ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Secure and Dynamic Search Scheme over Encrypted Cloud Data Using Fuzzy Logic

Sushant Lokhande [1], Akshaykumar Dhawale [2], Shivali Shinde [3], Anuja Pandit [4], Prof Swati Khodke[5]

B.E. Student, Dept. of Computer Engineering, JSPMS BSIOTR, Wagholi Pune, India[1,2,3,4]

Assistant Professor, Dept. of Computer Engineering, JSPMS BSIOTR, Wagholi Pune, India[5]

ABSTRACT: With the appearance of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to fetch this data. For privacy concerns, secure searches over encrypted cloud data have inspired several research works under the single owner mode. In this project, we propose schemes to deal with Privacy preserving to enable cloud servers to perform secure search without knowing the actual data of both key-words and trapdoors. In this project we introduce idea of improving accessibility of Cloud using if the concept of Fuzzy, we have tried to present a model for evaluating users fulfillment in cloud computing.

KEYWORDS: Several owners, Cloud computing, Fuzzy logic, Data Privacy;

I. INTRODUCTION

Cloud storage is used for storing the data. Cloud storage stores the large amount of data and it stores data for long time. It is a model of data storage in which the digital data is stored in logical pools. The physical storage requires multiple servers is typically owned and managed by hosting company. The cloud storage providers are responsible for keeping the data available and accessible whenever it is required and also physical environment protected and running. Organizations and peoples lease or buy storage capacity from the providers to store organizations, users, or applications data.

To provide a search we are going to enter the word. By using this word we are going to search the files which contain this word. To protect from disclosing the result we propose a novel dynamic secret key generation protocol and a new data user authentication rule. The main contributions of this paper are listed as, We supervise experiments on real-world Datasets to verify the effectiveness and capability our suggest schemes. In this paper we are also going to generate the graph related to the file search with the time required for search.

II. RELATED WORK

In[1]Author the ability of preferentially sharing encrypted data with unlike users through public cloud storage might really ease security distress by possibility data disclose in the cloud. A key test to design such encryption idea lies in the well -organized management encryption keys. The preferred flexibility of allocating any group documents with any group of users by attaining weight age different encryption keys to be used for different documents. On the other hand , this involves the need of securely distributing to users by a large number of keys for both encryption and search, and those users have to progress to store the received keys. The in-direct need for secure communication, storage, and complexity clearly cause the unreasonable approach In this paper, we concentrate on this practical problem, by suggesting the novel concept of key aggregate searchable encryption (KASE) and instantiating the idea through a real KASE scheme, in which a data owner wants to share out a single key to a user for distributing a large number of documents, and the user needs to present a single trapdoor to the cloud for questioning the shared documents.[2] We study the setting in which a user stores encrypted documents (e.g. e-mails) on an un-trusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Work in this area has largely focused on search criteria consisting of a single keyword. If the user is actually interested in documents containing each of several keywords (conjunctive keyword search) the user must either give the server capabilities for each of the keywords individually and rely on an intersection calculation (by either the server or the user) to determine the correct set of documents, or alternatively, the user may store additional information on the server to facilitate such searches [4] Public-key encryption with keyword search is a versatile tool. It allows a third party knowing the search trapdoor of a keyword to search encrypted documents containing that keyword without decrypting the documents or knowing the keyword. However, it is shown that the keyword will be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is in a polynomial size. We address this problem with a keyword privacy enhanced variant of PEKS referred to as public-key encryption with fuzzy keyword search. In PEFKS, each keyword corresponds to an exact keyword search trapdoor and a fuzzy keyword search trapdoor.

III. ARCHITECTURE

Implementation Details:
We now describe the design of our proposed work, which considers multiple data owner, multiple data users, application server and semi trusted cloud storage.

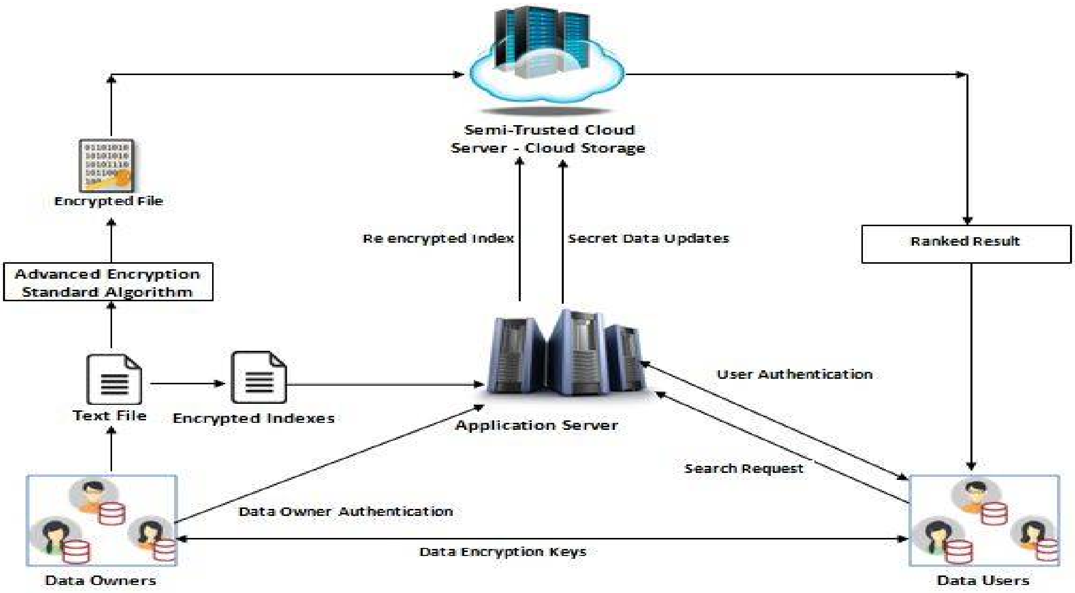

Fig 1. System Architecture

In this application data owners are responsible for encryption of the file and upload encrypted file to cloud storage with the index of file. Data users are responsible for the file which he requires it sends request for file and getting a key in response to request. By using this key data user decrypt this file and get plain text file which he require. Application server Application server again encrypt the index file of authenticated user and send that re-encrypted file to the cloud server. Define a multi-owner model for privacy preserving keyword search over encrypted cloud data. We systematically construct a secure search, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords. but also allows data owners to encrypt keywords with self-chosen keys and allows valid data users to query without knowing these keys. This system provides Efficient multiple keyword searching by using fuzzy logic.

Advantages:
: Not depend upon the static keywords set.
: Extra Authorization for the Data User and Data Owner
: Sharing security key with only designated Data User.
: Performance is better then Earlier systems.
: Secure search .
: Quick search of multiple keywords

IV. ALGORITHM

ECC : Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods.
1.select the file type then select plain text from the file
2.After selecting file select the output file
3.After selecting output file check if file compress or not
4.if the file compress then check the plain text is converted to cypertext or not(encrypted file)
5.if text in file are hidden or converted to cypertext then encryption is successful.
6.for retrieving encrypted, hidden, compressed message select the output file for retrieving output file enter key or password.

Key generation:-
parameters (q, FR, a, b, G, n, h).
1. Select a random number d, $d \in [1, n - 1]$
2. Compare Q = dG.
3. public key is Q and private key is d.

A public key Q = (xq, yq) associated with the domain parameters (q, FR, a, b, G, n, h) is validated using the following procedure
1. Check that $Q \neq O$
2. Check that xq and yq are properly represented elements of Fq
3. Check if Q lies on the elliptic curve defined by a and b.
4. Check that nQ = O

N-Gram Algorithm:
We are using N-GRAM Algo for searching keywords presents in file. It is actually perform on keyword search using scanning of all character in file on gram level. we are seprate each character on 1^{ST} level then compare each character with our keyword .this procedure is repeat until we are reaching n-level .After reaching n level we are achieving the result releted with our keyword(search result). Fuzzy Query is used to search documents using fuzzy implementation that is an approximate search based on edit distance algorithm.
We can implement fuzzy query by using two fuzzy algorithm:

Levenstein Algorithm.
s=string.
D=distance value.
T=threshold distance
S= (s1,s2,s3 ....)
Set of strings.
Input = (s1,s2,.. sn)
For all strings calculate D
All Ds of S which are less than T.
Return to user.

V. CONCLUSION

In this project, we explore the problem of secure search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data.

REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", *Proc. 13th ACM Conf. Comput. Commun. Security*, pp. 79-88, Oct. 2006.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren and W. Lou, "Privacy-preserving public auditing for secure cloud storage", *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[3] D. Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data", *Proc. IEEE Int. Symp. Security Privacy*, pp. 44-55, Jan. 2000.

[4] 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.

[5] M. Armbrust, , A, . Fox, , R, . Griffith, , A, et al., "A view of cloud computing", *Commun. ACM*, vol. 53, no. 4, pp. 50-58, 2010.

[6] "Public key encryption with keyword search", *Advances in Cryptology-Eurocrypt 2004*, pp. 506-522, 2004.

[7] C. Wang, N. Cao, J. Li, K. Ren and W. Lou, "Secure ranked keyword search over encrypted cloud data", *Proc. IEEE Distrib. Comput. Syst.*, pp. 253-262, Jun. 2010.

[8] Z. Xu, W. Kang, R. Li, K. Yow and C. Xu, "Efficient multi-keyword ranked query on encrypted data in the cloud", *Proc. IEEE 19th Int. Conf. Parallel Distrib. Syst.*, pp. 244-251, Dec. 2012.

[9] M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data", *Proc. IEEE 31th Int. Conf. Distrib. Comput. Syst.*, pp. 383-392, Jun. 2011.

[10] P. Golle, J. Staddon and B. Waters, "Secure conjunctive keyword search over encrypted data", *Proc. Appl. Cryptography Netw. Security*, pp. 31-45, Jun. 2004.

[11] L. Ballard, S. Kamara and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data", *Proc. Inf. Commun. Security*, pp. 414-426, Dec. 2005.

[12] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data", *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222-233, Jan. 2014.

[13] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, et al., "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking", *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 3025-3035, Nov. 2014.

[14]K. Ren, C.Wang, Q.Wang *et al.*, “Security challenges for the public cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[15] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.

[16] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[17] O. Goldreich and R. Ostrovsky, “Software protection and simulation on oblivious rams,” *Journal of the ACM (JACM)*, vol. 43, no. 3,pp. 431–473, 1996.