

Secure and Efficient Commercial Data Retrieval in Cloud Computing

Kummari. Ilayaraja

Dept of CSE
Vaishnavi Institute of Technology
Tirupati, AP, India

A. Uday Kishore

Dept of CSE
Vaishnavi Institute of Technology
Tirupati, AP, India.

Abstract- In Cloud computing, cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk. It follows that sensitive data has to be encrypted prior to outsourcing for data privacy. However, data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data files. Also outsourcing data to the cloud causes loss of control over data on a data owner's part. This loss of control over data is further intensified with the lack of managing users' access to the data from practical cloud computing perspectives. We address these challenging issues, a privacy-preserving data search Scheme is proposed, and that can support both the identifier -based and feature-based product searches. Specially, two novel index trees are constructed and encrypted, that can be searched without knowing the plaintext data. Data user is enabled to create queries to retrieve data by the Data user query. The index value is attached to every data and it is stored in the cloud. If the user wants to retrieve the data from cloud then the given index value is to be matched with the index value.

Keywords:- Cloud computing, secure data access, keyword search.

I. INTRODUCTION

Cloud storage services allow the users to outsource their data in the cloud storage servers and retrieve them whenever and wherever required. This avoids the cost of building and maintaining their data store. But the users need to provide privacy for the data and also to be able to search it without losing privacy. The users always search their documents through keyword in plaintext, which may leak privacy of users in cloud storage environment. So allowing a cloud service provider (CSP), whose purpose is mainly for making a profit, to take the custody of sensitive data, raises underlying security and privacy issues. To keep user data confidential against an untrusted cloud, a natural way is to apply cryptographic approaches, by disclosing the data decryption key only to authorized users. In this paper we propose an efficient, secure and privacy preserving keyword search scheme which supports multiple users with low computation cost and flexible key management.

II. RELATED WORK

A number of different mechanisms have been proposed for security aspects in cloud computing. Some of the researchers have suggested the following strategies to support secure access in cloud computing. Private Searching on streaming data (2005). In this paper

R. Ostrovsky and W. Skeith [1] considered the problem of private searching on streaming data. He showed that in this model we can efficiently implement searching for documents under a secret criteria (such as presence or absence of a hidden combination of hidden keywords) under various cryptographic assumptions. The results can be viewed in a variety of ways: as a generalization of the notion of a Private Information Retrieval as positive results on privacy - preserving data mining; and as a delegation of hidden program computation. Searchable symmetric encryption allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions.

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky [2] presented two constructions that show secure under new definitions. Interestingly, in addition to satisfying stronger security guarantees, the new constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. They also

consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. The SSE is formally defined in this multi - user setting, and presents an efficient construction. Private searching on streaming data is a process to dispatch to a public server a program, which searches streaming sources of data without revealing searching criteria and then sends back a buffer containing the findings. From an Abelian group homomorphic encryption, the searching criteria can be constructed by only simple combinations of keywords, for example, disjunction of keywords. The recent breakthrough in fully homomorphic encryption has allowed us to construct arbitrary searching criteria theoretically.

Here consider a new private query, which searches for documents from streaming data on the basis of keyword frequency, such that the frequency of a keyword is required to be higher or lower than a given threshold. This form of query can help us in finding more relevant documents. Based on the state of the art fully homomorphic encryption techniques, we give disjunctive, conjunctive, and complement constructions for private threshold queries based on keyword frequency. Combining basic constructions, further presented a generic construction for arbitrary private threshold queries based on keyword frequency. The protocols are semantically secure as long as the underlying fully homomorphic encryption scheme is semantically secure.

III. OBJECTIVES

To enable ranked searchable symmetric encryption for effective utilization of outsourced and encrypted cloud data under the proposed model, our system design should achieve the following security and performance guarantee. Specifically, we have the following goals:

- Ranked keyword search: to explore mechanisms for designing effective ranked search schemes.
- Security guarantee: to prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the “as – strong – as - possible” security strength.
- Efficiency: above goals should be achieved with minimum communication and computation overhead.

IV. PROPOSED SYSTEM

Here the new proposed scheme called Secure and Efficient Commercial Data retrieval System is introduced. This new system uses the method of Flexible ranking mechanism which allows users to provide a rank and can personally decide how many Matched files will cloud returns. The basic idea is to construct a matrix that allows the cloud to filter out certain percentage of matched files. The new scheme reduces the querying overhead and also computational costs.

The Secure & Efficient Commercial Data retrieval System protects user privacy which allows each user to retrieve matched files on demand. This is not an easy work, because the cloud needs to correctly filter out files according to the rank of queries without knowing anything about user privacy. This has two extensions: the first extension shows the least amount of modifications from the Ostrovsky scheme, and the second extension provides privacy by leaking the least amount of information to the cloud.

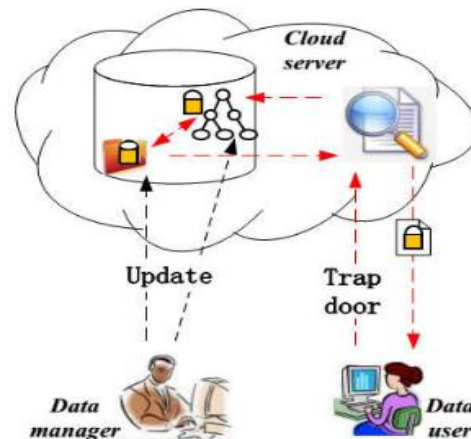


Fig 1 Encrypted product information retrieval system model.

As shown in Fig. 1, the entire product retrieval system model is composed primarily of three entities: the data manager, the cloud server and the data user. The primary responsibilities of these three entities are presented in the following. The data manager is responsible for managing the product and collecting the product information. In addition, the data manager needs to encrypt the product information file by a symmetric encryption technique before outsourcing the data to the cloud server.

To improve the security of the files, each file is encrypted by a single secret key, and the keys of different files are independent. Furthermore, to improve the search efficiency, an index structure is constructed for the outsourced data. At first, an identifier index structure is constructed based on the hash function and height - balanced binary search tree. Then, a feature vector tree is built for all the feature vectors of the product, and it is encrypted by the secure kNN algorithm.

When a data user wants to search a set of chosen products, she needs to generate a trapdoor to describe her interest. Two types of the trapdoor can be provided, i.e., a set of hash values of the desired product information files or a set of feature vectors. For the first type of trapdoor, a set of encrypted files with the same hash identifiers are returned, and for the second type trapdoor, the most relevant encrypted files are returned. The data user can

obtain the plaintext files by decrypting the returned files with the help of the symmetric secret keys. These secret keys are provided by the data manager.

The cloud server stores all the data uploaded by the data manager. When a data user needs to search the data in the cloud, she first generates a trapdoor, which is sent to the cloud server. A search engineer is employed by the cloud server to act as a bridge between the data users and the encrypted data. Though the cloud server cannot get the plaintexts of the data, it should be capable of sending the accurate search result of the trapdoor to the data users. Of course, the returned data are ciphertext, and the data user needs to decrypt them by the symmetric secret keys which are provided by the data manager.

V. EXPERIMENTAL RESULTS

We evaluate the search efficiency of our scheme. First, we evaluate the construction time of the index structures of the product information. Specifically, we compare our scheme with the MRSE scheme [14]. To decrease the bias of the data manager who is responsible for generating the vectors and the hash values, in this paper we employ the Enron Email Data Set [15] to test our scheme.

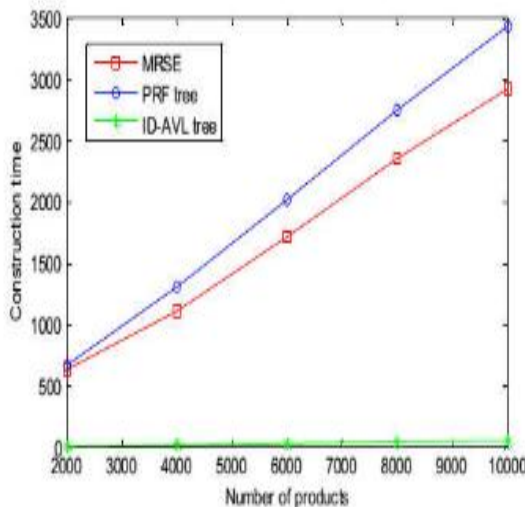


Fig 2 Construction time of the index structures.

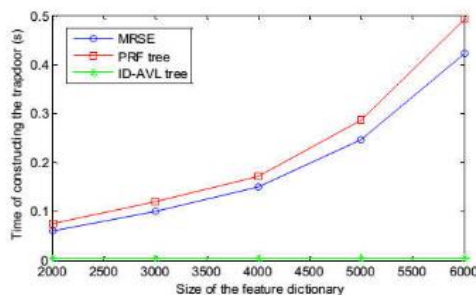


Fig 3 Time of constructing the trapdoors.

VI. CONCLUSION

In this paper, we designed a secure and efficient product information retrieval scheme based on cloud computing. Specifically, two index structures, including a hash value AVL tree and a product vector retrieval tree, are constructed, and they support an identifier - based product search and feature - vector -based product search, respectively. Correspondingly, two search algorithms are designed to search the two trees. To protect the product information privacy, all the outsourced data are encrypted. The product information is symmetrically encrypted based on a set of independent secret keys, and the product vectors are encrypted based on the secure kNN algorithm. Security analysis and simulation results illustrate the security and efficiency of the proposed scheme.

REFERENCES

- [1] www.100EC.cn. 2016 Monitoring Report on the Data of China's E-commerce Market [EB/OL].<http://www.100ec.cn/zt/16jcbg/>,2017-0 24.
- [2] Amazon. Amazon S3. <http://aws.amazon.com/s3/>
- [3] Apple i Cloud. <http://www.icloud.com/>
- [4] Google App Engine. <http://appengine.google.com/>
- [5] Golle P.Staddon J,Waters B. Secure Conjunctive Keyword Search over Data[C]. Springer, 2004.
- [6] Song D X,Wanger D.Perrig A. Practical Techniques for Searched on Encrypted Data[C].IEEE,2000.
- [7] Boneh D,Di Crescenzo G,Ostrovsky R. et al. Public Key Encryption with Keyword Search: EUROCRYPT [C].Springer.
- [8] Rhee H S.Park J K,Susilo W. et al. Trapdoor Security in A Searchable Public-Key Encryption Scheme with A Designated Tester[J].Journal of Systems and Software,2010,83(5):763-771.-
- [9] Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." IEEE Internet Computing 16.1 (2012): 69-73.
- [10] Song, Dawn Xiaoding, David Wagner, and Adrian Perrig. "Practical techniques for searches on encrypted data." Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000.

Author's Profile



Kummari Ilayaraja. Pursuing M.Tech at Vaishnavi Institute of Technology, Department Of CSE, Tirupati, AP, India.



A.Uday Kishore Working as a Assistant Professor in Vaishnavi Institute of Technology, Department Of CSE, Tirupati, AP, India.