Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in SaaS Cloud Computing

Sudhirkumar T Khelkar, Prof. Harish K. Barapatre

***Abstract*— The innovation in cloud computing has encouraged the data owners to outsource their data managing system from local sites to profitable public cloud to increase affordability of services. But people can like full benefit of cloud computing, if we are able to report very real secrecy and security concerns that come with loading sensitive personal information then we have to increase security, privacy. In view of the huge number of data users, documents in the cloud, it is important for the search facility to agree multi keywords query and arrange for result comparison ranking to meet the actual need of data recovery search and not regularly distinguish the search results.**

Related mechanisms on searchable encryption emphasis on single keyword search or Boolean keyword search, and often sort the search outcomes. In our system, we explain and solve the interesting problem of privacy preserving multi keywords ranked search over encrypted cloud data, and create a set of strict privacy necessities for such a safe cloud data application system to be effected in real. We can add Document owner accounts, Cloud Server account, Admin account and grant permission to various privileges to different user.

***Index Terms*— Cloud computing, SaaS, Cloud Server, Admin Server, Ranking, Boolean Keyword**

I. INTRODUCTION

Information explosion happened on internet. Digital data is generated on youtube.com, Facebook, Picasa server, Twitter. Data storage is going form Giga bytes to Peta Bytes.

Cloud computing is a Web-based model, where cloud clients can supply their information into the cloud [1]. By loading information into the cloud, the data owners stay unbound after the capacity of storage. Thus, to safeguard sensitive information integrity is an essential task.

The data owner has to be outsourced in the encoded system to the public cloud and the data operation is founded on plain text keyword search. We select the efficient measure of "coordinate matching". Technique. Coordinate matching is used to measure the parallel amount. Coordinate matching captures the significance of data documents to the search query keywords. There are multiple checks to provide security. Data owners can encrypt data and decrypt data as per requirement [2].

The search facility and privacy protection over encrypted cloud data channel is essential. If we study huge amount of data documents and data users in the cloud, it is hard for the necessities of performance, usability, plus scalability. Concerning to encounter the real data recovery, the huge amount of data documents in the cloud server achieve to outcome relevant rank instead of returning not able to separate outcomes. Ranking scheme cares multiple keyword search to recover the search correctness [3].

We can create various user logins in cloud and every user is getting separate services and privileges.

Today's Google network search devices, data users offer set of keywords instead of unique keyword search importance to retrieve the maximum significant data. Coordinate matching is a synchronize pairing of query keywords which are relevance to that document to the query. It remains the interesting job on behalf of how to relate the encrypted cloud search. The difficult of multi-keyword ranked search over encrypted cloud data is resolved by using stringent privacy necessities then numerous multi-keyword semantics. Among numerous multi-keyword ranked semantics, we choose coordinate matching [4][5][6]. Our contributions are summarized as follows,

For the first time, we locally test system using Tomat version 6.

Classification of users on cloud is maintained.

Data user, Data owners, Admin such separate roles defined to maintain cloud.

1) Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is given, an experiments on the real-world data set further show the proposed schemes indeed introduce low overhead on computation and communication

II. PROBLEM STATEMENT

On-demand data is deposited on internet, people are writing their opinion on Facebook. Twitter is creating huge data with "likes" and "dislike" of user/subscriber. It is essential for the search facility to permit multi keyword search query and make available result comparison ranking to see the effective data retrieval requirement.

To develop the search result accuracy as well as to enrich the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search regularly yields extreme coarse results. The searchable encryption method supports to give encrypted data as documents and agrees a user to firmly search over single keyword and retrieve documents of concern. System should provide privileges to data owner to manage data at their wishes to provide highest privacy on public cloud domain.

III. PROPOSED SOLUTION

We propose an effective system where any authorized user can do a search on an encrypted data with multiple keywords, without revealing the keywords he searches for, nor the data of the documents that match by the query. Authorized users can make search processes by definite keywords on the cloud to retrieve the relevant documents.

Sudhirkumar T Khelkar, Yadavrao Tasgaokar Institute of Engineering and Technology Karjat, Thane, India

Prof. Harish K. Barapatre, Yadavrao Tasgaokar Institute of Engineering and Technology, Karjat, Thane, India

Our proposal system facilitates that a group of users can query the database provided that they possess so called trapdoors for the search terms that authorize the users to include them in their queries. Our proposed system is able to perform multiple keyword search in a single query and ranks the results so the user can retrieve only the most relevant matches in an ordered manner. And we establish a set of strict privacy requirements. Among numerous multi keyword semantics, we select the effective principle of "coordinate matching".

IV. SYSTEM OVERVIEW

The system architecture is concerned by creating a simple structural framework for Figure 1 shows the outline of the system.

Fig 1 Search over Encrypted Cloud Data

Architectural Model The proposed system contain data users, the cloud server and the administration server. When the users have right to access in the server from their local system, they select the file which have to upload on the cloud. This selected files is saved on the location where all the users files are saved (Because there is not only single user, there are multiple user which cannot interact directly). Now from that location, the user uploads the data file on the cloud.

When the data is uploaded, if the user wants to share that uploaded files, he/she can share with the registered users along with the private key.

When the data files are uploaded on the cloud, the server can't know the contents of data files because the data files are encrypted. When the shared users wants to access the file, he/she requests the decryption key. Then the decryption key is sent to their registered mail account. By using that decryption key, the contents of the data file gets decrypted and the users can download the data file. If any attackers can access the cloud server then he/she cannot get the contents of the actual data files. The cloud server is only responsible for storage of data files.

Security Goals

In this paper, we proposes scheme in which function design satisfy security goals.

Multi keyword Search over Multiple data owner: This paper allow multiple search over encrypted data files. This allows the server to ranked the searched result among different users and return the most frequent results.

User scalability: This paper allow new data users to register and login to this system without disturbing other users.

• User revocation: This paper allow that only registered data users can perform right search.

• Security Process: This paper prevent attacker from eavesdropping. When the files is shared which is in the encrypted form, another users wants the keywords to decrypt the data files.

Multi-Keyword Search

In this paper, user can search multiple file names. This proposed system also search the "wildcard words" keyword which means if the data file name is abcd.txt and the user search ab then it shows all the data files that contain the letter ab simultaneously.

V. SYSTEM MODULE

A. Authentication and Authorization

In this module, the data user register with their user id, Password, email-Id, mobile number and gender then user can access the database. After registration completed, user access the database by giving the user-id and their password.

B. Uploading and Downloading

In this module, Files are uploaded to the server after file is encrypted by the encryption method. This encryption is done by AES (Advanced Encryption Standard) Algorithm and generate key. This Encrypted Data is in the form of Binary and stored in Cloud. User needs decryption key to download the data files.

C. File Sharing

In this module, the uploaded files are shared to the multiple users. In this system, the Private Key of the Data which is shared will be send via a secure channel called Gmail. This decryption key is used by the user at the time of download the files.

D. Key Generation

In this module, when the user wants to access the data files then the server send the decryption key. Through this decryption key, the user who wants to access the data file, uses this decryption key to decrypt the files with the help of private key sent at the time of file sharing.

E. Admin Module

In this module, admin can view the details of all the registered users. Admin can see the status of the shared files among multiple users.

F. Algorithm & Protocol Used

There are two types of algorithm used in this system.

a) Encryption: This is used to encrypt the data files. This convert the plain text into the cipher text. This uses the AES (Advanced Encryption Standard) algorithm.
b) Decryption: This is used to decrypt the data files. This convert the cipher text into the plain text. This uses the ADS (Advanced Decryption Standard) algorithm

VI. CONCLUSION AND FUTURE WORK

In this paper, we solve the problem of secure multi keyword search for multiple data owners in the SaaS based cloud computing. We introduced a AES algorithm for creating encryption. A new data user authentication protocol which is used to protect the system from attackers and authenticate only the registered users.

In our future work, we work on wild keyword searching methods and we are planning to implement on the public cloud. We are surveying Azure, Google Cloud platform and AWS Cloud for this purpose.

REFERENCES

[1]Jyothi Koodi1, G. Srinivasachar, "Privacy-Preserving Multi-keyword Ranked Search Over Encrypted Cloud Data" International Research Journal of Engineering and Technology (IRJET) , Volume: 02 Issue: 03 June-2015

[2] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.

[3]A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, 2006.

[4] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in Proc. of CRYPTO, 2007. [3] M. Abdalla, M. Bellare, D. Catalano, E.

[5]Kiltz, T. Kohno, T. Lange,J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," J. Cryptol., vol. 21, no. 3, pp. 350–391, 2008.

[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. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.