



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

Survey on Multi-keyword Search in Cloud Computing

Ashwini Sude, V.D.Shinde

M.E. Student, Department of Computer Engineering, Rajarshi Shahu College of Engineering, Pune, India

Professor, Department of Computer Engineering, Rajarshi Shahu College of Engineering, Pune, India

ABSTRACT: Recently the attractiveness towards the cloud computing is growing tremendously. More clients now days are opting to outsource data management on cloud because of its low cost in management and greater convenience. For sake of confidentiality, data which have sensitive should be encoded before uploading to the cloud server, which retrieve data using keyword based document retrieval. With the appearance of cloud computing, it has turned out to be progressively prominent for the owners of data to make available their information to public cloud servers at the time of permitting data users to retrieve this information. For some privacy reasons, a secure search on encrypted cloud information has boosted some of the research works in the single owner model. Nonetheless, number of cloud servers practically speaking don't simply work for only one owner; rather, they can serve number of owners to use the pros brought by cloud computing. In the survey, the recent searching techniques are analyzed to find an effective solution for the retrieval of data from encrypted multiple cloud data. Also present some ranking algorithms to rank the search results. It will improve the user search experience.

KEYWORDS: Privacy preserving, anonymization, data mining, information security.

I. INTRODUCTION

Cloud computing is the use of assets which are passed on as a service over a network framework. The name brought from the use of a cloud-shaped picture as a reflection for the multifaceted establishment it contains in structure diagrams. Cloud computing depends remote administrations with a customer's data, calculation and software. The cloud suppliers manage the infrastructure and platforms on which the applications run. End users access cloud-based applications by utilizing distinctive web browsers or a desktop or compact application while the business programming and customer's data are stored on servers at a remote area.

Cloud computing permits organization to get applications which are created by them, up as well as running quicker, with enhanced manageability and minimum support, also empowers IT to all the quickly modify resources to meet fluctuating and capricious business request. Cloud computing is a model for empowering advantageous, on-interest system access to a common pool of configurable figuring resources that can be immediately provisioned and released with immaterial administration effort or service provider interaction.

To make data secure and to block depicted gain control in the cloud, important data such as emails, health records, photos, documents etc. may be encrypted by owner of data before storing it on cloud. Be that as it may, obsoletes the customary information use service depending on plaintext keyword search.

II. RELATED WORK

In paper [1] authors proposed a secure, efficient as well as dynamic search system, that supports the accurate multi-keyword ranked search as well as the dynamic erasure as well as injection of documents. They also developed an important keyword balanced binary tree as the index, as well as implemented a "Greedy Depth-first Search" algorithm to get good efficiency than linear search.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

In paper [2] authors proposed an effective method which solves the issue of synonym-based multikeyword ranked search on cloud data which is encrypted. They have worked on two facts: synonym-based search as well as similarity ranked search. The outcomes of finding can be accomplished when approved cloud clients input the equivalent words of the predefined keywords, not same or fuzzy matching keywords, due to the conceivable equivalent word substitution and/or her absence of precise information about the information. Authors likewise gave two secure frameworks to address privacy issues in two threat models.

In paper [3] authors have boosted to give the answer the issue of ranked keyword search over encrypted data remotely stored in cloud server. Authors made use of the asymmetric encryption technique in the place of the traditional symmetric encryption, the IBE of Boneh Franklin technique. Also the transformational TF-IDF makes ranked search feasible which the users may extract these most significant files instead of files maybe just contain the keyword as well as has no important relationship with the keyword.

In paper [4] authors have tried to increase the data discovery as well as client searching experience by going down Secure Ranked Fuzzy Multi Keyword Search. In RFMS an ideal opportunity to make the list at the DO is minimize as it were. Likewise, the overhead of creating the trapdoor for every query generated by DU is dispensed with on DO. The DU specifically queries the Cloud Server C.

In paper [5] authors designed SMOADS model which provides a secured information sharing system via the dynamic manager idea that minimizes the chance of hacking without compromising working. The multi layered security control using Dynamic Manager (DM), Multiple Owners (MO), and Centralized Certificate Authority (CA) all these are used for making access system robust as well as has been confirmed by simulations. Examinations amongst static and dynamic manager execution were shown by CloudSim, and the reaction time for Dynamic Manager is observed to be at standard with the outcome as well as in-accordance with Static Manager. Further, the chances of hacking diminishment have been marked by numerous conditions, which concrete the idea of a secured framework.

In paper [6] authors has given study of methods protecting privacy in the case of cloud computing. In summary, they have divided the methods in four kinds: 1) k-anonymity dependent method 2) randomized dependent method, 3) differential privacy dependent method, and 4) encryption dependent method. By nature, privacy-preserving data mining is a multidisciplinary field. Authors believe that it needs close participation amongst scientists and specialists from the fields of security, data mining, public policy and law.

In paper [7] authors implemented a basic MRSE system by making use of secure inner product computation, after that they have modified it to meet divers privacy needs in two levels of threat models. By studies investigating privacy as well as efficiency guarantees of given system is provided. The test results show given system indeed has minimum overhead on calculation and communication.

Table 1: Survey Table

Paper Name	Proposed work	Advantages	Disadvantage
A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data	Z. Xia, X. Wang, X. Sun and Q. Wang	Greedy Depth-first Search	deal with the deletion and insertion of documents flexibly
Multi-keyword ranked search supporting synonym query over encrypted data in cloud	Z. Fu, X. Sun, Z. Xia, L. Zhou and J. Shu	synonym-based search & similarity ranked search	very efficient and effective in supporting synonym-based searching



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

computing			
RSAE: Ranked Keyword Search over Asymmetric Encrypted Cloud Data	C. Guo, Q. Song, R. Zhuang and B. Feng	asymmetric encryption technique	search feasible
Secure ranked fuzzy multi-keyword search over outsourced encrypted cloud data	N. S. Khan, C. R. Krishna and A. Khurana	RFMS	DO is minimize to a great extent
SMOADS - Secured Multi-Owner Attribute-based Data Sharing in cloud computing	P. Varalakshmi, A. R. Shajina and V. Selin soniya	SMOADS	provides a secured data sharing system

III. PROPOSED SYSTEM

Information owners have an collection of documents. To engage effective search operations on these documents which will be encrypted, information owners at first a secure searchable index on the keyword set extracted from files, at that point they submit searchable index to the administration server. Finally, information owners encrypt their documents and outsource the relating encoded records to the cloud server. After accepting searchable index, administration server again encrypts searchable index for the legal data owners as well as the forwards the re-encrypted index towards the cloud server. At the time when owner of data wants to search keywords on these files which are encrypted and also stored on the cloud server, he first calculates the related trapdoors as well as sends them to the administration server. After the data user is genuine by the administration server, the administration server will promote re-encrypt the trapdoors and forwards it to the cloud server. After receiving the trapdoor, the cloud server looks for the encrypted index of each information owner as well as returns the analyzed set of encrypted documents. To enhance retrieval of the file exactly as well as save communication cost, a user of data will tell the cloud server a parameter as well as cloud server would give back the top-k related documents to the data user. Once the data client gets the top-k encrypted documents from the cloud server, he will decrypt these retrieved documents.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

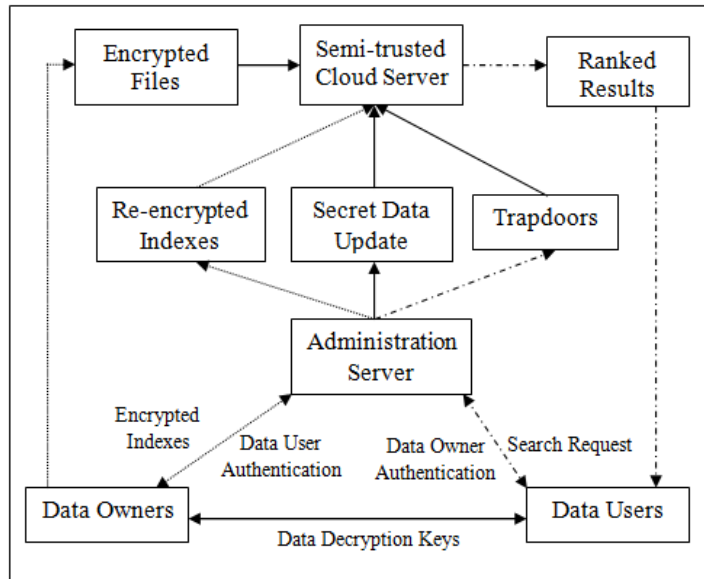


Fig 2: Proposed system architecture

IV. CONCLUSION

This survey summarized some recent searching and ranking techniques. These searching techniques are useful for the searching of particular data over encrypted data in cloud and ranking methods are used for make the ranking of search results. From this survey, some key issues are listed, which are solve by searching methods such as, keyword and data privacy, efficient search, scalability, efficiency, ranking of results, data and query confidentiality etc. The limitations of recent searching methods are also discussed here.

REFERENCES

1. Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2,
2. Z. Fu, X. Sun, Z. Xia, L. Zhou and J. Shu, "Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing," 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), San Diego, CA, 2013, pp. 1-8.
3. C. Guo, Q. Song, R. Zhuang and B. Feng, "RSAE: Ranked Keyword Search over Asymmetric Encrypted Cloud Data," Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on, Dalian, 2015, pp. 82-86.
4. N. S. Khan, C. R. Krishna and A. Khurana, "Secure ranked fuzzy multi-keyword search over outsourced encrypted cloud data," Computer and Communication Technology (ICCCT), 2014 International Conference on, Allahabad, 2014, pp. 241-249.
5. P. Varalakshmi, A. R. Shajina and V. Selin soniya, "SMOADS - Secured Multi-Owner Attribute-based Data Sharing in cloud computing," 2013 Fifth International Conference on Advanced Computing (ICoAC), Chennai, 2013, pp. 318-324.
6. A. Monreale and W. H. Wang, "Privacy-Preserving Outsourcing of Data Mining," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 2016, pp. 583-588.
7. A. Karapakula, M. Puramchand and G. M. Rafi, "Coordinate matching for effective capturing the similarity between query keywords and outsourced documents," Sustainable Energy and Intelligent Systems (SEISCON 2012), IET Chennai 3rd International on, Tiruchengode, 2012, pp. 1-7.