Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 12, pp.24719-24721, December, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

A SURVEY OF EFFICIENT SEARCHING SCHEMES FOR ENCRYPTED DATA OVER CLOUD

***Vrushali R. Charde and Nitin S. More**

Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune, India

ARTICLE INFO

Article History:
Received 14th September, 2015
Received in revised form
20th October, 2015
Accepted 15th November, 2015
Published online 30th December, 2015

Key words:

Cloud computing,
Trapdoor,
Searchable encryption,
Privacy-preserving,
Ranked search.

ABSTRACT

Cloud computing is an important platform for the data owners to store their data from local sites to commercial public cloud providing high flexibility and economic savings. But the cloud storage systems are most vulnerable for the data security due to their internal data sharing among the servers. By applying strong cryptography techniques, data is stored in the cloud. But eventually this doesn't solve the problem of storing process as cloud provides big storage capacity, so performing the search on this huge encrypted data in the cloud is posing a real challenge. To solve this problem, many ideas are proposed to perform the search over the encrypted data, but no system is providing complete accuracy as this mainly depend on the document content. Here, some novel approaches are discussed and also an idea of constructing a special tree-based index structure is constructed that proposes a "Greedy Depth-first Search" algorithm that provides efficient multi-keyword ranked search.

Citation: Vrushali R. Charde and Nitin S. More, 2015. "A Survey of Efficient Searching Schemes for Encrypted Data over Cloud", *International Journal of Current Research,* 7, (12), 24719-24721.

INTRODUCTION

The number of internet users across the globe is increasing exponentially. So that the data by the users need to be store at huge storage spaces, and the cloud is the best solution for this. Due to the complex computational structure of cloud and its data handling techniques, it is unable to provide the security for all the stored data in the cloud. As Cloud Computing becomes prevalent as more sensitive information is being centralized over the cloud, such as emails, health records, government documents, etc. are being stored in the cloud. By storing their data into the cloud, the data owners gets relief from the stress of data storing and its maintenance so as to enjoy the on-demand high-quality data storage service. As data owners and cloud server are not in the same trusted domain and may put the outsourced data at risk, because cloud server can no longer be trusted. Therefore, the sensitive data usually should be encrypted before outsourcing for the privacy of data. So the cloud service providers manage for applying the cryptography algorithms to encrypt the data before storage process. And they provide original data to the users by using decryption the same on their request. The solution doesn't end here only as cloud system allocates a huge storage space for the users, so users are free to take advantage of this and store an enormous number of documents.

****Corresponding author: Vrushali, R. Charde***
Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune, India

Again this creates the problem of searching the document in the cloud as all are present in the encrypted state. The common solution to this is after getting the user keyword for searching; every document needs to decrypt first and then the keywords need to match in every word of the document to retrieve the desired one. But this process takes much more time to search for the documents. So a need for proper and fast searching technique arises that can examine the documents in the cloud without decryption the data to save the cost of cloud service provider and time of the end users. However, data encryption makes data utilization a very challenging task as there are a lot of outsourced data files. Also, in Cloud, the data owners share their data with a large number of users. The individual users are interested in retrieving only specific data files they are interested in. So, one of the most common technique is to extract the files selectively through keyword-based search in spite of retrieving all the encrypted data. Such keyword-based search technique allows the users to extract the data of their interest selectively, and this method has been widely applied in plain-text search scenarios, such as Google search. To search for the encrypted data, many searchable encryption techniques have been developed in recent years. The searchable encryption schemes build up an index for each keyword of interest and relate the index with the files that contain a keyword. Creating the trapdoors of keywords within the index information allows efficient keyword search where both file content and keyword privacy are well-secured. Although allowing to performing searches securely and effectively, the

existing searchable encryption techniques do not suit for cloud computing scenario as they support only exact keyword search. That is, there is no interruption of minor typos and format inconsistencies. It is quite common that users searching input might not be an exact match of those pre-defined keywords due to the possible typos, like PO BOX and P.O. Box and user's lack of exact knowledge about the data.

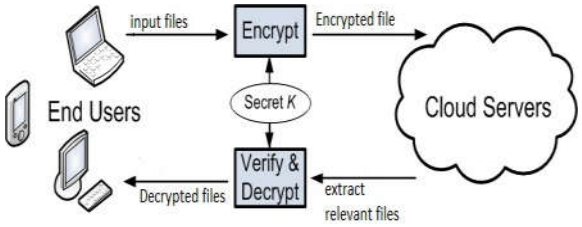

Fig. 1. Basic architecture of encryption and decryption of files over the cloud

Above figure 1 illustrates the basic architecture of the encryption and decryption technique that shows that the end users uploads its file in the cloud which was stored in cloud server in encrypted format. And after applying the different searching techniques on encrypted files, the user after its authentication gets the files that are matching to the keyword the is searching for, and then the user decrypts the required file. The secret key K is the private key or the public key that is used for the authentication process and is only known to the data owner and the authenticated user. For further proceeding of this paper, Section II is dedicated to related works, Section III for result and comparison and Section IV for the conclusion and future work.

Related Work

Cloud computing offers great data utilization of encrypted data but searching over encrypted data is a very challenging task as there are vast numbers of outsourced files are presents.

However, data owners might want the selected files related to query they entered. So keyword searching over encrypted data emerged as a good technique to find the required data from the cloud. (CengizOrencik and ErkaySavas, 2012) aimed to achieve an efficient system based on Private Information Retrieval (PIR) where any authorized user can perform their search on a remote database having multiple keywords that he is retrieving. The proposal facilitates that a user can query the database provided that they possess trapdoor for the searched terms that authorize the users to include them in their queries. Moreover, this system is capable of performing searching for multiple keywords in a single query and gives the results so that he user can retrieve only the top matches.

On contrast to this Cong Wang *et al*., 2012 stated that search operations on encrypted data will increase the cost of processing and will also increase the network traffic. Cong Wang proposed a new theory that reduces the processing overhead that generally obstacles the search system. The author uses build index along and the keyword frequency based relevance score. It implements a secure ranked based keyword search method. In this method, order-preserving mapping scheme is used where small encrypted files are processed first, and then large encrypted files are processed. Authors present a theory for retrieving documents that make use of Ranked Searchable Symmetric Encryption, Order Preserving Symmetric Encryption, and One Many Order Preserving Mapping. This method is used to achieve high accuracy and security. Also, it avoids unwanted retrieval and traffic problem. But system fails if multiple keywords are fed as input, with such input searching speed also increases.

Table 1. Review summary

Sr. No	Tittle	Mechanism	Advantage	Disadvantage
1	Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data[10]	Greedy Depth-first Search Algorithm	Supports accurate multi-keyword ranked search. Supports dynamic insertion & deletion of documents. Provides Security using the kNNalgorithm.	Symmetric measures are used. Data owner is responsible for updating information & sending them to the cloud server.
2	Efficient and Secure Ranked Multi-keyword Search on Encrypted Cloud Data [1].	It gives privacy-preserving ranked keyword search scheme based on PIR that allows multi-keyword queries with ranking capability.	Provides blinded encryption techniques for accessing the contents of the retrieved documents.	Computation & Communication costs of this method are little high as every searched word in a fired query requires many homomorphic encryption operations both on the server and the client side.
3	Enabling Efficient Multi-keyword Ranked Search Over Encrypted Mobile Cloud Through Blind Storage [4].	It utilizes the relevance score and k-nearest neighbor techniques to obtain an efficient multi-keyword search method that can return the ranked search results depending on accuracy.	Provides confidentiality of documents & index, trapdoor privacy, better efficiency regarding functionality	It requires the computation of relevance scores for all documents contained in the database. It causes huge computation overload to the cloud server and is therefore not suitable for large-scale data sets
4	Fuzzy keyword search over encrypted data in cloud computing.[5]	The main idea is to formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy.	Enhances system usability by returning matching files. Effective utilization of stored encrypted data in fuzzy search is obtained.	Sorting of the searched results according to the relevance criteria is not obtained.
5	TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud [6].	It proposes traffic and energy saving encrypted search (TEES), bandwidth and energy efficient encrypted search architecture over the mobile cloud.	It reduces the energy consumption by 35~55 % by offloading computation of relevance scores to the cloud server.	Implementation of TEES has security enhancement. But essential security defects of this encryption approach cannot be completely resolved.

The above methods are based on exact query matching, but it did not implement the similarity matching. Dan Boneh *et al*., Presents an attribute based encryption approach with prediction encryption scheme. Other schemes easily overcome the drawbacks of technique. Since it makes use of two

different schemes, it is highly secure and faster. Since on cloud, the data is located at remote locations. Hence, it is a challenging task to access and retrieve data from such remotely located information. Here Smith generates a one key for the email gateway and by using this key email gateway get access to check "urgent" keyword in email without reading the complete email. By doing so, the desirable work of both parties can be done, and the privacy of the system also will not get compromised. Here identity-based encryption is used for the purpose of the encryption. The disadvantages of the above systems are 1.refreshing keywords, 2.secure channel removal, 3.multiple keyword processing. Paper (Hongwei *et al.,* 2015) explains searchable encryption for multi-keyword ranked search on stored data. To develop an efficient multi-keyword search scheme k-nearest technique is used which returns the ranked searched results based on the accuracy. In paper (Li *et al.,* 2010), the main idea is to form and solve the problem of fuzzy keyword searching over the encrypted cloud data while maintaining keyword privacy. This basic idea is taken, but it is for multi-keyword ranked search (MRSE scheme) in our proposed system. Paper (Jian Li *et al.,* 2015) explains the Traffic and Energy saving Encrypted Search (TEES) architecture for mobile cloud storage applications. This architecture offloads the computation from mobile devices to the cloud and optimizes the communication between mobile client and cloud. TEES achieves the efficiency through employing and modifying the ranked keyword search on the encrypted search platform, which has been widely employed in cloud storage systems.

Mehmet Kuzu *et al*., 2015 introduces a method of locality sensitive hashing which is a high dimensional space searching technique .which uses a hashing technique to create trap door for searching encrypted documents in the cloud. As the hashing technique is one way, it cannot reverse engineer to recheck the outcomes, and also, this method takes a little while to search the document due to granular hashing process. Due to different cryptography methods, searchable encryption schemes can be constructed using public key cryptography or symmetric key cryptography. (Curtmola *et al.,* 2006) uses Searchable Symmetric Encryption (SSE) that allows a party to store its data on the server in a private manner. Also, multi-user SSE is constructed which is very efficient on the server side: on giving a trapdoor, the server only needs to evaluate a pseudo-random permutation to determine if the user is revoked or not. Here, only the owner of the data is capable of submitting search queries.

The main advantage is that heavier authentication is provided here. (Chang and Mitzenmacher, 2005) Makes use of PIR (Private Information Retrieval) queries for searching over the cloud. This method uses bloom filter gives storage space that can be useful to store some extra information. It hides the identity of the communication also keeps the semantic of the encrypted data. But it will not preserve the privacy and correctness of the data. A ranked search scheme over encrypted cloud data using multi-keyword is introduced in (Zhihua Xia *et al.,* 2005), where the greedy depth-first search algorithm is used to provide efficient multi-keyword ranked search. This scheme can flexibly achieve sub-linear search time and also deals with deletion and insertion of documents.

RESULTS AND COMPARISON

By the above survey, we compare some mechanism used for the searching schemes on encrypted data.

Conclusion

This complete paper narrates the different methodologies on Search Schemes for Encrypted Data over Cloud each having its advantages and disadvantages. And in a majority of the systems the accumulated problem with them is, they are taking more time to search the data. Authors like Jianfeng Wang *et al*. depicts a method of searching data using a tree-based method with fuzzy logic where the system is an emphasis on reducing the cost (Hongwei *et al.,* 2005). Boneh *et al*., 2012 shows a method of key based searching technique. Whereas Y.-C. Chang (Kuzu *et al.,* 2012), uses Private Information Retrieval query with bloom filters to search for the encrypted data. So these methods are never talking about reducing the time complexity of the system.

REFERENCES

Boneh, D., G. Di Crescenzo, R. Ostrovsky, and G. Persiano, 2004. "Public key encryption with keyword search," in Advances in Cryptology Eurocrypt, Springer, pp. 506–522.

CengizOrencik and ErkaySavas, 2012. "Efficient and Secure Ranked Multi-keyword Search on Encrypted Cloud Data", ACM 978-1-4503, March.

Chang, Y. C. and M. Mitzenmacher, 2005. "Privacy preserving keyword searches on remote encrypted data," in *Proceedings of the Third International Conference on Applied Cryptography and Network Security*. Springer-Verlag, pp. 442–455.

Cong Wang *et al*., 2012. "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE Transactions on Parallel and distributed systems, vol. 23, no. 8, August.

Curtmola, R., J. Garay, S. Kamara, and R. Ostrovsky, 2006. "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, pp. 79–88.

Hongwei Li, DongxiaoLui, Yuanshun Dai, "Enabling Efficient Multi-keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", IEEE Transactions, vol. 3, no. 1, Mar. 2015.

Jian Li, Ruhui Ma, and Haibing Guan, 2015. "TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud ", IEEE Transactions, vol. 3, no. X..

Kuzu, M., M. S. Islam, and M. Kantarcioglu, 2012. "Efficient similarity search over encrypted data," in *Data Engineering (ICDE), IEEE 28th International Conference on*. IEEE, pp.1156–1167.

Li, J., Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, 2010. "Fuzzy keyword search over encrypted data in cloud computing", in *INFO COM, Proceedings IEEE*. IEEE, pp. 1–5.

Zhihua Xia, Xinhui Wang, Xingming Sun, and Qian Wang, 2015. "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", *IEEE Transactions on Parallel and distributed systems*, Vol. no.

****