International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

A Survey on Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data

Athira Sankar[1], Soumya Murali[2]

[1]PG Scholar, [2]Assistant Professor
Sree Buddha College of Engineering, Kerala Technological University, India.

Abstract - *Cloud computing is a type of computer paradigm for storing and accessing data and program over the network. With the increase in the data's, more and more data owners outsource their document to the cloud server for convenience. The sensitive data should be encrypted before outsourcing to the cloud for privacy preserving. In this paper presents a secure multi-keyword ranked search scheme over encrypted cloud data. Here a vector space model is used. A greedy depth first search (GDFS) is used for index structure. GDFS provide efficient multi-keyword rank search. A KNN algorithm is used to encrypt the index and query. Thus calculate the relevance score between encrypted index and query vector.*

1. INTRODUCTION

Cloud computing is a new model for the IT infrastructure [1], which deals with storing huge amount of information. The advantage of cloud computing is providing reliability, cost saving, backup and recovery. A general method for protecting data confidentiality is to encrypt the data before outsourcing to the cloud server.

This paper proposes a multi-keyword ranked search method and it simultaneously support dynamic operations like update and deletion.

Here the documents are represented by vector space model. Vector space model uses a TF*IDF model for index construction. Two secure search schemes are used: basic dynamic multi-keyword ranked search (BDMRS) scheme in the known cipher text model and the enhanced dynamic multi-keyword ranked search (EDMRS) scheme in the known background model.

The objective of the work is to design a searchable encryption scheme that supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection. The second objective is to design a special tree-based index, so the search complexity of the proposed scheme is fundamentally kept to logarithmic.

2. RELATED WORKS

Security and privacy is one fundamental challenge to public cloud [2].

Multi tenancy is an important attribute of cloud computing. Resource utilization can be optimizing by using CSPs. CSP often use hardware virtualization to hide a computing platform's physical characteristics.

More and more data are produced by the individual and enterprise. So the sensitive information is encrypted before outsourcing it to the cloud. Searchable encryption provides a high level of data confidentiality and integrity. A searchable encryption scheme employs a prebuilt encrypted search index with appropriate tokens securely search over the encrypted data via keywords without first decrypting it.

In this paper proposes [2], cryptographic cloud storage. Cryptography storage consists of three components: a data processor (DP) , a data verifier (DV), and a token generator (TG) .

Cryptographic storage services are: Cryptographic Cloud Storage, associate degree Enterprise architectures, Elliptic Curve Cryptography (ECC), D- DJSA symmetric key algorithm, Homomorphic Encryption, RSA algorithm and cloud computing.

The benefits of cryptographic storage are confidentiality assurance, geographic restrictions, electronic discovery, and reducing risk of security breaches. A cloud service provides proper security and privacy mechanisms which would make the cloud atmosphere safe and protected place for their customers and they keep full faith on the cloud service providers.

C.Gentry[4]proposes a fully homomorphism implementation on cloud. A fully homomorphic encryption is a new concept of security. It provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data. A fully Homomorphic encryption to the security of Cloud Computing analyze and improve the existing cryptosystem to allow servers to perform various operations requested by the client and Improve the complexity of the homomorphic encryption algorithms according to the length of the public key.

Jin L et al [5] proposes a fuzzy keyword search over encrypted data in cloud computing. The advanced technique for constructing fuzzy keyword sets are Wildcard-based

Fuzzy Set Construction, AES Encryption, Grams-Based Technique.

AES is a block cipher technique with block size of 128 bits or 256 bits. Wildcard – based technique is straightforward approach where all the variants of the keywords have to be listed even if an operation is performed at the same position. One of the most efficient techniques for constructing fuzzy set is based on gram.

Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud [6] enabling keyword search directly over encrypted data. The design goals of the multi-keyword fuzzy search are multi-keyword fuzzy search, privacy guarantee, result accuracy, no predefined dictionary. Two important techniques are used in design, are bloom filter and locality-sensitive hashing (LSH). A Bloom filter is a bit array of m bits that initially set to 0.

Locality-sensitive hashing (LSH) reduces the dimensionality of high-dimensional data. LSH hashes input items so that similar items map to the same buckets with high probability.

3. CONCLUSION

Data security and privacy is one of the biggest challenges in cloud computing. There are many important techniques for secure and dynamic keyword search over an encrypted cloud. Among that greedy depth-first search method is used to obtain better efficiency for tree index structure.

ACKNOWLEDGEMENT

We are grateful to our project guide and PG Coordinator Prof. Minu Lalitha Madhav for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department

REFERENCES

[1] xia et al.: "a secure and dynamic multi-keyword ranked search scheme over encrypted cloud data", IEEE transactions on parallel and distributed systems, vol. 27, no. 2, february 2016

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan-Feb. 2012.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Financ. Cryptography Data Secur., 2010, pp. 136–149.

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2009.

[5] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE Proc. INFOCOM, 2010, pp. 1–5.

[6] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi keyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, 2014, pp. 2112–2120.