KGRAM-BASED COMPOSITE SECRET SIGN SEARCH OVER ENCRYPTED CLOUD INFORMATION

Srinivasan.S[1], Sujith.L[2], Thummala Prasanth[3], Venkatesh.R[4], SELVA KUMAR.A[5]

B.E, (Computer Science and Engineering, T.J.S Engineering College, Tamilnadu, India.

ABSTRACT

A Large number of data owners have moved our data into cloud servers. Cloud data owners prefer to outsource documents in an encrypted form for the function of confidentiality preserving. Therefore it is essential to develop efficient and reliable cipher text search method. One challenge is that the relationship between documents will be normally concealed in the procedure of encryption, which will lead to major search accuracy performance degradation. All access the data from cloud by using the keyword based search. The secure multi-keyword ranked search from the encrypted data from the cloud, top-k search problem for big data encryption against privacy breaches, and attempt to identify an efficient and secure solution to this problem. It accessible operations like update, delete, insertion of documents. Here using tree structure and nebulous search method for retrieve the data from the cloud. These types of techniques are used to solve the problem of keyword guessing attack. The blowfish algorithm for the encryption process. We propose a group multi-keyword top-k search scheme based on the idea of partition, where a group of tree-based indexes are constructed for all documents. We combine these methods together into an efficient and secure approach to address our proposed top-k similarity search here to reduce statistical attacks. The extensive experimental results on real-life data sets demonstrate that our approach can significantly improve the capability of defending the privacy breaches, the scalability and the time efficiency of query processing over the state-of-the-art methods. It can achieve sub-linear search time and the search result like a number of file retrieval also deal with deletion and insertion of documents flexibly.

Keyword: - *Cloud Computing, Internet Protocol, JAVA, J2EE, JAVA Servlets, Modules, Testing, Use Case Diagrams, Net Beans, etc…*

1. INTRODUCTION

Cloud computing infrastructure is a promising new technology and greatly accelerates the development of large scale data storage, processing and distribution. However, security and privacy become major concerns when data owners outsource their private data onto public cloud servers that are not within their trusted management domains. To avoid information leakage, sensitive data have to be encrypted before uploading onto the cloud servers, which makes it a big challenge to support efficient keyword-based queries and rank the matching results on the encrypted data. Most current works only consider single keyword queries without appropriate ranking schemes. In the current multi-keyword ranked search approach, the keyword dictionary is static and cannot be extended easily when the number of keywords increases. Furthermore, it does not take the user behavior and keyword access frequency into account. For the query matching result which contains a large number of documents, the out-of-order ranking problem may occur. This makes it hard for the data consumer to find the subset that is most likely satisfying its requirements. In this paper, we propose a flexible multi-keyword query scheme, called MKQE to address the aforementioned drawbacks. MKQE greatly reduces the maintenance overhead during the keyword dictionary expansion. It takes keyword weights and user access history into consideration when generating the query result. Therefore, the documents that have higher access frequencies and that match closer to the users' access history get higher rankings in the matching result set.

1.1 Existing System

- The keyword-based information retrieval, which are widely, used on the plaintext data to the search from cloud server. A traditional way to reduce information leakage is data encryption.
- However, this will make server-side data utilization, such as searching on encrypted data, become a very challenging task. In the recent years, researchers have proposed many cipher text search schemes by incorporating the cryptography techniques.
- These methods need massive operations and have high time complexity. In this system have lot of security issues are there Keyword Guessing Attack will happened the hackers can easily guess the keyword than they can easily hack our content from cloud server.
- Existing search system will provide the result only based on the Boolean keyword matching system, it means weather it will find the exactly file name same as the keyword than the file will retrieved from the server, it won't provide any search result for misspelled keywords. And also the existing search system never provide the result based on similar keyword.

1.2 Objective

The Scope of my dissertation is to provide various types of search options for the users to retrieve the maximum number of file search from the encrypted data in the cloud. Here we can generate lots of keywords for each file using fuzzy search algorithms on uploading the file. While searching files, retrieve the maximum additional files by matching the corresponding generated fuzzy keywords with the file name of all files available in the cloud server. We can showcase the performance report of all these enhanced search mechanism by providing the statics based on different condition.

1.3 Contribution

In this system have lot of security issues are there Keyword Guessing Attack will happened the hackers can easily guess the keyword than they can easily hack our content from cloud server. Existing search system will provide the result only based on the Boolean keyword matching system, it means weather it will find the exactly file name same as the keyword than the file will retrieved from the server, it won't provide any search result for misspelled keywords. And also the existing search system never provide the result based on similar keyword

2. LITERATURE SURVEY

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. In this paper, we describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today. Cloud Storage is currently one of the most widely used applications of cloud. As usage of cloud is increasing, critical and personal data is also being outsourced making it important to maintain confidentiality and integrity of this data. A basic way of protecting data is encrypting it before outsourcing, but the retrieval of required files from the encrypted cloud becomes a problem which requires searching over the encrypted data. Various schemes have been proposed to deal with this issue of searching over encrypted cloud data, however none of the existent schemes provide optimum user search experience resembling plaintext search. In this paper we propose Privacy Preserving Synonym Based Fuzzy Multi-Keyword Ranked Search Over Encrypted Cloud Data, a scheme which enhances user search experience to a paramount by providing both fuzzy and synonym based multi-keyword ranked search, thereby taking encrypted search experience

closer to free text search engines. The scheme additionally improves upon index generation time and search time in comparison to existing schemes by utilizing a binary tree based dynamic index. Experimental results portray the effectiveness of this proposed scheme as it reduces the search time, i.e. the time for finding the desired documents, by 90% along with minimizing overhead of updating index when new files need to be uploaded (index generation time) as compared to the existing efficient indexing schemes in literature for a similar dataset. Optimization of search time together with index generation time has not been achieved to this extent before.

3. PROPOSED SYSTEM

- The competent search scheme to search the documents from the cloud server using multi-keyword. Here we using the nebulous keyword set it will create the all feasible misspell keywords.
- Search keyword get encrypt and it will check with the collection of original encrypted the file name in the cloud server if the keyword will get matched then we connect the nebulous keyword set for that particular keyword and it search the file list based on that nebulous keywords, it will retrieve the files from the cloud server and here we consider the searching performance also.
- Extensive experimental results on real-life data sets demonstrate that our proposed approach can significantly improve the capability of defending the privacy breaches, the scalability and the time efficiency of query processing over the state-of-the-art methods.

3.1 Advantages of Proposed System

- It take the keyword access frequencies into account when the system generates the ranked list of the returning results.
- The data owner can control the level of query unlink ability without sacrificing accuracy and better protect data privacy.

4. RESULT

Fig.No.1 Screenshot of the Project

Fig.No.2 Screenshot of the Project

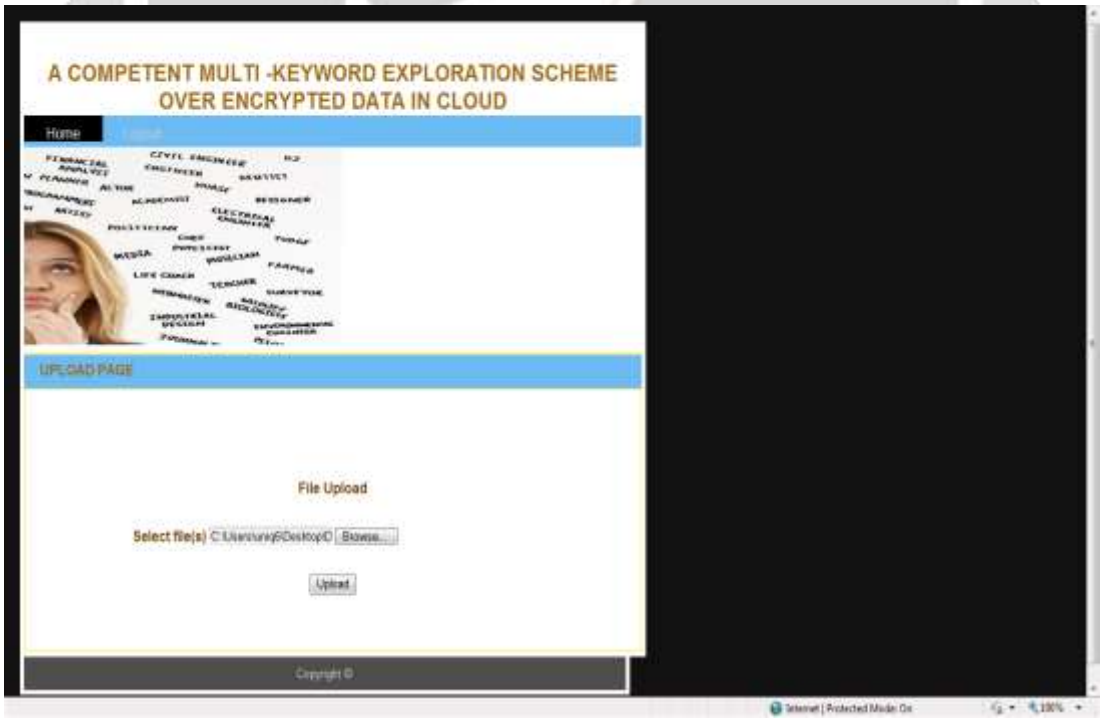

Fig.No.3 Screenshot of the Project

Fig.No.4 Screenshot of the Project

Fig.No.5 Screenshot of the Project

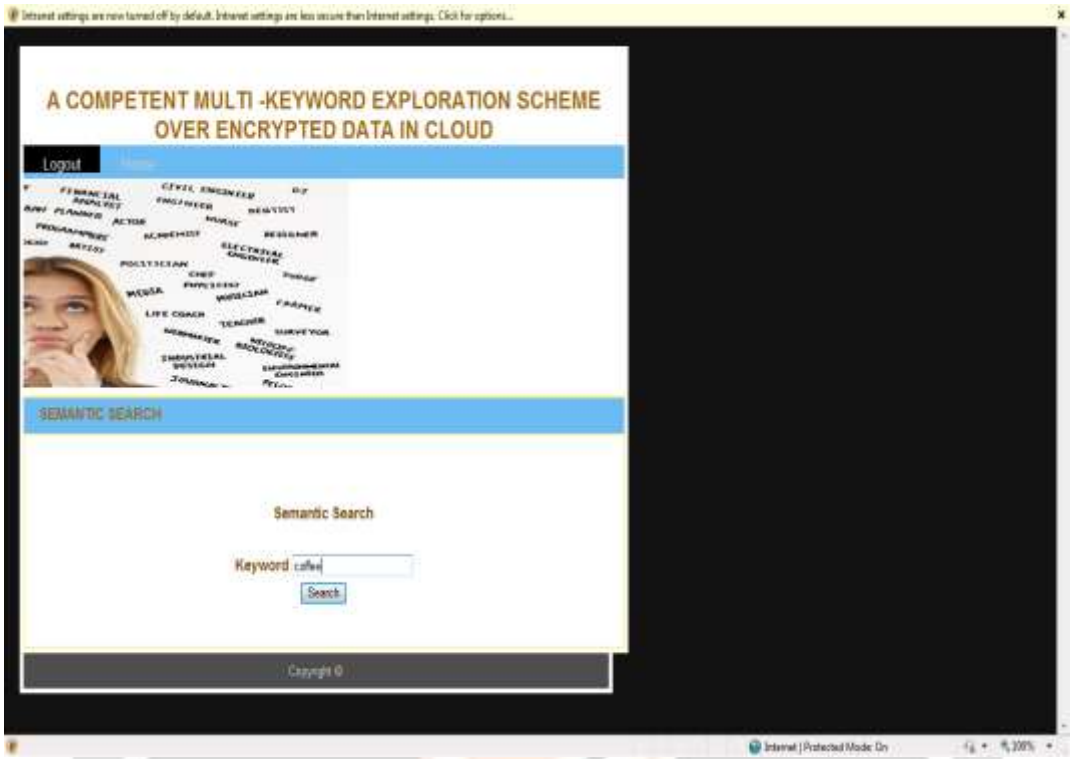

Fig.No.6 Screenshot of the Project

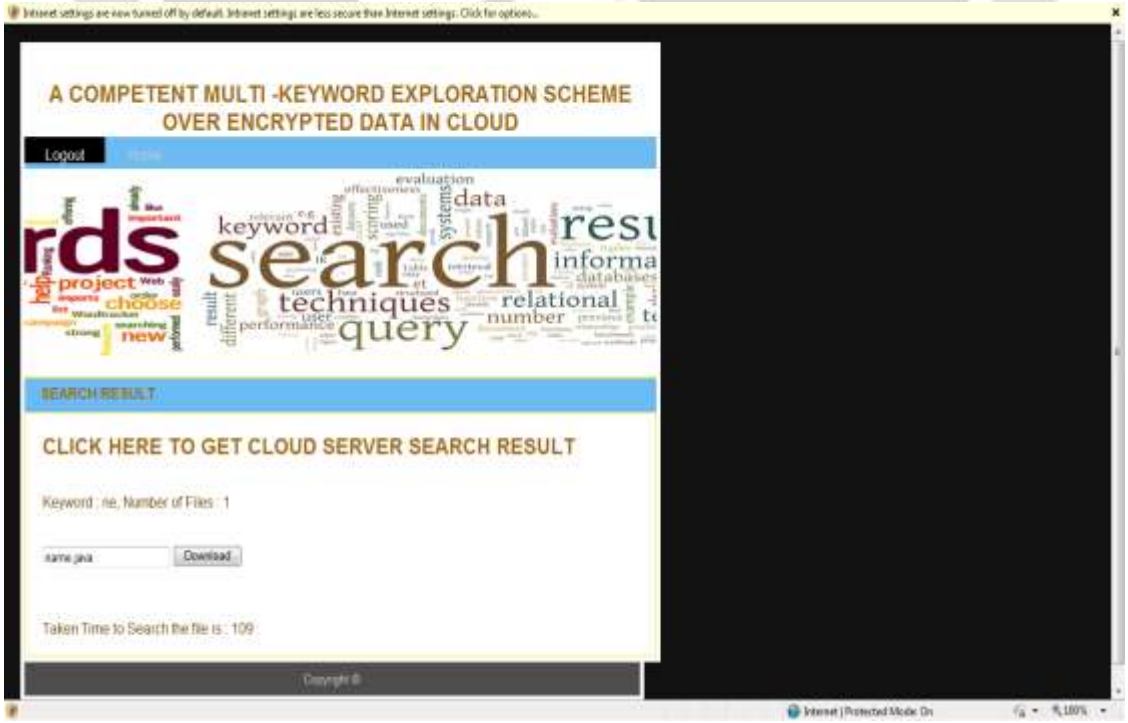

Fig.No.7 Screenshot of the Project

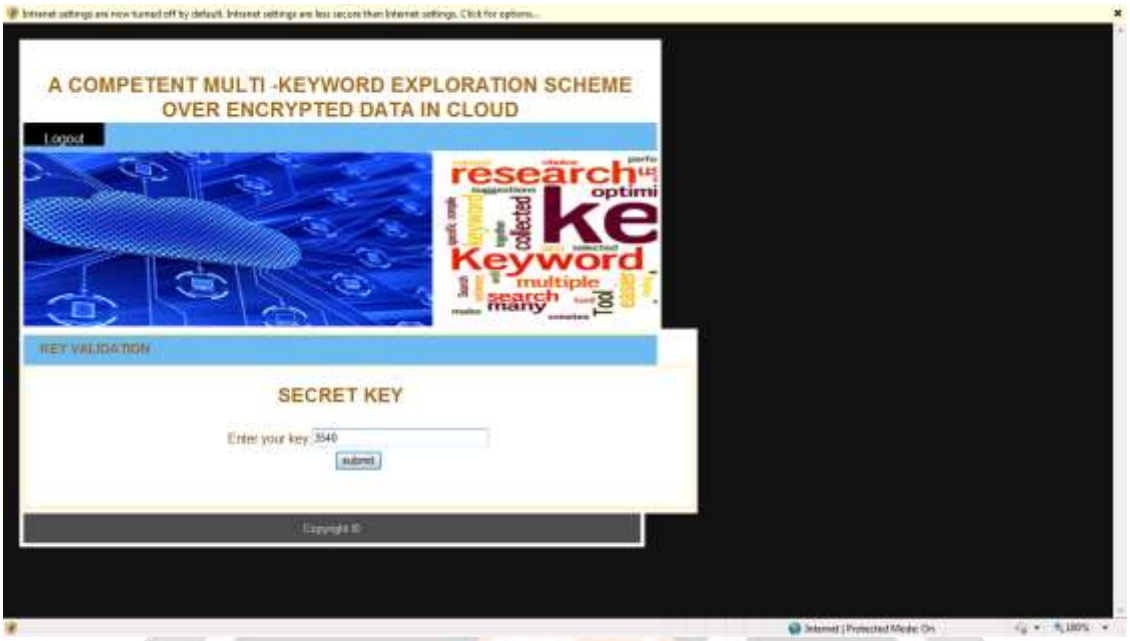

Fig.No.8 Screenshot of the Project

5. CONCLUSIONS

A secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. The cloud server traverses different paths on the index, and the data user receives different results but with the same high level of query accuracies in the meantime. The keyword-based search is such one widely used data operator in many database and information retrieval applications, and its traditional processing methods cannot be directly applied to encrypted data. Therefore, how to process such queries over encrypted data and at the same time guarantee data privacy. Then, in order to improve the search efficiency, we design the group multi-keyword top-*k* search scheme, which divides the dictionary into multiple groups and only needs to store In the sense no need to give exact filename to download the file, if you are going to give maximum number of time repeated words, that time also original file will be downloaded in decrypted format. This helps to maintain the security of the files in the cloud.

6. REFERENCES

1. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.
2. B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in IEEE International Conference on Computer Communications, 2014, pp. 2112–2120.
3. M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient similarity search over encrypted data,” in IEEE 28th International Conference on Data Engineering (ICDE), 2012, pp. 1156–1167.
4. C. Wang, K. Ren, S. Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity search over outsourced cloud data,” in 2012 Proceedings of IEEE INFOCOM, 2012, pp. 451–459.
5. C. Orencik, M. Kantarcioglu, and E. Savas, “A practical and secure multi-keyword search method over encrypted cloud data,” in IEEE Sixth International Conference on Cloud Computing (CLOUD), 2013, pp. 390–397.
6. M. Li, B. Lang, and J. Wang, “Compound concept semantic similarity calculation based on ontology and concept constitution features,” in Tools with Artificial Intelligence (ICTAI), 2015 IEEE 27th International Conference on, 2015, pp. 226–233.