ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

A Survey on Ranked Multi-Keyword Search in Cloud Computing

Swaranjeet Singh, D.H.Kulkarni

M. E Student, Department of Computer Engineering, SKN College of Engineering Vadgaon, BK, India

Professor, Department of Computer Engineering, SKN College of Engineering Vadgaon, BK, India

ABSTRACT: privacy and ownership of the graphs in the cloud has become a major concern. proposed a treebased ranked multi-keyword search scheme for multiple data owners specifically, by considering a large amount of data in the cloud, we utilize the tfi-df model to develop a multi-keyword search and return the top-k ranked search results. to enable the cloud servers to perform a secure search without knowing any sensitive data. most cloud server do not serve single user, it give service to multiple user at the same time. this project consist of functions in which user can search multiple file and send the file to multiple user at the same time. it has ranking search technique in which most frequent searches are shown. Integrity of data is checked by third party auditor for better service by cloud.

KEYWORDS: AES, Cloud computing, Encryption, Multiple owners, Privacy preserving, Ranking

I.INTRODUCTION

1.1 Background

Most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing. For example, to assist the government in making satisfactory policies on health care service, or to help medical institutions conduct useful research, some volunteer patients would agree to share their health data on the cloud. To preserve their privacy, they will encrypt their own health data with their secret keys. In this scenario, only the authorized organizations can perform a secure search over this encrypted data contributed by multiple data owners. Such a Personal Health Record sharing system, where multiple data owners are involved, can be found at mymedwall.com. Compared with the single-owner scheme, developing a full-fledged multi-owner scheme will have many new challenging problems. First, in the single owner scheme, the data owner has to stay online to generate trapdoors (encrypted keywords) for data users. However, when a huge amount of data owners are involved, asking them to stay online simultaneously to generate trapdoors would seriously affect the flexibility and usability of the search system. Second, since none of us would be willing to share our secret keys with others, different data owners would prefer to use their own secret keys to encrypt their secret data. Consequently, it is very challenging to perform a secure, convenient, and efficient search over the data encrypted with different secret keys. Third, when multiple data owners are involved, we should ensure efficient user enrolment and revocation mechanisms, so that our system enjoys excellent security and scalability.

1.2 MOTIVATION

Protecting data privacy in the cloud is not straightforward, as encryption alone can limit cloud's usage in computation. Data sharing is another crucial utility function, i.e., sharing data files with each other. In personal health record system, data user (e.g., a patient) should have the ability to access his/her top-k data files about a specific case from different data owners (e.g., health monitors, hospitals, doctors). Similarly, the employees in an enterprise should have the ability to search data files outsourced by other employees. Recent work proposed a privacy-preserving ranked multi-keyword search in a multi-user model (PRMSM), which addresses the multi-keyword search problem in the multiple data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

owners model. However, PRMSM is inefficient and potentially expensive for frequent queries due to matching various ciphertexts from different data owners even for the same query.

II. REVIEW OF LITERATURE

1. Practical Techniques for Searches on Encrypted Data Techniques provide *provable secrecy for encryption, in the sense* that the untrusted server cannot learn anything about the plaintext given only the ciphertext[1].
2. "Secure Indexes" Secure indexes are a natural extension of the problem of constructing data structures with privacy guarantees such as those provided by oblivious and history independent data structures[2].
3." Network Applications of Bloom Filters: A Survey" survey the ways in which Bloom filters have been used and modified for a variety of network problems, with the aim of providing a unified mathematical and practical framework for them and stimulating their use in future applications[3].
4." Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions
" Define SSE in the multi-user setting, and present an efficient construction that achieves better performance than simply using access control mechanisms[4].
5. " Secure and privacy preserving keyword searching for cloud storage services "Here o on the condition of preserving user data privacy and user querying privacy. Performance analysis shows that the SPKS scheme is applicable to a cloud environment[5].
6. " Preferred keyword search over encrypted data in cloud computing "Paper establish a set of privacy requirements and utilize the appearance frequency of each keyword to serve as its ”weight”. A preference preprocessing mechanism is then explored to ensure that the search result will faithfully respect the user’s preference[10].
7. " Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud "Propose a novel multi- keyword fuzzy search scheme by exploiting the locality-sensitive
hashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionaryand effectively supports multiple keyword fuzzy search [11].
8. " An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing " Public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. We aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the fi le retrieval accuracy[12].
9. " Privacy preserving multi-keyword text search in the cloud supporting similarity basedranking "Present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on *term frequency* and the *vector space model* with *cosine similarity measure* to achieve higher search result accuracy[13].
10. " Shared and searchable encrypted data for untrusted servers,” Journal of Computer Security, "construct a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search[15].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

III. PROPOSED SYSTEM ARCHITECTURE

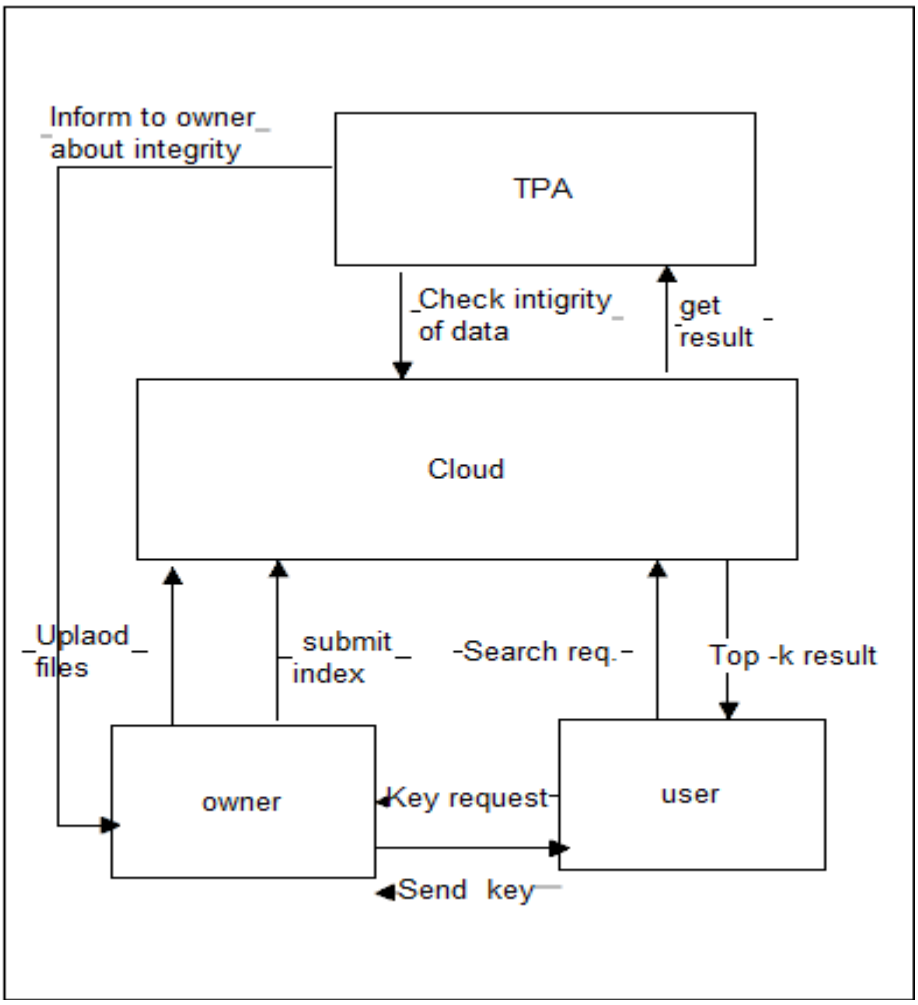

Fig.1: System architecture

IV. SYSTEM OVERVIEW

Proposed system will provide security to data. Secure search protocol is propose in which cloud server can perform secure search without knowing the actual value of keywords and trapdoors. In multiowner and multiuser cloud computing model, four entities are involved such as data owners, data users, cloud server and TPA .Data owners have collection of files. Data owners build secure searchable index of keyword set. Data owners submit keyword index to server. Data owners encrypt files and outsource encrypted files to cloud server. Encrypted keyword index to the cloud server. When data user wants to search over files from cloud server, he first computes the corresponding trapdoors and submits them then encrypted trapdoors andsubmit them to cloud server. Cloud server searches encrypted index of data owner and returns top-k relevant encrypted files to the data user. When data user receives top-K files from cloud server, then data user download files and decrypts these files. Third party auditor checks integrity of data and inform to owner.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Advantages-

1 .The proposed scheme allows multi-keyword search over encrypted files which would be encrypted with different keys for different data owners.

2.The proposed scheme allows new data owners to enter this system without affecting other data owners or data users.

V. CONCLUSION

This paper summarizes various searching techniques in the encrypted cloud data. The survey on different techniques to search over the encrypted data solves the problem of ranked search over encrypted cloud data. All these methods allow users to perform keyword searching while improving the security of the user query. The cloud server performs searching over the encrypted data but server does not know the sensitive information behind the data collection.

REFERENCES

[1] D. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data," in: SP'00, Berkeley, CA, 2000.
[2] E. Goh, "Secure indexes," Cryptology ePrint Archive, pp. 216 – 216, 2003.
[3] A. Broder, M. Mitzenmacher, "Network applications of bloom filters: A survey," Internet Math., vol. 1, no. 4, pp. 485 – 509, 2002.
[4] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895 – 934, 2011.
[5] Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," J NETW COMPUT APPL., vol. 35, no. 3, pp. 927 – 933, 2012.
[6] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, "Secure ranked keyword search over encrypted cloud data," in: ICDCS'10, Genoa, Italy, 2010.
[7] C. Liu, L. Zhu, J. Chen, "Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud," J NETW COMPUT APPL., vol. 86, pp. 3 – 14, 2017.
[8] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," in: INFOCOM'11, Shanghai, China, 2011.
[9] A. Ibrahim, H. Jin, A. Yassin, D. Zou, "Secure rank-ordered search of multi-keyword trapdoor over encrypted cloud data," in: APSCC'12, Guilin, China, 2012.
[10] Z. Shen, J. Shu, W. Xue, "Preferred keyword search over encrypted data in cloud computing," in: IWQoS'13, Montreal, Canada, 2013.
[11] B. Wang, S. Yu, W. Lou, Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in: INFOCOM'14, Toronto, Canada, 2014.
[12] S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.
[13] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.
[14] Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE T Parall Distr., vol. 27, no. 2, pp. 340 – 352, 2016.
[15] C. Dong, G. Russello, N. Dulay, "Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, vol. 19, no. 3, pp. 367 – 397, 2011.