ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Comparative Study of Searchable Encryption Schemes over Cloud Servers: A Survey

Akash Kumar Verma
Dept. of Computer Science and Engg
MMM University of Technology
Gorakhpur, Uttar Pradesh, India

Dr.S.P.Singh
Dept. of Computer Science and Engg
MMM University of Technology
Gorakhpur, Uttar Pradesh, India

Abstract: Storing data over cloud servers is very common. However, security issue is a major concern. Data uploaded by owner of data over cloud severs should be secure. To secure data, owner of data first encrypt their data and then upload it on cloud servers. This is the way how data are secure on cloud. But again, security problem arises when we talk about the searching of data over cloud servers. The keywords used for searching over cloud in the form of plain text makes vulnerable. This is another security concern. There are various encrypted searching schemes have been derived. In this paper, we have defined some of them. Specifically attribute based keyword searching scheme and privacy preserving searching schemes are defined. After then we have concluded which is good in performance and security as well.

Keywords: Cloud Computing; Security Issue; Encrypted Searching Scheme; keywords based searching; attribute based searching; Privacy Preserving;

I. INTRODUCTION

When we say "sky is the limit", then in the present scenario we are literally touching that limit. With cloud, we are all pervasive in this world accessing any data form any corner of this planet. Cloud computing is a frugal innovation which revolutionizes the digital world.

In the past people used to download software or run an application on a physical computer or a server in their building, but now can access same application through internet. Updating your Facebook status, firing off mails on the move or checking your balance on the phone, all are based on cloud. This technology has so penetrated in our daily activities that life seems to be impossible without it.

Its significance lie with the flexibility to adapt with current infrastructure, reduce the capital expenditure and enhances the collaboration and very importantly reduces the data loss with enhanced security.

During this decade cloud computing technologies, have achieved much advancement. However, cloud computing suffers from various security issues-

- Storing data securely on cloud servers
- Secure data accessing from cloud servers
- Searching for the data on cloud servers
- Preventing data from cloud service providers

These are the major security concerns where researches are going on during the recent years. A trust gap between information proprietors and cloud specialist organizations exists dependably and it is self-evident. As owners of data, will have no direct control over their data once it is transferred/uploaded to cloud servers. To protect their data usually owner of data first, encrypt their data on their own site and then they upload them on the cloud servers. This protects from unwanted access or malicious use from cloud server providers and external attackers too. But problem in this case arise when searching is done by authorized users or owner of data's itself, because searching over plain text is simply easy in the comparison of searching over cipher text. Another solution for searching is to download whole data locally, decrypt it then search and it will be more difficult because of bandwidth and computation problem.

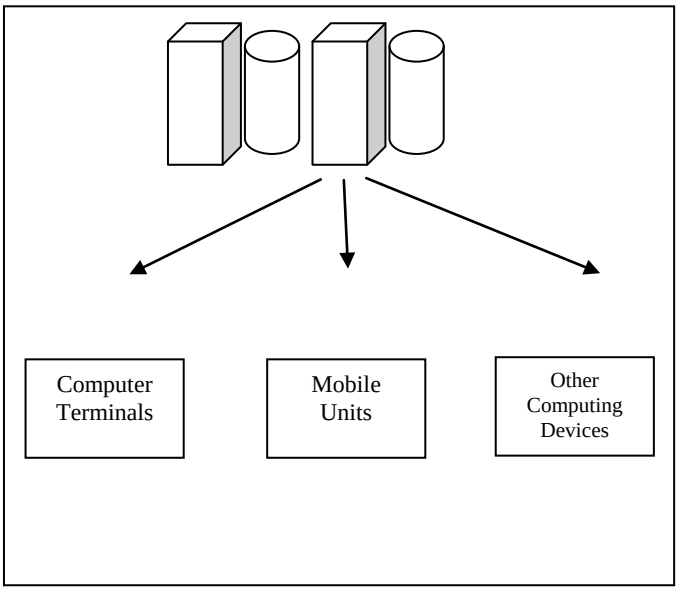

Figure1. Architecture of cloud computing

Searching data from cloud is also the major security issue, as we know that the logs are maintained every time when a user logged into system and accesses data from cloud. Whenever user authenticate on server and search data from cloud server using keywords, log will be updated on the database of cloud server provider, if any external attacker attacks on cloud server and gets access of database he/she can misuse the keywords from logs for assuming the data stored on cloud server. Attacker may assume what type of data is stored on server. Therefore, many researches have been completed for secure search over encrypted data.

Searching using encryption keyword over encrypted data is a new technique in cloud computing technology. However, it takes extra computation but gives more secure search. There are many papers defined the encrypted keyword searching technique over cloud servers [1] [2] [3] [4][5] [6] [7] [8] [9] [10]. Most of them use searchable index scheme. These indexes are generated or build in that manner that cloud servers can't deduce plaintext from these indexes, when authorized users are searching data or doing any operation on cloud servers by using

these indexes. These plans generate these indexes based on keywords, extracted from owner's datasets. These encrypted indexes are uploaded to the cloud servers with their encrypted dataset on cloud servers. Server returns the related data to authorized users after searching using index based keywords.

In this paper, we have compared the existing index based keyword searching schemes. We have study these plans in detail and compare the efficiency and performance of them.

This section was the complete and brief introduction about security related issues of cloud computing and problems related to searching technique over cloud servers. The second section is about the system architecture of search over data. Third section explains the brief study of different searching schemes. Conclusion of the paper is in the last section of this paper.

II. SYSTEM ARCHITECTURE

Mostly, cloud service providers are assumed to be less honest. The cloud servers are expected as safe but sometimes the service providers access the information uploaded on servers. Though data uploaded on servers are encrypted, and cloud service providers does not have the decryption key. But the algorithm used to encrypt the data is known to them. This makes less honest to them.

There is well accepted model for cloud computing is of three entity. Where entities are:

- Cloud Service Provider
- Owner of data and
- Authorized Users

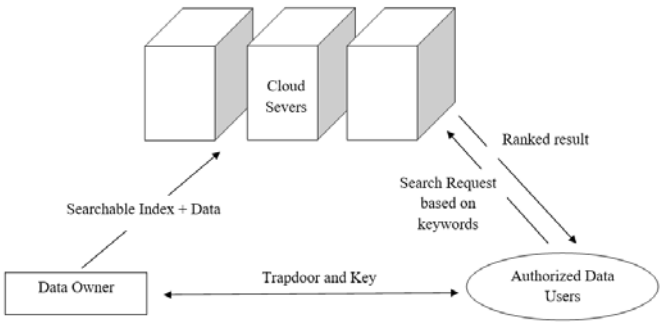

Figure2. System Architecture of Searchable Encryption

The same architecture model is also used in searching over cipher data as shown in figure. The entity owner of data has a collection of data which is much confidential and sensitive. Owner of data wants to use cloud servers to store his/her sensitive data. He will upload these data but before uploading these data he/she will first encrypt data to secure information. With encryption of data a searchable index will be generated for searching of data. These searchable indexes are generated based on properties of data. These properties are basically the keywords that will useful to search the data. Based on this keyword an index vector for data is generated and will be encrypted. Now the encrypted index will be bind with data and uploaded on cloud servers. This index vector will work as trapdoor for the authorized users which will help him in searching the interested data.

As per the request based on these keywords, a result will be given to authorized user. This result will be rank based result; the best match keywords will be on result's first rank and so on. User will then decrypt these cipher data using the decryption key given by owner of data.

III. ENCRYPTION KEYWORD SEARCHING SCHEMES

There are different explores are finished on searchable encryption plans. Some of them are on Symmetric searchable encryption plan and other are on Asymmetric Searchable encryption [1]. After this work, a few plans [6] [4] [3] are proposed to enhance the security definition and pursuit productivity. Plot in [11] fathom the outcome positioning pursuit using request safeguarding methods. With recurrence, related data, they can rank item and return more exact outcome. The benefit of SSE is effectiveness since it regularly receives quick cryptographic primitives like square figures, pseudorandom capacities or hash capacities. Its burden is that the record refresh is wasteful and it doesn't bolster conjunctive or disjunctive watchwords seek.

Another scheme for encryption keyword searching is asymmetric searchable encryption (ASE) based on public key. In this scheme, anyone can upload and encrypt the data on cloud servers who have public key. But the permission to decrypt the data and searching will have only to those authorized users who have private key. In the paper [5] the first searchable encryption scheme based on public key cryptography is introduced. Paper [7] [12] [13] propose some research on conjunctive keyword search. Then in paper [14] and [10] issues concerned with keyword conjunction and range query are discussed. The favorable position is it can bolster complex looking solicitation. The disservice is wastefulness since it is outstanding that most asymmetric searchable encryption plans depend on matching operation on elliptic bends, which is much slower than SSE in light of square figures or hash capacities. Every one of the plans communicated above just give single catchphrase hunt.The better way is to search in cloud server is best match keyword search. But it is usual that exact keyword searching not possible all time due to different matches of same word. Like if there is word "engineer" then there will be different matches can be "Engineers" and "Engineering". It can also be possible the user wants to search all types of "engineers" such as "Computer Engineers", "Mechanical Engineers" or "Electrical Engineers". So, the index vectors should be form in such a way or algorithm that generates the keywords to from index should be in such a way so that result can be match with these keywords also. However, the result will be rank based such as best match result will be on first rank and worst match keywords match will be on last rank.

With the recent advancement in searching schemes with query [15] developed an efficient privacy preserving circular range searching scheme. This scheme specifically achieves circular range searching on R-tree based searching encryption scheme. It also includes a third party to the system. After comparison with existing schemes it is found that this scheme is more efficient in terms of token generation, searching and encryption. It also preserves the privacy of searching query.

In the paper [8] the author has protected the right of user as this provide a fine grained search with self-generated search capabilities. That will make user and owner independent to be always online for the authorization. As many paper gives the concept of single owner scenario, this paper focus this challenging scenario and make a scheme for multiple owner who can outsource their encrypted data to cloud servers from where multiple users can access data with encrypted searchable index. An attribute based encryption scheme inspires the author from where author presented an attribute based search scheme

with efficient user revocation (ABKS-UR). This paper formalizes the security definition and proves the proposed ABKS-UR scheme selectively secure against chosen-keyword attack. To build confidence of data user in the proposed secure search system, this scheme also design a search result verification scheme.

IV. CONCLUSION

The cloud computing is most advance topic for researcher and a lot of researches have been done on this technology. Still many researches are on-going on this topic. Still there are many issues being there with cloud computing in which security issue is major concern. Beside the storage security issue searching with plain text also a security concern in cloud computing. There are many researches for encrypted searching schemes.

In this paper, we have compared a lot of schemes for searchable encryption. Attribute based keyword searching technique with user revocation plays an important role for searchable encryption scheme. Efficient privacy preserving is another scheme for preserving the privacy of user. There are some searching schemes using symmetric searchable encryption scheme and some are asymmetric searchable scheme. We have also compared based on their performance and security.

V. ACKNOWLEDGMENT

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I am grateful to my guide Dr. S.P. SINGH for the guidance, inspiration and constructive suggestions that helped me in the preparation of this progress report. I wish to thank my parents who have been always been a source of inspiration for their never-ending support and love throughout completion of the report and I am also thankful my friends who have helped in successful completion of the partial report.

.

VI. REFERENCES

[1] D. Xiaodong, S. David, and W. Adrian, “Practical Techniques for Searches on Encrypted Data £,” 2000.

[2] K. Liang, X. Huang, F. Guo, and J. K. Liu, “Privacy-Preserving and Regular Language Search over Encrypted Cloud Data,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 10, pp. 2365–2376, 2016.

[3] R. O. Curtmola Reza, Juan Garay, Seny Kamara, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” *Scis 2012*, pp. 1–8, 2012.

[4] E.-J. Goh, “Secure Indexes,” An early version this Pap. first Appear. Cryptol. ePrint Arch. Oct. 7th, pp. 1–18, 2003.

[5] D. Boneh and G. Di Crescenzo, “Public Key Encryption with keyword Search,” pp. 1–15.

[6] Y. Chang and M. Mitzenmacher, “Privacy Preserving Keyword Searches on Remote Encrypted Data,” pp. 442–455, 2005.

[7] P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search Over Encrypted Data.”

[8] W. Sun, S. Member, and S. Yu, “Protecting Your Right Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud,” vol. 27, no. 4, pp. 1187–1198, 2016.

[9] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” *IEEE INFOCOM 2014 - IEEE Conf. Comput. Commun.*, vol. 27, no. 4, pp. 226–234, 2014.

[10] E. Shi, J. Bethencourt, D. Song, A. Perrig, E. Shi, T. H. Chan, and D. Song, “Multi-Dimensional Range Query over Encrypted Data,” 2007.

[11] D. Olmedilla, “Zerber + R : Top-k Retrieval from a Confidential Index,” pp. 439–449, 2009.

[12] Y. H. Hwang and P. J. Lee, “Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System,” pp. 2–21, 2007.

[13] L. Ballard, S. Kamara, and F. Monrose, “Achieving Efficient Conjunctive Keyword Searches over Encrypted Data,” pp. 414–426, 2005.

[14] D. Boneh and B. Waters, “Conjunctive , Subset , and Range Queries on Encrypted Data,” pp. 1–29.

[15] H. Ren, H. Li, H. Chen, M. Kpiebaareh, and L. Zhao, “Efficient privacy-preserving circular range search on outsourced spatial data,” *2016 IEEE Int. Conf. Commun. ICC 2016*, 2016.

