International Journal of Computer Sciences
July'2016 Issue
ISSN Number: 4142 3453

Enhanced privacy searching for multiple data owners in cloud computing

S. Mounika[1], Dr. A. Subramanyam[2]

[1]M.Tech.,PG Scholar, Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

[2]Professor, Dept of CSE,Dean of Engineering,Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa

ABSTRACT:

Privacy and security are the most important issues in cloud computing. To achieve high flexibility and to reduce cost, many data owners are outsourcing their data management system to public cloud. Data must be encrypted locally before outsourcing to protect data privacy. The data encryption reduces the data utilization based on simple keyword search. Observing the view of cloud computing, it has become augmenting popular for data owners to outside supplier their information to public cloud servers while allowing data users to regain this data. To relate to seclusion, safe searches over encrypted cloud data have provoke more research works under the sole owner model. However, most cloud servers in practice do not just Serve unique owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we suggest -To keep safe the secrecy and several owner model search several keywords and Ranked. To make possible cloud servers to execute safe to look omission knowing the real information of both keywords and trapdoors, To keep alive the privacy of related scores between keywords and files and rank the search result, we suggest a novel Additive Order and Privacy Preserving Function family and dynamic hidden key creation rule and a new data user to establish as genuine rule. User will encrypt their data locally. Before encrypting data, the index will be created. Trusted third party will use all these indexes to search data similar to the search query of user. Using these search results, cloud server will send encrypted document to the user. In this 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 first offer a basic idea for the multi keyword ranked search over encrypted cloud data (MRSE) based on effective comparison measure of coordinate matching, i.e. as many matches as possible, in order to capture the significance of data documents to the search query. Then we give two considerably developed multi keywords ranked search encryption schemes to reach many tough privacy requirements in two differ threat models

Index Terms- Ranked Keyword Search, several owners, privacy preserving, dynamic hidden key, Cloud Computing, Privacy Preserving, Trusted Third Party, Keyword Search, Encryption.

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort of service provides interaction. Cloud computing means a remote server that access through the internet which helps in business applications and functionality along with the usage of computer software[3]. Cloud computing saves money that users spend on annual or monthly subscription. Due to advantage of cloud services, more and more sensitive information are being centralized into the cloud servers, such as emails, personal health records, private videos and photos, company finance data, government documents, etc.

So to provide end-to-end data confidentiality assurance in the cloud, confidential data has to be encrypted before outsourcing to protect data privacy.

Now-a-days thousands of information is common everyday online. Daily new and additional information is outsourced due to growth in storage plus requirements of users, then essentially semi-trusted servers. 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. To safeguard
information privacy in the cloud, the data owner has to be outsourced in the encoded system to the public cloud and the data operation is founded on plaintext keyword search. We select the efficient measure of "coordinate matching". Coordinate matching is used to measure the parallel amount. Coordinate matching captures the significance of data documents to the search query keywords. The search facility and privacy protective over encrypted cloud data are 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 undistinguishable outcomes. Ranking scheme cares multiple keyword search to recover the search correctness. 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.

The main contributions of this paper are listed as follows:
• We define search data on clued that data is hidden format and also providing the privacy when search the multiple
keywords.
• We suggest an capable data user authentication rule, which stop attackers to disclose hidden key and only genuine
data user can do search.
• We suggest a approach that performs multiple key word search and rank them properly.
• We suggest an Additive Order and Privacy Preserving Function family (AOPPF) which allows the cloud server
produces the file that rank properly.
• We supervise experiments on real-world Datasets to verify the effectiveness and capability
our suggest schemes

II. RELATED WORK

Single keyword searchable encryption schemes [3]–[11], [18] usually build an encrypted searchable index such that its content is hidden to the server unless it is given appropriate trapdoors generated via secret key(s) [2]. It is first studied by Song et al. [3] in the symmetric key setting, and improvements and advanced security definitions are given in Goh [4], Chang et al. [5] and Curtmola et al. [6].Our early work [18] solves secure ranked keyword search which utilizes keyword frequency to rank results instead of returning undifferentiated results. However, it only supports single keyword search.To enrich search functionalities, conjunctive keyword search [12]–[15] over encrypted data have been proposed.These schemes incur large overhead caused by their fundamental primitives, such as computation cost by bilinear map, e.g. [13], or communication cost by secret sharing,e.g. [12]. As a more general search approach, predicate encryption schemes are recently proposed to support both conjunctive and disjunctive search. Boolean keyword searchable encryption schemes support multiple keywords ranked search over encrypted cloud data while preserving privacy as we propose to explore in this paper.

A. Privacy Preserving multi-keyword ranked search over encrypted cloud data:

Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper[1], for the first time, they define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). To improve the search result and privacy, they introduce different MRSE schemes.

B. Verifiable Privacy-Preserving Multi-Keyword Text

Search in the Cloud Supporting Similarity-Based Ranking: In this paper[2], they have proposed tree-based index structure methods for multi-dimensional algorithm to improve the search efficiency. They have proposed two new secure index schemes to meet the stringent privacy requirements under strong threat models.

C. Secured Multi-keyword Ranked Search over Encrypted Cloud Data: In this paper [3], 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. A variety of multi- keyword semantics are available, an efficient similarity 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 MRSE algorithm.

D. Privacy Preserving Keyword Searches on

Remote Encrypted Data : Consider the problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing specific keywords, keeping the keywords themselves secret and not to endanger the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In [4], solutions for this problem under well-defined security requirements are offered. The schemes are efficient as no public-key cryptosystem is involved. Indeed, 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 theme taken is of storing data remotely on other server and retrieving that data from anywhere via mobile, laptop etc.

E. Cryptographic Cloud Storage: When the benefits of using a public cloud infrastructure are clear, it introduces significant security and privacy risks. In fact, it seems that the biggest obstacle to the adoption of cloud storage (and cloud computing in general) is concern over the confidentiality and integrity of data. In [5], an 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.

F. Providing Privacy Preserving in Cloud Computing: 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 design. The [6] paper tells the importance of protecting individual's privacy in cloud computing and provides some privacy 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 involve 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 allow indexed search as well as doesn't hide user's identity. Thus, these two drawbacks are overcome in our proposed system.

G. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data: On one hand, users who do not necessarily have prior knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. This paper has defined and solved the problem of effective yet secure ranked keyword search over encrypted cloud data[7]. 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 practical deployment of privacy-preserving data hosting services in Cloud Computing. For the first time, the paper has defined and solved 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. The proposed ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms. The idea of proposed ranking method is used in our proposed system in order to enhance the security of data on Cloud Service Provider.

H. Privacy-Preserving Public Auditing for Secure Cloud Storage: Cloud storage is widely used now days by user to outsource their data.[8]The large size of outsource data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. In this paper, third part auditing (TPA) is introduced. we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind.

We have again visit the issue of easy to search symmetric encryption, which give permeation a client to store its data on a external server in such a way that it can search without disclosing the data . We generate more affords to add new security and new work. Motivated by subtle problems in all previous security definition for SSE, we propose new definitions and point out that the existing notions have significant practical disadvantages contrary to the natural use of easy to find encryption.[1]

Disadvantages:

They only give the assurance to security for users that fulfil all their searches at once. We notice this limitation by introducing stronger definition that guarantee security even when users perform more realistic searches. Analysis give guidance to the choice the size of cipher text space . At the end suggest a unique and efficient transformation that can be applied to any OPE scheme. Our deep study shows that the transformation yields a scheme with more result safety in that the scheme oppose the one-wayness and window one-wayness attacks[2]. We

opened the new way on how to get this notion, but the more efficient variant is certainly required. Second, how to construct SCF-PEKS scheme secure against keyword guessing attacks without requiring bilinear pairing operations would be very interesting[3].

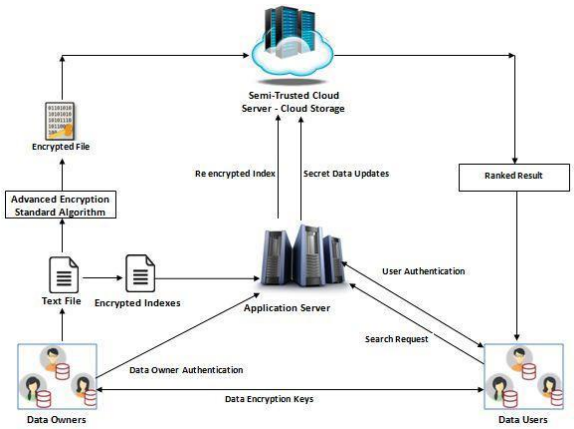

Fig1: System Architecture

III.PROPOSED SYSTEM

Consider the Cloud data hosting service contains four different entities, as listed in fig. 1: the data owner, the data user, the trusted third party, and the cloud server. Consider data owner will registers on cloud for cloud computing service. Anonymous algorithm is used to process the registration information of user and then saves anonymous data to registration database. The data owner has a collection of data documents D to be outsourced to the cloud server in the encrypted form E. Before outsourcing, the data owner will first build an encrypted searchable index I from D to enable searching capability over E for effective data utilization. The data owner will outsource the encrypted document collection D to the cloud server and encrypted index to the trusted third party. The trusted third party will check the integrity of outsourced data without violating user privacy policies. Anonymous identifiers are assigned to user using efficient algorithms. The data user send the encrypted search query to the cloud server along with his session ID. This encrypted search query is transferred to the trusted third party for processing by cloud server. The trusted third party will search index using "string matching" and sends the search results to the cloud server which returns the corresponding set of encrypted documents to the data user.

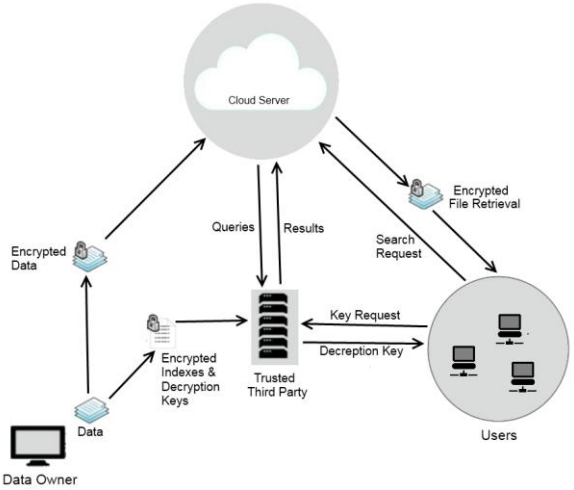

Fig.2 Architecture of search over encrypted data cloud

To enable ranked search for effective utilization of outsourced cloud data under the aforementioned model, our system design should simultaneously achieve security and performance guarantees as follows. Multi-keyword ranked search. To design search schemes which allow multi-keyword query and provide result similarity ranking for effective data retrieval, instead of returning undifferentiated results. Privacy-preserving. To prevent the cloud server from learning additional information from the data set and the index, and to meet privacy requirements. Efficiency. Above goals on functionality and privacy should be achieved with low communication and computation overhead. To improve the document retrieval accuracy, the search result should be ranked by the cloud server according to some ranking criteria. Finally, the access control mechanism is employed to manage decryption capabilities given to users and the data collection can be updated in terms of inserting new documents, updating existing documents, and deleting existing documents.

IV. Privacy Requirements for MRSE

In the related literature, such as searchable encryption is that the server should study nothing but search results. With this general privacy picture, we discover and create a set of strict privacy necessities specially for the MRSE framework. Data privacy, the data owner can resort to the traditional symmetric key cryptography to encrypt the data before outsourcing, and effectively prevent the cloud server into the outsourced data. Index privacy, if the cloud server infers any association between keywords and encrypted documents from index. Therefore, the searchable index should be built to prevent the cloud server from acting such kind of association attack.

Keyword Privacy, as users generally wish to have their search from existence showing to others like the cloud server, the most vital concern is to hide what they are searching, i.e., the keywords specified by the corresponding trapdoor. The trapdoor can be generated in a cryptographic way to protect the query keywords.
Trapdoor, the trapdoor generation function should be a randomized one instead of being deterministic. The cloud server should not be able to deduce the connection of any given trapdoors, i.e, to determine whether the two trapdoors are formed by the same search request. Otherwise, the deterministic trapdoor generation would give the cloud server benefit to collect frequencies of dissimilar search requests concerning different keyword(s), which may further disturb the aforesaid keyword privacy requirement. . Access Pattern, within the ranked search, the access pattern is the sequence of search results where every search result is a set of documents with rank order.

Our proposed system consists of the following modules:

- Data User Module
- Data Owner Module
- File Upload Module with Encryption
- FileDownload Module with Decryption
- Rank Search Module

Data User Module

Data users are users on this system, who will be able to download files from the cloud that are uploaded by the data owners. Since the files stored on the cloud server could be in huge numbers, there is a search facility provided to the user. The user should be able to do a multi-keyword search on the cloud server. Once, the result appears for the specific search, these users should be able to send a request to the respective data owners of the file through the system (also called trap-door request) for downloading these files. The data users will also be provided a request approval screen, where it will notify if the data owner has accepted or rejected the request. If the request has been approved, the users should be able to download the decrypted file.

Data Owner Module

In this module, the data owners should be able to upload the files. The files are encrypted before the files are uploaded to the cloud. The data owners are provided an option to enter the keywords for the file that are uploaded to the server. These keywords are used for the indexing purpose which helps the search return values very quickly. These files when once available on the cloud, the data users should be able search using the keywords. The data owners will also be provided with a request approval screen so they are able to approve or reject the request that are received by the data users.

File Upload & Encryption Module

In this module, the data owners should be able to upload the files. The files are encrypted before the files are uploaded to the cloud. The data owners are provided an option to enter the keywords for the file that are uploaded to the server. These keywords are used for the indexing purpose which helps the search return values very quickly. These files when once available on the cloud, the data users should be able to search using keywords. The data owners will also be provided with a request approval screen so that they are able to approve or reject the request that are received by the data users. The file before upload will have to be encrypted with a key so that the data users cannot just download it without this key. This key will be requested by the data users through the trap-door. The encryption of these files uses RSA algorithm so that unauthorized users will not be able to download these files.

File Download & Decryption Module Data users are users on this system, who will be able to download files from the cloud that are uploaded by the data owners. Since the files stored on the cloud server could be in huge numbers, there is a search facility provided to the user. The user should be able to do a multi-keyword search on the cloud server. Once, the result appears for the specific search, the users should be able to send a request to the respective data owners of the file through the system (also called trap-door request) for downloading these files. The data users will also be provided a request approval screen, where it will notify if the data owner has accepted or rejected the request. If the request has been approved, the users should be able to download the decrypted file. The file before download will have to be decrypted with a key. This key will be requested by the data users through the trap-door request. Once the key is provided during the download, the data users will be able to download the file and use them.
Rank-Search Module This module allows the data users to search the files with multi-keyword rank searching. This model uses the frequently used rank searching algorithm for present the output for multi-keywords. "Coordinate Matching" principle will be adopted for the multi-keyword searching. This module also takes care of creating an index for faster search.

V.RESULTS

Multiple users are created at a centralized location for the data owners and data users. We can see that either of the users can access the system once they login. The exchange of communication between data owners

and data users is strictly through E-mail system which enables the system to be secured. Since the contents are encrypted and kept in the cloud, public viewing of these files is impossible. The files or contents can be viewed only after the consent of the data owners, after getting the secret key.

VI.CONCLUSION AND FUTURE

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol The previous work mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search was provided over encrypted cloud data using efficient similarity measure of co-ordinate matching. The previous work also proposed a basic idea of MRSE using secure inner product computation for multi-keyword ranked search. There was a need to provide more real privacy which this paper presents. In this paper, the method is proposed to perform the multi-keyword ranked search over cloud data. the proposed system will perform secure search over encrypted data in cloud computing.

.

REFERENCES

[1] Ning Caoy, Cong Wangz, Ming Liy, Kui Renz, and Wenjing Louy "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data ", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, IEEE 2014

[2] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Hou, Y.T., Hui Li,"Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking ", IEEE Transactions on Parallel and Distributed Systems, IEEE 2014.

[3] Ankatha Samuyelu Raja Vasanthi ," Secured Multi keyword Ranked Search over Encrypted Cloud Data", 2012.

[4] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[5] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan. 2010.

[6] Jain Wang, Yan Zhao , Shuo Jaing, and Jaijin Le, "Providing Privacy Preserving in Cloud Computing",2010.

[7] Y. Prasanna, Ramesh . "Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data", 2012.

[8] Cong Wang, Chow, S.S.M., Qian Wang, Kui Ren , Wenjing Lou," Privacy-Preserving Public Auditing for Secure Cloud Storage ", IEEE Transactions on Computers, IEEE 2013.

[9] M. Abdalla, M. Bellare, D. Catalano, E. 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.

[10] 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.

[11] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. S. III, "Public key encryption that allows pir queries," in Proc. of CRYPTO, 2007.

[12] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. of ACNS, 2004, pp. 31–45.

[13] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. of ICICS, 2005.

[14] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. of TCC, 2007, pp. 535–554.

[15] R. Brinkman, "Searching in encrypted data," in University of Twente, PhD thesis, 2007.

[16] Y. Hwang and P. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Pairing, 2007.

[17] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. Of EUROCRYPT, 2008.

[18] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.