RESEARCHERID
THOMSON REUTERS

[Patange, 5(4): April 2018] ISSN 2348 – 8034
DOI- 10.5281/zenodo.1216749 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

MULTIKEYWORD SEARCH SCHEMA FOR CLOUD DATA

Dr.K.V.Ranga Rao[*1] & Dr.B.Vijayakumar[2]

[*1]Professor, CSE Dept,Vidya Jyothi Institute of Technology, Aziz Nagar,c.b.post

[2]Professor and HOD,CSE Dept,Vidya Jyothi Institute of Technology, Aziz Nagar,c.b.post

ABSTRACT

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF×IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a Greedy Depth-first Search algorithm to provide efficient multi-keyword ranked search. The secure KNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

Keywords: *cloud computing, cloud servers,KNN algorithm, encrypt.*

I. INTRODUCTION

Distributed computing is the utilization of registering assets (equipment and programming) that are conveyed as an administration over a system.The name originates from the common utilization of a cloud-formed image as a reflection for the unpredictable foundation it contains in framework outlines. Cloud processing depends remote administrations with a client's information, programming and calculation. Distributed computing comprises of hard product and programming assets made accessible on the Web as oversaw outsider administrations. These administrations normally give access to cutting edge programming applications and top of the line systems of server PCs.

Structure of cloud com putting How Circulated processing Capacities. The target of conveyed figuring is to apply ordinary supercomputing, or high-performance enlisting power, normally used by military and research offices, to perform many trillions of computations for each second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

ISSN 2348 – 8034
Impact Factor- 5.070

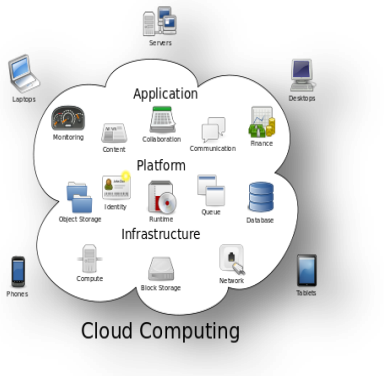

Figure 1: Structure of cloud

II. EXISTING SYSTEM

Yu *et al.* constructed a cloud storage auditing protocol with key-exposure resilience by updating the user's secret keys periodically. But it also brings in new local burdens for the client because the client has to execute the key update algorithm in each time period to make his secret key move forward. For some clients with limited computation resources, they might not like doing such extra computations by themselves in each time period. It would be obviously more attractive to make key updates as transparent as possible for the client, especially in frequent key update scenarios. Wang *et al.* proposed a public privacy-preserving auditing protocol. They used the random masking technique to make the protocol achieve privacy preserving property.

Disadvantages of Existing System:
Existing system don't like auditing protocol with verifiable outsourcing of key updates. Third party has the access to see client's secret key without encryption. No verification system available for client's for to check validity of the encrypted secret keys when downloading them from the TPAAll existing auditing protocols are all built on the assumption that the secret key of the client is absolutely secure and would not be exposed.

Proposed System:
We propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this new paradigm, key-update operations are not performed by the client, but by an authorized party. The authorized party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client downloads the encrypted secret key from the authorized party and decrypts it only when he would like to upload new files to cloud. In addition, the client can verify the validity of the encrypted secret key.We design the first cloud storage auditing protocol with verifiable outsourcing of key updates. In our design, the third-party auditor (TPA) plays the role of the authorized party who is in charge of key updates.We formalize the definition and the security model of the distributed storage reviewing convention with obvious outsourcing of key updates. We additionally demonstrate the security of our convention in the formalized security display and legitimize its execution by solid usage.

Focal points OF PROPOSED Framework: The TPA does not know the genuine mystery key of the customer for distributed storage reviewing, however just holds a scrambled form. In the definite convention, we utilize the blinding system with homomorphism property to shape the encryption calculation to scramble the mystery keys held by the TPA. It influences our convention to secure and the unscrambling operation proficient. Meanwhile, the TPA can finish key updates under the scrambled state. The customer can check the legitimacy of the encoded mystery key when he recovers it from the TPA. In expansion, the customer can confirm the legitimacy of the scrambled mystery key. Cloud storage auditing protocol with verifiable outsourcing of key updates are. The client can verify the validity of the encrypted secret key when he retrieves it from the TPA. The security model of the cloud storage auditing protocol with Verifiable Outsourcing Of Key Updates.

ISSN 2348 – 8034
Impact Factor- 5.070

III. SYSTEM ARCHITECTURE

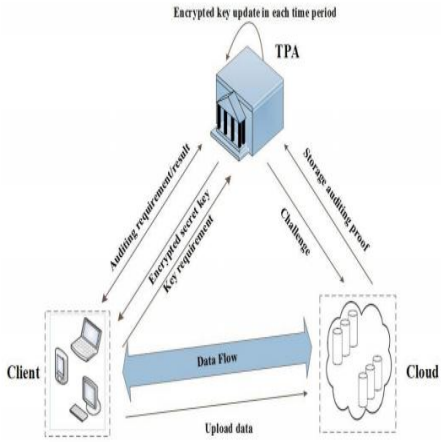

Figure 2: System model of our cloud storage auditing

IV. OUTPUT SCREENS

Screen1:

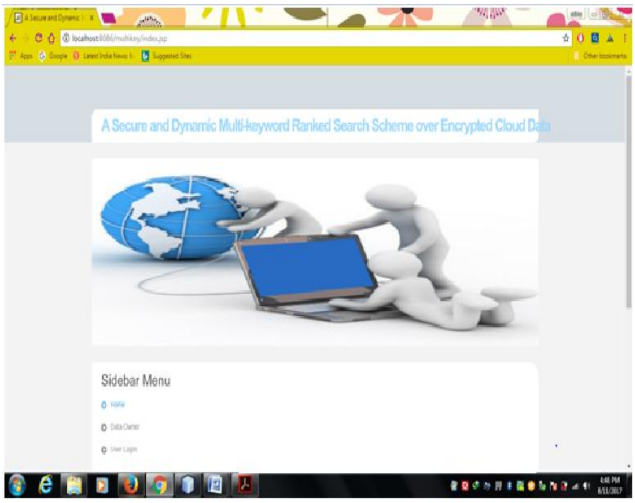

Figure:4.1 Home page

This screenshot refers to the Home page, where can be registered with data owner login and user login.

ISSN 2348 – 8034
Impact Factor- 5.070

Screen 2:

Figure:4.2 Data Owner Login

To Login the Data owner, click on Data Owner and give the userid and password, click the login button.

Screen 3:

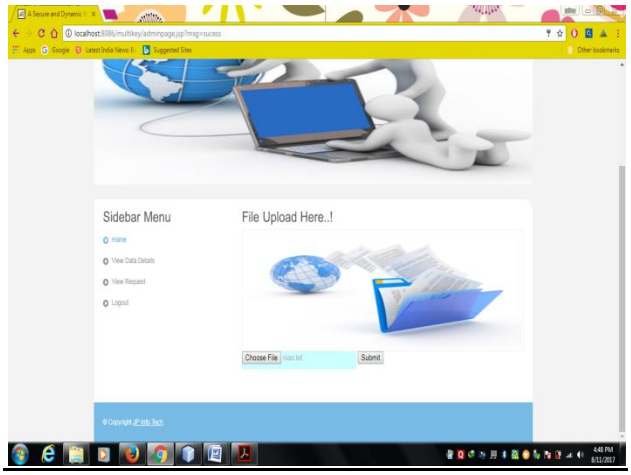

Figure:4.3 Upload Page

After Login the data owner page it shows the next page to File Upload and choose the file which you want to upload and click on the submit button. After submitting to view the uploaded file click on view data details.

To view the uploaded file click on view request.To Logout from the Page, kindly click on Logout button.

ISSN 2348 – 8034
Impact Factor- 5.070

Screen 4:

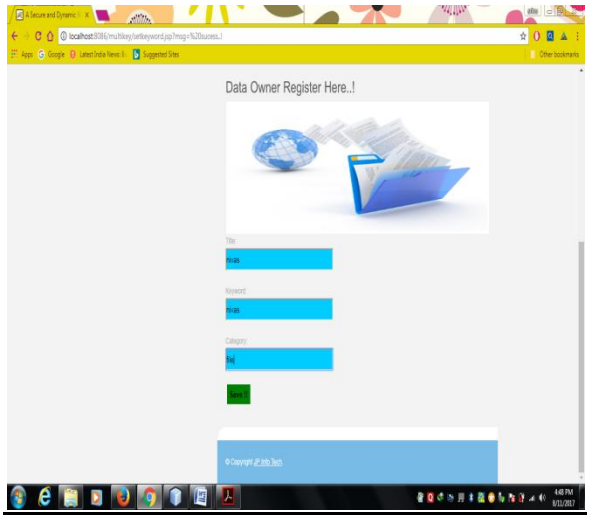

Figure: 4.4 Keyword

To save the Data owner registration enter the details, Title, keyword and category and click on save button. The file will be save as the keyword name entered.

Screen 5:

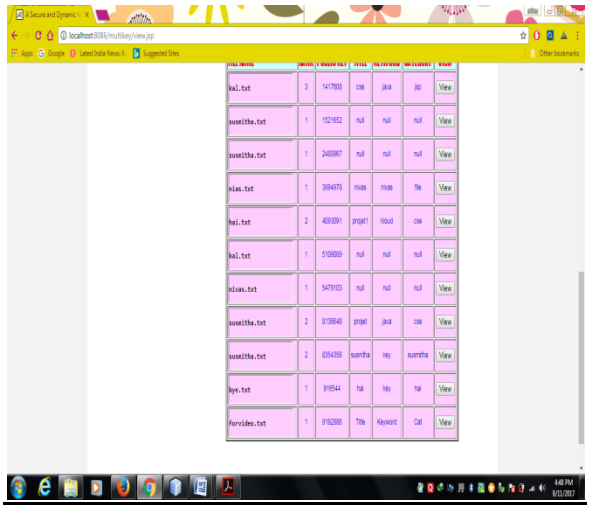

Figure: 4.5 File details

This screen shows the list of uploaded files and to view the uploaded file click on view button.

Screen 6:

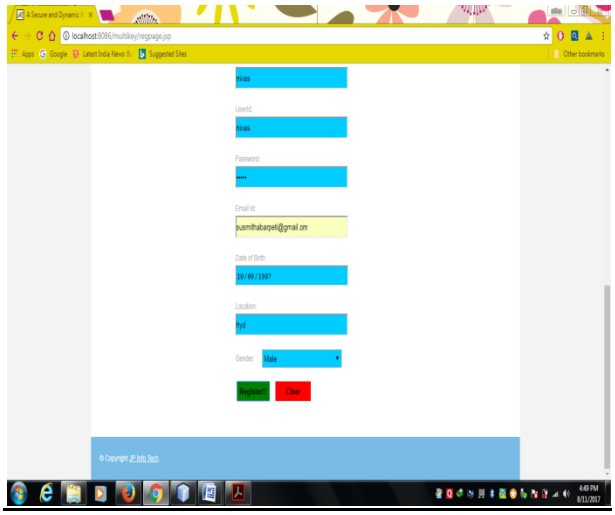

Figure: 4.6 User register

To register the user login, click on the user button in fig: 6.1, it displays the above screen and enter User name, user id, password, email id, Date of birth, location and gender from drop down, click on Register button

Screen 7:

Figure: 4.7 User login

After registration of user Login, To login the user click on user login button, a page will be displayed and enter the userid, password and click on Login button.

ISSN 2348 – 8034
Impact Factor- 5.070

Screen 8:

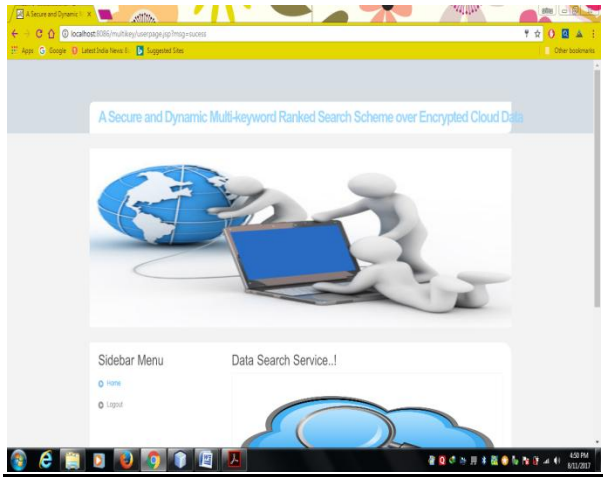

Figure: 4.8 User home page

To Logout the page, click on Logout button.

Screen 9:

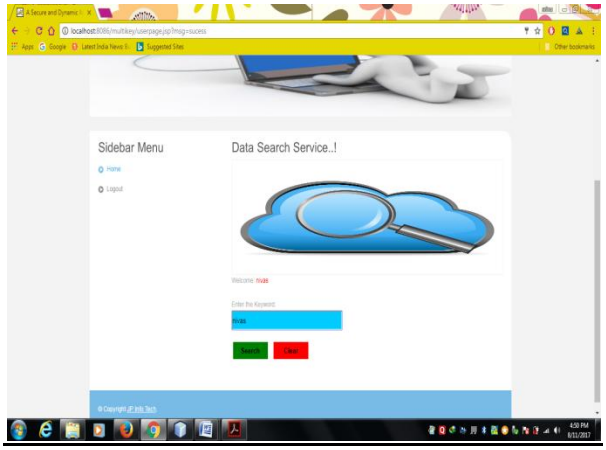

Figure: 4.9 Search

In order to search the required file name enter the keyword in the Enter the Keyword textbox and click on search button.

ISSN 2348 – 8034
Impact Factor- 5.070

Screen 10:

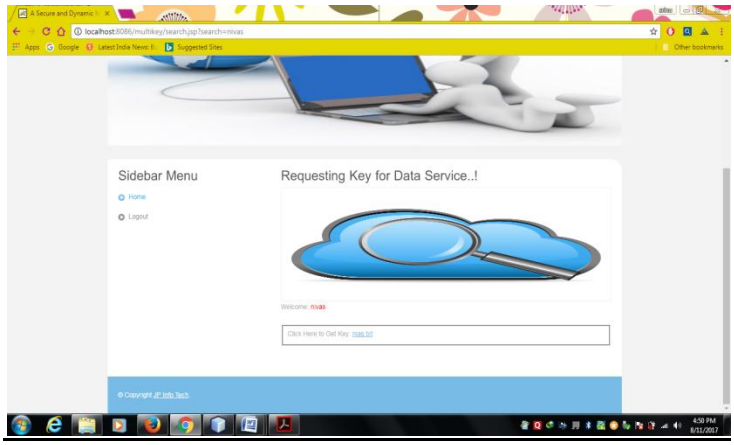

Figure: 4.10 Requesting key for data service

Enter the keyword to get the details of the file in the text box.

Screen 11:

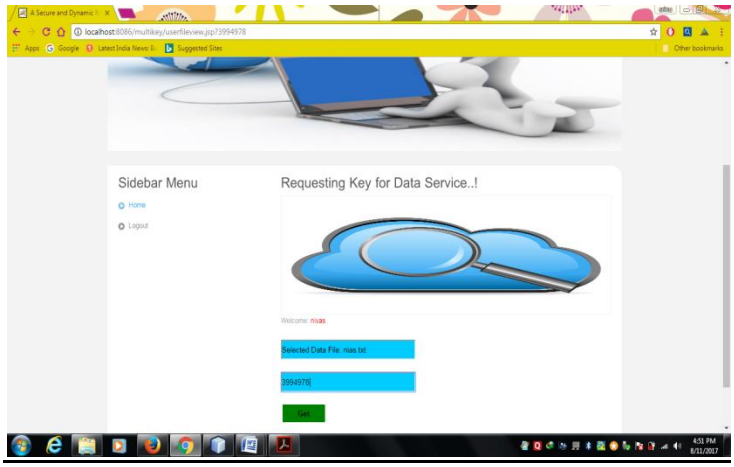

Figure: 4.11 Requesting key for data service

After entering the details shown in fig 4.10 this page appears, Enter the file name and keyword to get the file.

ISSN 2348 – 8034
Impact Factor- 5.070

Screen 12:

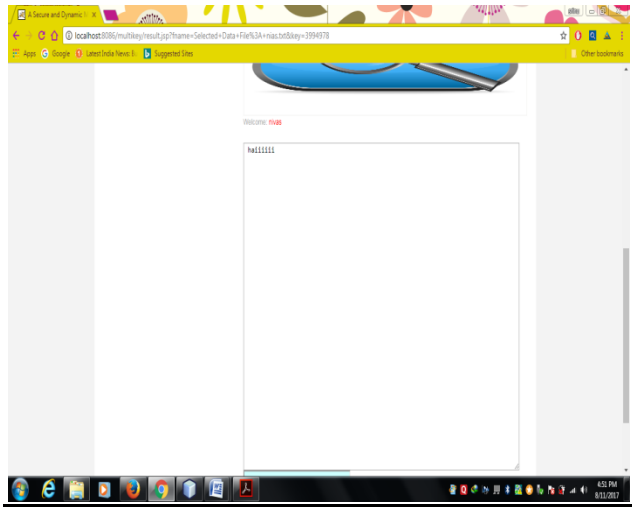

Figure:4.12 Uploaded file

It shows the file which got uploaded.

Screen 13:

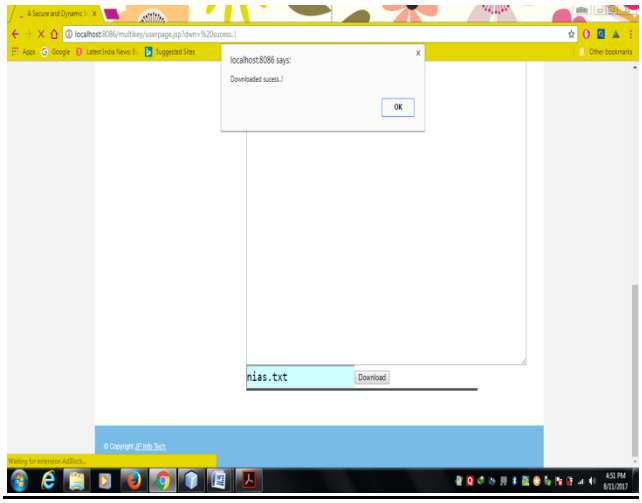

Figure: 4.13 Download success

Use the link to download the file.

V. CONCLUSIONS

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. We construct a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme is protected against two threat models by using the secure kNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme. There are still many challenge problems in symmetric SE schemes. In the proposed plot, the information proprietor is in charge of creating refreshing data and sending them to the cloud server.Thus, the data owner needs to store the unencrypted index tree and the information that are

necessary to recalculate the IDF values. Such an active data owner may not be very suitable for the cloud computing model.

It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. In addition, as the most of works about searchable encryption, our scheme mainly considers the challenge from the cloud server. Actually, there are many secure challenges in a multi-user scheme. Firstly, all the users usually keep the same secure key for trapdoor generation in a symmetric SE scheme. In this case, the revocation of the user is big challenge. If it is needed to revoke a user in this scheme, we need to rebuild the index and distribute the new secure keys to all the authorized users. Secondly, symmetric SE schemes usually assume that all the data users are trustworthy. It is not practical and a dishonest data user will lead to many secure problems. For example, a dishonest data user may search the documents and distribute the decrypted documents to the unauthorized ones. Even more, a dishonest data user may distribute his/her secure keys to the unauthorized ones. In the future works, we will try to improve the SE scheme to handle these challenge problems.

REFERENCES

1. *K. Ren, C.Wang, Q.Wang et al., "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.*
2. *S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136–149.*
3. *C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.*
4. *O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.*
5. *D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.*
6. *D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.*
7. *D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.*
8. *E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.*
9. *Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.*
10. *R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.*
11. *J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp.1–5.*
12. *M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156–1167.*
13. *C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451–459.*
14. *B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014.*
15. *P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.*
16. *Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proceedings of the First international conference on Pairing-Based Cryptography. Springer-Verlag, 2007, pp. 2–22*