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

Srishailam Agirishetty
M.Tech Student, Department of CSE, AVN Institute of Engineering & Technology, Telangana, India.

G Anitha
Associate Professor, Department of CSE, AVN Institute of Engineering & Technology, Telangana, India.

Dr. Shaik Abdul Nabi
Professor, Head of CSE Department, AVN Institute of Engineering & Technology, Telangana, India.

Abstract – In context of the building up comprehensiveness of scattered setting up, a routinely broadening number of data proprietors are engaged to outsource their data to cloud servers for astounding convenience and decreased cost in data affiliation. In any case, tricky data should be encoded before outsourcing for security necessities, which obsoletes data utilize like watchword based record recuperation. In this paper, we show an ensured multi-catchphrase orchestrated look devise over mixed cloud data, which in the meantime invigorates dynamic engage operations like cancelation and advancement of stories. We build up an exceptional tree-based record structure and propose a "Covetous Depth-first Search" computation to give productive multi-watchword masterminded scan for. The safe kNN figuring is utilized to scramble the chronicle and question vectors, and meanwhile ensure adjust tremendousness score estimation between encoded record and request vectors.

Index Terms – Multi-keyword ranked search over encrypted cloud data, OTP, Product resemblance, Cloud, Data owners.

1. INTRODUCTION

Cloud computing is a conversational phrase used to express a variety of dissimilar types of computing ideas that occupy large number of computers that are connected through a real-time communication network i.e Internet. In science, cloud computing is the capability to run a program on many linked computers at the same time. The fame of the term can be recognized to its use in advertising to sell hosted services in the sense of application service provisioning that run client server software on a remote location. Cloud computing relies on sharing of resources to attain consistency and financial system alike to a utility (like the electricity grid) over a network. The cloud also centers on maximize the effectiveness of the shared resources. Cloud resources are typically not only shared by multiple users but as well as dynamically re-allocated as per demand. This can perform for assigning resources to users in dissimilar time zones. This mechanism must take full advantage of the use of computing powers thus decreasing environmental damage as well, since less power, air conditioning and so on, is necessary for the same functions.

2. RELATED DATA

MULTI-KEYWORD RANKED SEARCH OVER ENCRYPTED (MRSE):

Now a day's cloud computing has become essential for many utilities, where cloud customers can slightly store their data into the cloud. Its huge suppleness and financial savings are attracting both persons and enterprise to outsource their local complex data management system into the cloud. To safe guard data privacy and struggle unwanted accesses in the cloud and away from, sensitive data, for example, emails, personal health records, photo albums, videos, land documents, financial transactions, and so on, may have to be encrypted by data holder before outsourcing to the business public cloud; on the other hand, obsoletes the traditional data use service based on plaintext keyword search. Furthermore, apart from eradicating the local storage management, storing data into the cloud supplies no purpose except they can be simply searched and operated. Thus, discovering privacy preserving and effective search service over encrypted cloud data is one of the supreme importance. Ranked search can also gracefully remove redundant network traffic by transferring the most relevant data, which is highly attractive in the "pay-as-you-use" cloud concept. For privacy protection, such ranking operation on the other hand, should not reveal any keyword to related information. To get better the search result exactness as well as to improve the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search often give up far too common results. And each keyword in the search demand is able to help narrow down the search result further. "Coordinate matching", as many matches as possible, is an efficient resemblance measure among such multi-keyword semantics to refine the result significance, and has been widely used in the plaintext information retrieval (IR) community. Encryption is a helpful method that treats encrypted data as documents and allows a user to securely search through a single keyword and get back documents of interest. On the other hand, direct application of

these approaches to the secure large scale cloud data utilization system would not be necessarily suitable, as they are developed as crypto primitives and cannot put up such high service-level needs like system usability, user searching experience, and easy information discovery. Even though some modern plans have been proposed to carry Boolean keyword search as an effort to improve the search flexibility, they are still not sufficient to provide users with satisfactory result ranking functionality. The solution for this problem is to secure ranked search over encrypted data but only for queries consisting of a single keyword. The challenging issue here is how to propose an efficient encrypted data search method that supports multi-keyword semantics without privacy violation. In this paper, we describe and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving exact system wise privacy in the cloud computing concept. Along with various multi keyword semantics, select the efficient resemblance measure of "coordinate matching," it means that as various matches as possible, to confine the significance of data documents to the search query. Particularly, inner product similarity the numbers of query keywords show in a document, to quantitatively calculate such similarity assess of that document to the search query. The search query is also illustrates as a binary vector where each bit means whether corresponding keyword appears in this search request, so the resemblance could be exactly calculated by the inner product of the query vector with the data vector. we propose a basic idea for the MRSE using secure inner product computation, which is modified from a secure knearest neighbour (kNN) method, and then give two considerably improved MRSE method in a step-by-step way to accomplish different severe privacy needs in two risk models with enlarged attack competence.

3. SYSTEM ARCHITECTURE

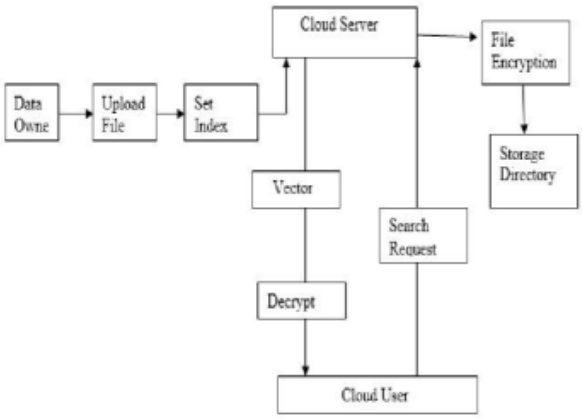

Fig. 1 Architecture diagram of the MRSE Implementation

In this technique the following are the different things which we have to implement

i) Cloud Setup

ii) Cryptography cloud Storage

iii) Vector Model

Cloud Setup Firstly, we have to setup data owner and cloud server. So the data owner will then push the data into the cloud servers. When users outsource their confidential data onto the cloud, the cloud service providers are capable to control and check the data and the communication between users and the cloud will be secured.

Cryptography cloud Storage Secondly, while the data is uploaded into the Estorage and retrieve services. Since data may have confidential information, the cloud servers cannot be fully hand over in protecting data. For this cause, outsourced files must be encrypted. Any kind of information leakage that would change data privacy are regarded as Unacceptable.

Vector Model We used a series of searchable symmetric encryption systems that have been allowing search on cipher text. In the earlier, files are ranked only by the number of get back keywords, which damage search correctness.

SYSTEM

The system model in this paper involves three different entities: data owner, data user and cloud server.

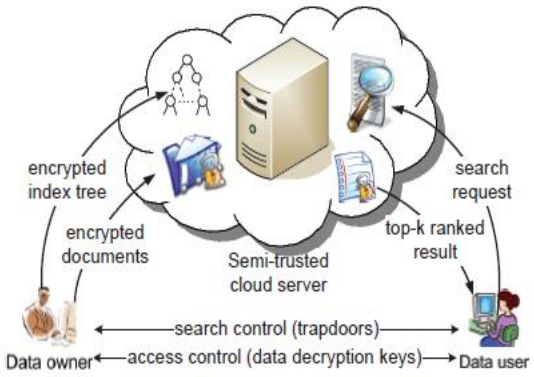

Fig. 2 system architecture

Data owner has a collection of documents F = {f1, f2, ..., fn} that he wants to outsource to the cloud server in encrypted form while still keeping the capability to search on them for effective utilization. In our scheme, the data owner firstly builds a secure searchable tree index I from document collection F, and then generates an encrypted document collection C for F. Afterwards, the data owner outsources the encrypted collection C and the secure index I to the cloud server, and securely distributes the key information of trapdoor generation (including keyword IDF values) and document decryption to the authorized data users. Besides, the data owner is responsible for the update operation of his documents stored in

the cloud server. While updating, the data owner generates the update information locally and sends it to the server.

Data users are authorized ones to access the documents of data owner. With t query keywords, the authorized user can generate a trapdoor TD according to search control mechanisms to fetch k encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key. Cloud server stores the encrypted document collection C and the encrypted searchable tree index I for data owner. Upon receiving the trapdoor TD from the data user, the cloud server executes search over the index tree I, and finally returns the corresponding collection of topk ranked encrypted documents. Besides, upon receiving the update information from the data owner, the server needs to update the index I and document collection C according to the received information.

The cloud server in the proposed scheme is considered as “honest-but-curious”, which is employed by lots of works on secure cloud data search. Specifically, the cloud server honestly and correctly executes search control (trapdoors) access control (data decryption keys) Semi-trusted cloud server encrypted index tree search request encrypted documents top-k ranked result.

4. CONCLUSION

This paper offers a sure, compelling and dynamic persecution plot that supports the correct search for several slogans and, furthermore, an extraordinary uprooting and a piano game plan. Let's compile a double balanced tree of unprecedented sentences as a summary and we propose a meaning of "Importance of the first attempt" to imply a change of affection rather than a direct interest. Additionally, you can run the parallel tracking process to reduce the cost of time. Chart security is guaranteed by two risk models that use the safe calculation of kNN. The exploratory results demonstrate the reasonableness of the proposed plot.

REFERENCES

[1] K. Ren, C.Wang, Q.Wang et al., "Security challenges for general society cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69– 73, 2012.

[2] C. Wang, N. Cao, K. Ren, and W. Lou, "Empowering secure and productive positioned watchword seek over outsourced cloud information," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467– 1479, 2012.

[3] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Protection saving multi-catchphrase content pursuit in the cloud supporting comparability based positioning," in Proceedings of the eighth ACM SIGSAC symposium on Information, PC and correspondences security. ACM, 2013, pp. 71– 82.

[4] C. Orencik, M. Kantarcioglu, and E. Savas, "A commonsense and secure multi-catchphrase look technique over encoded cloud information," in Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 390– 397.

[5] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure positioned multi-watchword scan for various information proprietors in distributed computing," in Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 2014, pp. 276–286.

[6] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic accessible symmetric encryption," in Proceedings of the 2012 ACM gathering on Computer and interchanges security. ACM, 2012, pp. 965– 976.

[7] S. Kamara and C. Papamanthou, "Parallel and dynamic accessible symmetric encryption," in Financial Cryptography and Data Security. Springer, 2013, pp. 258– 274.

[8] D. Money, S. Jarecki, C. Jutla, H. Krawczyk, M.- C. Ros¸u, and M. Steiner, "Exceptionally versatile accessible symmetric encryption with help for boolean questions," in Advances in Cryptology– CRYPTO 2013. Springer, 2013, pp. 353– 373.

[9] D. Money, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.- C. Rosu, and M. Steiner, "Dynamic accessible encryption in huge databases: Data structures and usage," in Proc. of NDSS, vol. 14, 2014.

[10] B. Gu and V. S. Sheng, "Attainability and limited union investigation for precise on-line - bolster vector learning," IEEE Transactions on Neural Networks and Learning Systems, vol. 24, no. 8, pp. 1304– 1315, 2013.