International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Cloud Server Misbehavior Detection Using Ranked Keyword Search Results Verification

A Shiny, Jayanth Das, M Venkat Aravind, C A Anirudh Srivatsaa, M Rahul

Abstract*: With the rising use and demand of cloud computing, more and more people tend to outsource their data to many cloud servers. Hence data security has become a huge necessity recently. Data owners who store their data in cloud servers must be securely able to manage and distribute their data without any hindrances. Introducing a secure and efficient verification scheme for ranked keyword search by adopting Searchable Symmetric Encryption can efficiently bring about a change in the cloud server environment. This is done so as to manage "honest but curious" cloud servers where doubt of misbehaving is relatively higher. To do this the data verification system is optimized by implementing a searchable symmetric encryption scheme. Now, with a secure exchange gateway the cloud server has less room for misbehaving. The cloud server is only aware that if it's unscrupulous conduct is recognized, it would be found with a high likelihood.

***Keywords*: Cloud Security, Data Outsourcing, Data Verification, Encryption.**

I. INTRODUCTION

With the rising use and request of cloud computing, an ever-increasing number of individuals will in general tend to re-appropriate their information to the cloud. This not only provides the users with ease of access to their data but also assures them a secure storage space on the cloud. Hence with the potential of billions of people storing tons of volumes of data in the cloud the cloud servers, the main entity responsible for storage of data attains a vital role in this entire system. The main concern that arises is if the cloud server could be trusted. Since it contains data which could be proven vital to some people, the server in which the data is stored must be a trusted, secure one. The data owners, the people who own the data and the verified data users who are allowed to access the data must be able to securely handle the information stored in the server without any hindrances from other entities. This is where the use of ranked keyword search comes into play. The rankedkeyword system used for exchanging data securely. But the exchange of data inevitably takes place through the cloud server so if it's a dishonest, the server can tend to intervene in the data exchange process. That is not only a potential threat for the data being exploited but also can cause harm to the data owners and users. So, the secure ranked keyword search results verification technique can actually detect if the data has been interfered with and can alert the users and owners that the cloud server is behaving dishonestly. This can be done by using the verification techniques mentioned in [12] by using the verifiable ranked searchable symmetric encryption scheme. This scheme can be integrated to the ranked keyword search result verification proposed in [10]. Thus, providing the data owners and users optimal security while accessing and storing their data on the cloud server.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
A Shiny, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.
Jayanth Das, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.
M Venkat Aravind, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.
C A Anirudh Srivatsaa, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.
M Rahul, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

II. LITERATURE SURVEY

Recently a great deal of studies related to cloud security and ranked keyword search results verification techniques have been increasing due to popularity the domain has gained over the past few years. The first ranked keyword search was [1], [2] and [3] which introduced the scheme of secure rank keyword search results verification to cloud security. Furthermore in [4] a multi keyword scheme was integrated which enables dynamic keyword usage with a more secure overall system. Then [5] accommodates a ranked searchable encryption scheme with multi keyword search in a cloud server. Succeeding which [6], [7], [8], proposed a system which optimized the existing schemes by incorporating a fuzzy keyword search. After which [9] proposed schemes which included multiple data owners to enhance the utility. Finally [10] proposes a system consisting of secure ranked keyword search where cloud servers tend to behave dishonestly. One of the first searchable symmetric encryption techniques used to deal with cloud server behavior was proposed by [11] and [12] proposed a Verifiable Ranked Searchable Symmetric Encryption (VRSSE) scheme to optimize the ranked searches.

III. PROPOSED SYSTEM

In this system the cloud server is assumed to be dishonest and it contains multiple data owners. The data exchange which takes place between the data and the users is reinforced by a searchable symmetric encryption scheme to enhance the security when the encrypted data exchange takes place so that the data can be verified to check the behavior of the sever. If malicious activity is detected the cloud server is held responsible, and is dealt with accordingly.

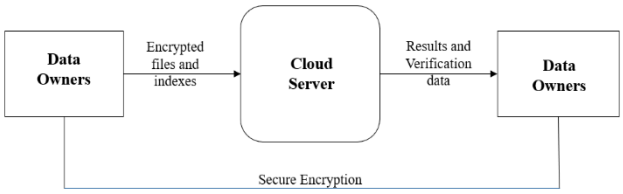

Fig. 1 Block Diagram of Proposed system

A. Data Owner

Data owner is the person who owns the data stored in the cloud server. They have a list of keywords corresponding to each of their files. During the process they overlook the ranked keyword search result verification and verify if the files are safe and monitor the behavior of the cloud server in which their data is stored. The data owner also exchanges the set of keywords to the verified data users so that they can access the file from the cloud server.

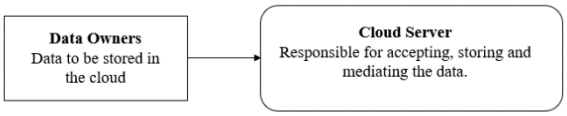

Fig. 2Data Owners

B. Data Users

Data user is the verified person who wants to access the files in the server. Theyinitiate the ranked keyword search result verification algorithm through encrypted keywords. The data user already knows the keywords corresponding to the files of the data owner which are given to them by the latter. The user enters the keyword of the file to which they want to access and obtains the file from the server. Further, they verify the authenticity of the encrypted data which is obtained from the cloud server and can identify if the cloud server is misbehaving.

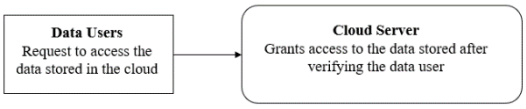

Fig. 3Data Users

C. Cloud Server

This is the main entity which stores data and connects user and data owner. The cloud server is responsible for approving the files of the data owners, verifying data users and mainly mediating the exchange of encrypted data based on the requests of the data users. In this system the server is assumed to be dishonest meaning it tends to meddle with the encrypted data and can be caught while doing said activity.

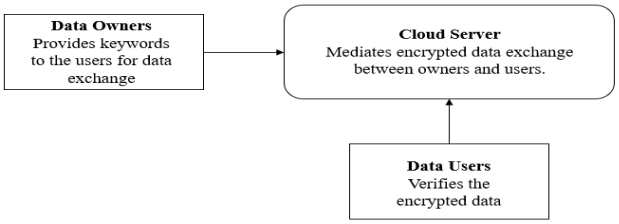

Fig. 4Cloud Server

D. Verification Technique

The verification technique used here is a searchable symmetric encryption method. First, theowner has the set of files and a keyword which they set for each file along with a file id and secret key stored in the server. Then the data users after getting verified by the server, request access to the files in the cloud server by using the keyword provided to them by the data owners separately. After the cloud server mediates the exchange of data between the data users, it provides them with search results related to the user's requests. The users can then check if the data is corrupted using searchable symmetric encryption. This allows the users to verify the correctness of the encrypted data. If the files are corrupted the users can detect it and the cloud server is reported and is punished appropriately. By using the system not only will the top-k rank searches can be easily verified but also can be used in a system where multiple data owners are involved.

IV. RESULTS AND DISCUSSION

The proposed system standardizes the ranked keyword search result verification method by adopting a searchable symmetric encryption scheme for verifying the ranked keyword search. This enhances security in a cloud server consisting of multiple data owners and a server which tends to behave dishonestly. Furthermore, data users can also efficiently verify search results. This system also prevents the cloud server from acquiring details about the data verification allowing the transfer to be more secure. Hence deterring the cloud server from dishonest behavior. Nevertheless, if the server behaves dishonestly it can be detected and punished accordingly.

V. CONCLUSION

In this paper, we suggest the usage of a searchable symmetric encryption scheme to verify the search results in order to deal with the misbehavior of cloud servers. This is done to provide a secure mediation of data between the data owners and data users. This technique can be further improved by optimizing the keywords and parameters of search which further induces more security to the files stored in the cloud server. Cloud security has become a highly important necessity recently and securing online data has become the need of the hour.

REFERENCES

1. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked key- word search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), 2010, pp. 253– 262.
2. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, 2011, pp. 829–837.
3. H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. IEEE ASIACCS'13, 2013, pp. 71–81.
4. Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multi-keyword ranked query on encrypted data in the cloud," in Proc. IEEE Parallel and Distributed Systems (ICPADS'12), 2012, pp. 244–251.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

5. A. Ibrahim, H. Jin, A. A. Yassin, and D. Zou, "Secure rank- ordered search of multi-keyword trapdoor over encrypted cloud data," in Proc. IEEE Asia-Pacific Conference on Services Computing (APSCC'12), 2012, pp. 263–270.
6. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEEINFOCOM'10,2010,pp.1–5.
7. M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS'11), 2011, pp. 383–392.
8. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014, pp. 2112–2120.
9. W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud com- puting," in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA: IEEE, 2014, pp. 276–286.
10. Wei Zhang, Yaping Lin, Gu Qi, "Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing", in IEEE Transactions on Cloud Computing, vol. 6, no.1, 2018, pp. 74-86.
11. Qi Chai, Guang Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers", in 2012 IEEE International Conference on Communications (ICC), 2012.
12. Qin Liu, XiaohongNie, Xuhui Liu, Tao Peng, Jie Wu, "Verifiable Ranked Search over dynamic encrypted data in cloud computing", in 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), 2017.