Advanced Research in Electrical and Electronic Engineering
p-ISSN: 2349-5804; e-ISSN: 2349-5812 Volume 5, Issue 1 January-March, 2018, pp. 78-81
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Different Techniques for Ciphertext Retrieval over Encrypted Data

Muhammad Asif Khan[1] and Dr. RuWei Huang[2]

[1,2]School of Computer, Electronics and Information, GuangXi University, Nanning, China
E-mail: [1]1036400476@qq.com, [2]ruweih@126.com

Abstract—*In recent years, Cloud computing provides strong grip and flexible access on outsource data, cloud storage, data privacy is major concern from to outsource their data, authenticated users are allowed to access this storage to prevent important and sensitive data. For data protection and utilization we encrypt our sensitive data before outsourced our data because cannot trust storage server, are un-trusty but on other hand, data retrieval in encrypted format from cloud, is challenging task for data utilization, was encrypted from plaintext to ciphertext, when retrieves from cloud storage. However, searchable encryption schemes used Boolean search but they are unable to make data utilization for huge data and failed to handle multi-users access to retrieve ciphertext from cloud and users authentication. In this paper, we are using ranked keyword search over encrypted data by going k-documents at storage and using a Hierarchical Clustering Method is designed to guide more search semantics with an additional feature of making the system to cope the demand for fast ciphertext k-search in large scale environments explored the relevance score such as massive and big cloud data. This threshold divides the resulting clusters into sub-clusters until the necessity on the maximum size of cluster is reached. To make fetching search to be secure and privacy-preserving, it is built an index for searching on cloud data and retrieve the most relevant files from cloud. To defending privacy breaches from unauthorized users, users will go through authentication process and data retrieval time as well.*

1. INTRODUCTION

Cloud computing works as a portable device on cloud, we can access outsource data from cloud anywhere in the end users. Users can be dishonest and cloud data can be damaged or misuse by unauthorized user when it is allowed an access by unauthorized user. It could be possible that there are malicious cloud servers which do not protect user's sensitive data truly. We use a technique to encrypt our data before outsource and it will be in un-recognizable format which is secure by malicious server. This ciphertext cannot be read or edit without authentication which is only allowed to data owner. Cloud server and data owner are not involved in this encrypted process; they are also in untrusted domain. However, there is a drawback of this encrypted technique to download all data from cloud and decrypt in plain text. This is inefficient way to download all data .we do not want all data from cloud when we need to retrieve required ciphertext from cloud. This is the challenging problem how to retrieve accurate ciphertext.

Searching Encryption Schemes (SE) were proposed in series [1, 2] to retrieve ciphertext from cloud, keyword data retrieval is the most popular and widely used in plaintext retrieval. These schemes used keyword to find the relevant files but there is lots of unwanted files are retrieved which matched with the user search query. This was not the proper results of given schemes, it needed to search in ranked search which are related to users interest. To overcome previous schemes drawback, it was presented schemes [3, 4, 5] that supported top-k multi keyword data retrieval. These schemes were able to retrieve top-k files which are related to user's search but still insufficient to bring in practical. Ranked keyword search scheme was contracted [6] they proposed Multi-keyword top-*k* Similarity search over encrypted data. Their scheme was to improve the efficiency purpose where group of tree-based indexes are constructed and same query will work to go different visiting path on the indexes for all documents and capable to defending the privacy breaches.

Our proposed search is based on Ranked keywords search which based on double keyword ranking search and Hierarchical Clustering method to get accessed on huge data, using secret key to make sure data is going to authentic user hands.

2. SYSTEM ARCHITECTURE

Cloud computing has three main entities which are involved to retrieve ciphertext from cloud. These three entities have important role with each other because when we search outsource data, they interact and respond to each other according their query requirement, their interaction is based authentication if authentication and verification fail this whole system could not be in connection anymore. Our Framework three entities are data owner, cloud server and data users.

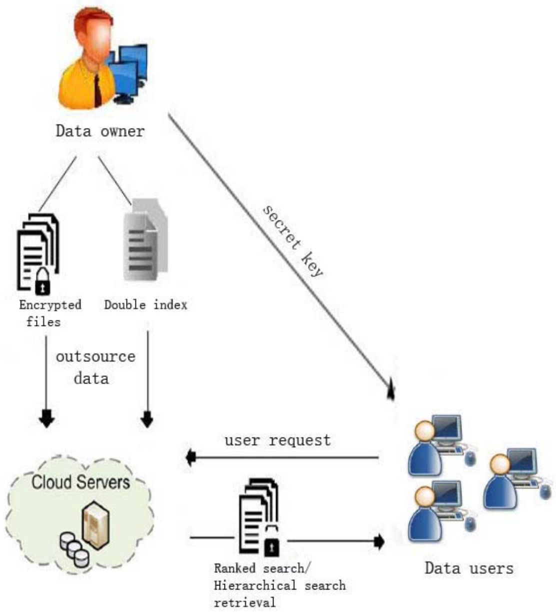

Figure 1: System Architecture

3. DATA OWNER

Data owner has n data files and these files are wanted to outsource on the cloud server, these files will not be outsourced directly on the cloud server, files are built in searchable index files and which is based on the main exact word w in the file for searching from collection of data. Data files collection are gotten file's index and applying AES (Advanced Encryption Techniques) to encrypt the desired data to the cloud server. These files are outsourced [7, 8, 9] which help to data utilization on cloud, encrypted files are searched by users and helps to keep the precision in the results and files utilization. Data owner has right to confirm the data users resquest of data retrieval then they will get the final secret key to download the ciphertext files to plaintext files.

4. CLOUD SERVER

In our proposed system cloud server do not work as

Malicious or un-trusted way because we are using our cloud as completely authorized and it does not allow malicious attack or dishonest process because if some wants to access the data from cloud ,users need to verify their selves and pass the authentication process then they will be allowed to access the outsource data. Our scheme makes a secure and honest server.

5. DATA USER

Data users could be malicious or dishonest that's why they need to pass the authorization process to get in the proposed system. User searches the given keyword kw from collection of the files by passing authorization process and get a secret form by using backdoor bw way to cloud server. When server gets the request by backdoor bw and cloud server will search the index i of the files which is in the form of double index form and retrieve the file from the data collection on cloud and send back to the user. These results are based on hierarchical index search and ranked keyword search which have the most relevant files results in sequence which are on top k-retrieval documents. Proposed model offers authorize users to get secret key via their Email address as they registered their selves by authentication process.

6. LITERATURE REVIEW

There are different techniques, were proposed to search ciphertext from the cloud which is already in encrypted format for security concern but there are some drawback in previous given schemes. There are some common ways of protecting user's data which are AES encryption to outsource data on cloud, index in ranked search, Hierarchical index search, and user authentication process to fetch the data and owner authentication.

7. TECHNIQUES FOR SEARCHES ON ENCRYPTED DATA

Sequential Scan method is proposed by song et al [1] SWP gave an idea of searchable encryption to solve the problem but it did not guarantee and security of data but this scheme was eligible to search on encrypted data. It was based on scanning ciphertext, according to this scheme, we can make partition of one file into multiple words and scanning the whole file by searching the single keyword but it has low efficiency because our file size increase the searching time will be increased according to the file size. Actually, they started with basic techniques and encryption algorithm works on data secrecy little bit as an initial step. They showed those hidden searches, control searches and how to extend this technique. This scheme has different steps like how to encrypt, searching technique and decryption of cloud data. First of this technique is pre encryption, they hided all keyword search on cloud and keep unauthorized party away from it. Server is considered as un-trusty in cloud computing, it can be malicious server so it does not know anything when user send some data to the cloud. Second step of this technique is to searching on cloud. The data is searched by the user and searching algorithm will return the results of keyword search from data cloud that which files are matching with user's entry. The user will get fetched file by searching and decrypt the file in plain text in third step. Because on the cloud, always files are outsource after encryption process as we mentioned in first step of technique

8. SECURE SEARCHABLE INDEXES

Goh[10] continued the research on song et al [1]. Secure search scheme was constructed secure index for documents on cloud ,it worked as searching on cloud according to given keyword by users and retrieve the files without decryption.

This proposed scheme was based on index and it developed an index using Bloom filters, keywords are assigned to each file in code word and stored in the index. For searching ciphertext file, whether this file exist in ciphertext according to keyword. Boneh et al [11] proposed a searchable encryption scheme based on Asymmetric Cryptography, according to this scheme, public key will used to encrypting and unloading the data on the cloud server but for searching data private key will be used for authorized users on the cloud. Here we can get the idea of authorized users can access our system by using index search.

9. RANKED KEYWORD SEARCH

C.Wang and W.Lou [12] worked on efficient ranked keyword searching on encrypted data and constructed a scheme which supports the problem of effectively utilization and stored the encrypted data on cloud server. It works on based of indexes allocated while data are outsourced and stored on the cloud. It works as simple and effectively to retrieve data from the cloud by searching keyword and user will get all the documents results which relate to the given query. Multi keyword search by using keyword search on encrypted data easily. Ranked based data retrieval of the data documents is possible when data is encrypted before outsource data and this is the advantage of this scheme. Files are searched at k-documents and retrieve the files which relates to the query.

10. HIERARCHICAL INDEX SEARCH

P. Gupta et al [13] proposed a hierarchical clustering technique for retrieving data from cloud, they used inverted file (IF) index to divide the documents into the ordered clustered and similar cluster is divided into mega clusters. The system will select first cluster which is more similar to the given keyword from user side, this search will go to the bottom of this cluster and move to next one. H. Li[14] constructed hierarchical model for cloud computing and basic purpose of this scheme was to identify the identity-base authentication of the users to get in the system on the cloud computing and non-authorized users will be kept away from the system for security reasons.

11. CONCEPT SEARCH TECHNIQUES

There are method that can read the user's searching interest and what kind of contents is being searched on it. The schemes were constructed by Gauch et al [15, 16] to keep the record of user's search documents. Same like cookies work on web pages to save the user record and next time when we user just on alphabet of keyword which entered before in our search, it automatically pick up the keyword so it help us to make our system more and more simple for retrieving data from the cloud and it will not consume more time to go in searching and retrieve the results. Liu et al [17] proposed a scheme earlier then Gauch which includes user profile method based on users, searching history and Open Directory Project (ODP). One profile is used for user to keep the record of different users categories and it store all the users search record when user search to retrieval data. If another user tries to search on same category then the system will select the path of user's search. We can make searching more simple and convenient, if user enter two or more keyword (which already searched or retrieved) and they are making one sentence, these two words' path will be followed first to start searching on cloud.

12. ORDER PRESERVING SYMMETRIC ENCRYPTION

During the encrypted process when we outsource data to the cloud, we need to keep data in sequence and it will help while retrieving data from cloud in numerical sequence and this paper has Order Preserving Systematic Encryption. It allows efferent range queries on encrypted data as well as indexing Agrawal et al [18].

13. OUR ACHIEVEMENTS

In this paper data owner encrypt the data and allocate the indexes to the documents which are used to search the file by Ranked keyword search and Hierarchical index search including data owner has access to delete or modify the files. Authorized users can send the request for the desired file and search by searching algorithm and data owner will approve the downloading request and user will get the secret key to download the file at the end. Order preserving technique is being used to maintain the order of encrypted file on cloud when data owner outsource the data. User will get the secret key by Email address when data owner approve the downloading request of documents then user can download the file by whole authentication way.

14. CONCLUSION

Our proposed searchable encryption scheme can be used efficiently to fulfill Hierarchical index search and Ranked keyword search on outsource data and fully secured. Ranked keyword search and Hierarchical index search use search encryption technique and allocation of double index to the documents before outsource on cloud which help to make searching speed faster(due to concept search technique) and get more accurate searching results as relevant files. Gmail account is used for make clearance of legal user, user proves himself as authorized user, get secret key on Email ID, and it is helpful in improving security.

REFERENCES

[1] D.X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," *2000 IEEE Symposium on Security and Privacy, Berkeley*, California, USA, May 14-17, 2000, pp.44–55, 2000.

[2] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," *Advances in Cryptology – EUROCRYPT 2004, International Conference on*

the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, pp.506–522, 2004.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” I*NFOCOM 2011. 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, 10-15 April 2011, Shanghai, China, pp.829–837, 2011.

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” 2010 *International Conference on Distributed Computing Systems, ICDCS* 2010, Genova, Italy, June 21-25, 2010, pp.253–262, 2010.

[5] R. Huang, X. Gui, S.Yu and W. Zhuang "Research on Privacy-Preserving Cloud Storage Framework Supporting Ciphertext Retrieval" *International Conference on Network Computing and information Security* 2011.

[6] N. Xiaofeng Ding, Peng Liu and Hai Jin “Privacy-Preserving Multi- keyword Top-k Similarity Search over Encrypted Data” in *Transactions on Dependable and Secure Computing, IEEE,* 2016.

[7] D.-G. Feng, M. Zhang, Y. Zhang, and Z. Xu, “Study on cloud computing security,” *Journal of software*, vol. 22, no. 1, pp. 71–83, 2011.

[8] H. Takabi, J. B. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, 2010.

[9] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[10] E.-J. Goh, “Secure indexes”, *Cryptology ePrint Archive, Report 2003/216.*

[11] D. Boneh, D. Di Grecenzo, R. Ostrovsky and G Persiano, “public key encryption with keyword search” in *Advance in Crytology- Eurocrypt* 2004,pp.506-522, Springer Berlin Heidelberg, 2004.

[12] C. Wang, N. Cao, J. Li, K. Ren and W. Lou" Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data" *IEEE Transaction On Parallel and Distributed System,* VOL. 23, NO. 8 Aug, 2012.

[13] P. Gupta and A. K. Sharma,"a framework for hierarchical clustering based indexing in search engines"*IEEE 1st International Conference on Parallel, Distributed and Grid Computing* 2010.

[14] H. Li, Y. Dai, L. Tian, and H. Yang, ``Identity-based authentication for cloud computing," in *Cloud Computing*. Berlin, Germany: Springer-Verlag, 2009, pp. 157166.

[15] S. Gauch, J. Chaffee, and A. Pretschner, “*Ontology-based personalized search and browsing,*” *ACM WIAS, vol. 1, no. 3-4, pp. 219–234, 2003.*

[16] M. Speretta and S. Gauch, “Personalized search based on user search histories,” *in Proc. of IEEE/WIC/ACM International Conference on Web Intelligence, 2005.*

[17] F. Liu, C. Yu, and W. Meng, “Personalized web search by mapping user queries to categories,” in *Proc. of the International Conference on Information and Knowledge Management (CIKM)*, 2002.

[18] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu.” Order Preserving Encryption for Numeric Data”, In ACM SIGMOD *international conference on Management of data*, pages 563 574, 2004.