International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1590-1593 www.ijaem.net ISSN: 2395-5252

Multi-Keyword Search Over Encrypted Data in Hybrid Clouds by Using RSA

Miss Gauri A. Banore, Prof. A.A. Chinchamalatpure
ME Final year CSE, Dr. Sau. K.G.I.E.T. Amravati, Maharashtra
Prof, Dr. Sau. K.G.I.E.T. Amravati, Maharashtra

Submitted: 05-06-2022 Revised: 17-06-2022 Accepted: 20-06-2022

ABSTRACT—There is various type of algorithm which are going to be search, we encrypted metadata file, here we can propose a mechanism in which we can search a file by using the metadata technique. The metadata of the file will be present in to the encrypted form so searching the metadata into the encrypted form is quite typical, so we are proposed the mechanism in which the keyword, encrypted keyword-based search as well as the particular content-based search going to be workout. In proposed the hole application will evaluate encrypted metadata and will convert that or give the output with the index of the document as well.

IndexTerms—Hybrid cloud, multi-keyword ranked search, privacy-preserving, searchable encryption, RSA algorithm.

I. INTRODUCTION

The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before out-sourcing.[1] However, this will cause a huge cost in terms of data usability. For example, the existing techniques on keyword-based information retrieval, which are widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical. The secure RSA algorithm is utilized to encrypt the index and query vectors,[2] and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure,[3] the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

II. OBJECTIVE

To enable secure, efficient, accurate and dynamic multi-keyword ranked search over outsourced encrypted cloud data under the above models, our system has the following design goals. Dynamic. The proposed scheme is designed to provide not only multi-keyword query and accurate result ranking, but also dynamic update on document collections. Search efficiency. The scheme aims to achieve sublinear search efficiency by exploring a special tree-based index and an efficient search algorithm. Privacy-preserving the scheme is designed to prevent the cloud server from learning additional information about the document collection,[4][5] the index tree, and the query. The specific privacy requirements are summarized as follows,

1) Index confidentiality and query confidentiality. The underlying plaintext information, including keywords in the index and query, TF values of keywords stored in the index, and IDF values of query keywords, should be protected from cloud server;
2) Trapdoor unlink ability. The cloud server should not be able to determine whether two encrypted queries (trapdoors) are generated from the same search request;
3) Keyword privacy. The cloud server could not identify the specific keyword in query, index or document collection by analyzing the statistical information like term frequency. Note that our proposed scheme is not designed to protect access pattern, i.e., the sequence of returned documents.
4) Index Encryption: in this to achieve the level of security proposed methodology finds the required data index and perform the index encryption.

III. PROBLEM DEFINITION

In existing the challenge problems in symmetric SE schemes. In the proposed scheme, the data owner is responsible for generating updating

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1590-1593 www.ijaem.net ISSN: 2395-5252

information and sending them to the cloud server. Thus, the data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values.[6][7] Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. In addition, as the most of works about searchable encryption, our scheme mainly considers the challenge from the cloud server.

IV. PROPOSED WORK

In existing there is very effectively the techniques of data updating are utilizing but there is a big problem in working with sharing keys and decrypted data with other users which may disturb the security as well in this an unencrypted index key is used for ranking which may break security as well[8]. so that we proposed a mechanism inwhichthe encrypted index term key will get generated and perform the evaluation for the multi-keyword searching in all encrypted cloud storage.

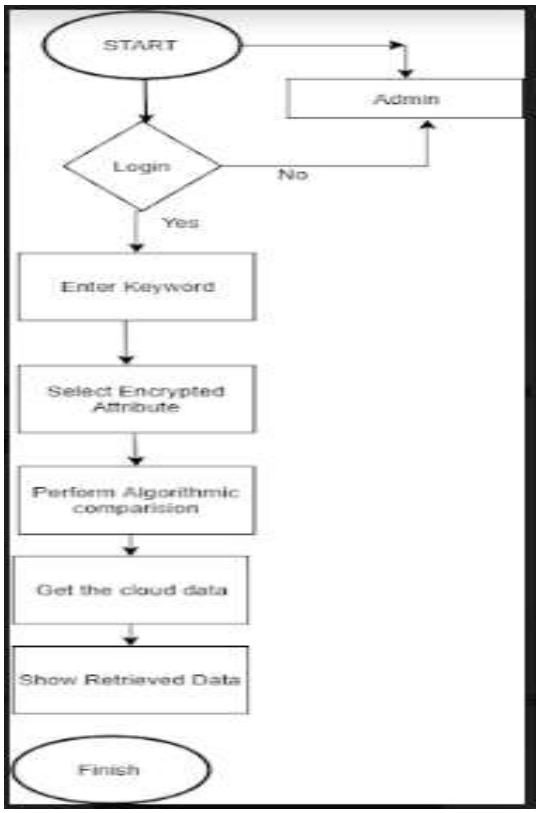

Fig.Flow of Proposed Work

V. IMPLEMENTATION

The definition-use chain method was used in this type of testing. These were particularly useful in nested statements. In this type of testing all the loops are tested to all the limits possible. In this part of the testing each of the conditions were tested to both true and false aspects. And all the resulting paths were tested. So that each path that may be generated on particular condition is traced to uncover any possible errors.[9][10] This type of testing selects the path of the program according to the location of definition and use of variables. This kind of testing was used only when some local variables were declared.

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

1.Key-Generation

I. Choose two distinct prime numbers p and q.

II. Find n such that n = pq.
n will be used as the modulus for both the public and private keys.

III. Find the totient of n,$\phi(n)$
$\phi(n)=(p-1)(q-1)$

IV. Choose an e such that $1 < e < \phi(n)$,
and such that e and $\phi(n)$ share no divisors other than 1 (e and $\phi(n)$ are relatively prime).e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation
$de \equiv 1 \pmod{\phi(n)}$.
In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or $\phi(n)$. This is often computed using the Extended Euclidean Algorithm, since e and $\phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e.
d is kept as the private key exponent. The public key has modulus n and the public (or encryption) exponent e.
The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption

I. Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.
II. When Person B wishes to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.
III. Person B computes, with Person A's public key information, the ciphertext c corresponding to c

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1590-1593 www.ijaem.net ISSN: 2395-5252

$\equiv m^e \pmod n$.

IV. Person B now sends message "M" in ciphertext, or c, to Person A.

3. Decryption

I. Person A recovers m from c by using his/her private key exponent, d, by the computation $m \equiv c^d \pmod n$.

II. Given m, Person A can recover the original message "M" by reversing the padding scheme.

This procedure works since,
$c \equiv m^e \pmod n$,
$c^d \equiv (m^e)^d \pmod n$,
$c^d \equiv m^{de} \pmod n$.
By the symmetry property of mods,
We have that
$m^{de} \equiv m^{de} \pmod n$.
Since $de = 1 + k\phi(n)$,
we can write,

$m^{de} \equiv m^{1+k\phi(n)} \pmod n$,
$m^{de} \equiv m(m^k)^{\phi(n)} \pmod n$,
$m^{de} \equiv m \pmod n$.

VI. ENCRYPTION ARCHITECTURE

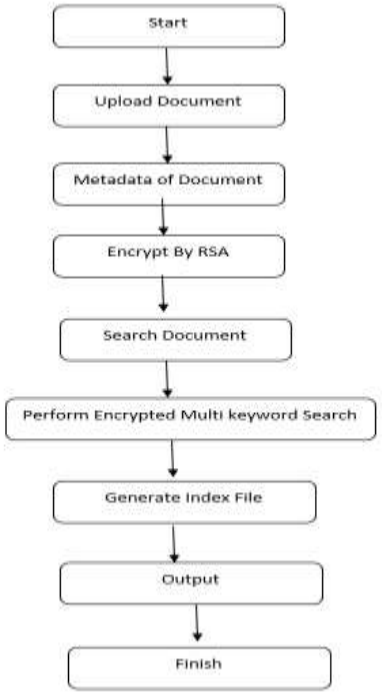

Fig. Block Diagram of Encrypted Multi keyword search by using RSA.

VII. RESULT ANALYSIS

There are multiple documents uploaded with the keywords, we are performing the operations using GDFS, kNN, RSA.
In GDFS, after searching Then we apply edge weightage, then apply indexing and get the final index.
In kNN, after searching, calculate the distance then sort the indices then select the top keyword then apply filtrations and get the final index.
In RSA,after searching, apply keyword weightage then extract the metadata then apply content extraction then indexing by document size after that indexing by content then get the final index.

Fig. Chart of Indexing

VIII. ADVANTAGES

1. Proposed mechanism will help to find the encrypted multi-keyword
2. Proposed system will perform keyword base encryption
3. Proposed system will help to perform content-based search approach
4. Proposed system helps to index the files

IX. FUTURE SCOPE

A secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. In proposed mechanism the system will search and give a better acknowledgement of search document. In this the search document stored with integrated mechanism in which the encrypted keyword-based document searching efficiency can be improved so that the proposed mechanism will helps to get keyword-based searching over encrypted data. In future the mechanism can be improved with high level search mechanism so that the proposed system can be help.

X. CONCLUSION

In the proposed scheme, the data owner is responsible for generating updating information and sending them to the cloud server. Thus, the data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search.

REFERENCES

[1]. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Compute., vol. 16, no. 1, pp. 69–73, Jan-Feb. 2012.
[2]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Finance. Cryptography Data Secure., 2010, pp. 136–149.
[3]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2009.
[4]. O. Gold Reich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996.
[5]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Adv. Crypto l.-Euro-crypt, 2004, pp. 506–522.
[6]. D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Proc. Adv. Crypto l., 2007, pp. 50–67.
[7]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secure. Privacy, 2000, pp. 44–55.
[8]. E.-J. Goh, "Secure indexes," IACR Crypto l. E-Print Archive, vol. 2003, p. 216, 2003.
[9]. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Secure., 2005, pp. 442–455.
[10]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE Proc. INFOCOM, 2010, pp. 1–5.