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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Cloud Security with Multi-Keyword Search Over Encrypted Data with Multiple Data Owners

Prof.S. S. Dixit[1], Suvena Shetty[2], Akash Takale[2], Mugdha Ambatkar[2], Tanmay Tripathi[2]

HOD, Department of Information Technology, PVG's COET, Pune, Maharashtra, India[1]

B. E Student, Department of Information Technology, PVG's COET, Pune, Maharashtra, India[2]

ABSTRACT: In a cloud computing system we are developed the system providing security for information. In this system, data owner can upload different file using AES algorithm in the encrypted format for maintaining the security. For protection concerns, secure ventures over encrypted cloud information have motivated a few research works under the single owner model. In our system we developed this system for multiple owners' model with different functionality. In this system, we propose plans to tree based ranked multi-keyword search scheme for multiple data owners (TBMSM), to efficiently develop novel search protocol based on bilinear pairing, which enables different data owners to use different keys to encrypt their keywords and trapdoors. In cloud server module, view all users, data owners and all encrypted file also. User also view attacker of the system. Datauser can search over encrypted data using hash value md5 algorithm. Data Users can also fuzzy keyword algorithm search technique also used moreover; User can download file at particular place only as well as at particular times only.

KEYWORDS: Attacker System,Cloud Computing, Data Owner, MultiKeyword Search, Fuzzy keyword Search

I. INTRODUCTION

Encryption on sensitive data before outsourcing can preserve data privacy. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem.The category of search function, including secure ranked multi-keyword search, and similarity search. A different data owner can upload this any filein a encrypted format then encrypted index is generated. This encrypted index goes to administrator system.Different data owners can upload files on a cloud so for every file is stored in encrypted format.Whern user can search that file with different searching techniques like fuzzy keyword search,Hash value search and multukeyword search.Data owners uploaded file store on a cloud server An answer for this issue is to download all the hidden information and make the first information utilizing the hidden key, yet this is not practical cause it make additional overhead In this paper, Data owner can file upload in different file in encrypted format using AES 128 bit or 192 bit or 256 bit. When user can search any file then after checking authentication user get file.If user want to download that file then data user request to data owner.After getting the request user can send the key for download the file. hence , propose when user search keywords that time give the security and demonstrate the bring about positioning structure to make simple cloud servers to perform safe excluding knowing the real value of both keywords and trapdoors, We proposed fuzzy keyword search, using this we can easily search the information. We also introduced any file can download from particular location only.Also find out attacker of system if any user enter 3 time wrong key.

II. LITERATURE SURVEY

H. Li, et al.[1] Introduced concept is to refer address this issue by developing the fine-grained multi-keyword search schemes over encrypted cloud. The proposed plan can bolster confounded rationale look through the blended "AND",

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

"OR" and "NO" tasks of catchphrases. The upgraded plans supporting grouped sub-lexicons (FMSCS) to enhance proficiency. Disadvantage of this system is to develop the highly scalable searchable encryption to enable efficient search on large practical databases.

W. Zhanget al.[2] proposing schemes to deal with secure ranked multi-keyword search in a multi-owner model. To rank the search results and preserve the privacy of relevance scores between keywords and files, propose a novel Additive Order and Privacy Preserving Proposed. Construct a novel secure search protocol for trapdoor and index. Disadvantage of this system approach is not computationally efficient even for large data set and keyword set.

J. Li et al.[3]for study of formalize and provide solution of the problem of effective fuzzy keyword search over encrypted cloud data as well as preserving keyword privacy. To generate an advanced technique (i.e., wildcard-based technique) to construct the storage-efficient fuzzy keyword sets by exploiting a significant observation on the similarity metric of edit distance. Drawback of this system is to develop the highly scalable searchable encryption to enable efficient search on large practical databases.

SofianeMounineHemamet al.[4] is proposed the load balancing between volunteer nodes that provide the cloud services. Chooses and erases the reproductions of a cloud benefit without corruption of the heap adjusting, utilizing for this the Markov Chain Models. How to handle large amount of data approach is not computationally efficient even for large data set and keyword set.

M. Armbrustet al.[5] Study about all information about cloud computing. We got all kind of information of cloud computing. Different applications passed as services over the Internet and the and software systems hardware in the data centres that provide those services over Cloud Computing. We got information of different kind of web services as well as where a cloud computing are used. Necessary of cloud computing in a real time applications. We also know information about the risk in cloud computing, different classes of utility in in cloud computing and also we got cost estimate of cloud to deployed.

D. Song et al[6] study about framework which describes cryptographic schemes for the problem of searching on encrypted data. It additionally gives evidences of security to the subsequent crypto frameworks. This plan is provably secure for remote seeking on scrambled information utilizing an untrusted server. This framework seeks information remotely from untrusted server. This framework gives the evidences of security that required for crypto frameworks. This framework worked proficiently for question segregation as they are basic and quick. Just O(n) stream figure required for encryption and hunt calculation.

R. Curtmola et al[7] gather information to another gathering privacy, while keeping up the capacity to specifically look over it. The concentration of dynamic research and a few security definitions this issue are occurred. In this framework we propose new and more grounded security definitions. Permit two manifestations that we permit secure under our new definitions. With fulfilling more grounded security guarantees, and this is more proficient than every past development. In new framework chip away at SSE just considered the setting where just the proprietor of the information is equipped for submitting seek questions.The normal expansion where a discretionary gathering of gatherings other than the proprietor can submit look inquiries. We formally characterize SSE in this multi-client setting, and present a productive development.

Xu, W. Kang et al[8] is to provide a viable solution for multikeyword ranked query problems over encrypted data in the cloud environment. First introduced the problem, analyze the existing solutions and design a novel algorithm called MKQE to address the issues.MKQE uses a partitioned matrices approach. Structure another trapdoor age calculation, which can take care of the out-of-arrange issue in the returned outcome set without losing the information security and protection property. Furthermore, the weights of the keywords are taken into consideration in the ranking algorithm when generating the query result. The DC has high probability to retrieve the files they really need. The simulation experiments confirm that our approach can achieve better performance with a satisfactory security level. In the proposed, we will explore new approaches to further enhance multi-keyword query capabilities. We are designing new algorithms to provide extra functionalities such as semantic query and fuzzy keyword query.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

III.METHODOLOGY USED IN PROPOSED SYSTEM

A.METHODOLOGY

In our system data owner can upload different files in encrypted format using AES 128/192/256 algorithm. AES algorithm follows following steps as below

- **AES Algorithm For Encryption.**

Input:
128_bit /192 bit/256 bit input(0,1)
secret key(128_bit)+plain text(128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists:sub byte, shift byte, mix columns, add round key.

Output:
cipher text(128 bit)
Data users can search the file on encrypted data using MD5 algorithm hash value .MD5 algorithm follows following steps as below

- **MD5(Message-Digest Algorithm)**

Steps 1:A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
Steps 2: The output of a message digest is considered as a digital signature of the input data.
Steps 3:MD5 is a message digest algorithm producing 128 bits of data.
Steps 4: It uses constants derived to trigonometric Sine function.
Steps 5: It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
Steps 6: Most modern programming languages provides MD5 algorithm as built-in functions.
Data users can search the file using fuzzy keyword search algorithm. Fuzzy keyword search algorithm follows following steps as below

- **Fuzzy Keyword Search :-**

Inputs:-
1.C=(F_1,F_2,…,F_n)
2.W={W_1,W_2,…,W_n}
3.Edit distance *d*
4.A searching input (*w*, *k*) (k<=d)
For Normal Search Set Up
Π=(Setup(1^λ), Enc(*sk*, ·), Dec(*sk*, ·))
T_{wi}= *f*(*sk*,w_i)

For Fuzzy Keyword

The wildcard-based fuzzy set of *wi*with edit distance *d* is denoted as *Swi,d={Swi*,0, *Swi*,1, · · · , *Swi,d}*.

d=1 $(2L+1)*26+1$
d=2 $C_1^{L+1}+C_1^{L}*C_1^{L+2}C_2^{L+2}$

For Searching Input:-
Π=(Setup(1^λ), Enc(*sk*, ·), Dec(*sk*, ·))

Twi= f(sk,wi) *Tw'i= f(sk,w'i)* for each *w'i∈Swi,d*

Step1 $FID_{wi}Enc(sk,FID_{wi}||w_i)\{(\{T_{w'i}\}w_{'i\in Swi,d}, \quad Enc(sk,FID_{wi}||w_i))\}_{wi\in W}$
Step 2$\{Tw'\}w'\in S_{w,k}$

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

International Journal of Innovative Research in Computer and Communication Engineering

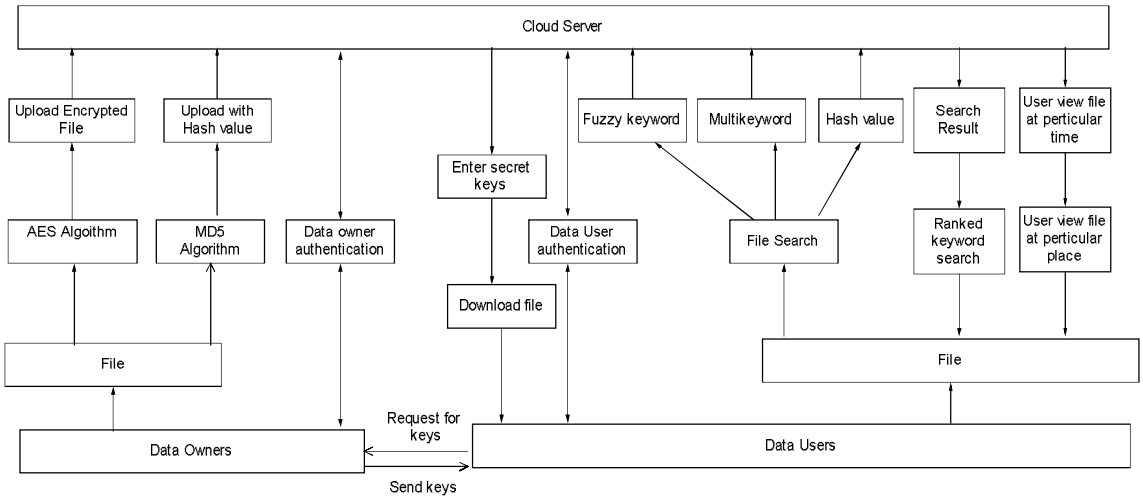
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Step 3 Enc(sk,$FID_{wi}||w_i$)

B. PROPOSED SYSTEM



System Architecture

In this proposed system consist of mainly 3 modules data owners, data users and cloud server.In our proposed system first data owner registration with login with proper authentication. Data owner upload files using AES algorithm in encrypted format, this file is store on the cloud and also upload file with hash value using MD5 algorithm .Data User registration and login with proper authentication, After login user search different file with Multikeyword search, Fuzzy keyword search and Search using hash value also.After Searching user view the file and send request to particular data owner.Data owner accept request and send secret keys to user.Data user enter secret keys and download file at particular time and particular place.If user enter 3 times wrong key user become attacker. Cloud server view the attackers of the system and number of file upload and download on the cloud.

C.RESULTS AND DISCUSSION

In our experimental setup, In table 1,find out number of file upload and file download.In our experimental setup,in our system number file upload and download of files.

Sr.No	Number of File Upload	Number of File Download
1	35	15

Table1: No. Upload and download files

In our experimental setup, In table 2, find out number of file upload and file download.In our experimental setup,in our system number file upload and download of files.

Sr.No	No of Search Keyword 1	No of search Keyword 2	No of Search Name
1	15	16	18

Table1: No. file Search by keywords

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

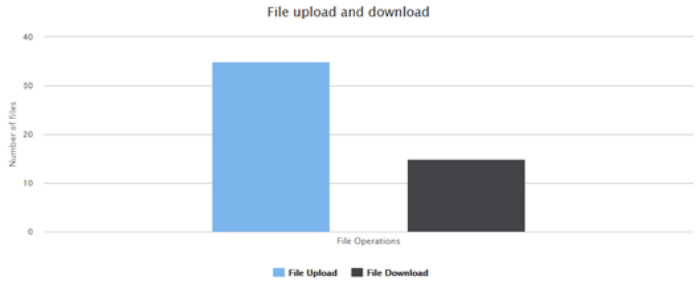
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

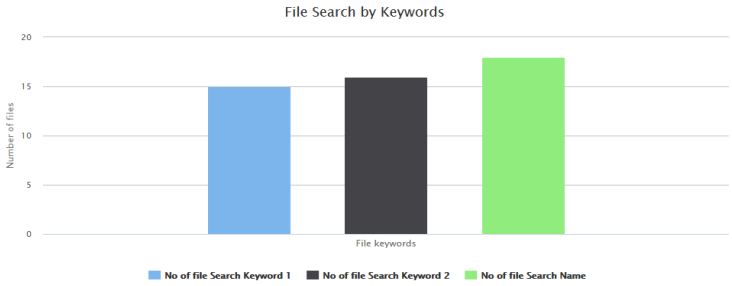
Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

From above data, In graph 1,we can see the no. of file upload and no of file download in thegraph; we see 35 files upload by different data owners and 15 different users are download inthe graph.



From above data, In graph 2,we can see the no. of file search keyword and file name also and no of file keyword 2 in the graph; we see 15 files search by keyword and 16 files search by keyword2 by different users and 18 files search by file name are shown in the graph..



IV. CONCLUTION

In this study, we consider a multiple data owners model in cloud computing and propose an efficient ranked Multikeyword search scheme over encrypted data. In this system, user can search using different searching techniques like Multikeywordsearch,Fuzzy keyword search and Hash Value Search.Upload a file in encrypted format for maintain the security. User can download any file in particular place and particular time only.In future, we can provide more security technique to our system like fragmentation. In the fragmentation technique we can store the file in the different types of fragments.

REFERENCES

[1]D. Song, D. Wagner, and A. Perrig**, "Practical techniques forsearches on encrypted data,"** in Proc. IEEE Int. Symp. Security Privacy,Nagoya, Japan, Jan. 2000, pp. 44–55.
[2]R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, **"Searchablesymmetric encryption: Improved definitions and efficient constructions,"**in Proc. 13th ACM Conf. Comput. Commun. Security,Oct. 2006, pp. 79–88.
[3]C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, **"Secure ranked keywordsearch over encrypted cloud data,"** in Proc. IEEE Distrib.Comput. Syst., Genoa, Italy, Jun. 2010, pp. 253–262.
[4] Xu, W. Kang, R. Li, K. Yow, and C. Xu**, "Efficient multikeywordranked query on encrypted data in the cloud,"**inProc. IEEE 19th Int. Conf. ParallelDistrib. Syst., Singapore, Dec.2012, pp. 244–251.
[5] W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, **"Secure distributedkeyword search in multiple clouds,"** in Proc. IEEE/ACM 22nd Int.Conf. Quality Service, Hong Kong, May 2014, pp. 370–379.
[6] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "**Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data"**, in IEEE Transaction on dependable and secure computing, vol 13, no. 3, May/June 2016.
[7] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "**Secure ranked multi-keyword search for multiple data owners in cloud computing**," in Proc. 44th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw, Jun. 2014, pp. 276–286.
[8]J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "**Fuzzy keyword search over encrypted data in cloud computing**," in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5