ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

PRIVACY PRESERVING MULTI-KEYWORD RANKED SEARCH OVER ENCRYPTED CLOUD DATA

KARPAGAVALLI.A
LAKSHMI PRIYADARSHINI.P
Sri Vidya College of Engineering
&Technology,
Virudhunagar ,
India.
(UG Scholars)

RAMYA.P
Assistant Professor / IT
Sri Vidya College of Engineering
& Technology,
Virudhunagar,
India.

Abstract-The advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching", i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use "inner product similarity" to quantitatively formalize such principle for similarity measurement. We first propose a basic MRSE scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

Keywords-Cloud computing, security, MRSE**.**

1. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources [1]. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud, especially when the data produced by them that need to be stored and utilized is rapidly increasing. To protect data privacy and combat unsolicited accesses in cloud and beyond, sensitive data, e.g., emails, personal health records, photo albums, tax documents, financial transactions, etc., may have to be encrypted by data owners before outsourcing to commercial public cloud [2]; this, however, obsoletes the traditional data utilization service based on plaintext keyword search. The trivial solution of downloading all the data and decrypting locally is clearly impractical, due to the huge amount of bandwidth cost in cloud scale systems. Moreover, aside from eliminating the local storage management, storing data into the cloud serves no purpose unless they can be easily searched and utilized. Thus, exploring privacy-preserving and effective search service over encrypted cloud data is of paramount importance. Considering the potentially large number of on demand data users and huge amount of outsourced data documents in cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability and scalability. On the one hand, to meet the effective data retrieval need, large amount of documents demand cloud server to perform result relevance ranking, instead of returning undifferentiated result. Such ranked search system enables data users to find the most relevant information quickly, rather than burdensomely

sorting through every match in the content collection [3]. Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the "pay-as-you use" cloud paradigm. For privacy protection, such ranking operation, however, should not leak any keyword related information. On the other hand, to improve search result accuracy as well as enhance user searching experience, it is also crucial for such ranking system to support multiple keywords search, as single keyword search often yields far too coarse result. As a common practice indicated by today's web search engines (e.g., Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. And each keyword in the search request is able to help narrow down the search result further. "Coordinate matching" [4], i.e., as many matches as possible, is an efficient principle among such multi-keyword semantics to refine the result relevance, and has been widely used in the plaintext information retrieval (IR) community. However, how to apply it in the encrypted cloud data search system remains a very challenging task because of inherent security and privacy obstacles, including various strict requirements like data privacy, index privacy, keyword privacy, and many others.

2.LITERATURE SURVEY

The Privacy Preserving Keyword Searches on Remote [1]-Main objective is to get the access to user's data which is stored remotely from anywhere according to user's convenience. A user *U* wants to stock up his files in an encrypted form on a far-flung file server *S*. Afterward the user *U* wants to professionally get back some of the encrypted files contain exact keywords, keeping the keywords themselves clandestine and not to cause danger to the security of the tenuously store files.

Providing Privacy Preserving in Cloud Computing[2]-Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and needs to be considered at every phase of plan. The paper tells the Importance of protecting individual's privacy in cloud computing and provides some seclusion preserving technologies used in cloud computing services. Paper tells that it is very important to take privacy into account while designing cloud services, if these engage the collection, processing or sharing of personal data. From this paper, main theme taken is of preserving privacy of data.This paper only describes privacy of data but doesn't let indexed search as well as doesn't hide user's identity.

Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data [3]-This paper has definite and solved the problem of effectual yet safe and sound rank keyword search over Encrypted cloud data .Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency) thus making one step closer towards sensible consumption of privacy-preserving data hosting services in Cloud Computing. The idea of proposed ranking method is used in our future system in order to enhance the security of information on Cloud Service Provider.

Single Keyword Search Over Encrypted data on cloud [4]-Main idea is to formalize and solve the problem of effective single keyword search over encrypted cloud data while maintaining keyword privacy. When directly applied in large joint data outsourcing cloud environment they go through next shortcoming.

Secured Multi-keyword Ranked Search over Encrypted [5]- Main focus is on the solution of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm. To make sure safety of stored data, it is have to encrypt the data before storing the cloud. In these existing systems the algorithms used are cryptographic.

Privacy Preserving Data Sharing With Anonymous ID obligation [6] - Main objective is to assign user an anonymous ID. This technique is used iteratively to dispense these nodes ID numbers ranging from 1 to N. This assignment is anonymous in that the identities received are strange to the other members of the group. In obtainable and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and Computational requirements.

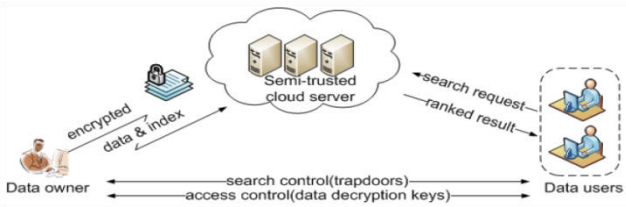
3. PURPOSED WORK

While the computation and communication cost in the query procedure is linear with the number of query keywords in other multiple-keyword search schemes our proposed schemes introduce nearly constant overhead while increasing the number of query

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

keywords. We demonstrate a thorough experimental evaluation of the proposed technique on a real-world dataset: the Enron Email Dataset. We randomly select different number of emails to build dataset. The whole experiment system is implemented by C language on a Linux Server with Intel Xeon Processor 2.93GHz. The public utility routines by Numerical Recipes are employed to compute the inverse of matrix. The performance of our technique is evaluated regarding the efficiency of two proposed MRSE schemes, as well as the trade off between search precision and privacy .As a more general search approach, predicate encryption schemes are recently proposed to support both conjunctive and disjunctive search. Conjunctive keyword search returns "all-or-nothing", which means it only returns those documents in which all the keywords specified by the search query appear; disjunctive keyword search returns undifferentiated results, which means it returns every document that contains a subset of the specific keywords, even only one keyword of interest.

3.1 Architecture



3.2 Modules

The DataUser Module include the user registration login details.The Data Owner Module helps the owner to register them details and also include login detailsThe File Upload Modul help the owner to upload his file with encryption using RSA algorithm.This ensure the files to be protected from unauthorized user.The Rank Search Module ensure the user to search the file that are searched frequently using rank search.The File Download Module allows the user to download the file using his secret key to decrypt the downloaded data.The View Uploaded and Downloaded File allows the Owner to view the uploaded files and downloaded files.

4. RESULT ANALYSIS

5. CONCLUSION

In this paper, for the first time we define and solve the problem of multi-keyword ranked search over encrypted cloud data, and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching", i.e., as many matches as possible, to effectively capture similarity between query keywords and outsourced documents, and use "inner product similarity" to quantitatively formalize such a principle for similarity measurement. For meeting the challenge of supporting multi-keyword semantic without privacy breaches,we first propose a basic MRSE scheme using secure inner product computation, and significantly improve it to achieve privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset show our proposed schemes introduce low overhead on both computation and communication. As our future work, we will explore supporting other multi-keyword semantics (e.g.,weighted query) over encrypted data, integrity check of rank

order in search result and privacy guarantees in more stronger threat model.

REFERENCES

[1] J. Ioannidis, A. Keromytis, and M.Yung /2005/ Privacy Preserving Keyword Searches on Remote.

[2] Ulrich Greveler, Benjamin Justus, Dennis Loehr/2011/ Providing Privacy Preserving in Cloud Computing.

[3] Cengiz Örencik , Erkay Savas/2012/ Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data.

[4] Mr. Mahesh Lanjewar , Swapnali Ghadge, Sneha Mane, Priti Dalvi /Apr 2012/ Single Keyword Search over Encrypted Data in Cloud Computing.

[5] C. R. Barde, Pooja Katkade, Deepali Shewale, Rohit Khatale/Feb2014/ Secured Multi-keyword Ranked Search over Encrypted Cloud Data.

[6] Shiba Sampat Kale, Prof. Shivaji R Lahane./2014/ Privacy Preserving Data Sharing With Anonymous ID Assignment.