:
7.569

doi cross ref

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

Scan to save the contact details