© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

An Efficient Search Method over an Encrypted Cloud Data

Dipeeka Radke, Nikita Hatwar, Lila Gouda , Minal Shambharkar, Parul Gajimwar, Ruchika Raut
Department of Computer Science and Engineering, Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

Cloud data owners used to transfer data in an encrypted form for the purpose of privacy preserving. Therefore it is important to develop efficient & reliable cipher text search techniques. In encryption technique, the relation between the data is hidden, which make them to perform deterioration. In earlier days it was not possible to upload the encrypted data on the cloud. Now a days the number of internet users are increasing & day by day the number of data is also increasing. According to the growth of increasing number of data it is important to provide security to the cloud data. For providing security to the data on the cloud, it should be first converted into encrypted form before transferring it & it can be regain effectively. Along with this more additional features can also be provided with the search techniques like dynamic update operations. In this paper a hierarchical clustering method is used to support more search methods & also to complete the demand for fast cipher text search method for big data environments. For the huge number of users & the data in the cloud, it is important for the search method to include multi keyword query for arranging the comparison of ranking for the proper need of data regain search and not regularly famed the search results. In this system, the interesting problem of privacy preserving multi keywords ranked search over encrypted cloud data can be explain and solve. And also used to create strict privacy for safe cloud data application so that the system should be effected in real world.

Keywords: Multi-Keyword Ranked Search, Security, Cipher text Search, Privacy preserving

I. INTRODUCTION

Now a days, cloud computing is a demonstrative field in information technology with the increased rate of data externalization over cloud data privacy of sensitive data becomes a big issue. For the security purpose data is encrypted before externalization but encrypted data is very difficult to be recover easily. Cloud computing can be accepted as a model for delivering information technology services (like storage space, networking, applications etc.) in which facility are provided from internet using web base tools, rather than a direct connection to server. Cloud computing provides two tools hardware & software resources from a shared pool according to user's demand. So this technology releases user from burden of management efforts and also from headaches of installation and maintenance. In these days, we are seeing that a thousand of information is common every day online. Daily new and additional information is added by different data owner. Then how we can store this additional data and new information. For this we want to create number of databases daily, but this is not possible for us to create the number of databases daily. To overcome this concept the cloud is invented. It is used to store the data and information. The data which is store in cloud may be accessed by any data user. Therefore we are providing a privacy to that data. In cloud computing there are three categories of services. The services are IAAS (Infrastructure as a service), PAAS (Platform as a service) and SAAS (software as a service).

From this three services we are using IAAS service because IAAS client have true control over there infrastructure than user of PAAS and SAAS. The main use of IAAS is that it include the actual deployment and development of PAAS, SAAS
Services models.

Infrastructure as a service (IAAS):-
In this, software is made available to the user as a service. A User can demand computing infrastructure, storage infrastructure and network infrastructure etc from services provider. In this user is not the actual owner of the infrastructure, but has control over operating systems, deployed application, storage etc.

Platform as a service (PAAS):-
In this, software is made available to the user as a service. Programming Languages and tools are provided by service provider to deployment and develop services. A user has no control over their basic infrastructure but has control over the deployed applications.

Infrastructure as a service (IAAS):-
In this, software is made available to the user as a service. Cloud application are generally accessible from various devices like tablet, laptop, mobile, PC, servers, workstation etc. The user has no control over the basic platform and infrastructure.

II. PROBLEM STATEMENT

Actually huge amount of data documents and large number of on-demand data users in the cloud, this difficulty is going as a challenge. Now it is essential for the search facility to give the permission to multi keyword search query and make the result available. To develop the search result correctly as well as to improve the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search. The searchable encryption method helps to give encrypted data as documents and agrees a user to hard search over single keyword and retrieve documents of field.

III. LITERATURE SURVEY

Many enterprises are moving their valuable data to the cloud because of the advantages of storage as a service. The advantage of this are the cost is less, it can be easily ascendable and can also be accessed from anywhere at any time. In this, trust between cloud user and data provider is very important. To establish their trust security is used as a parameter. Cryptography is used to provide trust.

To provide security to searchable encryption cipher text method is used. Many researcher have been working for developing good searchable encryption technique. Lots of interest is generated by cloud computing to provide solution for data transferring and for high quality data services. As the data and the cloud's size is increasing the searching of the relevant data is consider to be a challenge, rank search technique is used for faster search.

Now a days, more and more people are motivated to transfer their data to public cloud servers for great facility and reduced costs in data management. For considering privacy issues sensitive data should be encrypted before transferring to cloud server. This paper present a secure and efficient multi keyword rank search method over encrypted data which supports dynamic update operations like deleting and inserting of documents.

IV. PROPOSED SYSTEM

We are developing an effective system where any legal user can do a search on an encrypted data with multiple keywords, without leakage of the keywords he searches for, nor the data of the cloud that match. Authorized users can make the search process by using keyword to look in the document from the cloud. Our system provides the facility that a group of users can query the database provided that they can easily access the data from the cloud anywhere at any time. Our proposed system is able to perform multiple keyword search in a single query and ranks the results so the user can use only the most exact matches in proper order. And set of strict privacy is built according to the requirements. We consider the most effective procedure among number of multi keyword semantics.

V. SYSTEM OVERVIEW

The system architecture is worried for the system, by creating a simple framework. In this system, it defines all the frame of the project which describes the function of the structure in detail and the main aim behind this project is to plan a proper solution for the problem identified by the file.

The below Figure 1 shows the summary of the structure. There are three parts in our system architecture: Data Owner, Data user and Cloud Server.

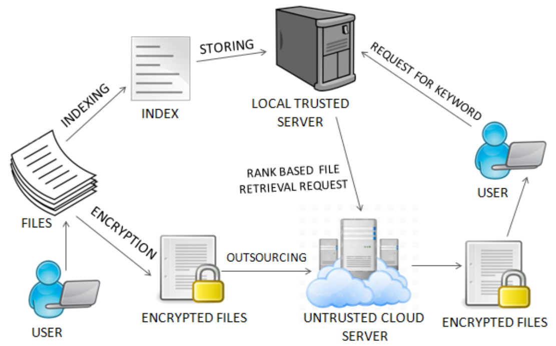


Figure 1

- ✓ Data Owner is a developer for the developing of the database.
- ✓ Data Users are those who can easily access the file from the database.
- ✓ Cloud Server gives the facility of accessing information to the users.

Data owner has amount of data records that he wishes to outsource on cloud server in encrypted form. Before outsourcing, data owner will first construct a secure searchable index from a set of diverse keywords removed from the file collection and store both the index and the encrypted file on the cloud server. We under take the approval between the data owner and users is done. To search the file collection for a given keyword, certified user creates and submits a search request in a secret forma trapdoor of the keyword to the cloud server. Upon getting the search request, the server is in charge to search the index and return the matching set of files to the user. We study the secure ranked keyword search problematic as follows: the search result must be returned giving to definite ranked relevance principles, to develop file retrieval correctness for users. Though, cloud server must study unknown or little about the important principles themselves as they reveal major sensitive information against keyword privacy. To decrease bandwidth, the user may send possible value k along with the trapdoor and cloud server only sends back the top-k most appropriate files to the user's concerned keyword.

Design Goals:

To allow ranked searchable symmetric encryption for effective utilization of externalization cloud data under the previously mentioned model, project design should achieve the following security and performance guarantee specifically it has the following goals

1. Ranked Keyword Search: To explore various existing mechanism for secure searchable encryption and to build a framework for effective ranked search.

2. Security guarantee: To making the outsourced data secure by preventing cloud server from learning plaintext or files.

3. Achieving Efficiency: Above goals should be achieved with minimum communication and computation overhead.

Modules

Our proposed system consists of the following modules:

- ✓ Data Owner Module
- ✓ Data User Module
- ✓ Cloud Server Module
- ✓ Security Module

Data Owner:

Data owner have a main authority to maintain amount of data records that he wishes to outsource on cloud server in encrypted form they also have an authority that they can make three or four admin not more than that. The data owners have the authority that can be able to upload the files. The files are First get encrypted before the files are uploaded to the cloud server. The data owners provides an option to enter the keywords for the file that are being uploaded to the server. These files are available on the cloud, the data users should be able to search the keywords. The data owners will also be provided with a request screen so they are able to accept or reject the request that are received by the data users.

Data User:

Data user have the ability to download the files which are available on the cloud. The files which are available on the cloud is uploaded by the data owner. Data owner are nothing but they are the admins. There are numerous files available on the cloud server, there is a one option that is search option to search any file from the cloud. After, searching the file the result shows various files related to the searched one, the user can also be able to download that file and use the downloaded data.

Cloud Server:

In cloud server, the data which is stored on the cloud is in encrypted format. The huge number of files are arrange in sequential order and stored the number of files into cluster like hierarchical clustering. Hierarchical clustering are used to arrange the related type of data into a single cluster. Cloud server provides the files to the users to use the data which is on the cloud. In cloud server the cloud gets the request which send by the users and give the response to the request by providing to the related files into that cluster.

Security:

In this module, security is provided by privacy preserving we are providing a strong security which is known as AES (Advanced Encryption Standard). While, uploading the file it is necessary to first encrypt the file then after encryption we can upload the file. The User can search for the file after searching for the file the user user can download it but before downloading that file the user gets a key for decryption and then the user gets a decrypted file.

VI. OUTPUT

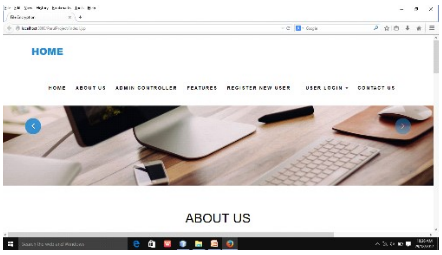
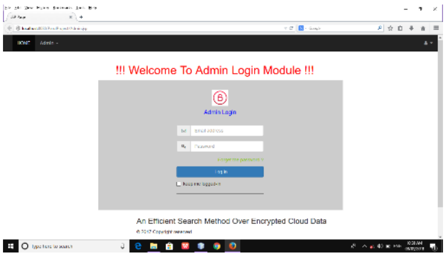


Figure 2. Home Page


!!! Welcome To Admin Login Module !!!

An Efficient Search Method Over Encrypted Cloud Data

© 2017 Copyright reserved

Figuer 3. Admin Login

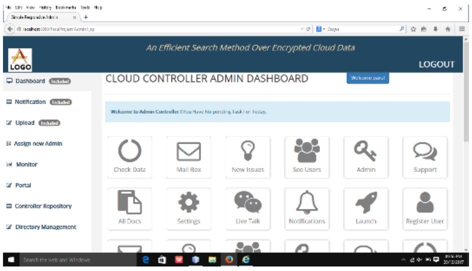


Figure 4. Admin Dashboard

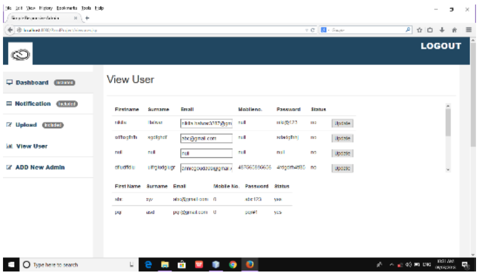


Figure 5. View User

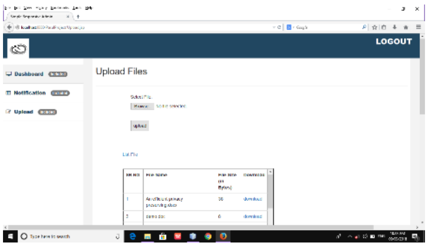


Figure 6. Upload

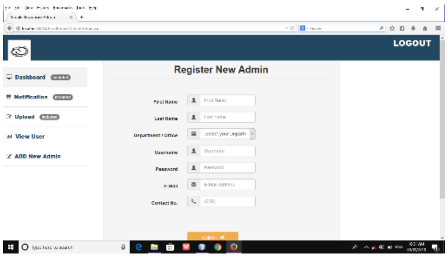


Figure 7. Create New Admin

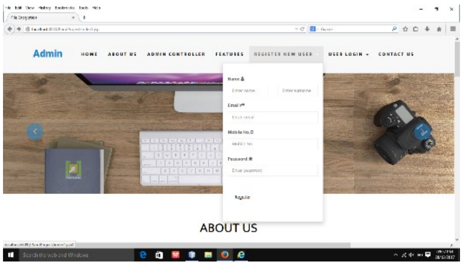


Figure 8. User Registration

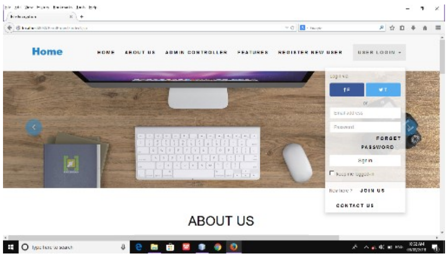


Figure 9. User Login

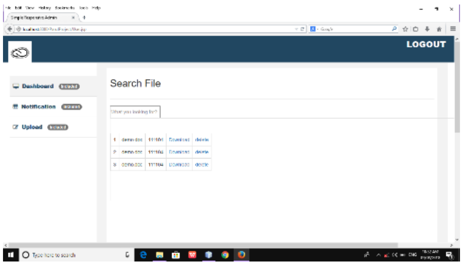


Figure 10. User Search

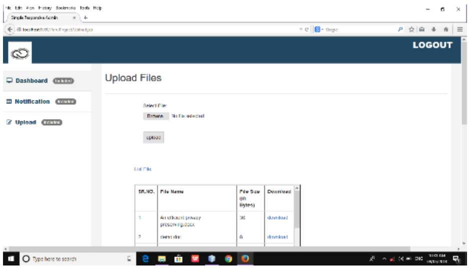


Figure 11. User Upload

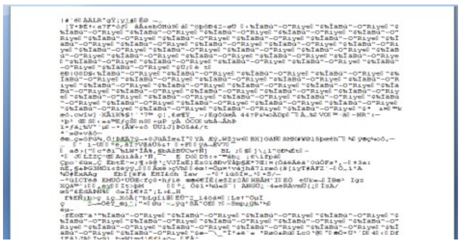


Figure 12. Encrypted File

VII. CONCLUSION

In this project, firstly we describe and solved the difficult of multi-keyword ranked search over encrypted cloud data, and create a various of privacy demands. Between many multi-keyword, we select the able similarity measure of “Equal matching”, i.e., as different matches as likely, to effectively capture the applicability of externalization documents to the query .In our future work, we will search related other multi keyword meaning over encrypted data and checking the completeness of the rank order in the search result keywords. For convention the challenges of related multi-keyword completeness without privacy breaks, we propose a basic idea of AES. Detailed observation after studying privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world data set show our future systems introduce low overhead on both computation and communication.

VIII. REFERENCES

[1]. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 4, APRIL 2016

[2]. "An Efficient and Privacy Preserving in Multi-Keyword Ranked Search over Encrypted Cloud Data,"(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (4) , 2016, 1875-1879

[3]. Madane S.A, "Comparison of Privacy Preserving Single- Keyword Search and Multi-Keyword Ranked Search Techniques over Encrypted Cloud Data", 2014 International Journal of Computer Applications (0975 - 8887) Volume 126 - No.14, September 2015.

[4]. Ning Cao et al.,"Privacy-Preserving MultiKeyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, jan 2014.

[5]. Wenhai Sun et al., "Privacy-Preserving Multikeyword Text Search in the Cloud Supporting Similarity-based Ranking", the 8th ACM Symposium on Information, Computer and Communications Security, Hangzhou, China, May 2013.

[6]. 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," in Proc. 8th ACM SIGSAC Symp. Inform., Comput. Commun. Security, Hangzhou, China, 2013, pp. 71-82.

[7]. Shih-Ting Hsu et al.,"A Study of Public Key Encryption with Keyword Search", International Journal of Network Security, Vol.15, No.2, PP.71-79, Mar. 2013.

[8]. C. Wang, N. Cao, K. Ren, and W. J. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467-1479, Aug. 2012.

[9]. Kui Renetal.,"Towards Secure And Effective Data utilization in Public Cloud" IEEE Transactions on Network, volume 26, Issue 6, November / December 2012.

[10]. N. Cao,"Privacy-preserving multi-keyword ranked search over encrypted cloud data",INFOCOM, 2011 Proceedings IEEE,IEEE, (2011).

[11]. H. Pang, J. Shen, and R. Krishnan, "Privacy-preserving similarity based text retrieval," ACM Trans. Internet Technol., vol. 10, no. 1, pp. 39, Feb. 2010.

[12]. C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst., Genova, ITALY, 2010, pp. 253-262.