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. 6, Issue 3, March 2018

Fast Phrase Search for Encrypted Cloud Storage

S.Geetha[1], N.Saranya[2], D. Vimala Devi[3], D.Nivetha[4]

U.G, Department of Computer Science &Engineering, CK College of Engineering & Technology, Cuddalore, India.[1,2,3]

Asst. Professor, Department of Computer Science& Engineering, CK College of Engineering &Technology, Cuddalore, India.[4]

ABSTRACT: Cloud computing is a technology,which provides low cost,scalable computational capacity. The storage and access of document have been major problem in this area.While,many schemes have been proposed to perform conjunctive keyword search,less attention has been noted. In this paper,we present a phrase search technique based on bloom filters,which is faster than existing system. Our techniques uses conjunctive keyword search to support functionalities. This approach also described the false positive rate.

KEYWORDS: Phrase Search,Conjunctive Keyword Search,Bloom Filters, False Positive Rate, Hashing

I .INTRODUCTION

Cloud computing has generated much interest in the research community in recent years.to search over encrypted documents stored on cloud many schemes has been proposed but less attention have been noted on more search techniques.To overcome the storage and access of confidential documents stored in cloud.we proposed a phrase search using bloom filters which is faster than existing system.our techniques uses an conjunctive keyword which is drawback of existing system to get the stored document faster and access secure This approach also described the false positive rate for the keyword search.

II .RELATED WORK

Boneh et al. proposed one of the earliest works on keyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealing data content. Waters et al. investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches. Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords. Other interesting problems, such as the ranking of search results and searching with keywords that might contain errors termed fuzzy keyword search, have also been considered. The ability to search for phrases was also recently investigated. The ranking of search results was looked at by Wang. The authors described a solution based on the commonly used TFIDF (Term Frequency X Inverse Document Frequency) rule and the use of order preserving symmetric encryption. Liuet considered the search for potentially erroneous keywords termed fuzzy keyword search. The index-based solution makes use of fuzzy dictionaries containing various misspelling of keywords including wildcards. Some of the existing system has examined the security of the proposed solutions and, where flaws were found, solutions were proposed.

III .PROPOSED SYSTEM

OBJECTIVE:

- To reduced the search time
- To enable the multi keyword search over cloud data

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. 6, Issue 3, March 2018

SCOPE:

- The scheme is also scalable, where documents can easily be removed and added to the corpus.
- We also describe modifications to the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on stored data.

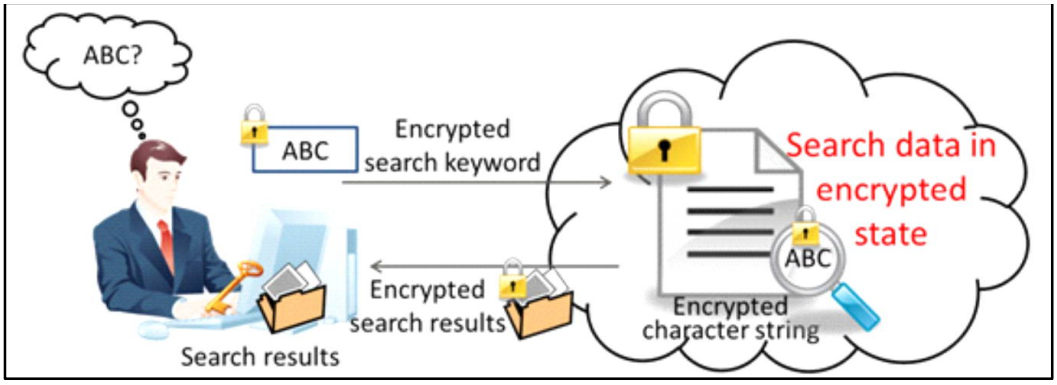

Fig.1: Proposed system architecture.

IV .METHODOLOGY & DISCUSSION

In this approach we used three methodology which is used to retrieve data from cloud fast and secure .The algorithm and protocol is used to encrypt the files and keyword and took the value for all keywords and file to decrypt the file faster stored in the cloud server.Here we using an realtime cloud Drive HQ to store document

- AES ALGORITHM
- TDES ALGORITHM
- HASHING

MODULES:

- System Framework
- Data Owner
- Data User
- Cloud Server

MODULES DISCUSSION:

System Framework: In this framework, we designed a standard keyword search protocol. During setup, the data owner generates the required encryption keys for hashing and encryption operations. Then, all documents in the database are parsed for keywords. Bloom filters tied to hashed keywords and n-grams are attached. The documents are then symmetrically encrypted and uploaded to the cloud server. To add files to the database, the data owner parses the files as in setup and uploads them with Bloom filters attached to the cloud server. To remove a file from the data, the data

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. 6, Issue 3, March 2018

owner simply sends the request to the cloud server, who removes the file along with the attached Bloom filters. To perform a search, the data user enters keyword then it computes and sends a trapdoor encryption of the queried keywords to the cloud to initiate a protocol and returns accurate file. Here we implement some modules they are Data Owner, Data User and Cloud Server.

Data Owner: In Data Owner module, Initially Data Owner must have to register their detail and after login he/she has to verify their login through OTP. Then data Owner can upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users.

Data User: In Data User module, Initially Data Users must have to register their detail and then login into cloud. Data Users can search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive the decryption key in registered mail

Cloud Server: In this module, we develop Cloud Server module. In Cloud Server module, Cloud Provider can view all the Data owners and data users' details. CP can able see the files in cloud uploaded by the data owners.

V .EXPERIMENTAL RESULTS

Dataowner should login to the cloud server to upload files in the cloud. While Register is done the OTP sends to the owner mail. When the OTP is verified then the home page of Data Owner will be displayed.

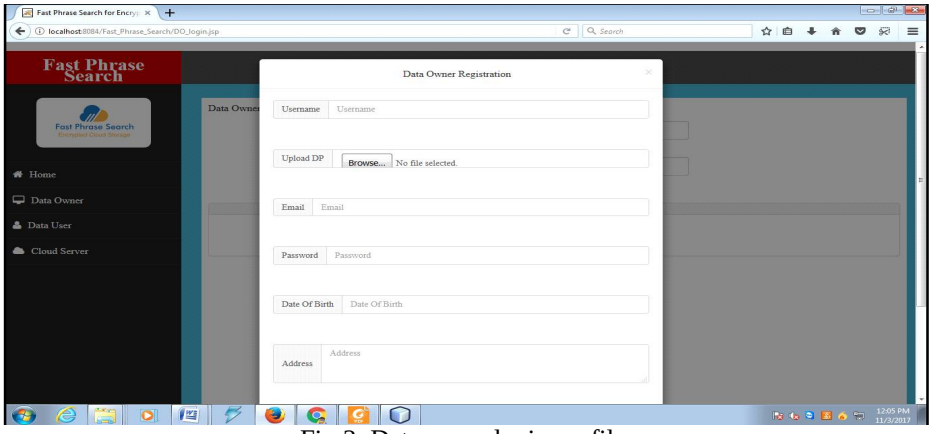

Fig.2: Dataowner login profile.

Datauser also need to login in the cloud.The role of the user is to search the file uploaded by the user While,register is done the data user profile home page will be displayed.

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. 6, Issue 3, March 2018

Fig.3: data user profile .

After login is done,the home page have various module. The file will be upload by user by giving conjunctive keyword to store in cloud. The keywords and files are encrypted and hash value will be stored in database.

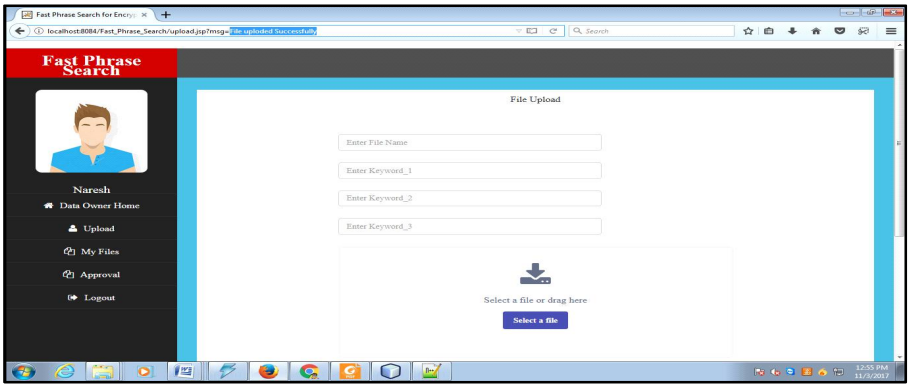

Fig.4: dataowner upload file.

when the data user needed a file,he/she search the keyword and request the file from the data owner .when the searched query is matched with hash value in database it show the exact file.The status of file approved or rejected also displayed.

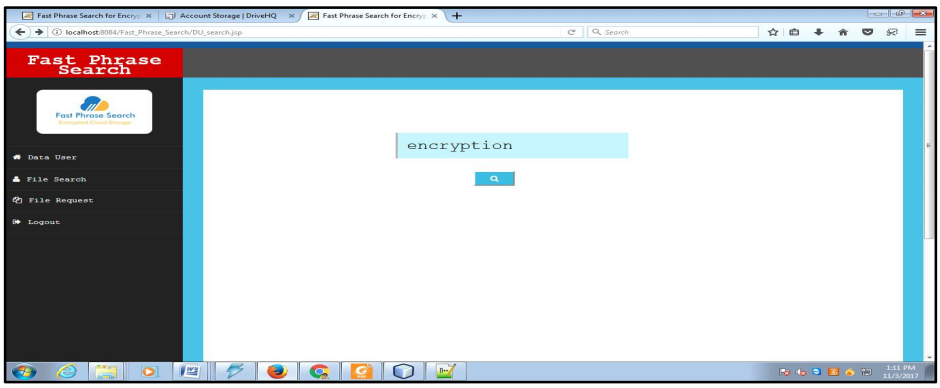

Fig 5: Datauser query search

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. 6, Issue 3, March 2018

While, the datauser requested file is approved.The decryption key is send to the user mail.By using the key user get the exact file faster and the file will be secured in the cloud.

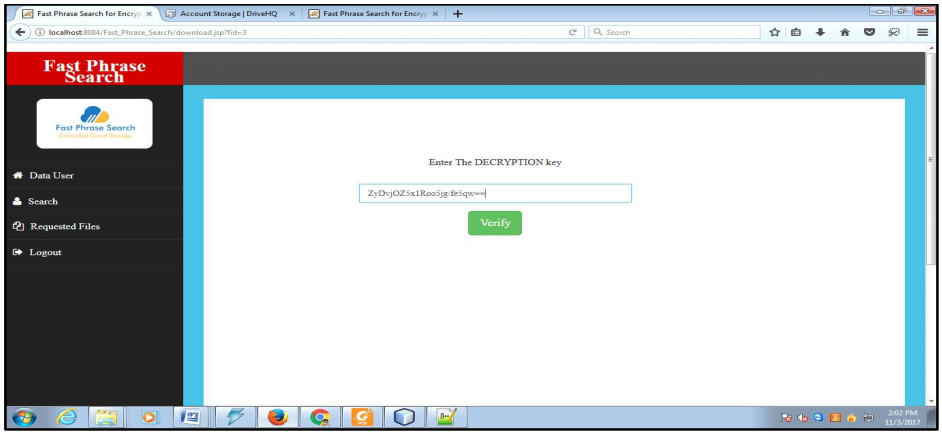

Fig 6: verify decryption key

The file searched by user is get faster without any delay and also dataowner file will be secured by using this technique.

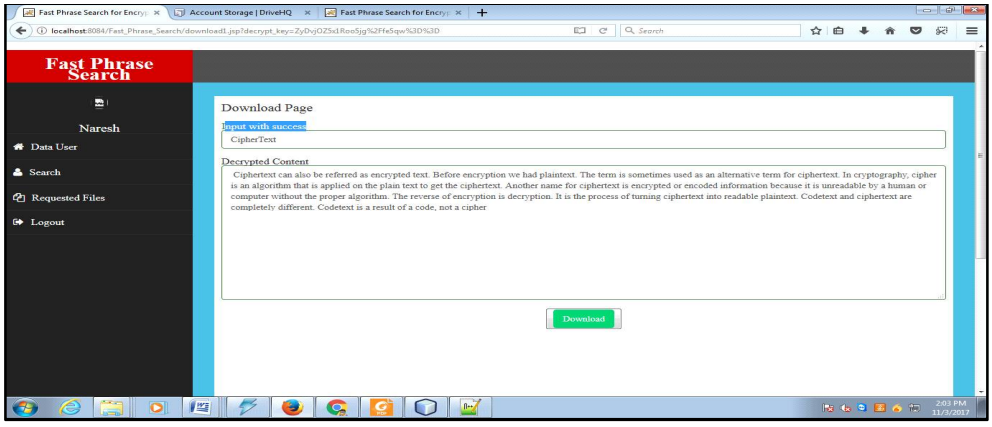

Fig 7: User get exact file faster

V .CONCLUSION AND FUTURE WORK

In this paper, we presented a phrase search scheme based on Bloom filter that is significantly faster than Existing approaches, requiring only a single round of communication and Bloom filter verifications.Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The technique of constructing a Bloom filter index enables fast verification of Bloom filters in the same manner as indexing. According to our experiment, it also achieves a lower storage cost than all existing solutions except where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application.

REFERENCES

[1] K. Cai, C. Hong, M. Zhang, D. Feng, and Z.Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.

[2] Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in IEEE Third International Conference on Cloud Computing Technology and Science, 2011, pp. 264–271.

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. 6, Issue 3, March 2018

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in International Conference on Distributed Computing Systems, 2010, pp. 253–262.

[4] M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Practical oblivious storage," in Proceedings of the Second ACM Conference on Data and Application Security and Privacy, 2012, pp.13–24.

[5] F. Kerschbaum, "Secure conjunctive keyword searches for unstructured text," in *International Conference on Network and System Security*, 2011, pp. 285–289.

[6] C. Hu and P. Liu, "Public key encryption with ranked multikeyword search," in *International Conference on Intelligent Networking and Collaborative Systems*, 2013, pp. 109–113.

[7] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," *IEEE Transactions on Consumer Electronics*, vol. 60, pp. 164–172, 2014.

[8] C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, "Relevance ranking for one to three term queries," *Information Processing and Management: an International Journal*, vol. 36, no. 2, pp. 291–311 , Jan. 2000.

[9] H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing," in *International Conference on Intelligent Networking and Collaborative Systems*, 2013, pp. 786–789.

[10] M. Zheng and H. Zhou, "An efficient attack on a fuzzy keyword search scheme over encrypted data," in *International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing*, 2013, pp. 1647–1651.

[11] S. Zittrower and C. C. Zou, "Encrypted phrase searching in the cloud," in IEEE Global Communications Conference, 2012, pp. 764 – 770

[12] C. Liu, L. Zhu, L. Li, and Y. Tan, "Fuzzy keyword search on encrypted cloud storage data with small index," in *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, 2011, pp. 269–273.

[13] P. F. Brown, P. V. deSouza, R. L. Mercer, V. J. D. Pietra, and J. C. Lai, "Class-based n-gram models of natural language," *Computational Linguistics*, vol. 18, no. 4, pp. 467–479, 1992.

[14] D. Jurafsky and J. H. Martin, *Speech and Language Processing: An Introduction to Natural Language Processing, Speech Recognition, and Computational Linguistics*. Prentice Hall, 2009.

.