IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 2, February 2025

A Study on Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

Mr. Aditya Sanjay Shukla
M. Tech Student, Department of Computer Engineering
Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal, Maharashtra, 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, wedefineandsolvethechallengingproblemofprivacy-preservingmulti-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, 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. With the great advent of the cloud computing the data owners are intent for outsource the complex data. As the encryption is done there is a necessary for the encrypted cloud data search service is importance. The stored data is relatively large so as, required multiple keywords in the search query and return document in the order of their relevance to these keywords searched. In this paper, the survey on searchable encryption focus on multiple keyword search*

Keywords: Privacy, Keyword Search, Multiple Keyword Search, Encryption

I. INTRODUCTION

When you store your photos online instead of on your home computer, or use webmail or a social networkingsite,youareusinga"cloudcomputing"service.Ifyouareanorganizationandyouwantto use, for example, an online in voicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a"cloud computing" service. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST):

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

The five essential characteristics are On-demand self-service, broad network access, Resource pooling, rapid elasticity, and measured service. The service models are Software as a Service (SaaS), Platform as a Service (PaaS), and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 2, February 2025

Infrastructure as a Service (IaaS). And deployment models are Private cloud, Community cloud, Public cloud, Hybrid cloud.

As the data are outsourcing to the public cloud there required data privacy, to enable this the owners may have to be encrypted the data before outsourcing to the commercial public cloud [2].In the traditional data utilization service is based on plain text keyword search and it is impractical to download all the data and decrypted locally, due to the huge bandwidth .So asto overcome these use a technique Keyword Ranking Search. 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. The search can be do neither plain text and not in the encrypted data or file, for that their use indexing for keyword and to avoid network traffic cost their use ranked search.

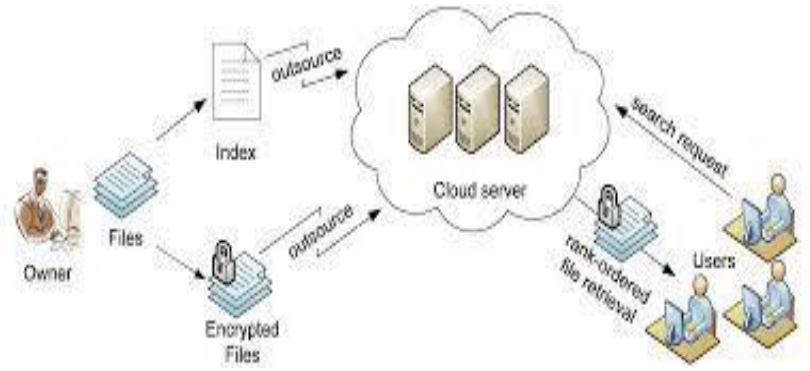

Fig. 1. Shows the Architecture of Search over Encrypted Data Using the Index Keyword.

- **Data Owner**: The data owner is responsible for generating a Message Authentication Code (MAC) and encrypting the data before outsourcing it to the cloud server. This ensures data confidentiality and integrity. The encrypted data is then transmitted securely to the server.
- **Server**: The server acts as the storage unit and query processor. It stores the encrypted data and performs Coordinate Matching to process client queries while ensuring data security. Since the data remains encrypted, the server cannot directly access the plaintext information, reducing the risk of unauthorized exposure.
- **Client**: The client initiates data retrieval by first requesting Access Control and Key authentication. This step verifies the client's identity and ensures that only authorized users can access the stored information. Upon successful authentication, the client sends a query to the server. The server processes the request using Coordinate Matching and returns the relevant encrypted data to the client for decryption.

This architecture effectively balances security and efficiency, enabling privacy-preserving search and retrieval in cloud environments. It ensures that sensitive information remains protected, even if the cloud server is compromised, by implementing robust encryption and authentication mechanisms.

II. LITERATURE SURVEY

Secured Multi-keyword Ranked Search over Encrypted Cloud Data

In cloud computing data possessors are outsourced their complex data management systems from local network site to the commercial public cloud for greater flexibility and economic savings. For the safety of stored data, the data must be encrypting before storing. It is necessary, that to invoke search with the encrypted data also. The specialty of cloud data storage should allow copious keywords in a solitary query and result the data documents in the relevance order. Main aim is to find the solution of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system wise privacy in the cloud computing paradigm. There are variety of multi keyword semantics are available, an efficient one is that measure of "coordinate matching" (as many matches as possible), to capture the data documents' relevancy to the search query is used. Specifically, "inner product similarity", i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query is used in the MRSE algorithm. The limitation of this paper was, the user's identity (ID) is not kept hidden. Due to this,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 2, February 2025

whoever outsources the data on Cloud Service Provider was known there. This maybe risky in some situations like where confidentiality of data needs to be maintained.3

Privacy Preserving Keyword Searches on Remote Encrypted Data

Consider the problem; a user U wants to store his files in an encrypted formon a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing some specific keywords, by keeping the keywords themselves secret and not to put in danger, the security of the remotely stored files. For example, a user needs to store old e-mail messages encrypted on a server managed by Google or another large vendor, and later retrieve certain messages while travelling with a mobile device. In a solution for this problem was well-defined and the security requirements are offered. The scheme is that as no public-key cryptosystem is involved. The approach is independent of the encryption method chosen for the remote files. They are incremental too. In that, user U can submit new files which are secure against previous queries but still searchable against future queries. From this, the main idea taken is that of storing the data remotely on other server and retrieving that data from anywhere via mobile, laptop etc.

Cryptographic Cloud Storage

The main benefits of using a public cloud infrastructure are clear; it introduces significant security and privacy risks. In fact, the biggest drawback is that the adoption of cloud storage (and cloud computing in general) is concern with the confidentiality and integrity of data. Overview of the benefits of a cryptographic storage service. For example, reducing the legal exposure of both customers and cloud providers, and achieving regulatory compliance is provided. Besides this, cloud services that could be built on top of a cryptographic storage service such as secure back- ups, archival, health record systems, secure data exchange and e-discovery is stated briefly.

Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data

Users who do not have prior knowledge of the encrypted cloud data, has to post process every retrieved file in order to find their matching interest; On the other hand, invariably retrieving of all the files containing the queried keyword will result in the network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, has defined and solved the problem of effective yet secure ranked keyword search over encrypted cloud data . In the ranked search enhances system usability by returning the matching files in a ranked order regarding to some certain relevance criteria (e.g., keyword frequency). This will make one step closer towards the practical deployment of privacy-preserving data hosting services in Cloud Computing.

In this paper for the first time, has defined and solved the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and thus established a set of strict privacy requirements for a secure cloud data utilization system in a reality. The ranking method helps to be efficient to return highly relevant documents corresponding to the search keyword terms.

Providing Privacy Preserving in Cloud Computing

The important issue for cloud computing was privacy, both in terms of legal compliance and user trust. This has to be considered at every phase of design. The paper tells the importance of protecting individual's privacy in cloud computing and provides some privacy preserving technologies which are used in cloud computing services. In this Paper, tells that it is very important to take privacy while designing cloud services. These involve the collection, processing or sharing of personal data. From this paper, main theme taken is of preserving privacy of data.

Enabling Efficient Fuzzy Keyword Search over Encrypted Data In Cloud Computing

In this paper, main idea is to formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy [8]. This basic idea is taken but it is for multi-keyword raked search (MRSE scheme) system. In [9], design of secure cloud storage service which addresses the reliability issue with near- optimal overall performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 2, February 2025

Achieving Secure, Scalable, and Fine-grained Data Access Controlling Cloud Computing

Achieving fine- grandness, scalability, and data confidentiality of access control simultaneously is a problem which actually still remains unresolved. The paper [10] addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. In [11], this paper there a privacy-preserving public auditing system for data storage security in Cloud Computing scheme is proposed. It utilizes the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which eliminates the burden of cloud user from the tedious and possibly expensive auditing task, it also alleviates the user's fear of his/her outsourced data leakage.

III. CONCLUSION

Their adopted different methods for preserving privacy on keyword search over the encrypted data. For the privacy preserving [2] [4] [6] [7] [8] [10] [11] describes several techniques and for privacy preserving multi-keyword search [3] [5] these describe some techniques. But in Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data takes less computational processing and more encryption is provided for the data or files. Here their uses ranking mechanisms (based on some criteria, i.e. keyword frequency) for the saving of bandwidth, in today's their uses are based on "pay- as-you-use" cloud paradigm. For the more and better encryption their use the homomorphism encryption technique and thus the computational processing is less

REFERENCES

[1] NIST Cloud Definition, Access Year January 2016, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[2] Kamara, Seny, and Kristin Lauter."Cryptographic cloud storage." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2010. 136-149.
[3] Ankatha Samuyelu Raja Vasanthi ," Secured Multi Keyword Ranked Search over Encrypted Cloud Data", 2012.
[4] Y.-C.ChangandM.Mitzenmacher,"PrivacyPreservingKeywordSearchesonRemote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.
[5] Y. Prasanna,Ramesh. "Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data", 2012.
[6] Jain Wang,Yan Zhao,Shuo Jaing, and Jaijin Le "Providing Privacy Preserving in Cloud Computing",2010.
[7] LarryA.Dunning,RayKresman,"PrivacyPreservingDataSharingwithAnonymousID Assignment",2013.
[8] J.Li,Q.Wang,C.Wang,N.Cao,K.Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE Infocom, Mar. 2010.
[9] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE Infocom, pp. 693-701, 2012.
[10] S. Yu, C. Wang, K. Ren, and W.Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE Infocom, 2010.
[11] C.Wang,Q.Wang,K.Ren,andW.Lou,"Privacy-PreservingPublicAuditingforData Storage Security in Cloud Computing," Proc. IEEE Infocom, 2010.