A Survey on Secure and Efficient Item Information Retrieval in Cloud Computing

Tahseen Begum[1], Dr. Shameem Akther [2]

[1]PG Scholar, Department of Computer Science and Engineering, KBN College of Engineering, Kalaburagi, India

[2]Professor & HOD Department of Computer Science and Engineering, KBN College of Engineering, Kalaburagi , India

Abstract: ***Cloud computing is a promising information technique (IT) that can organize a large amount of IT resources in an efficient and flexible manner. Increasingly numerous companies plan to move their local data management systems to the cloud and store and manage their product information on cloud servers. But for protecting data privacy, sensitive data has to be encrypted before outsourcing. An accompanying challenge is how to protect the security of the commercially confidential data, while maintaining the ability to search the data. The various searchable encryption techniques are used. Privacy problems have become very challenge one in a cloud computing environment. Privacy is the protection for the truthful use of personal information of cloud user. Privacy preserving data search schemes were designed to ensure that only legitimate users based on identifiers or keywords, and have the ability to search the data. These schemes safeguard the user's personal data but enable the server to return to the target ciphertext file according to the query request. Thus, we can ensure the security of user data and privacy while not unduly reducing the query efficiency.***

Keywords: Product information retrieval, cloud computing, information security

1. Introduction

Cloud computing is emerging technology. Cloud offers several applications to users. Cloud computing use the basic fundamental infrastructure is help full for coming model of service that has the several benefit of decreasing cost by sharing computing and storage resources. Without appropriate privacy solution for cloud become a large failure. Privacy means that the person to be free from all interference. Privacy control allows the person to maintain a degree of intimacy. Privacy is the protection for the truthful use of personal information of cloud user. Privacy problems have become very challenge one in a cloud computing environment. Cloud computing has made a drastic changes in IT field. Cloud computing service is a most recently used in IT area which offers different model. Cloud computing is emerging technology. Cloud offers several applications to user which consist of existing techniques combining with new technology, such technology shared different resources like hardware, software and some important information provided to users and other people on internet whenever needed. Increasing population using emerging technology along with privacy and security in cloud because most of user having high sensitive data while sharing those data user needs privacy, providing such secure and privacy-preserving of data services is the big challenge. Security and privacy protection may be impeding the functionality and data services performance. Privacy is a most important issue in cloud whenever user needs to make his individual data in secure mode. Preserving for the privacy of user, his data and identity in the cloud is very compulsory. The increase popularity of cloud computing, the concerned about privacy preserving are also getting more increased. But reaching the peak in providing and assurance the privacy-preserved data access in cloud is still in progress and needs much attention to the goal.

2. Related Works

Conjunctive keyword search: In [1] authors studied setting in which a user stores encrypted documents on an untrusted server. When a data user has several keywords he first generates trapdoor for each keyword. The search results are the intersection of the search results of each keyword. Conjunctive key search return the documents in which all the keywords specified by the search query appear. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. The Authors proposed first a scheme for which the communication cost is linear in the number of documents, but that cost can be incurred "offline" before the conjunctive query is asked. The security of this scheme relies on the Decisional Diffie-Hellman (DDH) assumption and proposed a second scheme whose communication cost is on the order of the number of keyword fields and whose security relies on a new hardness assumption. Both of the schemes provably meet the definition of security.

Cryptography: In [2] authors proposed the searchable encryption scheme in which each word in a document is encrypted independently, and the users need to scan the entire document to search for a certain keyword. Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. They described the cryptographic schemes for the problem of searching on encrypted data. They show how to support searching functionality without any loss of data confidentiality. The techniques provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext given only the ciphertext. The techniques provide controlled searching, so that the untrusted server cannot search for a word without the user's authorization. The techniques support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The techniques also support query isolation, meaning that the untrusted server learns nothing more than the search result about the plaintext.

Multi keyword ranked search: In secure multi-keyword ranked search scheme over encrypted cloud data [3] authors proposed a multi-keyword ranked search scheme, which supports both multi-keyword ranked search and dynamic update. In ranked keyword search, Relevance score is employed to make a secure searchable index and order-preserving mapping function is used. The proposed scheme is designed to provide not only multi-keyword query and accurate result ranking, but also dynamic update on document collections. To improve search efficiency, they designed tree based index structure which supports insertion and deletion update well without privacy leakage.

Coordinate matching: In [4] authors defined and solved the challenging problem of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).They established a set of strict privacy requirements for a secure cloud data utilization system. The coordinate matching technique is employed to capture the connection of information between data documents and requested query. This method is employed to find a variety of keywords within the document. The authors further used “inner product similarity” to quantitatively evaluate similarity measure. They proposed a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given.

In [5] authors proposed a multi-keyword ranked search over encrypted data based on hierarchical clustering index (MRSE-HCI). The author investigated the problem of maintaining the close relationship between different plain documents over an encrypted domain and proposed a clustering method to solve the problem. The author proposed the MRSE-HCI architecture to speed up server-side searching phase and designed a search strategy to improve the rank privacy. This search strategy adopts the backtracking algorithm upon the clustering method. In addition, a verification scheme was also integrated into their scheme to guarantee the correctness of the results.

In [6] authors presented a personalized multi keyword ranked search scheme in which an interest model of the users is integrated into the document retrieval system to support a personalized search and improve the users search experience. Specifically, the interest model of a data user is built based on his search history with the help of WordNet in order to depict his behaviors in fine grit level. However, this scheme does not support dynamic update operations because the document vectors are constructed based on all the documents. To address the limitations of the model of “one size fit all” and keyword exact search, authors proposed two PRSE schemes for different search intentions.

3. Conclusion

The various strategies for searching encrypted information over a cloud are used. Several searchable encryption techniques are analysed based on, conjunctive keyword, multi-keyword, search based on similarity measures, etc. The majority of strategies has drawback with them that is they are taking longer time to search the information also they are facing some privacy and security issues. While multi keyword search techniques supports more privacy and efficient retrieval of data. Therefore a major analysis is important which will provide privacy and minimize the searching time over encrypted information in the cloud.

References

[1] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2004, pp. 31_45.

[2] D. X. Song and D. A. Wanger Perrig, ``Practical techniques for searches on encrypted data,'' in *Proc. IEEE Symp. Security Privacy*, May 2000, pp. 44_55.

[3] C. Wang, N. Cao, K. Ren, and W. Lou, ``Enabling secure and efficient ranked keyword search over outsourced cloud data,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1467_1479, Aug. 2012.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi keyword ranked search over encrypted cloud data,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222_233, Jan. 2014.

[5] C. Chen *et al.*, “An efficient privacy-preserving ranked keyword search method,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 951_963, Apr. 2016.

[6] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546_2559, Sep. 2016.