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

An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data

Dipika Jadhav[1], Prasad Nagargoje[2], Varsha Jarhad[3].

U.G. Student, Department of Computer Engineering, NBN Sinhgad Technical Institute Campus, Ambegaon (bk), Pune, Maharashtra, India[1]

U.G. Student, Department of Computer Engineering, NBN Sinhgad Technical Institute Campus, Ambegaon (bk),Pune, Maharashtra, India[2]

U.G. Student, Department of Computer Engineering, NBN Sinhgad Technical Institute Campus, Ambegaon (bk), Pune, Maharashtra, India[3]

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. Uploaded is stored in different fragments as well as in replica also 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 owner's model with different functionality In this system, 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. Data owner can rank the different Multikeyword search over user; user can search over encrypted data using hash value md5 or SHA 256 algorithm. User 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 ranked Multiple data owners

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. Distributed storage framework, is set of storage servers, and gives long storage services over the Internet. Putting away information in an outsider's cloud framework causes grave to connect to over data secret. Typical hidden plans defend data secret however have some limitation to usefulness of the storage framework in light of the fact that a couple of operations are supported over hidden data. Service suppliers of cloud would promise to owner's information security utilizing like virtualization and firewalls. 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 generate encrypted indexes.Data Administrator can re-encrypted index then 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 type of replica's and fragments .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

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

make simple cloud servers to perform safe excluding knowing the real value of both keywords and trapdoors, System proposed fuzzy keyword search, using this we can easily search the information. We also introduced any file can download from particular location only.

1.1 MOTIVATION

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. However, all these schemes are limited to the single-owner model. Fuzzy keyword Search problem occurred in existing system.

1.2 OBJECTIVES

The goal of our system is to search An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data.

- Data owner file upload in fragments
- Data owner file upload in replica's
- User can search the encrypted data using multiple keywords.
- User can search the encrypted data using fuzzy keyword.
- User can download file at particular place as well as particular times only.

II. REVIEW OF LITERATURE

H. Li te.al [1] proposed concept is to refer address this issue by developing the fine-grained multi-keyword search schemes over encrypted cloud.The proposed scheme can support complicated logic search the mixed "AND", "OR" and "NO" operations of keywords. The enhanced schemes supporting classified sub-dictionaries (FMSCS) to improve efficiency. Disadvantage of this system is to develop the highly scalable searchable encryption to enable efficient search on large practical databases.

W. Zhang et.al[2] states that propose 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, To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. we propose a novel Additive Order and Privacy Preserving Proposed. Construct a novel secure search protocol for trapdoor and index.Approach is computationally used only for efficient even for small data set and keyword set Approach is not computationally efficient even for large data set and keyword set.

J. Liet.al [3] introducing aformalize 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. This paper includes the formalization and solution of the problem of effective fuzzy keyword search over encrypted cloud data as well as preserving keyword privacy. An efficient fuzzy keyword search scheme is not proposed based on the constructed fuzzy keyword sets.An fuzzy keyword search scheme is proposed based on the constructed fuzzy keyword sets.

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

Sofiane Mounine Hemamet.al [4] states the load balancing between volunteer nodes that provide the cloud services.Selects and deletes the replicas of a cloud service without degradation of the load balancing, using for this the Markov Chain Models.Approach is not computationally efficient even for large data set and keyword set. Our solution allows a better system reliability and reduces the response time of the users by distributing their requests between the volunteer nodes.

M. Armbrust et.al [5] proposed got all information about cloud computing. User 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 also provides proofs of security for the resulting crypto systems. This scheme is provably secure for remote searching on encrypted data using an untrusted server. This system searches data remotely from untrusted server. This system provides the proofs of security that required for crypto systems. This system worked efficiently for query isolation as they are simple and fast. Only O(n) stream cipher required for encryption and search algorithm.

R. Curtmola et.al[7] states a Searchable symmetric encryption (SSE) system is enables a gathering to outsource the capacity of his information to another gathering private, 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. We 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. We consider the normal expansion where a discretionarygathering of gatherings other than the proprietor can submit look inquiries. We formally characterize SSE in this multi-client setting, and present a productive development.

C. Wang et.al[8] proposed this system, for the first time we introduce and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards exprimental deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). At specific study to view that new solution enjoys “as-strong-as possible” security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

W. Kang et.al [9] have aim to provide a viable solution for Multikeyword ranked query problems over encrypted data in the cloud environment. We first introduced the problem, analyse the existing solutions and design a novel algorithm called MKQE to address the issues. MKQE uses a partitioned matrices approach. The encrypted data increases and more keywords need to be introduced, then the searching infrastructure can be naturally expanded with the minimal overhead. We also design a new trapdoor generation algorithm, which can solve the out-of-order problem in the returned result set without losing the data security and privacy property. Furthermore, the weights of the keywords are taken into consideration in the ranking algorithm when generating the query result. In the proposed, we will explore new approaches to further enhance multi-keyword query capabilities. Data owner 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

W. Zhang et.al[10] proposed this system, for the first time, we explore the problem of secure distributed keyword search in a multi-cloud paradigm. We 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 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.

III. SYSTEM OVERVIEW/ SYSTEM ARCHITECTURE

In a cloud computing system we are developed the system providing security for information. Encryption on sensitive data before outsourcing can preserve data security. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem. In this system, data owners can upload different file in encrypted format. 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 owner's 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. Data owner upload file in encrypted format as well as file upload using replica's and fragments. 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.

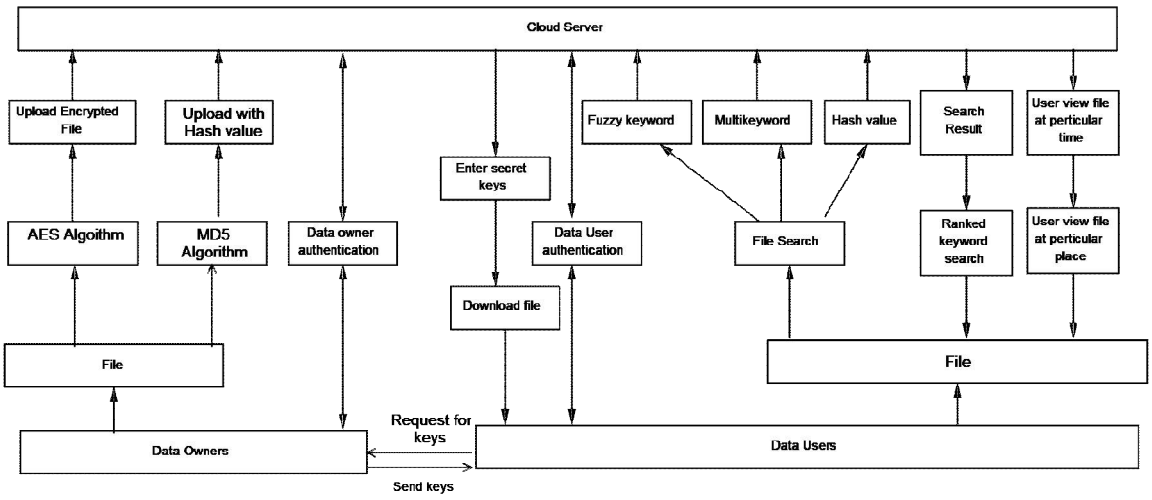


Fig.Proposed System Architecture

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

EXPLANATION:

1. In our proposed system first data owner registration with login with proper authentication.
2. Data owner upload files in encrypted format, in replica's and in fragments this file is store on the cloud.
3. 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.
4. After Searching user view the file and send request to particular data owner.
5. Data owner accept request and send secret keys to user.
6. Data user enter secret keys and download file at particular time and particular place.
7. If user enter 3 times wrong key user become attacker. Cloud server view the attackers.

IV. MATHEMATICAL MODEL

Set Theory:-

S={s, e, X, Y,Φ}

Where,

s = Start of the program.

1. Log in System

2. Search the keyword which we want to search.

e = End of the program.

File which is search by user.

X = Input of the program.

Input should be user file name.

Y = Output of the program.

Proper name of file which is store in cloud will match then user can download correct file

X, Y ∈ U

This module help the owner to upload his file with encryption using ECC algorithm. the Owner to view the uploaded files and downloaded files

Let U be the Set of System.

U= {Sk1,Sk2,SK3,R1,R2,D}

Where Sk1,Sk2,SK3,R1,R2 are the elements of the set.

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

Sk1=Search first keyword

SK2= Search second keyword

SK3= Search Third keyword

R1=Get Accurate result

R2= Error in the accessing of the system

D=Download File

SPACE COMPLEXITY:

No of file are more store on a cloud ,so space complexity is more

TIME COMPLEXITY:

Keyword search using similarity join query so we got file fastly.

If (n>1) then checking similar keyword .so,time required for similarity check is less.So the time complexity of this algorithm is O(n^n).

Failures:

1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

Success:

1. We get file which want to search.
2. We get accurate file.

V. ALGORITHM

AES Algorithm For Encryption.

AES(advanced encryption standard).It is symmetric algorithm.It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

- **Input:**
- 128_bit /192 bit/256 bit input(0,1)
- secret key(128_bit)+plain text(128_bit).

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

- **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)

MD5(Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

- **Steps:**
- 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.
- The output of a message digest is considered as a digital signature of the input data.
- MD5 is a message digest algorithm producing 128 bits of data.
- It uses constants derived to trigonometric Sine function.
- 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.
- Most modern programming languages provides MD5 algorithm as built-in functions.
- We design 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. Based on the constructed fuzzy keyword sets, we further propose an efficient fuzzy keyword search scheme. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search

Fuzzy Keyword Search

This algorithm is used for searching purpose.

- **Inputs:-**
- 1.C=(F_1,F_2,…,F_n)

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

- 2.$W=\{W_1,W_2,\ldots,W_n\}$
- 3.Edit distance *d*
- 4.A searching input (*w, k*) (k<=d)
- For Normal Search Set Up
- $\Pi=(\text{Setup}(1^{\lambda}), \text{Enc}(sk, \cdot), \text{Dec}(sk, \cdot))$
- 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 $C^1_{L+1}+C^1_L*C^1_{L+2}C^2_{L+2}$
- Forsearching input:
- $\Pi=(\text{Setup}(1^{\lambda}), \text{Enc}(sk, \cdot), \text{Dec}(sk, \cdot))$
- $Twi = f(sk,wi)$ $Tw'i= f(sk,w'i)$ for each $w'i \in Swi,d$
- Step1
- FID_{wi} $\text{Enc}(sk,FID_{wi}||w_i)$
- $\{(\{T_{w'i}\}w'_{i \in Swi,d}, \text{Enc}(sk,FID_{wi}||w_i))\}_{wi \in W}$
- Step 2
- $\{Tw'\}w' \in S_{w,k}$
- Step 3
- $\text{Enc}(sk,FID_{wi}||w_i)$
- **Output:-**
- Get Expected result which is search by the user.

Algorithm of Replica's

Using this algorithm data owner upload file in different replicas.

- **Input:-**File
- **Process:-**Enter number of replica's

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

- **Output:-**File replica's

Algorithm's for Fragments

Using this fragments algorithm data owner can upload file in different fragments.

- **Input:-**File
- **Process:-**Enter number of Fragments
- **Output:-**File Fragments

VI. RESULTS

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

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.

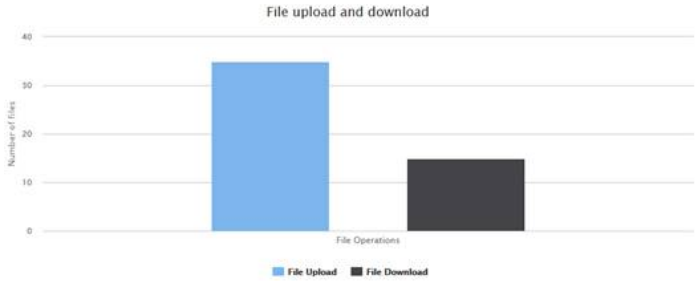
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

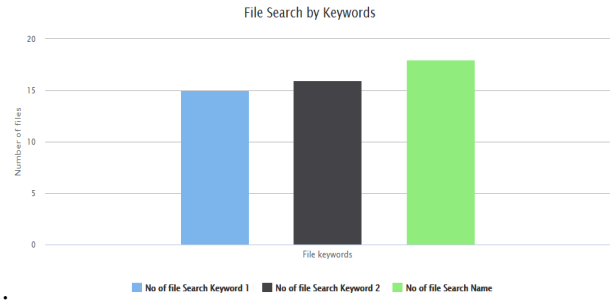
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019



From above data, In graph 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 searced by file name are shown in the graph.



VII. 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, the 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.

VIII. ACKNOWLEDGEMENT

This work is supported in a Multi-keyword search system of any state in India. Authors are thankful to Prof. S.A. Chiwhane Assistant Professor for their guidance, Faculty of Engineering and Technology (FET), Savitribai Phule Pune University, Pune for providing the facility to carry out the research work.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[5] . 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.

[6] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, **"Fuzzy keywordsearch over encrypted data in cloud computing,"** in Proc.IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5.

[7] 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.

[8] Q. Liu, C. C. Tan, J. Wu, and G. Wang, **"Efficient informationretrieval for ranked queries in cost-effective cloud environments,"** in Proc. IEEE INFOCOM, 2012, pp. 2581–2585.

[9] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, **"Secure rankedmulti-keyword search for multiple data owners in cloud computing,"** in Proc. 44th Annu. IEEE/IFIP Int. Conf. DependableSyst. Netw, Jun. 2014, pp. 276–286

[10] Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, MC. Rosu, and M. Steiner. **"Dynamic searchable encryption in very large databases: Data structures**
implementation." In Proc. of NDSS, 2014