Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

PRIVACY PRESERVING SEARCH OVER ENCRYPTED DATA OF MULTIPLE DATA OWNER

Aditya R. Jadhav
Computer engineering Savitribhai Phule Pune University
G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India

Prasad Deshpande.
Department of Computer engineering Savitribhai Phule Pune University
G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India

SachinWalunj.
Department of Computer engineering Savitribhai Phule Pune University
G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India

ABSTRACT

The advent of cloud computing, data owners are driven to uploads their complicated information management systems from native sites to business public cloud for excellent flexibility and economic savings. Except protective information privacy, sensitive information must be encrypted before uploading, that obsoletes ancient information utilization supported plain text keyword search. Thus, enabling an encrypted cloud information search service is of overriding importance. Considering the massive variety of information users and documents in cloud, it's necessary for the search service to permit multi-keyword question and supply result similarity ranking to satisfy the e□ective information retrieval would they like. Related works on searchable encoding concentrate on single keyword search or Boolean keyword search, and barely differentiate the search results. During this paper, for the first time, we have a tendency to done and solve the difficult downside of privacy preserving multi-keyword ranked search over encrypted cloud information (PSEM), and establishes a collection of strict privacy needs for such a secure cloud information utilization system to become a reality. Among varied multi-keyword semantics, we elect the e□cient principle of coordinate matching, i.e., as lots of matches as potential, to capture the similarity between search question and information documents, and additional use real similarity to quantitatively formalize such principle for similarity checking. we have a tendency to first propose a basic PSEM theme exploitation secure real computation, then considerably improve it to satisfy di□erent privacy necessities in 2 levels of threat models. Through analysis work privacy and e□ciency guarantees of projected schemes is given, and experiments on the real-world data-set more show planned schemes so introduce low expenditure on computation and communication.

KEYWORDS: Cloud Data Security, Multi-Keyword Matching, Multiple Owner, Encrypted Data

INTRODUCTION

In our project we focusing on cloud security in which mainly we consider cloud server is Semi trusted. Because we are not believe on cloud server full trusted hence we are considering cloud server as Semi-Trusted. In our project we are contributing three important things 1. Multi-Keyword Search, 2. Multiple Data Owner, 3. Secure Searching and 4. Security to Our Data. Till now there were no such system that contributing thing in one project hence we are going to combine all these things in one project. We are combining this all module in one project because of this we are mainly focusing cloud security. Data owner has rights provide security to his own file and for Data User to search and use such file he has to take all the permission from Data Owner. This way we are not providing whole rights to cloud server to secure Data Owner's file. Cloud server is responsible for making searching mechanism encrypted and also to store file in secure manner. As less are stored in encrypted format by Data owner neither cloud server nor a Data user access the file without knowing decryption keyword. Both cloud server and Data User has only one way to access the file is by knowing the keyword which is provided by Data Owner. Also we are making secure searching mechanism for Data User by which even other person who not registered in cloud. We are providing search key for each Data User for searching over Cloud not able access the file server. Using only this search key Data user is able to Search over cloud server. Cloud server is responsible providing each user the unique search key. Data owner responsibility is while uploading file he has to encrypt their own file and

keep each file decryption key. When Data User want to access the file he send request to file owner. Upon receiving this request Data Owner has rights to provide access key on his interest. By this way Data owner secure his own file. Thus we are achieving full security to our data over cloud server or cloud computing.

GOALS AND OBJECTIVES

The system is designed in order to fulfill the following objectives. The objectives of the proposed system are as follows:

SYSTEM FEATURE: - To modify privacy protective graded multi-keyword search within the multi-owner and multi-user cloud surroundings, our system style ought to at the same time satisfy security and performance goals.

MULTI-KEYWORD SEARCH OVER MULTI-OWNER DATA:-The projected theme ought to permit multi-keyword search over totally di□erent encrypted files which might be encrypted with di□erent keys from di□erent information homeowners. It additionally must permit the search among completely di□erent Data.

DATA USER REVOCATION: -This scheme should ensure that only valid data users can perform valid search. However, once a data user revoked, he can no longer perform valid search over encrypted stored data.

INFORMATION OWNER SCALABILITY:-The projected theme ought to permit new information owners to enter this technique while not touching alternative information owners or information users, i.e., the theme ought to support information owner quantifiability.

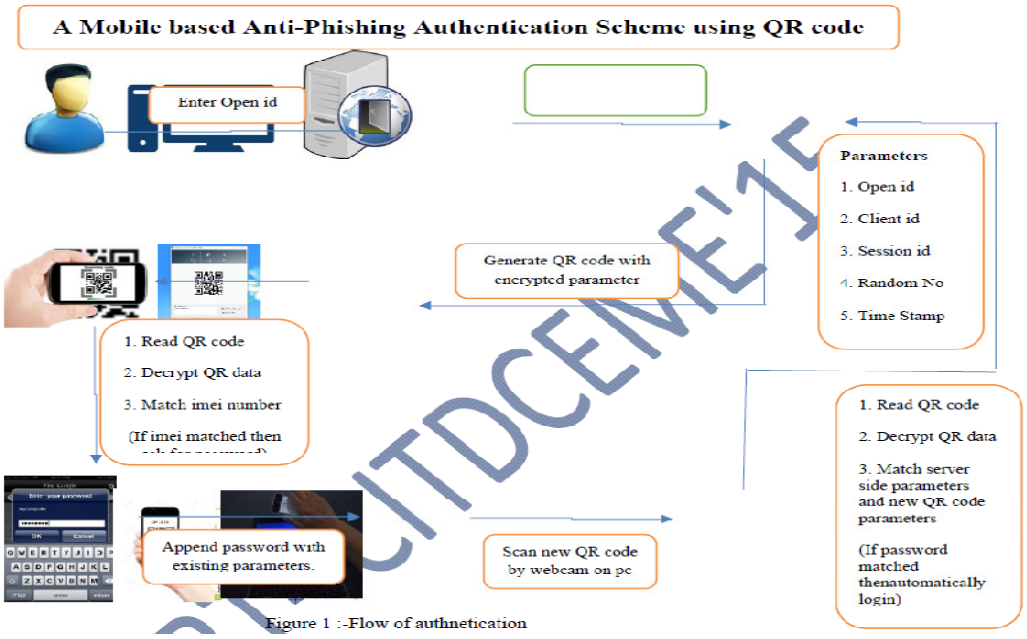

Figure 1 :-Flow of authnetication

In this system, user key is generated after registration for security. The user uploads the desired File to server, which is securely stored using a User's key to access it. The user uploads the desired File to server which is securely stored using a User's key to access it. Along with the secured storage of the file, the keywords or index related to that file is also stored in the Server. System will generate a search key for each user after approval from admin (one-time). The User enters a keyword in order to retrieve the associated File. Using that keyword along with the user's key and search key a trapdoor is calculated. This Trapdoor along with a search key used in this calculation is sent to the server. The keyword and the User's key is calculated at the server side from the Trapdoor that was received. The Calculated keyword is searched through the stored keywords and the list of similar found keywords associated with that files are Finally Displayed to the user. The Owner of the file has the Right to provide access to other user for each file out of

which the transmitted key plays a part in its Secured Storage. Will approve search requests of various users one-time after accessing the system.

LITERATURE SURVEY

1. Wei Zhang, Student Member, IEEE, YapingLin,"Privacy Preserving Ranked MultiKeyword Search for Multiple Data Owners in Cloud Computing"[1]
In this paper, they propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To show cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, they systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and less, they propose a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eaves leaving secret keys and pretending to be legal data users submitting searches, they propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Furthermore, PRMSM supports e□cient data user revocation. Extensive experiments on real-world datasets confirm the e□cacy and e□ciency of PRMSM.

2. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data"[2]
In this paper, for the first time, they done and solve the challenging problem of privacypreserving multi-keyword ranked search over encrypted cloud data (PSEM). They establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multikeyword semantics, they choose the e□cient similarity checking of coordinate matching, i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use inner product similarity to quantitatively evaluate such similarity measure. They first propose a basic idea for the PSEM based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two di□erent threat models.

3. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data"[3]
In this paper, for the first time they done and solve the problem of e□ective yet secure ranked keyword search over encoded cloud data. Ranked search greatly fulfill system usability by returning the matching less in a ranked order regarding to certain significant criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy preserving data hosting services in Cloud Computing. They first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its ine□ciency. To achieve more practical performance, they then propose a definition for ranked searchable symmetric encryption, and give an e□cient design by properly utilizing the existing cryptography primitive, order-preserving symmetric encryption (OPSE)

4. L. Ballard, S. Kamara, and F. Monrose, "Achieving e□cient conjunctive keyword searches over encrypted data"[4]
They present two provably secure word searches over symmetrically encrypted data. Their first scheme is based on Shamir Secret Sharing and it can provide the most reliable search technique in this context to date. Although the size of its trapdoors is linear in documents being searched, we empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation they provide an alternative based on bilinear pairings that yields constant size trapdoors. This latter construction is not only asymptotically more e□cient than previous secure conjunctive keyword search schemes in the symmetric setting, but incurs significantly less storage overhead.

5. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking"[5]
In this paper, they present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multiple-keyword search and search result ranking, they

propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, they propose a tree-based index structure and various adaption methods for multidimensional (MD) algorithm so that the practical search efficiency is much better than that of linear search.

CONCLUSION

We analyze the problem of secure multiple keyword search for multiple data owners and multiple data users in the cloud computing environment. Di□erent from former works, our schemes enable authenticated data users to achieve secure, advantageous, and e□cient searches over multiple data owner's data. To e□ciently authenticate data users and detects attackers, who cheat the secret key and perform illegal searches, we propose a secret key generation and a new data user authentication system. To enable the cloud server to perform secure search among multiple owners data encrypted with unique secret keys, we systematically construct a secure searching mechanism. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a feasible Order and Privacy Preserving Function family. Moreover, we show that our approach is computationally e□cient, even for large data and keyword sets. As our future work, on one hand, we will consider the problem of secure fuzzy keyword search in a multi-owner paradigm. On the other hand, we plan to implement our scheme on the commercial clouds.

REFERENCES

[1] Wei Zhang, Student Member, IEEE, YapingLin,"Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing"information: DOI 10.1109/TC.2015.2448099, IEEE Transactions on Computers JOURNAL OF LATEX CLASS FILES, VOL. 6, NO. 1, JANUARY 2015

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacypreserving multi-keyword ranked search over encrypted cloud data, in Proc. IEEE INFOCOM11, Shanghai, China, Apr. 2011, pp. 829837.

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, Secure ranked keyword search over encrypted cloud data, in Proc. IEEE Distributed Computing Systems (ICDCS10), Genoa, Italy, Jun. 2010, pp. 25326

[4] L. Ballard, S. Kamara, and F. Monrose, Achieving e□cient conjunctive keyword searches over encrypted data, in Proc. Information and Communications Security(ICICS05), Beijing, China, Dec. 2005, pp. 414426.

[5] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, Privacy-preserving multikeyword text search in the cloud supporting similarity-based ranking, in Proc. IEEE ASIACCS13, Hangzhou, China, May 2013, pp. 718