IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data

Sunil S.M[1], Vijeth K.S[2], Puneeth Kumar A[3]

Dept. of ISE, SJBIT, Bangalore [1 2,3]

Abstract: The innovation in cloud computing has encouraged the data owners to outsource their data managing system from local sites to profitable public cloud for excessive flexibility and profitable savings. But people can like full benefit of cloud computing, if we are able to report very real secrecy and security concerns that come with loading sensitive personal information. Allowing an encrypted cloud data search facility is of great significance. In view of the huge number of data users, documents in the cloud, it is important for the search facility to agree multi keywords query and arrange for result comparison ranking to meet the actual need of data recovery search and not regularly distinguish the search results. Related mechanisms on searchable encryption emphasis on single keyword search or Boolean keyword search, and often sort the search outcomes. 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.

I INTRODUCTION

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. 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 achieve 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 learn large 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. Due to inherence safety and privacy, it remains the interesting job on behalf of how to relate the encrypted cloud search. The difficult of multi-keyword ranked search over encrypted cloud data is resolved by using stringent privacy necessities then numerous multi-keyword semantics. Among numerous multi-keyword ranked semantics, we choose coordinate matching. Our contributions are summarized as follows,

1) For the first time, we explore the problem of multi keyword ranked search over encrypted cloud data, and establish a set of strict privacy requirements for such a secure cloud data utilization system.

2) We propose two MRSE schemes based on the similarity measure of "coordinate matching" while meeting different privacy requirements in two different threat models.

3) Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is given, an experiments on the real-world dataset further show the proposed schemes indeed introduce low overhead on computation and communication.

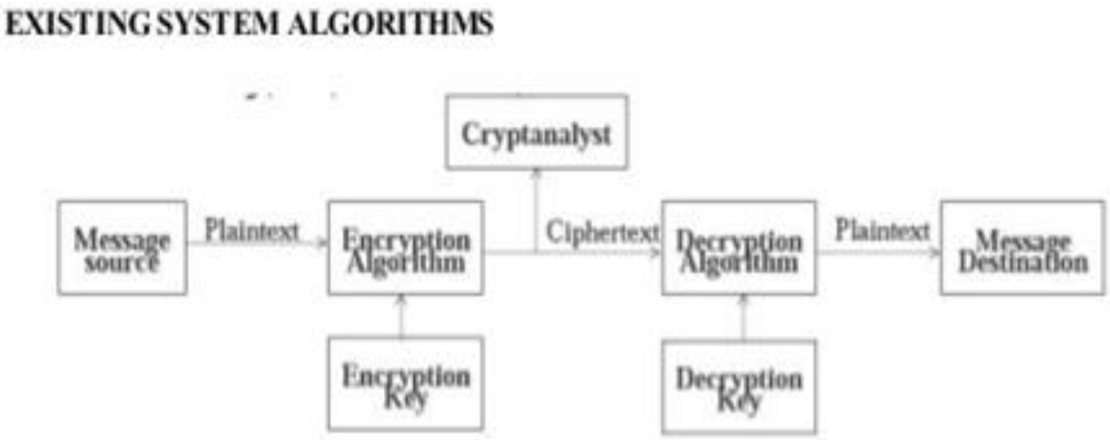
RELATED WORK

Searchable encryption schemes enable the clients to store the encrypted data into the cloud and execute keyword search over ciphertext domain. Due to different cryptography primitives, searchable encryption schemes can be constructed using public key based cryptography or symmetric key based cryptography. Song et al. proposed the first symmetric searchable encryption scheme (SSE) , and the search time of their scheme is linear to the size of the data collection. Goh proposed formal security definitions for SSE and designed a scheme based on Bloom filter. The search time of Goh's scheme is O (n), where n is the cardinality of the document collection. Curtmola et al. proposed two schemes (SSE-1 and SSE-2) which achieve the optimal search time. Their SSE-1 scheme is secure against chosen-keyword attacks (CKA1) and SSE-2 is secure against adaptive chosen-keyword attacks (CKA2). cloud server. Thus, the SE schemes are expected to support the insertion and deletion of the documents. There are also several dynamic searchable encryption schemes. In the work of Song et al., the each document is considered as a sequence of fixed length words, and is individually indexed. This scheme supports straightforward update operations but with low efficiency. Goh proposed a scheme to generate a sub-index (Bloom filter) for every document based on keywords. Then the dynamic operations can be easily realized through updating of a Bloom filter along with the corresponding document. However, Goh's scheme has linear search time and suffers from false positives. In 2012, Kamara et al. constructed an encrypted inverted index that can handle dynamic data efficiently. But, this scheme is very complex to implement. Subsequently, as an improvement, Kamara et al. proposed a new search scheme based on tree-based index which can handle dynamic update on document data, stored in leaf nodes. However, their scheme is designed only for singlekeyword Boolean search. In, Cash et al. presented a data structure for keyword/identity tuple named "TSet". Then, a document can be represented by a series of independent T-Sets. Based on this structure, Cash et al. proposed a dynamic searchable encryption scheme. In their construction, newly added tuples are stored in another database in the cloud, and deleted tuples are recorded in a revocation list. The final search result is achieved through excluding tuples in the revocation list from the ones retrieved from original and newly added tuples. Yet, Cash et al.'s dynamic search scheme doesn't realize the multi-keyword ranked search functionality.

Problem Statement

Downloading all the data from the cloud and decrypt locally is obviously impractical.

Algorithm



REFERENCES

[1] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 2016.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, 2000, pp. 44–55.

[3] E.-J. Goh, "Secure indexes," IACR Cryptol. ePrint Archive, vol. 2003, p. 216, 2003.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 79–88.

[5] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 2–22.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM, Apr. 2011, pp. 829–837.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. secur., 2013, pp. 71–82.