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

Advanced Searching Method over Encrypted Cloud Data for Multiple Data Owners to Download File at Particular Location

Viraj Ghorpade[*], Akshay Kudale[**], Pranay Kukadkar[**] , Ram Sakore[**],Shrikant Salve[**]

Department of Information Technology, MIT Academy of Engineering, Alandi(D), India

ABSTRACT: With the coming of cloud computing, it has turned out to be providing security for information. In this system, data owner can upload different file in form of encrypted format. For insurance concerns, secure endeavours over scrambled cloud data have propelled a couple of research works under the single proprietor demonstrate. In our system we developed this system for multiple owner's model with different functionality In this system, we propose plans to tree based ranked multi-keyword search scheme for multiple data owners (TBMSM), We efficiently develop novel search protocol based on bilinear pairing, which enables different data owners to use different keys to encrypt their keywords and trapdoors. We can rank the different Multikeyword search over user; we can search over encrypted data using hash value md5 or SHA 256 algorithm. We 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: Cloud computing, Fuzzy keyword search, Multi-keyword,Rankedmultiple data owners.

I. INTRODUCTION

In a cloud computing system we are developed the system providing security for information. Encryption on sensitive data before outsourcing can preserve data security. Be that as it may, information encryption makes the conventional information usage benefit dependent on plaintext watchword look through an exceptionally difficult issue. In this system, data owners can upload different file in encrypted format. For assurance concerns, secure endeavours over scrambled cloud data have propelled a couple of research works under the single proprietor show. In our system we developed this system for multiple owners' model with different functionality. User login with proper authentication, view file, file search using Multikeyword search, fuzzy keyword search, send request, display messages And for download any file from particular place and particular time only. Send secret keys and token to authenticate users only. Cloud view info of user and data owner info. Also view file in encrypted format. In this system, we propose plans to tree based ranked multi-keyword search scheme for multiple data owners (TBMSM), We efficiently develop novel search protocol based on bilinear pairing, which enables different data owners to use different keys to encrypt their keywords and trapdoors. We can rank the different Multikeyword search over user; we can search over encrypted data using hash value md5 or SHA 256 algorithm. We 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.

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

W. Zhang et 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

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

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.

SofianeMounineHemam et 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 centers 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 privaty, 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.

W. Zhang et al[9] introducing for the first time, explore the problem of secure distributed keyword search in a multi-cloud paradigm.First introduced a distributed keyword search model. Based on this model, we introduced two schemes. Scheme I proposes to cross-store all encrypted keywords, files and secret keys on cloud servers, which achieves high efficiency and anonymity for data owners. Scheme II introducing to systematically construct a keyword distributing

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

strategy and a file distributing scheme, which achieves convenient search and strong security requirements. In feature, we extend both schemes with shamir's secret schemes to achieve better availability and robustness. The experiment results demonstrate that both of our schemes can work efficiently based on a real word data set.

Q. Liu et al[10]introduced a scheme based on an ADL to allow secure differential query services for a cloud environment. By using our scheme, users of different ranks can retrieve different percentages of files that match their queries so as to make the cloud services more scalable and flexible. The main drawback is that the assumption of having a trusted third party may not be realistic. For our future work, we will explore an extension of our solution that would apply to the case where we don't need to trust the ADL.

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.**

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)

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

denoted as *Swi,d={Swi*,0, *Swi*,1, · · · , *Swi,d}.*

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

For Searching Input:-

Π=(Setup(1^{λ}), Enc(*sk*, ·), Dec(*sk*, ·))

The wildcard-based fuzzy set of *wi* with edit distance *d* is

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

For fuzzy Keyword

- **Step1:** $FID_{wi}Enc(sk,FID_{wi}||w_i)\{(\{T_{w'i}\}w'_{i\in Swi,d}, Enc(sk,FID_{wi}||w_i))\}_{wi\in W}$
- **Step 2:** $\{Tw'\}w'\in S_{w,k}$
- **Step 3 :** $Enc(sk,FID_{wi}||w_i)$

B.PROPOSED SYSTEM APPROACH

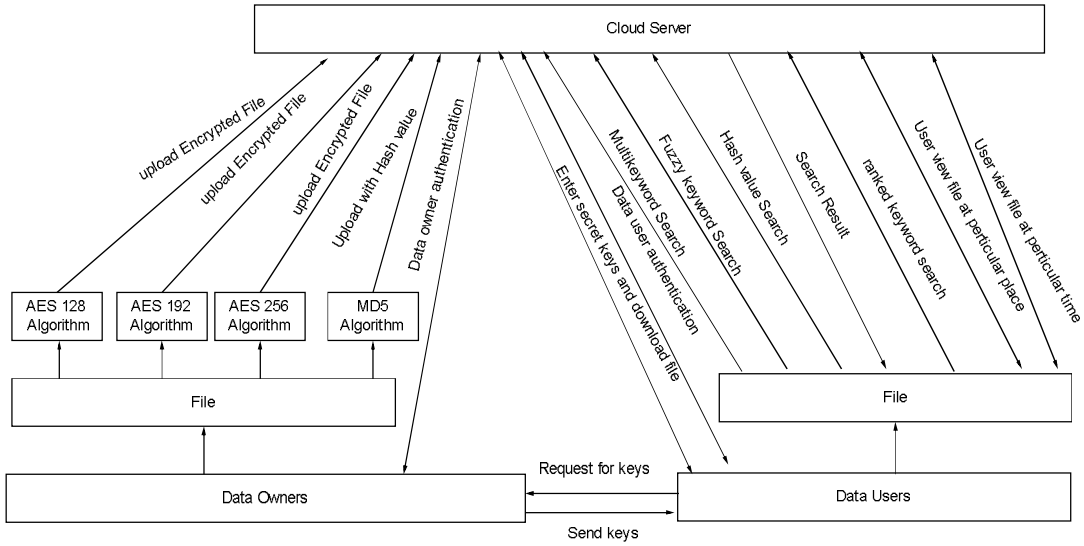


Fig.1 Block Diagram of Proposed System

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 AES128/ AES192/ AES256 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 enters secret keys and download file at particular time and particular place.If user enter 3 times wrong key user become attacker. Cloud servers view the attackers. User can view ranked multikeyword search also.

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

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

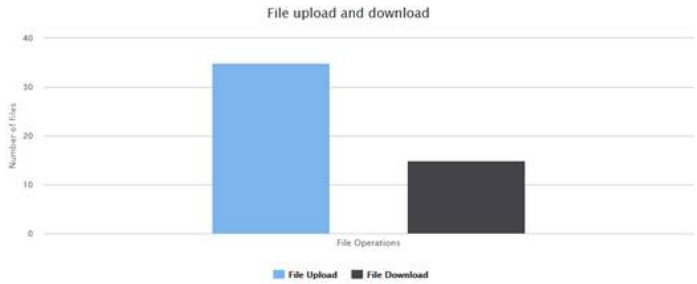
Vol. 7, Issue 5, May 2019

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

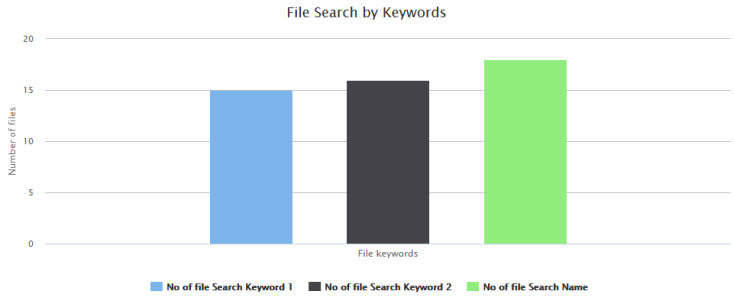
Table2 : No. file Search by keywords

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



Graph 1: File upload and download

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 filename are shown in the graph.



Graph 2: File Search by keywords

IV.CONCLUTION

The data that is stored over the cloud is encrypted. The encryption of the data has helped in providing a secure method of storage of data. As the data is being stored over the cloud, it can be accessed by the other authenticated members of the system. The future work can hold the solution to the fuzzy keyword searching mechanism. Data user can download file in particular time and particular place also. We can search over encrypted data using hash value md5 or SHA 256 algorithm. User can download file at particular place only as well as at particular times only. Attacker is also finding out to the system.

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

FEATURE WORK

In this system data owner can upload only file in text only in feature we upload file in format of image, pdf and video also. Provide more security to the system.

ACKNOWLEDGMENT

This work is supported in a Multikeyword search system of any state in india. Authors are thankful to Faculty of Engineering and Technology (FET), SavitribaiPhule Pune University,Pune for providing the facility to carry out the research work.

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. Parallel Distrib. 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

9 SofianeMounineHemam; OuassilaHioual ; OuidedHioual "**Load balancing between nodes in a volunteer cloud computing by taking into consideration the number of cloud services replicas**" 2017 3rd International Conference of Cloud Computing Technologies and Application(CloudTech)

10 M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,**"A view of cloud computing,"**Commun. ACM, vol. 53, no. 4,pp. 50–58, 2010.