International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Dynamic Secure Multi-Keyword Ranked Search over Encrypted Cloud Data

Ramesh Polisetti, Chikram Sridhar, Chenagoni Nagaraju
Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Group of Institutions, Telangana, India

ABSTRACT

Over the past few years, Companies have been moving IT Resources to the cloud at a rapidly increasing rate. The data owners are commanded to outsource their data to cloud servers for amazing security and reduced expense in data management. However, sensitive content would be encrypted before outsourcing for security concerned, which obsoletes data employment like keyword-based document retrieval. In this paper, we solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) which simultaneously supports dynamic update operations like deletion and insertion of documents wise privacy in the cloud computing concept. As a result, allowing an encrypted cloud data search service is of extreme impact. In view of a large number of data users and documents in the cloud, it is essential to permit several keywords in the search demand and return documents in the order of their relevant to these keywords. Also, we propose an alert system which will generate alerts when the un-authorized user tries to access the data from the cloud, the alert will generate in the form of mail and message. And the ElGamal Cryptosystem allow users to occupy in the ranking while the popularity of computing work is done on the server side by a process only on cipher text which leads data leakage and convinced data security.

Keywords : Dynamic multi-keyword ranked search, inner product similarity, ElGamal Cryptosystem, top k retrieval

I. INTRODUCTION

Cloud computing is a model for empowering pervasive, cooperative, on-demand system access to a common pool of configurable computing assets (e.g. Networks, storage, applications, and services) that can be quickly provisioned and discharged with negligible services exertion or services provider collaboration. Cloud Computing implies a remote server that entrance through the web which helps in business applications and usefulness alongside the use of PC programming. Cloud computing spares cash that clients spend on yearly or month to month subscription. Because of favorable position of cloud administrations, more touchy data are being unified into the cloud servers, for

example, messages, individual wellbeing records, private recordings and photographs, organization account information, government reports, and so on. To secure information protection, secret information must be encrypted before outsourcing, in order to give end-to-end information privacy confirmation in the cloud. Furthermore, in Cloud Computing, Data Owners may impart their outsourced information to an expansive number of clients, who may need to just recover certain particular information records they are occupied with amid a given session. A standout amongst the most well-known approaches to doing as such is through watchword based pursuit. This catchphrase seeks system permits clients to specifically

recover records of interest and has been broadly connected in plaintext look situations. Sadly, information encryption, which limits client's capacity to perform a keyword search and further requests the security of catchphrase protection, makes the conventional plaintext hunt techniques fail down encrypted cloud information. Positioned seek incredibly enhances framework ease of use by ordinary coordinating records in a positioned request with respect to certain pertinence criteria (e.g., keyword frequency).

II. SYSTEM STUDY

2.1 Presented System:

Existing searchable encryption policies permit a client to safely search over encrypted information through keywords without first decoding it, these systems bolster just routine Boolean keyword search, without catching any pertinence of the records in the search result. At the point when specifically connected in vast community oriented information outsourcing cloud environment, they experience taking after prevention.

Drawbacks of existing system

1. Single-keyword searches without positioning
2.Boolean keyword searches without positioning
3. Single-keyword searches with positioning
4. Try not to get important information.

2.2 Proposed system

As our proposed framework we pick the rule of direction coordinating, to recognize the confidence between the search query and information records. Particularly, we utilize internal information correspondence, i.e., the quantity of query keywords showing up in a report, to assess the confidence of that archive to the search query in direction coordinating rule. Every record is linked to a parallel vector as a sub-list where every piece speaks to whether the comparing keyword is contained in the

document.[1] The search query is likewise depicted as a double vector where every piece implies whether the relating keyword shows up in this search demand, so the closeness could be precisely measured by the inward result of query vector with information vector.

1) Demonstrating the issue of Secured Multi-keyword search over scrambled cloud information

2) Propose two plans taking after the standard of direction coordinating and internal item similitude. Also, we proposed the ready framework which will create cautions when the un-approved client tries to get the information from the cloud, the ready will produce as mail and message. furthermore, the DES encryption permits clients to possess in the ranking while the prominence of registering work is done on the server side by the procedure just on figure content which drives information leakage and information security is guaranteed.

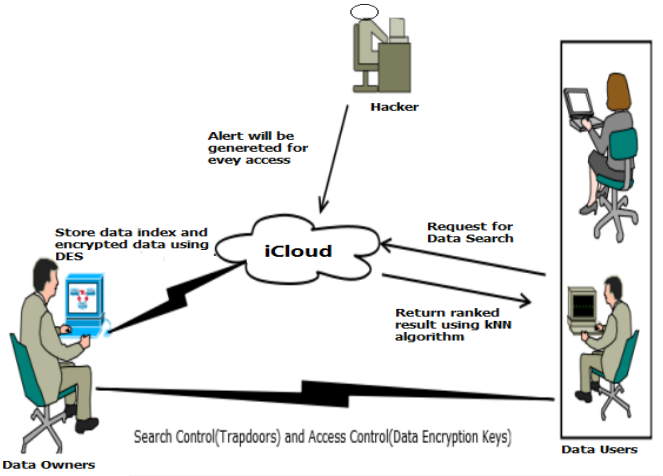

Figure 1. System Architecture for search over encrypted cloud data

Considering three unique substances, as represented in Fig1. Data owner, information client, and cloud server. Data owner has a gathering of information reports to be sent to the cloud server in the encoded group. To initiate the searching ability over encoded information, Data owner, before sending information will first form a scrambled searchable indication (record), and after that outsource both the list and the scrambled report gathering to a cloud server. To search the archive, an approved client require a relating trapdoor through search systems, After accepting from information clients, the cloud server is in charge of searching the record and giving back the comparing set of scrambled reports. To enhance archive recovery exactness, search result ought to be ranked by cloud server as indicated by some ranking criteria. Cloud server just sends back top-k records that are most applicable to the search query. In Fig1.There is each other substance is indicated i.e. Unapproved Client (Hacker). In the event that that unapproved client tries to get to any information from cloud then a ready will be produced as mail and message. The alarm is given to the approved individual who is a proprietor of that information.

III. SYSTEM IMPLEMENTATION

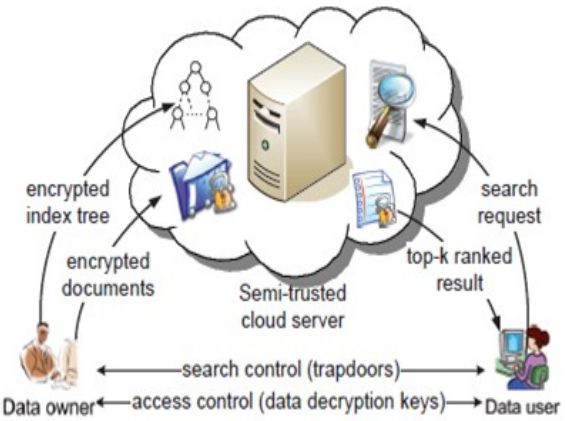

Figure 2. Architecture diagram of the MRSE Implementation

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 need to setup data owner and cloud server. So the data owner will then push the information to the cloud servers. At the point when clients outsource their classified information onto the cloud, the cloud service providers are equipped for controlling and checking the information and the correspondence amongst clients and the cloud will be secured.

Cryptography cloud Storage

Secondly, while information is transferred into the iCloud and recover administrations. Since information may have private data, the cloud servers can't be completely hand over in ensuring information. For this cause, outsourced documents must be scrambled. Any kind of data leakage that would change information protection is viewed as Unsuitable.

Vector Model

We utilized a progression of searchable symmetric encryption frameworks that have been permitting search on figure content. In the prior, records are ranked just by the quantity of getting back keywords, which harm search rightness.

IV. DESIGN GOALS AND SYSTEM FEATURES

1. Encryption Module This module is used to help the server to encrypt the document using DES Algorithm and to convert the encrypted document to the Zip file with an activation code and then activation code send to the user for download.

2. Multi-keyword Module This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after a search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list.

3. File upload Module This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on the flowchart. The admin can upload the file after the conversion of the Zip file format.

3.1 System Features

To activate ranked search for effective utilization of outsourced cloud data, our system design should simultaneously achieve security and performance guarantees as follows.

1. Secured Multi-keyword Ranked Search: To design search schemes which allow multi-keyword query and provide result similarity ranking for valuable data retrieval, instead of returning undifferentiated results.

2. Privacy: To prevent cloud server from learning additional information from dataset and index, and to meet privacy requirements.

3. The effectiveness with high performance: Above goals on functionality and privacy should be achieved with low communication and computation overhead.

V. ALGORITHMS USED

5.1 ElGamal Cryptosystem

ElGamal cryptosystem, called Elliptic Curve Variant, is based on the Discrete Logarithm Problem. It derives the strength from the assumption that the discrete logarithms cannot be found in the practical time frame for a given number, while the inverse operation of the power can be computed efficiently.

Generation of ElGamal Key Pair

Each user of ElGamal cryptosystem generates the key pair through as follows −

Choosing a large prime p. Generally, a prime number of 1024 to 2048 bits length is chosen.

Choosing a generator element g.

This number must be between 1 and p − 1, but cannot be any number.

It is a generator of the multiplicative group of integers modulo p. This means for every integer m coprime to p, there is an integer k such that gk=a mod n.

Choosing the private key. The private key x is any number bigger than 1 and smaller than p−1.

Computing part of the public key. The value y is computed from the parameters p, g and the private key x as follows −

y = gx mod p

Obtaining Public key. The ElGamal public key consists of the three parameters (p, g, y).

Encryption and Decryption

The generation of an ElGamal key pair is comparatively simpler than the equivalent process for

RSA. But the encryption and decryption are slightly more complex than RSA.

ElGamal Encryption

Suppose sender wishes to send a plaintext to someone whose ElGamal public key is (p, g, y), then Sender represents the plaintext as a series of numbers modulo p.

To encrypt the first plaintext P, which is represented as a number modulo p? The encryption process to obtain the ciphertext C is as follows −

Randomly generate a number k;

Compute two values C1 and C2, where −

C1 = gk mod p

C2 = (P*yk) mod p

Send the ciphertext C, consisting of the two separate values (C1, C2), sent together.

Referring to our ElGamal key generation example given above, the plaintext P = 13 is encrypted as follows −

Randomly generate a number, say k = 10

Compute the two values C1 and C2, where −

C1 = 610 mod 17

C2 = (13*710) mod 17 = 9

o Send the ciphertext C = (C1, C2) = (15, 9).

ElGamal Decryption

To decrypt the ciphertext (C1, C2) using private key x, the following two steps are taken −

Compute the modular inverse of (C1)x modulo p, which is (C1)-x , generally referred to as decryption factor.

Obtain the plaintext by using the following formula −

C2 × (C1)-x mod p = Plaintext

In our example, to decrypt the ciphertext C = (C1, C2) = (15, 9) using private key x = 5, the decryption factor is

15-5 mod 17 = 9

Extract plaintext P = (9 × 9) mod 17 = 13.

5.2. K-Nearest Neighbor

K-nearest neighbor search identifies the top k nearest neighbors to the query. This technique is commonly used in predictive analytics to estimate or classify a point based on the consensus of its neighbors.

K-nearest neighbor graphs are graphs in which every point is connected to its k nearest neighbors. The basic idea of our new algorithm: The value of dmax is decreased keeping step with the ongoing exact evaluation of the object similarity distance for the candidates. At the end of the step by step refinement, dmax reaches the optimal query range Ed and prevents the method from producing more candidates than necessary thus fulfilling the optimality criterion. Nearest Neighbor Search (q, k) // optimal algorithm

1. Initialize ranking = index.increm-ranking (F(q), df)
2. Initialize result = new sorted-list (key, object) 3. Initialize dmax = w
4. While o = ranking.getnext and d,(o, q) I d,,, do

5. If do@, s> s dmax then result.insert (d,(o, q) , o)
6. If result.length 2 k then dmax = result[k].key

VI. HYPOTHESES

1. Data Encryption and decryption Result When ElGamal Cryptosystem algorithm is applied on the data then we get encrypted data. And that encrypted data is stored in the cloud. The user can access the data after downloading and decrypting the file. For encryption and decryption keys are provided.

2. Ranking Result When any User request for the data then Ranking is done on requested data using the k-nearest neighbor algorithm. For ranking coordinate matching‖ principle is used. After ranking user gets the expected results of the query.

3. Alert System Results If any unauthorized User tries to access or updating the data in the cloud, then the alert will be generated in the form of mail and messages. The alert intimates the authorized user.

VII. CONCLUSION

Thus we proposed the problem of multiple-keyword ranked search over encrypted cloud data, and construct a variety of security requirements. From various multi-keyword concepts, we choose the efficient principle of coordinate matching. We first propose secure inner data computation. Also, we achieve effective ranking result using the k-nearest neighbor technique.

VIII. REFERENCES

[1]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829- 837, Apr 2011.

[2]. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M.Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50-55, 2009.

[3]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.

[4]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan. 2010.

[5]. A. Singhal, "Modern Information Retrieval: A Brief Overview," IEEE Data Eng. Bull., vol. 24, no. 4, pp. 35- 43, Mar. 2001.

[6]. I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.

[7]. D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

[8]. E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.

[9]. Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[10]. R. Curtmola, J.A. Garay, S. Kamara, and R.Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.