Privacy Preserving And Multi Keyword Ranked Search

Shreejit Pillai[1], Gaurav Ransing[2], Navanath Ransing[3], Sumit Markad[4], Prof. Nilesh Sable[5]
Department of Computer Engineering
[1, 2, 3, 4] JSPM's Imperial College of Engineering and Research, Pune
[5]Professor,Imperial College Of Engineering and Research, Pune, India

Abstract-*Due to cloud computing it has become very popular for data owners to outsource data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However most cloud servers in practice do not serve just one owner instead they support multiple owners to share benefits brought by cloud computing. In this system we propose schemes to deal with privacy preserving ranked multi keyword search in a multi owner environment to enable cloud servers to perform secure search without knowing the actual data of both keywords we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance course between keywords and files, we propose a novel additive order and privacy preserving function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data owners submitting searches we propose a dynamic secret key generation key protocol and a new data user authentication protocol.*

Keywords-Multi Keyword Search, User Privacy, Multi Owner, Dynamic Secret Key.

I. INTRODUCTION

Cloud storage system, is set of storage servers, and provides long-term storage services over the Internet. Storing data in a third party's cloud system causes grave to connect to over data secret. Normal hidden schemes defend data secret but have some limitation to functionality of the storage system because a few operations are supported over hidden information. Building a grave storage system that compatible several functions is endurance when system is distributed. Service providers of cloud would pledge to owners data security using phenomenon like virtualization and firewalls. These phenomenon do not protect owner's data privacy from the CSP itself, since the CSP control whole of cloud hardware, software, and owners' data. Hiding the sensitive data before send outside can stored data confidentiality against CSP. Data hidden makes the conventional data utilization service based on plaintext keyword search a very challenging problem. A solution to this problem is to download all the hidden data and create the original data using the hidden key, but this is not practical cause it create extra overhead. In this paper, we suggest when search multiple owner multiple keywords that time provide the privacy and show the result in ranking form to make easy cloud servers to perform safe search excluding knowing the real value of both keywords and trapdoors, we properly build a novel safe search rule. So that various data owners use distinct keys to hide their files and keywords. Genuine data users can get a query excluding knowing confidential keys of these various data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggest a family which preserves privacy, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To protect from disclosing the result we propose a novel dynamic secret key generation and a new user authentication protocol.

II.RELATED WORK

Secure Keyword Search in Cloud Computing

The privacy concerns in cloud computing motivate the study on secure keyword search. It first defined and solved the secure ranked keyword search over encrypted cloud data. In one of the paper they proposed a scheme that returns the top-*k* relevant files upon a single keyword search. Cao et al. and Sun et al. extended the secure keyword search for multi-keyword queries. Their approaches the list of keywords and apply matrix multiplications to hide the actual keyword information from the cloud server, while still allowing the server to find out the top-*k* relevant data files. Xu et al. proposed MKQE (Multi-Keyword ranked Query on Encrypted data) that enables a dynamic keyword dictionary and avoids the ranking order being distorted by several high frequency keyword. Li et al. , Chuah et al., Xu et al. and Wang et al. proposed fuzzy keyword search over encrypted cloud data aiming at tolerance of both minor types and format inconsistencies for users' search input further proposed privacy-assured similarity search mechanisms over outsourced cloud data. In other paper, they proposed a secure, efficient, and distributed keyword search protocol in the geo-distributed cloud environment. The system model of these previous works only consider one data owner, which implies that in their solutions, the data owner and data users can easily

communicate and exchange secret information. When numerous data owners are involved in the system, secret information exchanging will cause considerable communication overhead. Sun et al. and Zheng et al. proposed secure attribute-based keyword search schemes in the challenging scenario where multiple owners are involved. However, applying CP-ABE in the cloud system would introduce problems for data user revocation, i.e., the cloud has to update the large amount of data stored on it for a data user revocation. Additionally, they do not support privacy preserving ranked multi-keyword search. Our paper differs from previous studies regarding the emphasis of multiple data owners in the system model. This paper seeks a solution scheme to maximally relax the requirements for data owners and users, so that the scheme could be suitable for a large number of cloud computing users.

III. STUDIES AND FINDINGS

- We define a multi-owner model for privacy preserving keyword search over encrypted cloud data.
- We propose an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation.
- We systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search with-out knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and al-lows authenticated data users to query without knowing these keys.
- We propose an Additive Order and Privacy Pre-serving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.
- We conduct extensive experiments on real-world datasets to confirm the efficacy and efficiency of our proposed schemes.

IV. SYSTEM ARCHITECTURE

The main purpose of the architecture is to provide privacy to the customers data and provide a suitable searching method to find their documents over cloud.

There will be 2 user roles.

- Admin
- User.

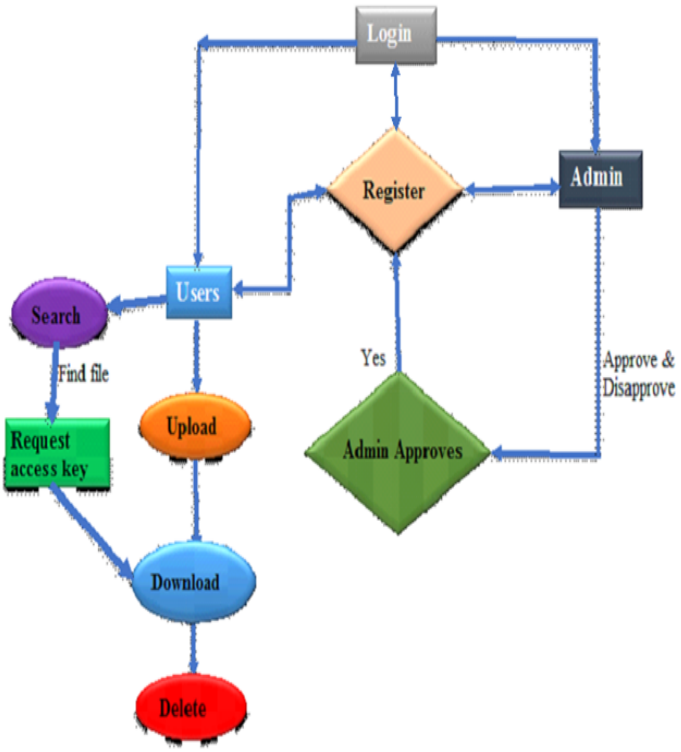


Fig - Architecture Diagram

1. ADMIN:

The admin is responsible for giving access of the cloud to the newly registered user. He accepts or rejects the request of the various users requesting for the access of the cloud.

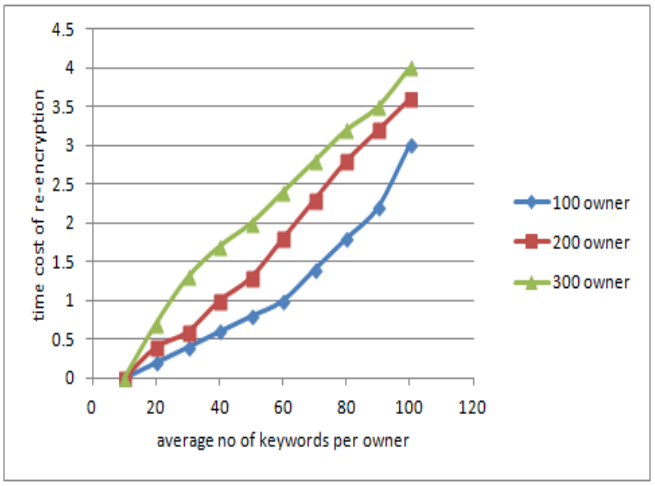
2. USER ROLE:

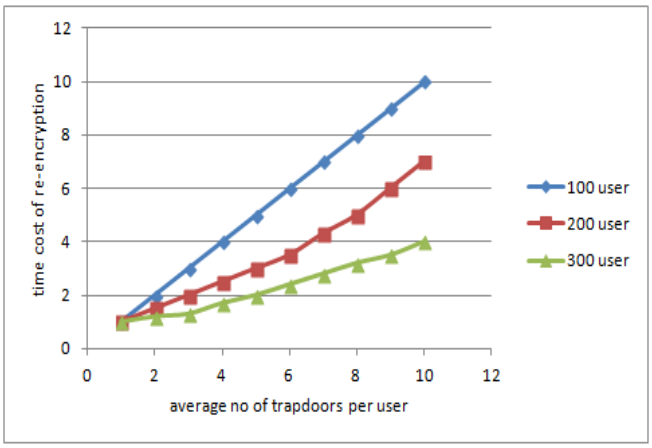
The user must register to the cloud by providing his credentials and a request is sent to the admin. Admin identifies the request and approve or reject .If admin approves the request an email is sent to the user's registered email-id containing user id and password for accessing the cloud. User will now login into the system using this user id and password and use the facilities of cloud like uploading documents, downloading or deleting a particular document, while user wants to upload a document he is asked to provide a particular access key for the document and multiple keywords for accessing the file later while uploading the document gets encrypted and stored in the cloud so that no any legitimate users can access the file without his permission. Our if file owner identifies that user and is ready to share the file then he will send a access key through mail to that user who wants that file. By using the received key the user can now successfully download that file. In this way a secure mechanism is maintained throughout the cloud. For privacy concerns, even if the key gets leaked by other user still that

user cannot access that particular file he needs the approval of the file owner.

V. RESULT

The multiple keyword based structures tend to create dynamic search functionalities such as single keyword search, similarity search, multi keyword search, ranked search and many more. The propose system will have greater advantage at outsourcing sensitive information such as emails, personal health records and many more. Cloud service providers that keep the data for users may access users sensitive information with proper authorization. The multiple schema based data will be primarily based on multi privacy requirements which will directly help the system in a dynamic manner. In depth analysis indicates multiple records are kept in the outsource system which may or may not be tracked in the current system.





VI. CONCLUSION

This system creates the privacy preserving environment for better and formal access of data. The data privacy is important and sensitive data must always be encrypted. Thereby establishing a set of strict privacy requirements for a secure cloud data utilization system proposing an idea for an MRSE based on inner product computation and then give to significantly improved MRSE schemes to achieve stringent privacy requirements in two different threat models. In the current scenario users need privacy to securely perform actions on the internet. This project will be a stepping stone to achieve complete privacy while using the internet. Therefore we created a dynamic cloud based system which used privacy preserving ranked multi keyword search to give results in a secure manner.

REFERENCES

[1] Chi Chen, Xiaojie Zhu, Peisong Shen, Jiankun Hu, Song Guo, Zahir Tari, and Albert Y. Zomaya, “An Efficient Privacy-Preserving Ranked Keyword Search Method” April 2016

[2] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, “Security analysis of authentication protocols for next-generation mobile and CE cloud services,” in Proc. IEEE Int. Conf. Consumer Electron,2011, Berlin, Germany, 2011, pp. 83–87.

[3] D. X. D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Security Privacy, BERKELEY, CA, 2000, pp. 44–55.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. EUROCRYPT, Interlaken, SWITZERLAND, 2004, pp. 506–522.