Chapter 33
Glorified Secure Search Schema Over Encrypted Secure Cloud Storage With a Hierarchical Clustering Computation

Shweta Annasaheb Shinde
VIT University, India

Prabu Sevugan
VIT University, India

ABSTRACT

This chapter improves the SE scheme to grasp these contest difficulties. In the development, prototypical, hierarchical clustering technique is intended to lead additional search semantics with a supplementary feature of making the scheme to deal with the claim for reckless cipher text search in big-scale surroundings, such situations where there is a huge amount of data. Least relevance of threshold is considered for clustering the cloud document with hierarchical approach, and it divides the clusters into sub-clusters until the last cluster is reached. This method may affect the linear computational complexity versus the exponential growth of group of documents. To authenticate the validity for search, minimum hash sub tree is also implemented. This chapter focuses on fetching of cloud data of a subcontracted encrypted information deprived of loss of idea and of security and privacy by transmission attribute key to the information. In the next level, the typical is improved with a multilevel conviction privacy preserving scheme.

INTRODUCTION

Individuals are profited with cloud computing as cloud computing reduces it work and make computing and storage simplified. (Liang, Cai, Huang, Shen & Peng, 2012), (Mahmoud & Shen, 2012), (Shen, Liang, Shen, Lin & Lou, 2012). Data can be stored remotely in the cloud server as data outsourcing and accessed publicly. This embodies a mountable, constant and low-cost method for public access of data as per the high productivity and mount ability of cloud servers, and so it is favored.

DOI: 10.4018/978-1-5225-8176-5.ch033

Sensitive privacy information is of concern. Data should be encrypted before sending to the cloud servers (Jung, Mao, Li, Tang, Gong & Zhang, 2013), (Yang, Li, Liu & M, 2014). The data encryption comes with it the difficulty of searching the data on the cloud servers. (Cao, Wang, Li,Ren & Lou, 2014) Encryption comes with it many of other security apprehensions. Secure Sockets Layer is used by Google search to encrypt the connection be the authors the google server and search user.

Nevertheless, if the user clicks from the authors site of search result, to another the authors site will identify the search terms the user has used.

On dealing with the above matters, the searchable form of encryption (e.g., (Song,Wagner & Perrig, 2000), (Li,Xu,Kang,Yow & Xu, 2014), (Li,Lui,Dai,Luan & Shen, 2014)) has been established as a basic method to allow searching over encrypted data of cloud, which profits the procedures. At first the owner of data will produce quite a few keywords rendering to the outsourced data. Cloud server will be used to store this encrypted keywords. When the outsourced data needs to be accessed, it can choice approximately appropriate keywords and direct the cipher text of the designated keywords to the cloud server. The cloud server then usages the cipher text to contest the outsourced keywords which are encrypted, and finally will yields the matching consequences to the user who search. To attain the like search effectiveness and accuracy over data which is encrypted as like plaintext search of keyword, a widespread form of research has been advanced in literature. Wang et al.(2014) recommended a ranked keyword search system which deliberates the scores of relevance's of keywords. Inappropriately, because of using order-preserving encryption (OPE)(Boldyreva,Chenette, Lee & Oneill, 2009) to attain the property of ranking, the planned arrangement cannot attain unlikability of trapdoor.

Later, Sun et al.(Sun,Wang,Cao,Li,Lou,Hou & Li, 2013)suggested a multi-keyword text search arrangement which deliberates the scores of relevance's of the keywords and exploits a multidimensional tree method to realize the authors organized query of search. (J. Yu, P. Lu, Y. Zhu, G. Xue, & M. Li, 2013) suggested a multi-keyword top-k retrieval organization which practices fully homomorphic encryption to encrypt the index/trapdoor and assurances high security. Cao et al. (2014) suggested a multi-keyword ranked search (MRSE), which put on machine of coordinate as the matching of keyword rule, i.e., it will return the data with the maximum matching of keywords. Even though many of the functionalities of search have been advanced in former literature on the way to exact and the authors organized searchable encryption, it is still problematic for searchable encryption to attain the similar user involvement as that of the plaintext search, like Google search. This mostly attributes to subsequent two issues. At first, query with user favorites is popular in the search of plaintext (Liang, Cai,Huang,Shen, & Peng, 2012), (Mahmoud & Shen, 2012). It allows tailored search and can more precisely represent requirements of users, but has not been methodically studied and maintained in the encrypted domain of data. At second, to further improve the user's experience on searching, a significant and vital function is to allow the multi-keyword search with the comprehensive logic operations, i.e., the "AND", "OR" and "NO" operations of keywords. This is vital for search users to trim the space of searching and rapidly classify the anticipated data.

Cao et al. advise the coordinate matching search scheme (MRSE) which can be the authors as a searchable encryption system with "OR" operation (Shen,Liang, Shen,Lin, & Luo, 2014) recommended a conjunctive keyword search scheme which can be observed as a searchable encryption scheme with "AND" operation with the refunded documents matching all keywords. Though, most current suggestions can only allow search with single logic operation, somewhat than the mixture of numerous logic operations on keywords, which encourages the work.