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 8, August 2019

Multi-Keyword Search System For Multiple Data Owners Over Encrypted Cloud Data With Systematic Ranking

Supriya V. Joshi[1], Abhijit A. Rajaguru[2]

P.G. Student, Department of Computer Science and Engineering, SKN Sinhgad College of Engineering Korti, Pandharpur, Maharashtra, India[1]

Assistant Professor, Department of Computer Science and Engineering, SKN Sinhgad College of Engineering Korti, Pandharpur, Maharashtra, India[2]

ABSTRACT : Cloud is a storage technology uses the central remote servers to maintain data and manage applications**.** currently , cloud computing have make evolution as an important aspects for IT industry with scalability, usability, pay as you use, cheap costing ,scalability, easy accessibility and improved flexibility. In a cloud environment client data can reside in any corner of the world as maintained and controlled outside their reach. So , there can be security and privacy issue with the client data. To ensure the privacy of data over cloud it is good to outsource the data in a encrypted format. In multiple data owner system each owner encrypt their data with different secrete key. To use such encrypted data efficiently, specific data structure is used called as indexing. This technique reduce the system efforts required for applying trapdoor separately for each data owner for single query. The two main goals have to achieve using this system are usability and accuracy in result and they make satisfied using multi-keyword query search. This also helps to reduce network overhead. The point to be noted that, data privacy is main issue while retrieving the result. For that a special encryption techniques are used. At the last, the worst analysis proves that, the system is secure and performance analysis demonstrates the efficiency of the system.

KEYWORDS : Multi-Keyword search, Indexing, Ranking, Multiple data owners, Security, Cloud storage, Privacy preserving.

I. INTROCTION

Cloud storage could be a system, wherever information is managed and maintained additionally keep a copy having blessings likes usability, information measure and price saving. as an example, Health care policies or in health facility conduct the analysis for study to own government satisfactory for . For that purpose some volunteer patients would comply with share their health information on the cloud. to create information secure , information owner can cipher their information with secrete key. due to this solely approved organization will perform a secure search over encrypted information. Considering on top of situation developing multi-owner system is sophisticated as compared to single owner system. in a very single information owner system, whenever information user send request for trapdoor(Encrypted Keyword) thus, owner ought to keep on-line all the time that is much not possible and unusable. Whenever great deal of knowledge house owners square measure concerned, it much not possible that, to raise them for keep on-line. additionally nobody needs to share our secrete key with others. it's obvious that every information owner can cipher there with completely different keys. So it little difficult to perform a secure search over knowledge encrypted with totally different keys while not effecting keyword linguistics security. Whenever multiple knowledge owner are concerned, the right enrollment of information house owners and authenticated user can increase the usability and measurability of 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 8, August 2019

Motivation factors :
Main assume that encourage to develop such novel system is protective knowledge privacy. Sharing knowledge files with alternative knowledge user by guaranteeing authentication is most significant task that is achieved by this method as a result of the info owner have authority to permit uses of information for specific user. like in enterprise one worker ought to access files outsourced by alternative worker. For the usability purpose of read it higher to convey the lead to hierarchal format. Privacy conserving and multi-keyword search (PRMSM) is achieved in recent work with success.

challenges :
Instated of single user system it is well challenging to develop a multiuser system for multiple data owners. For efficient search we are using tree-based index structure for each owner's data .In some cases data user needs to generate trapdoor for each data owner which is actually inefficient. Because the one to one relation in index and data owner . To overcome this limitation Merging needs to be done.

System Approach:
In this system, we are focusing on multiple data owners top-k query, where cloud server supposed to merge multiple data indexes encrypted with different keys to efficiently support top-k queries Recent work [2] point out the privacy-preserving ranked multi-keyword search in a multi-user model, which addresses the multi-keyword search problem in the multiple data owners model. However, it is inefficient and potentially expensive for frequent queries due to matching various cipher texts from different data owners even for the same query. In this system we are implementing the multi-source cloud system, in which each data owner generates a tree-based index for his/her data files and encrypts these data files with his/her corresponding key. To implement both privacy preservation and efficiency searches, we propose an efficient tree-based ranked multi-keyword search scheme . In this scheme, the cloud server is supposed to effectively merge multiple encrypted indexes, and securely perform the multi-keyword search without revealing the data owners' sensitive information, neither data files nor the queries. We are developing an efficient search protocol based on bilinear pairing, which enables different data owners to use different keys to encrypt their keywords and trapdoors. In order to rank the search results, we utilize the ranking scheme in the model and relevance scores of data files with the help of "Depth-First Search" algorithm to obtain the ranked results.

II. LITERTURE REVIEW

The main focus behind data outsourcing is that availability of data at any point with privacy preserving. To achieve data security encryption of data before outsourcing is important . while availability it good to have accurate result. For that purpose D. Song, D. Wagner, A. Perrig proposed as practical techniques for searches on encrypted data[3].The untrusted user cannot know anything about the plaintext is the advantage of this system. The arbitrary word search without the user's authentication is not possible.
one of the simplest arrangement known as Bloom filters area unit used for representing a group so as to support membership queries are explained to resolve verity of network issues with the aim of providing a unified mathematical and sensible framework for them and stimulating their use in future applications[5]
The beneficial thing is that, cloud server takes responsibility of sensitive data security against untrusted cloud service provider (CSP) by allowing decryption only for trusted user. The system achieves high performance by supporting keyword based on encrypted cloud data. Characteristics of cloud services are studied well during this paper and planned a completely unique system for secure and privacy preserving keyword searching (SPKS)scheme which permit CSP to participate within the decoding and come solely files containing sure keywords given by user. keyword search reduces each the procedure overhead needed to go looking on encrypted information and communication overhead needed to share fetched files. it's created positive that projected system semantically secure against adaptation chosen plaintext attacks. [6]
Wei Zhang proposed a system which deal with enhance security over keyword and trapdoors. Along with ranking facility additive order and privacy preserving function family(AOPPF) [7]
"Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud" deals with novel multi- keyword fuzzy search scheme which exploits the locality-sensitive hashing technique for encryption. The system scheme

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 8, August 2019

achieves fuzzy matching through algorithmic design rather than expanding the index file. There is no need to have predefined dictionary and effectively supports multiple keyword fuzzy search [8]

"An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing"[9] contains public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. the main motivation is to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the file retrieval accuracy. system contains an Efficient and Secure Privacy-Preserving approach(ESPPA) using probabilistic public key encryption and ranked keyword search. Moreover, scheme also verifies the integrity of data. So enhance ESPP algorithm to support efficient dynamic data operations and ranked keyword search over the encrypted big data in cloud as a future work.

III. PROPOSED SYSTEM

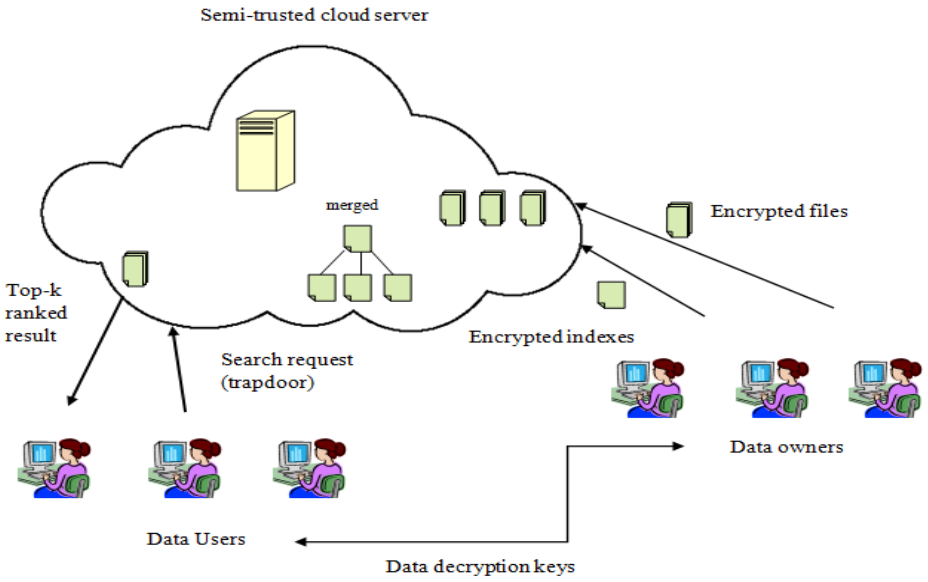

Fig.1 System Architecture

As shown in Figure the three entities involved in the system where data owner and data user are actors and third is cloud storage. Whenever data owner wants to upload file on cloud , say the collection of file as F. So before uploading the data on cloud owner firstly encrypt that file with secrete key and generate a tree based index structure for the file which helps to fetch the data when data user execute a multi keyword query search on cloud. Next simple task is to upload the index structure and encrypted file on cloud server

Now the cloud server have the index structure and encrypted file. Cloud server merge the encrypted index structure without harming the semantic security.

On the other hand side, the data user searches t keyword over encrypted files on cloud sever. Meanwhile the trapdoors T for the t keywords are get calculated and according to that trapdoor and index structure the most relevant files are get fetched without scanning each encrypted file. For the systematic view and user convenience the list of files are ranked according to the frequent search order.

The Tree-Based Multikeyword Ranked System is applied to search engine while fetching the multikeyword query result .

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 8, August 2019

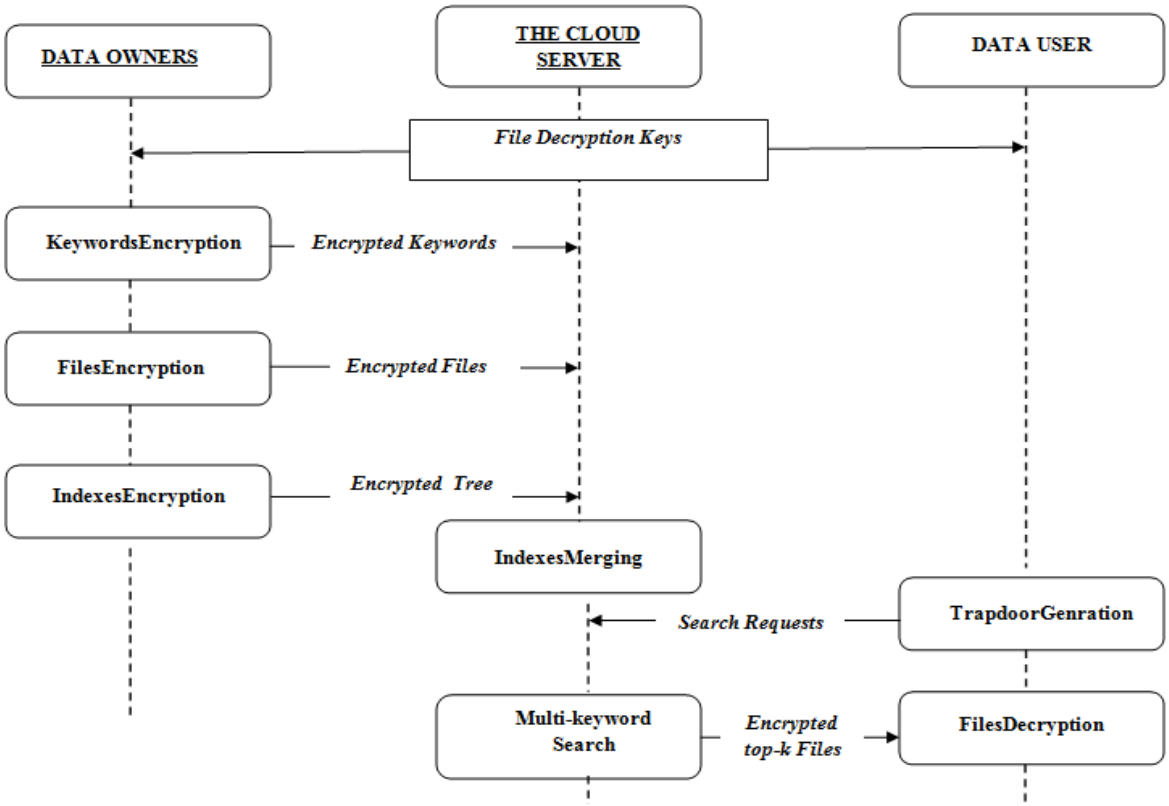

Figure 2.Tree Based Multikeyword Ranked Search Scheme

Data owner completes the task of KeywordEncryption by encrypting the keyword with secrete key. FileEncryption contains the typical symmetric encryption technique to encrypt the file. For the highly secure system the owner will also encrypt the index structure. Remember that, for better data security, each data owner will encrypt the same keyword with different secrete key and no need to share that secrete key with anyone. Now all the three encrypted data files are as encrypted keyword, encrypted file and encrypted Index tree structure are send to cloud server. Then cloud sever merge all the index tree uploaded by different data owners and generates a merged index tress structure. If data user wants to retrieve the file from cloud he will first generate the trapdoor for required file and submit it to the cloud server. cloud will only traverse the merged index tree of files instead of the actual whole files traversing. and returns the list of encrypted files according to the relevance score of keyword and the frequency of file used. Data user then have take owner permission for file decryption. To make a system more user friendly the system have to achieve some goals :

a. **Multiple data owner system giving ranked search result:**
The system should support multikeyword search on cloud data and give the ranked file list as a result. Note that the files are encrypted with different keys by different data owners.

b. Effective Searching :
The time required to fetch the result should to be minimum. For that purpose the index tree will be helpful. Authenticated user only needs encrypt the query once to search all the relevant files. This make the system more efficient than traditional existing system.

c. Data Security :
The system should have to prove their security over keyword semantics security, keyword security and relevance score security.

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 8, August 2019

Advantages Of The System:

a. Authenticated enrollment system and easy access to cloud data.
b. Provided efficient and timing saving search result over huge encrypted data.
c. A rigorous security is maintained using one of the best symmetric key encryption called as Triple DES(Data Encryption Standard).

IV. RESULTS AND DISCUSSION

Now we are going to take entire view of proposed system using the project screen snapshots following figure 3 shows the home page of targeted purposed system.

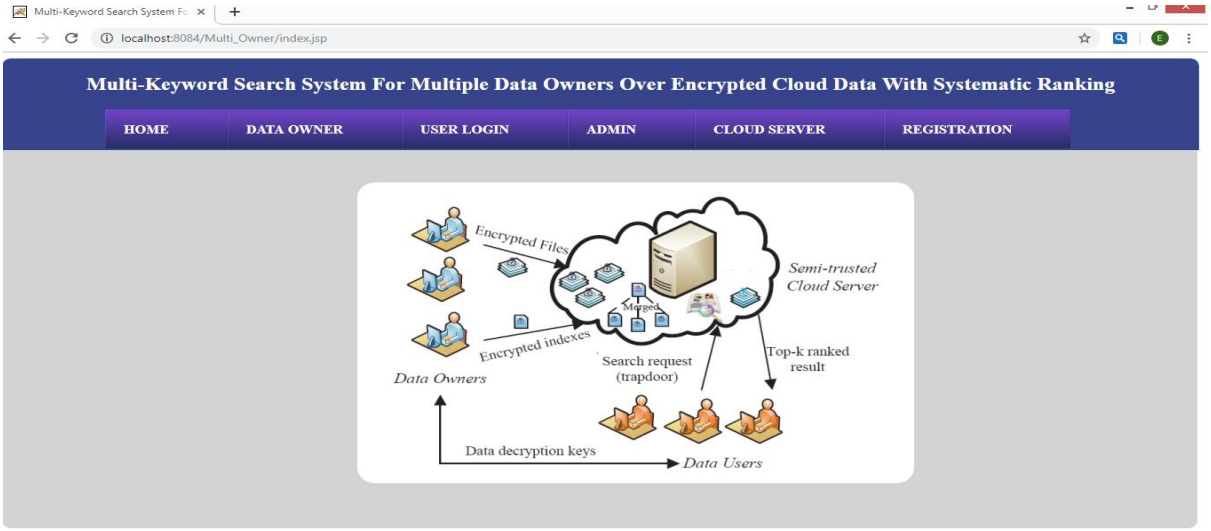

Figure 3. Home Page

The following figure 4 shows the best enrollment system through registration which takes the necessary information about system user where that entity select his role in the system as owner or as user.

Figure 4. Registration Page

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 8, August 2019

If the entity is already a system user, so he/she can access the system by login. As shown in figure 5 shows the Data owner login system.

Figure 5. Data Owner Login Page

Next important task is to upload the file on cloud. For that, data owner browse the file from the location and decide the keyword for the file. System will upload the encrypted file on cloud. Shown in figure 6.

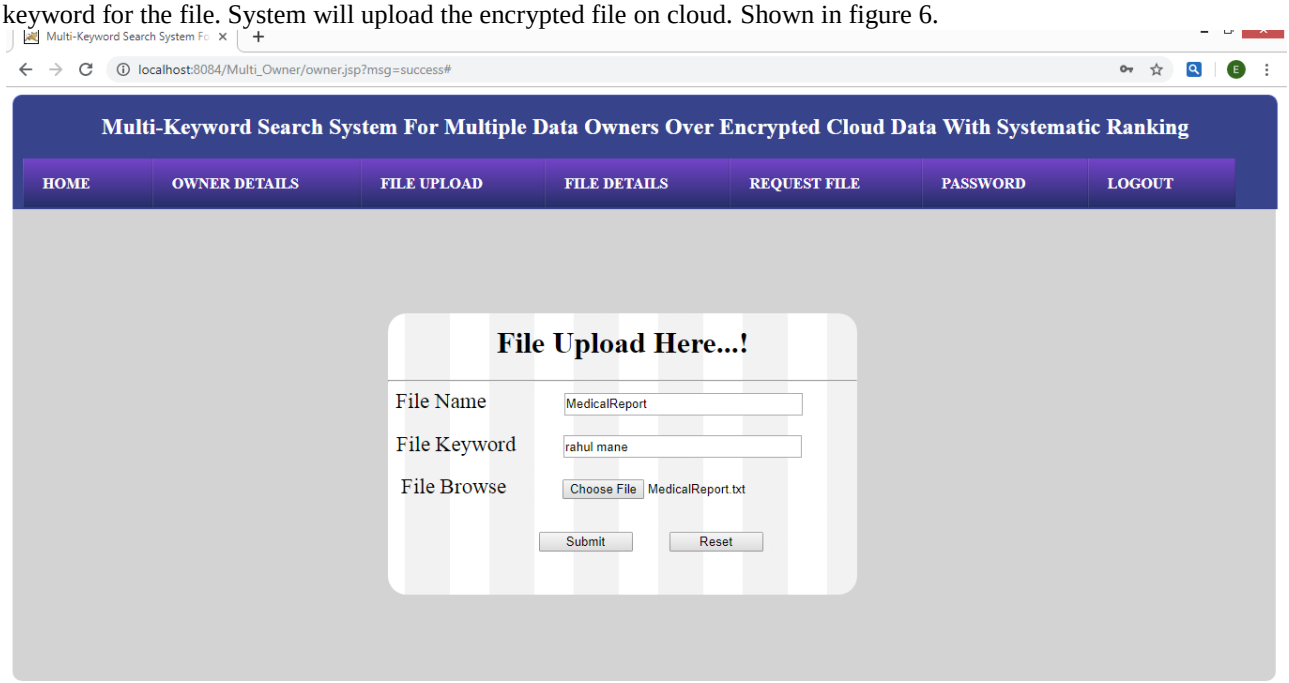

Figure 6. File Upload Page

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 8, August 2019

Whenever data user wants to retrieve the file it will first login to the system. Then It will search for a file using mulikeyword search and it will get the result as shown in following figure 7.

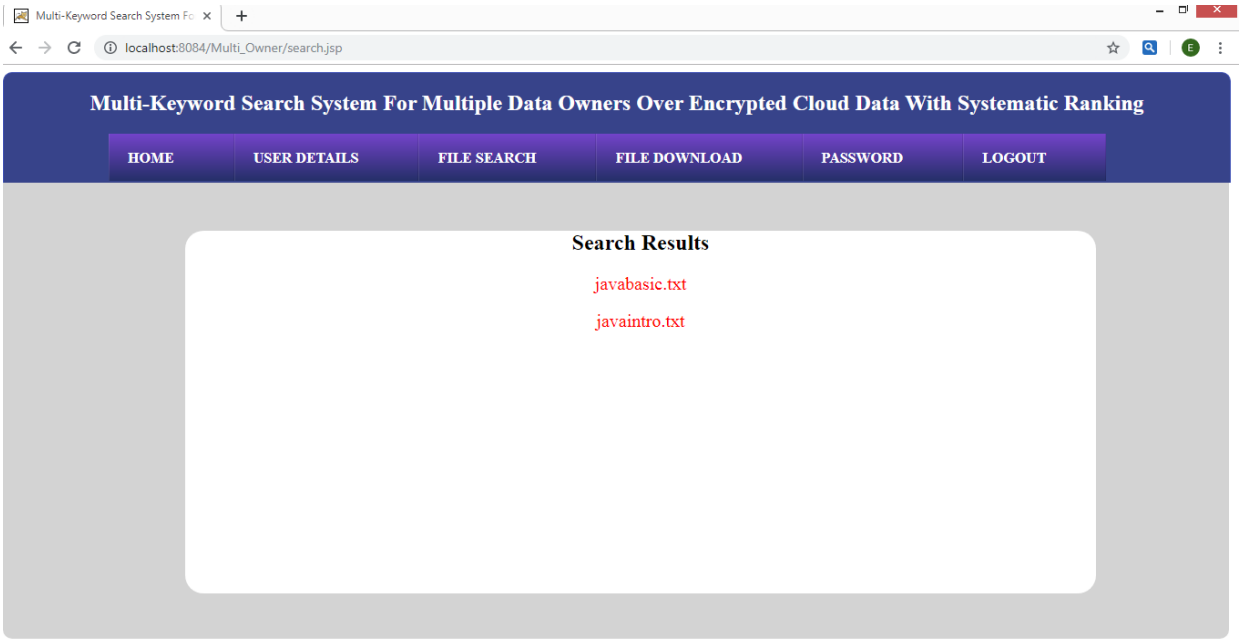

Figure 7. Search Result Page

Whenever the file owner allow user to download that file. User can download the file as plaintext using a unique decryption Key. as shown in figure 8.

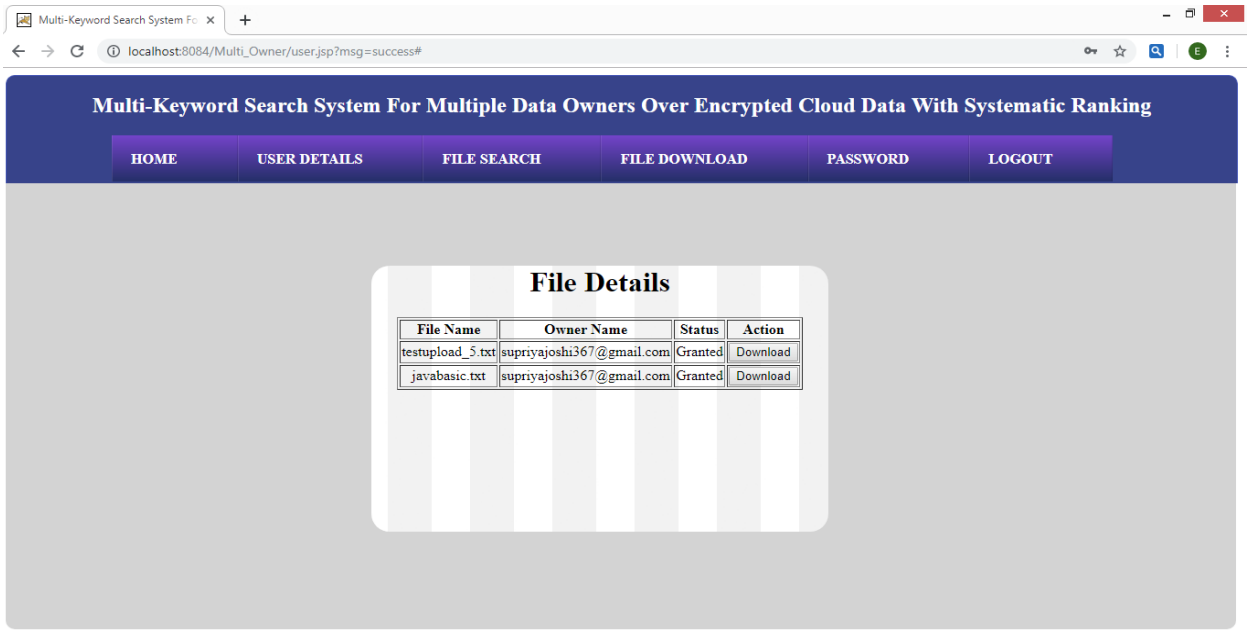

Figure 8. User File Download Page

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 8, August 2019

V. CONCLUSION AND FUTURE WORK

we consider the novel multiple data owners model in cloud computing and propose an efficient ranked multi keyword search scheme over encrypted data with easily accessible data at any corner of world. This system allows data owner to encrypt data different secrete keys. index structure will reduce the computational overhead required for encrypted file search on cloud.

In a future there is a scope to enhance authentication of user and security of system by using the higher technology algorithm such as Machine learning and Artificial Intelligence. That will also increase the scalability and accuracy of the system.

REFERENCES

1. "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data" by Tianyue Peng, Student Member, IEEE, Yaping Lin, Member, IEEE, Xin Yao, Student Member, IEEE, and Wei Zhang
2. W. Zhang, Y. Lin, S. Xiao, J. Wu, S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Trans Comput., vol. 65, no. 5, pp. 1566 – 1577, 2016.
3. D. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data," in: SP'00, Berkeley, CA, 2000.
4. E. Goh, "Secure indexes," Cryptology ePrint Archive, pp. 216 – 216, 2003.
5. Broder, M. Mitzenmacher, "Network applications of bloom filters: A survey," Internet Math., vol. 1, no. 4, pp. 485 – 509, 2002.
6. Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," J NETW COMPUT APPL., vol. 35, no. 3, pp. 927 – 933, 2012.
7. N. Cao, C. Wang, M. Li, K. Ren, W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," in: INFOCOM'11,Shanghai, China, 2011.
8. B. Wang, S. Yu, W. Lou, Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in: INFOCOM'14,Toronto, Canada, 2014.
9. S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.
10. Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE T Parall Distr., vol. 27, no. 2, pp. 340 – 352, 2016.