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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Secure Cloud Computing and Fuzzy Search for Multiple Data Owner and Data User

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: Cloud computing is a subversive technology that is changing the way IT hardware and software are designed and purchased. As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment and flexible resource management, etc. Enterprises of all sizes can leverage the cloud to increase innovation and collaboration.In this project, we propose schemes to deal with Privacy or security to enable cloud servers to perform secure search without knowing the actual data of both key-words. 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.

Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records and government confidential files, to the cloud. This is because once sensitive data are outsourced to a remote cloud, the corresponding data owners lose direct control of these data . Cloud service providers wouldpromise to ensure owners' data security using mechanisms like virtualization and firewalls.To apply the searchable encryption to cloud computing, some researchers have been studying further on how to search over encrypted cloud data efficiently. Li et al. [9] firstly proposed a fuzzy keyword search scheme over encrypted cloud data, which combines edit distance with wildcard-based technique to construct fuzzy keyword sets, to address problems of minor typos and format inconsistence.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II.RELATEDWORK

This paper is organized in the following section. Section IV will describe the proposed algorithm, the working of it with the help of mathematical model, Section VI show the result that how efficiently the data is searched over the cloud using the proposed algorithm. Finally conclusion and future work is described in Section VII.

III. IMPLEMENTATION

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.

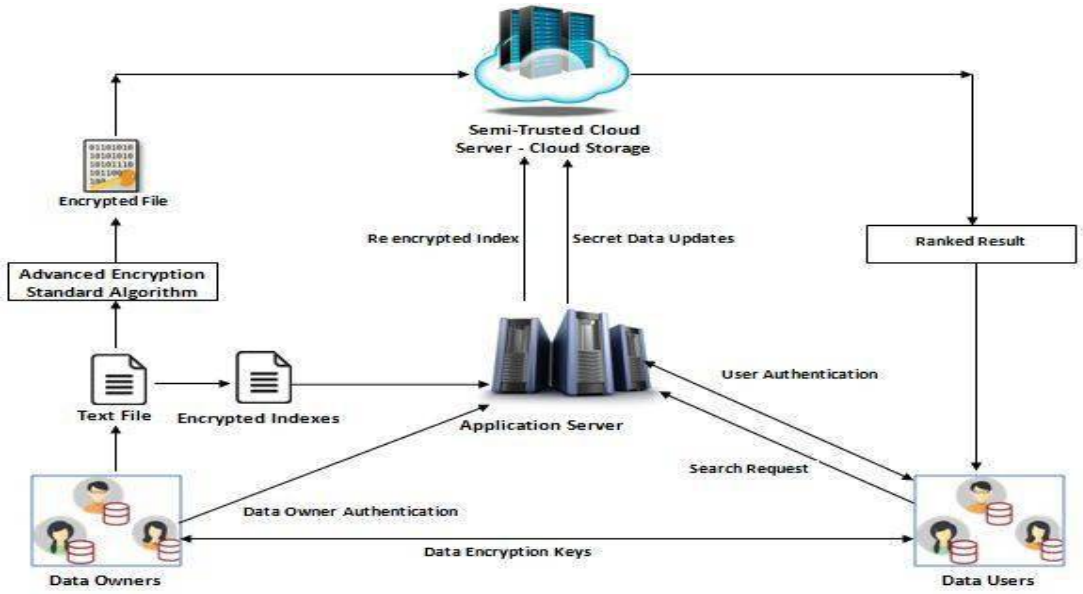

Fig 1. System Architecture

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 thenEarlier systems.
: Secure search .
: Quick search of multiple keywords

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

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 Pseduo code:-

parameters (q, FR, a, b, G, n, h).
1. Select a random number d, d ∈ [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:

Algorithms=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. MATHEMATICAL MODEL

System = S;
S = {I, P, O}
Input = InputP = Processing
I = {F, Ind, K}
F = Plain text Files I=Input
O = Output
Ind = Index File created from the Plain text file
K = K is the set of keywords / trapdoors, which will be used to find the Files.
O = {R_F, F}

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

R_F = Rankfor the files
F = Searched Files from encrypted data.

P = {O,F,C,W,T}

O: the data owner collection, denoted as a set of *m* data owners
O = (*O*1,*O*2, . . . ,*Om*).
Fi : the plaintext file collection of *Oi*, denoted as a set of *n* data file
Fi=(*Fi;*1, *Fi;*2,. . . ,*Fi;n*).

Ci: the ciphertext file collection of *Fi*, denoted as
Ci=(*Ci;*1, *Ci;*2,. . . ,*Ci;n*).
W: the keyword collection, denoted as a set of *u* keywords
W = (*w*1,*w*2, . . . ,*wu*).
Wi: *Oi*'s encrypted keyword collection of *W*, denoted as
Wi = (b*wi;*1, b*wi;*2, . . . , b*wi;u*).
f*W*: the subset of *W* which represents queried keywords, denoted as
f*W*= (*w*1,*w*2, . . . ,*wq*).
• *T*f*W*: the trapdoor for f*W*, denoted as
*T*f*W*= (*Tw*1 , *Tw*2 , . . . , *Twq*).
• *Si;j;t*: the relevance score of *t*th keyword to *j*th file of *i*th data owner.

V. STIMULATION RESULT

Fig 6.1 represents the result of the cloud data search file searching take less than 10seconds.System provide multiple security using cipher text key for avoiding hacking. It provide multiple file uploading and downloading.

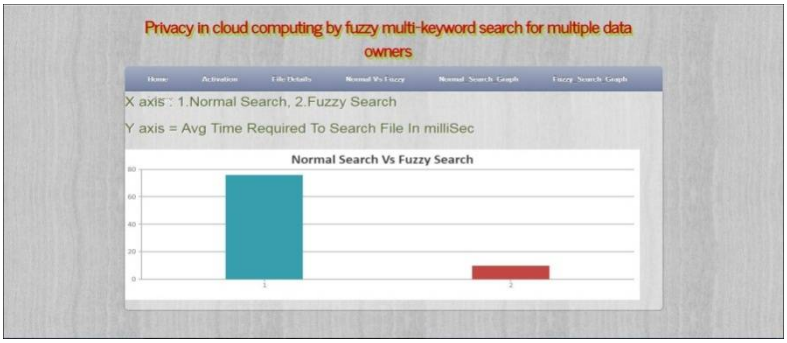

Fig 6.1 Result of cloud data search

VI. CONCLUSION AND FUTURE WORK

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. In this project, we propose schemes to deal with Privacy or security to enable cloud servers to perform secure search without knowing the actual data of both key-word. If users increases in the future then also performance of the system will not decreases.

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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

[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. IEEEINFOCOM*, 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.ParallelDistrib. 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]HarshaliAnantAgutale,`` A Survey and Security Analysis on One-To-Many Order Preserving Technique on Cloud Data",International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 11
[11]C.Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data,"IEEETrans.ParallelDistrib.Syst., vol.23, no.8, pp. 1467-1479, Aug. 2012.
[12]A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data :Zhihua Xia, Member, IEEE, XinhuiWang,Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE, 2015
[13]N Cao, C. Wang, M. Li,K.Ren, and W. Lou, "Privacy preserving keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol, 25, no. 1, pp. 222-223, Jan. 2014.
[14]L. Xiao, I.-L Yen, "Security analysis for order preserving encryption schemes," *Proc. of 46th Annual Conference on Information Sciences and System*, pp. 1-6, 2012.
[16]DhamaleSwapnali ,BagulSonali , DhadgeMadhuri , GaradPriyanka, Prof. Sonali A. Patil,`` A Survey on Efficient Data Integrity Checking with Group User Revocation in Cloud " IJIRCCE Vol.4,Issues 9,September 2016