IJRRECS/April 2016/Volume-4/Issue-4/5434-5439 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE APPROACH FOR CONTROLLING DYNAMIC FUNCTIONS ON DOCUMENT COLLECTION

P.Ekambharam[1], N.Sainath[2]

[1]M.Tech Student, Dept of CSE, Bharat Institute of Engineering and Technology, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Bharat Institute of Engineering and Technology, Hyderabad, T.S, India

ABSTRACT:

The technology of cloud computing was considered as an efficient model of infrastructure. In spite of different benefits of cloud services, outsourcing of sensitive data towards remote servers makes lots of privacy issues. In our work we introduce a secured method of multi-keyword ranked search above encrypted cloud data, which supports dynamic update functions of documents. We build a particular structure of tree-based index and suggest an algorithm of Greedy Depth-first Search to offer resourceful multi-keyword ranked search. Because of the usage of special tree-based index structure, the projected scheme can attain sub-linear search time and manage flexible deletion as well as insertion of documents. We build two secures schemes of search like basic dynamic multi-keyword ranked search scheme, and enhanced dynamic multi-keyword ranked search process.

Keywords: Cloud computing, Multi-keyword ranked search, Greedy Depth-first Search, Tree-based index, Privacy.

1. INTRODUCTION:

Because of cloud computing popularity, lots of data owners are outsourcing their data towards cloud servers for decreased expenditure in data management. But sensitive information has to be encrypted earlier than outsourcing for the needs of

privacy, which outdates data utilization. The providers of cloud service that maintain data for users might access users' sensitive information devoid of authorization and the common method for protecting the data privacy is to encrypt data previous to outsourcing. But on the other hand, this will cause very much cost regarding the usability of data [1]. Up to now many works were proposed in various models of threat for achieving several search functionalities but among the search of multi-keyword ranked gains much attention for its realistic applicability. Some of the researchers have considered general-purpose solutions with fully-homomorphic encryption for addressing the traditional problems but these methods are not realistic because of their high computational transparency for cloud sever as well as user. But most of the practical solutions, for instance searchable encryption have made particular contributions regarding efficiency as well as security. These schemes allow client to store up encrypted data to cloud and carry out keyword search above cipher-text domain [2][3]. In the recent times some of the dynamic methods were proposed to maintain inserting as well as deleting operations on document collection. These are important works as it is extremely possible that data owners need to update their data on cloud server. However few of dynamic methods manage effective process of multi-keyword ranked search. In our work we introduce a searchable method of encryption that supports multi-keyword ranked search above encrypted cloud data, which supports dynamic update functions of documents. Because of the usage of special tree-based index structure, the projected scheme can attain sub-linear search time and manage flexible deletion as well as insertion of documents and moreover the search complexity of projected scheme is basically kept to logarithmic. Proposed system can attain higher search effectiveness by means of execution of greedy depth-first search algorithm. Parallel search is flexibly carried out to decrease time cost of search process.

2. METHODOLOGY:

The methods of searchable encryption permit clients to store up encrypted data to cloud and carry out keyword search on cipher-text domain. Because of several methods of cryptography primitives, searchable encryptions are constructed by means of public key based cryptography or

symmetric key basis cryptography. Model of vector space and extensively used Term frequency x Inverse document frequency model are combined for retrieval of plaintext information, which supports ranked multi-keyword search. Term frequency is number of times a specified term appears in document. Inverse document frequency is attained through division of cardinality of document collection by number of documents that contains keyword. In representation of vector space, each of the documents is denoted by means of vector, whose elements are normalized values of Term frequency keywords in this document. Each of the queries is moreover denoted as a vector P, whose elements are normalized Inverse document frequency values of query keywords in document collection. Normally the Term frequency and Inverse document frequency vectors lengths are equivalent to total number of keywords. For permitting of secured and dynamic multi-keyword ranked search on outsourced encrypted data of cloud, our system contains several goals of design such as: Dynamic: The proposed scheme is considered to offer multi-keyword query as well as accurate result ranking, and dynamic update on collection of documents. Search efficiency: The proposal aims to attain sub-linear search efficiency by means of exploring special tree-based index as well as efficient search algorithm[4]. Privacy-preserving: The proposed system is prevents the cloud server from learning of added data concerning collection of document, index tree, as well as query.

3. AN OVERVIEW OF PROPOSED SYSTEM:

The proposed system model includes three separate entities such as owner of data, data user as well as cloud server, as shown in fig1. Data owner includes collection of documents that are to be outsourced towards cloud server in an encrypted form while managing ability to search on them for efficient usage. Data users are approved to access documents regarding data owner. Cloud server store up the collection of encrypted documents as well as encrypted searchable tree index for the data owner. The cloud server within proposed scheme is honest-but-curious, which is in usage by several works on safe cloud data search. Based on the data that was known by cloud server we implement the two threat models such as known cipher-text and Known Background Model. In the Known Cipher-text Model**,** cloud server knows only

collection of encrypted document, searchable index tree, as well as search trapdoor that is provided by approved user. In the known Background representation, when compared with known cipher-text model, cloud server in this model is equipped by additional knowledge and this data records the number of documents for each term frequency of particular keyword in the complete collection of documents. For resisting various attacks in several models we build two secures schemes of search such as basic dynamic multi-keyword ranked search scheme in the known representation of cipher-text, and enhanced dynamic multi-keyword ranked search method in known representation of background [5]. The unencrypted dynamic multi-keyword ranked search system is constructed on basis of vector space model as well as keyword balanced binary tree. On basis of unencrypted dynamic multi-keyword ranked search scheme, two secure schemes such as basic dynamic multi-keyword ranked search scheme, and enhanced dynamic multi-keyword ranked search method are constructed against two models of threat, correspondingly. In the construction of unencrypted dynamic multi-keyword ranked search index, we initially construct a tree node for every document in collection. These nodes are leaf nodes of index tree and finally nodes of internal tree are generated on the basis of these leaf nodes. The searching procedure of unencrypted dynamic multi-keyword ranked search process is a recursive process upon tree, titled as Greedy Depth first Search algorithm. Because of the usage of special tree-based index structure, the projected scheme can attain sub-linear search time and manage flexible deletion as well as insertion of documents. Basic dynamic multi-keyword ranked search method was analyzed based on predefined privacy needs such as Index Confidentiality as well as Query Confidentiality. Hence this method is flexible against cipher text-only attack as well as index confidentiality and query privacy is well protected [6]. On the basis of unencrypted dynamic multi-keyword ranked search scheme, we build basic dynamic multi-keyword ranked search by means of using secure algorithm of k nearest neighbors which is used to encrypt index and query vectors, and make sure precise relevance score calculation among encrypted index as well as query vectors. Basic dynamic multi-keyword ranked search is considered to attain goal of privacy

preserving in known model of cipher-text and this scheme will protect Index Confidentiality as well as Query Confidentiality in known model of cipher-text. In the known model of background, it is feasible for the cloud server to recognize a keyword as normalized Term frequency distribution of keyword can be accurately obtained from final calculated relevance scores. To suit various preferences of user for high accurate ranked results or else better protected keyword privacy, randomness are put flexible. Inherited from Basic dynamic multi-keyword ranked search scheme, enhanced dynamic multi-keyword ranked search scheme can continue index confidentiality as well as query confidentiality within known background representation.

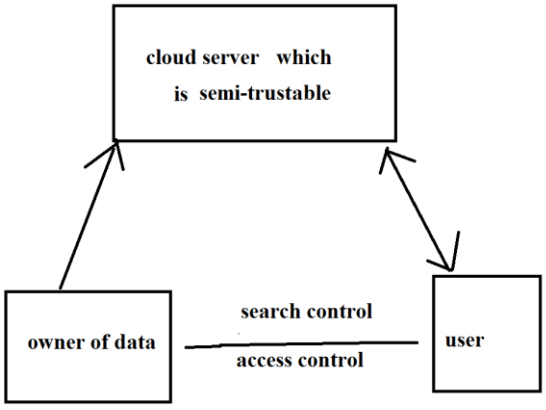

Fig1: System model

4. CONCLUSION:

The technology of cloud computing manages huge computing resources and facilitates users to benefit from suitable network access with great effectiveness and minimum economic transparency. However this technology brings lots of privacy issues during outsourcing of sensitive data towards remote servers. Here we introduce a secured method of multi-keyword ranked search above encrypted cloud data, which supports dynamic update functions of documents. Particularly the model of vector space and extensively used Term frequency x Inverse document frequency model are combined for building of index as well as generation of query. Due to usage of special tree-based index structure, the projected scheme can attain sub-linear search time and manage flexible deletion as well as insertion of documents. For resisting of various attacks in several models we build two secures schemes of search such as basic dynamic multi-keyword ranked search scheme in the known representation of cipher-text, and enhanced dynamic multi-keyword ranked search method in known representation of background.

REFERENCES

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.

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

[3] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.

[4] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword
fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014.

[5] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.

[6] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proceedings of the First international conference on Pairing-Based Cryptography. Springer-Verlag, 2007, pp. 2–22.