Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 7, July 2019, pg.179 – 182

A Survey on Searchable Symmetric Encryption and Approach for Multi-Keyword Search Over Encrypted Data on Cloud Server

Supriya V. Joshi[1]; Abhijit A. Rajaguru[2]
[1]Department of Computer Science and Engineering, Punyashlok Ahilyadevi Holkar Solapur University, India
[2]Department of Computer Science and Engineering, Punyashlok Ahilyadevi Holkar Solapur University, India
[1] supriyajoshi367@gmail.com; [2] abhijit.rajaguru@sknscoe.ac.in

Abstract: Now a days, cloud computing has evolved as an important paradigm for IT industry with reduced cost, pay as you use, scalability, easy accessibility and improved flexibility. In a cloud environment client data can reside in any corner of the world as maintained and controlled outside their reach. So, there can be security and privacy issue with the client data. To ensure the privacy of data over cloud it is good to outsource the data in a encrypted format. Encryption of data works quite pretty good with single data owner. But single owner scheme restrict the scalability of system which is not useful. So multiple data owners can outsources and access the data securely with encryption. While retrieving such encrypted data searchable symmetric Encryption technique is used which will be reviewed deeply in this paper. To increase usability of system, it is good to allow multi-keyword query search which leads to accuracy in result and ranked search result gives systematic view to the fetched result over encrypted data. Note that, retrieving the data privacy preservation is main issue. To achieve this some novel protocols are discussed in this survey paper.

Keywords: Multi-Keyword ranked search, multiple data owners, security, cloud storage, Privacy preserving.

I. INTRODUCTION

A. Background

Cloud is a storage point where multiple data sources i.e. owners store data for availability and security. For privacy preserving data owner allow authorized data user to see their data. For example, To have government satisfactory health care policies or in medical institution conduct the research for study. For that purpose some volunteer patients would agree to share their health data on the cloud. For privacy concern, data owner will encrypt their data with secrete key. By this only authorized organization can perform a secure search over encrypted data. Considering above scenario developing multi-owner system is complicated as compared to single owner system. In a single owner system, data owner have to stay online to generate a trapdoors (encrypted keywords) for data users. Whenever large amount of data owners are involved, it practically impossible that, to ask them for stay online. Secondly No one wants to share our secrete key with others. Meanwhile different data owners will encrypt their data with different key so it will become very difficult to perform secure search over the data encrypted with different keys. On the other hand side when multiple data owners are involved, an efficient user enrolment and revocation mechanism is required for system scalability.

B. Motivation

Protecting data privacy in the cloud is not straightforward, as encryption alone can limit cloud's usage in computation .Sharing data files with other data user by ensuring authentication is most important thing. For example in enterprise one employee should access files outsourced by other employee. In other streams such as in health monitoring system patient should able to see their own information uploaded by health monitors. For the usability point of view it better to give the result in ranked format. Privacy preserving and multi-keyword search (PRMSM) is achieved in recent work successfully. But little bit worry have to done on inefficiency and expenses required for frequent query search for a single query with multiple data owners data.

II. LITERATURE SURVEY

The main motivation behind the data outsourcing is that availability of data at any point with privacy preserving. Data security is achieved using encryption of data before outsourcing. While availability it good to have accurate result. For that purpose D. Song, D. Wagner, A. Perrig proposed as practical techniques for searches on encrypted data[2].The untrusted cannot anything about the plaintext is the advantage of this system. The arbitrary word search without the user's authentication is not possible.

"Secure Indexes" Secure index is the best solution for the problem of constructing data structures with privacy guarantees such as those provided by oblivious and history independent data structures[3]

Another randomized data structure Bloom filters for representing a set in order to support membership queries are explained to solve verity of network problems with the aim of providing a unified mathematical and practical framework for them and stimulating their use in future applications[4]

The private key encryption allow data owner to outsource data for limited user with symmetric encryption also the private key encryption prevents searching over encrypted data to achieve the Reza Curtmola purposed Searchable Symmetric Encryption technique[5]. This paper deals with multi user system and allow keyword based search. For more efficient output search result the ranking of files provided in secured ranked keyword search over encrypted cloud data.

It is profitable for cloud server to take responsibility of sensitive data security against untrusted cloud service provider (CSP) by allowing decryption only trusted user. The system not only support keyword based on encrypted data but also provide high performance. Characteristics of cloud services are studied well in this paper and proposed a novel system for secure and privacy preserving keyword searching (SPKS)scheme which allow CSP to participate in the decipherment and return only files containing certain keywords specified by user. Keyword search reduces both the computational overhead required to search on encrypted data and communication overhead required to share fetched files. It is proved that proposed system semantic security against adaptive chosen plaintext attacks.[6]

Ranked search enhance the system usability by fetching the matching files in a ranked order regarding to certain relevance criteria[7]. Cong Wang defines a order-preserving symmetric encryption(OPSE) technique. The system well worked on ranking of files But it will not support multi-keyword search

Wei Zhang proposed a system which deal with enhance security over keyword and trapdoors. Along with ranking facility additive order and privacy preserving function family(AOPPF) [8]

Many approaches have been proved to enable searching the encrypted data. Majority of these approaches are limited upto single keyword search or a Boolean search but not a multi-keyword search. Multi-keyword search gives more relevant result which will increases efficiency. For that, searchable encrypted index is modified in the paper. Also the number relevance score is considered for ranking of document. Besides from that, a little provisional work have to be done regarding misspelled keyword search since the paper only deal with similarity keyword match search.[9]

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 dictionary and effectively supports multiple keyword fuzzy search [10]

"An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing"[11]proposed a technique 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 file retrieval accuracy. we propose an Efficient and Secure Privacy-Preserving approach(ESPPA) using probabilistic public key encryption and ranked keyword search. Moreover, our scheme also verifies the integrity of data. we will enhance ESPP algorithm to support efficient dynamic data operations and ranked keyword search over the encrypted big data in cloud as a future work.

III. SYSTEM ARCHITECTURE

As Fig.1 shows, there are three entities in which two are actors i.e., data owners and data user where third is cloud storage. Data owners have a large collection of files F to outsource. To enable efficient multi-keyword search on the encrypted files, each data owner first builds a secure searchable tree-based index I which is required for efficient searching. The job of data owners is to encrypt their data files F with their keys and outsource both the encrypted tree-based index and data files to the cloud server.

When receiving the tree-based indexes, the cloud server merges multiple encrypted indexes without compromising data owners' privacy. When the data user searches t keywords over the encrypted files and fetch k encrypted files, he first computes the trapdoors T, and submits T and k to the cloud server. When receiving the trapdoors T and k, the cloud server begins searching the merged index tree I and returns the corresponding collection of the top-k ranked encrypted files.

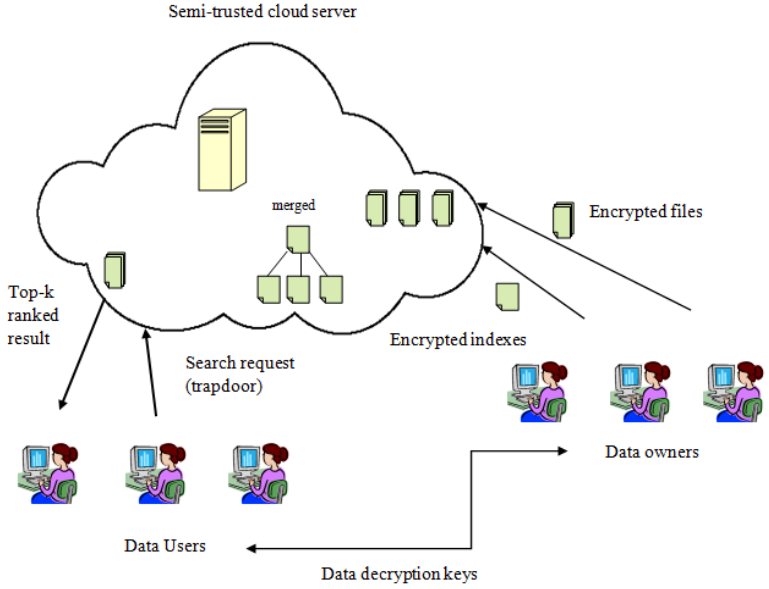

Figure 1 System Model

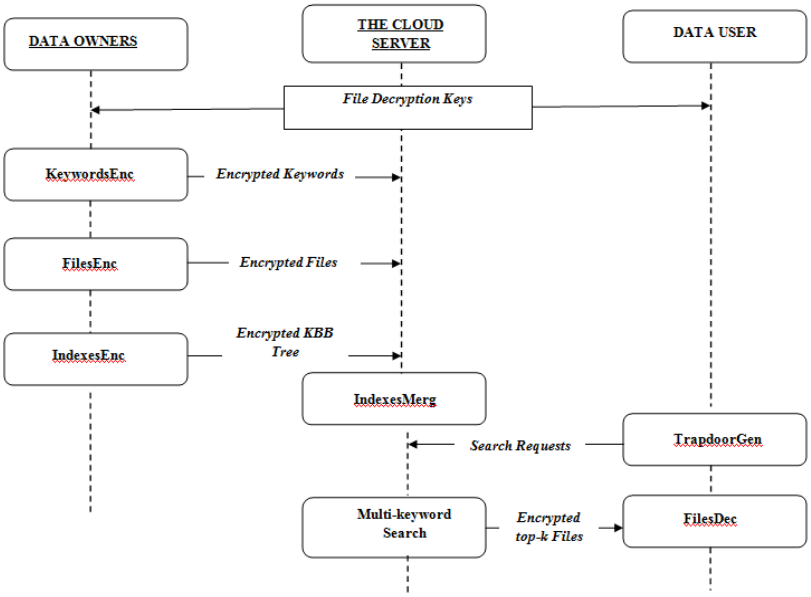

Figure 2 TBMSM Working Process

To meet the requirements of efficient multi-keyword ranked search in multiple data owners model, a novel TBMSM mechanism. Fig.2 shows the working processes of TBMSM.
The role of these three entities are as given below:

- *Data Owners*
  1) KeywordsEnc encrypts the keyword with data owners' secret key $k_{oi,w}$;
  2) FilesEnc utilizes the traditional symmetric encryption algorithm to encrypt data owners' files;
  3) IndexesEnc builds the tree-based index for each data owner and encrypts the KBB-tree with AOPPF.
  4) data owners upload encrypted keywords, files and KBB-trees to the cloud server.
- *Data Users*
  1) TrapdoorGen generates trapdoors with data users' secret key $k_{ui,w}$, and then submits trapdoors and the number of extracting files k to the cloud server;
  2) FilesDec decrypts encrypted files.
- *Cloud Server*
  1) IndexesMerg merges multiple encrypted trees;
  2) Multi-keyword Search runs the DFS algorithm to find out the corresponding files and returns the corrected top-k encrypted files to data users.

IV. ADVANTAGES

The system allows multi-keyword search over encrypted data on cloud. The encryption key is unique for each data owner which increases privacy.
New data owner can enter this system without affecting existing owners and users.

V. CONCLUSION

Various searching technique research papers are summarized in this survey. That explores different techniques of keyword searching where some deals with single keyword search and their problems are also overtaken by multi-keyword search technique. Meanwhile the security maintains matters a lot in system scalability is described in this system.

REFERENCES

[1] "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data" by Tianyue Peng, Student Member, IEEE, Yaping Lin, Member, IEEE, Xin Yao, Student Member, IEEE, and Wei Zhang
[2] D. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data," in: SP'00, Berkeley, CA, 2000.
[3] E. Goh, "Secure indexes," Cryptology ePrint Archive, pp. 216 – 216, 2003.
[4] A. Broder, M. Mitzenmacher, "Network applications of bloom filters: A survey," Internet Math., vol. 1, no. 4, pp. 485 – 509, 2002.
[5] 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.
[6] 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.
[7] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, "Secure ranked keyword search over encrypted cloud data," in: ICDCS'10, Genoa, Italy, 2010.
[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] 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.
[11] 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.

