International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Volume 5, Issue 3 (May-June, 2017), PP. 47-49

A SEARCHING TECHNIQUE FOR MULTI DATA OWNERS IN CLOUD COMPUTING USING MULTI KEYWORD SEARCH

[1] M Manimegalai, [2] Dr. S Kirubakaran, [3] S Dhanasekar

[1] PG Student , [2]Associate Professor, [3]Assistant Professor,
[1, 2, 3] Department of Computer science and Engineering,
Info Institute of Engineering, Coimbatore, India

***Abstract* — In cloud computing, the data owners outsource their data to public cloud server. For providing security, secure search over encrypted cloud has been used under single user model. But At times this has been supported by multiple owners to share benefits of cloud computing. To enable cloud server for secure search I have proposed a system with secret key generation and new data user authentication with multiple keyword search in multiple owner model for privacy preserving. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, I propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Secret Key generation is done by getting multiple keywords from the user.**

***Index Terms* — data user authentication, multiple keyword search, Multi owner model.**

I. INTRODUCTION

A Cloud Computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. Cloud Computing allows consumers and businesses to use applications without installation and access the personal files at any computer with internet access. In a Cloud Computing platform software is migrating from the desktop into the "clouds" of the Internet, promising users anytime, anywhere access to their programs and data.

a. The Cloud services
- Infrastructure as a service (IaaS): the 'raw' machines (servers, storage, networking and other devices) on which the service consumers install their own software, usually as virtual machine images are hosted as service in the Cloud.
- Platform as a service (PaaS): the development platform, environment providing services and storage are hosted in the Cloud.
- Software as a service (SaaS): the predefined application over the Internet or distributed environment is hosted as service in the Cloud.

b. Types of Cloud formations
- Public Cloud: Public Clouds are available to the general public or a large industry group and are owned and provisioned by an organization selling Cloud services.
- Private Cloud: Private Clouds exist within company's firewall and are managed by the organization. They are Cloud services created and controlled within enterprise
- Hybrid Cloud: Hybrid Clouds are a combination of the public and the private Cloud using services that are in both the public and private space.
- Community Cloud: It involves sharing of computing infrastructure in between organizations of the same community.

When sensitive data like email, Personnel health records, government confidential files are outsourced to public cloud, Data owners lose direct control on these data. It is the responsibility of Cloud Service Providers to ensure security using Virtualization and firewalls as Cloud Service Providers possesses full control of cloud hardware, software and owners data.

Encrypting data before outsourcing helps in providing security. But it is challenging problem for data utilization service based on plaintext keyword search. Solution is to download all encrypted data and decrypt them locally which will be impractical because it will cause a huge amount of communication overhead. Hence we need a secure search over encrypted data.

Secure search over encrypted data has recently attracted the interest of many researchers. Many define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is further developed some researchers. However, these schemes are concerned mostly with single keyword search. Extending these techniques for ranked multi-keyword search will incur heavy computation and storage costs. Secure search over encrypted cloud data is first defined by Wang et al. and further developed by many

researchers. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search. However, all these schemes are limited to the single-owner model.

In practical, Cloud supports multi data owners. When we go for multiple data owners we have new challenging problem. First, in single owner model scheme the data owner has to stay online to generate trapdoors for data users. When huge amount of data owners are involved asking them to stay online simultaneously to generate trapdoors will affect flexibility and trapdoors will affect flexibility and usability of system. Second, none of us would be willing to share our secret key as it may affect security. Different data owners would prefer to use their own secret keys to encrypt their secret data. But it will be challenging to perform a secure, convenient and efficient search.

Last, when multiple data owners are involved, we should ensure efficient search.

This paper is organized as follows. Section II formulates the problem. Section III investigates entities to perform privacy-preserving search data in the Cloud environment. Section IV focus on the Data user Authentication, section V describe about the Illegal search detection and Section VI about Data user revocation. Finally, conclusion is provided with insight for future work.

II. PROBLEM FORMULATION

I need to define a multi-owner model for privacy preserving keyword search over encrypted cloud data. First I need to propose an efficient data user authentication protocol, it not only prevents attackers from eavesdropping secret keys but also helps in finding the user who pretends to be legal data user performing searches. Also it enables data user authentication and revocation. Second I need to construct a secure search protocol which enables cloud server to perform secure keyword search without knowing the actual data of both keyword and trapdoors. Also it needs to allow data owners to encrypt keywords with self chosen keys and allows authenticated data users query without knowing these keys. At last I need to conduct extensive experiments on real world datasets to confirm the efficiency and worth of my proposed system.

III. ENTITIES INVOLVED

I intend four entities involved in this proposed system. They are

- Data Owners
- Data Users
- Cloud Servers
- Administrative servers

Data owners have a collection of files F. To have my proposed efficient there is a need to build a secure searchable index I on the keyword set W extracted from F. Submit I to administration server. All files F is encrypted as file C which is to be stored in cloud server. After receiving I the administrative server re encrypt I for authenticated data owners and outsource the re encrypted index to cloud server. Now data user can search t keywords over encrypted files on cloud. Data user needs to compute the corresponding trapdoors and submit them to the administrative server. Once data user authenticated by the administrative server, it re encrypts trapdoors and submit them to cloud server. On receiving the trapdoor T, the cloud server searches the encrypted index I of each data owner and returns the corresponding set of encrypted files.

IV. DATA USER AUTHENTICATION

The process of data user authentication involves following steps. Data user has to be authenticated by administrative server. The administrative server authenticates the contents of the conversation between user and server. If contents are authenticated both data user and server generates initial search key from their conversational contents. After initialization to make authentication successful data user has to provide historical data of their conversation. Now if authentication is successful, both data user and administrative server will change their secret keys based on the contents of conversation. Thus the secret key keeps changing dynamically. Without knowing the correct historical data the attacker may not be able to start a successful communication with the administrative server. The following is a sample format of authentication data.

Request Counter	Last request Time	Personally Identifiable data

Request Counter field indicates the number of search request that data user has submitted. Last request time designated to represent the historical data of his previous request time. Personally identifiable Data point to identify a specific user using telephone number, passport number, etc..,

The proposed method of user authentication is successful when the system is able to provide both the dynamically changing secret keys and the historical data of corresponding data user.

a. Authentication protocol

The authentication protocol has following steps.

- First data user prepares his authentication data by filling in all the fields based on historical data.
- Second data user encrypts his authentication data with his current secret key (ki). Also data user now generate new secret key (ki+1) based on the previous key. He stores both keywords.
- Upon receiving data users encrypted authentication data, the administrative server decrypts with current key (ki).

- If authentication is successful, the administrative server first generates new key (ki+1) and send back a confirmation data.
- After receiving a reply from administrative server the data user decrypts with new keyword (ki+1). If decrypted data contains the confirmation data the authentication is successful.
- Otherwise the authentication is considered as unsuccessful. The data user deletes the new key (ki+1).

Advantages of this proposed protocol are that after each successful authentication process the secret key will be dynamically changed based on their previous key and historical data. Also if attackers know nothing about the historical data he will not be able to construct legal authentication data. In addition when legal user authenticate successfully the previous secret key will be expired.

V. V ILLEGAL SEARCH DETECTION

When a user communicates administrative server the user authentication takes place using the key generated on user side and on cloud server. The authentication is based on dynamic secret key based on historic information. Even if any person has stolen the previous key they might be using same key which may not match with cloud server as the new key involves with previous key and some historic data. There will be a contradiction in keys between data user and administrative server. With the help of this illegal search can be detected.

VI. DATA USER REVOCATION

Data user revocation does not need to re-encrypt and update large amount of data stored on the cloud server. Instead the administrative server only need to update the secret data stored on cloud server. When a data user is continuously using wrong key for any consecutive times then his user account has to be blocked where he may not able to perform correct search. As he is no longer a legal data user he may not perform legal search. If no keywords are matched no secure search is allowed.

CONCLUSION

In this paper, the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment has been discussed. This scheme enable's authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. As future work, the search can ranked to make the scheme computationally efficient even for large data and keyword sets. On the other hand this scheme has to be implemented on the commercial clouds.

REFERENCES

[1] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member IEEE, JieWu, Fellow, IEEE, and Siwang Zhou, "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing" IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 5, MAY 2016

[2] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Int. Symp. Security Privacy, Nagoya, Japan, Jan. 2000, pp. 44–55.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[4] E. Goh. (2003). Secure indexes [Online]. Available: http://eprint. iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security,Oct. 2006, pp. 79–88.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology- Eurocrypt 2004, Springer, 2004, pp. 506–522.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Appl. Cryptography Network Security, Yellow Mountain, China, Jun. 2004, pp. 31–45

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 3025–3035, Nov. 2014.

[10] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multikeyword ranked query on encrypted data in the cloud," in Proc. IEEE 19th Int. Conf. Parallel Distrib. Syst., Singapore, Dec. 2012, pp. 244–251.

[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5.