A Well-organized Multi-User Searchable Encryption Organization without Question Conversion over Sub contracted Translated Data

Dr. P. Penchalaiah

[1]Associate Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

V. Deepthi

[2]PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

Abstract: Searchable Encryption (SE) schemes provide security and privacy to the cloud data. Then the existing Searchable Encryption approaches enable to the multiple users to the perform by search operation by the using various schemes and like the Broadcast of Encryption, Attribute Based Encryption, etc. By However, these schemes do not allow to multiple by users to perform of the search operation to over of the encrypted of data of multiple owners. By some of the Searchable of the Encryption schemes is involve by a Proxy Server is that can be allows to multiple of users to can perform of by the search and the operation. Then however these approaches is incur to the huge of the computational and also burden on that the proxy server is to be due to the repeated and of the encryption of that the user queries for that transformation of purpose so that as to be ensure of that users of to the query is to searchable and that over ofthe encrypted data into the multiple of the owners.

I. Introduction

Searchable Encryption schemes in support search operation efficiently only in a single owner and single user environment. Various schemes like BE, ABE support search operations in a single owner and multi-user environment. Some SE schemes involve a third party entity like Proxy Server (PS) , whose job is to transform each individual data owner’s index into a common index and also to transform each users query into a common query such that any user can search over any owner’s data.

II. Related work

The first SE scheme was proposed by using symmetric key encryption algorithm. SE by public key based approach was proposed by using Identity-Based Encryption (IBE). These approaches support search operation in a single owner and a single user environment, which allows only a single user to perform the search operation over the data of single owner. BE scheme allows multiple users to perform the search operation over the encrypted data. Another scheme supporting multiple users’ search operation is proposed by using CP-ABE. Keyword authorization based approach in supports search operation by multiple users. All these schemes support search operation in a single owner and multi- user environment, which allows the multiple users to perform the search operation over the encrypted data of a single owner. Multi-Keyword Ranked Search approach over the data of multiple owners is proposed. This approach supports search operation in a multi-owner and multi user environment, which allows multiple users to perform the search operation over the data of multiple owners. It incorporates Proxy Server (PS), which is responsible for transforming each owner’s encrypted index into a common index and also each user’s trapdoor into a common trapdoor such that any user can search over any owner’s index. As the queries frequently undergo transformation each time the user issues them, this approach incurs huge computational burden on PS due to the repeated transformation of queries again and again.

III. Proposed work

Searchable Encryption schemes provide security and privacy to the cloud data by storing data in encrypted form while enabling search over encrypted data. Searchable Encryption schemes in support search operation efficiently only in a single owner and single user environment. Various schemes like BE, ABE support search operations in a single owner and multi user environment. Some Searchable Encryption schemes involves a proxy server that allows multiple users to perform the search operation.

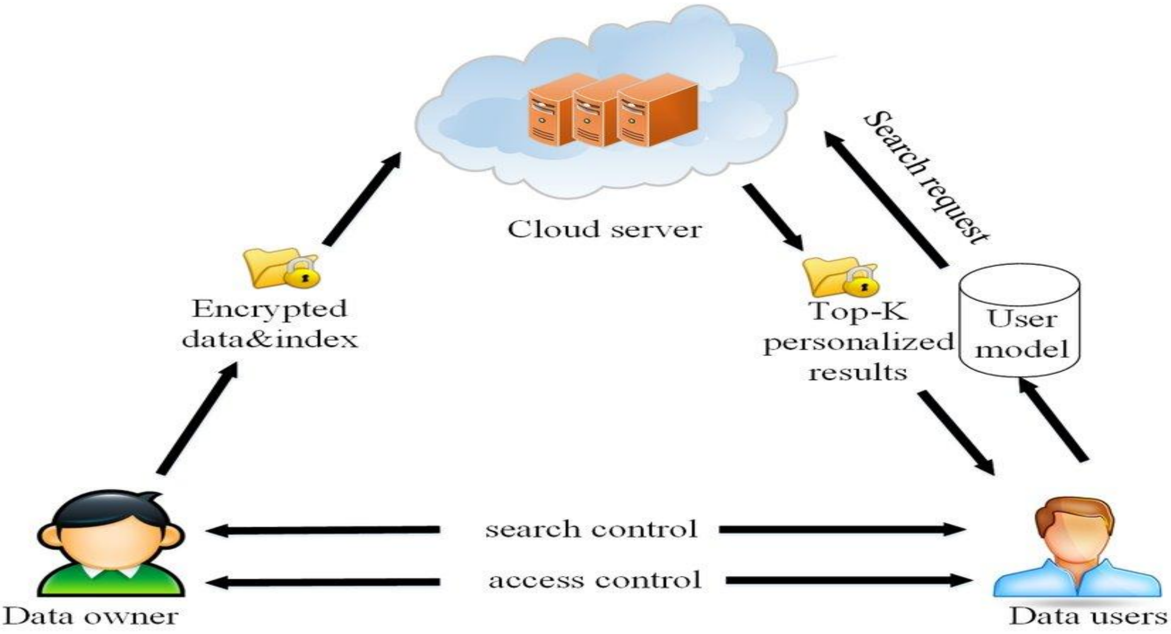


Figure.1: Architecture

IV. Experiment Results

The proposed approach is implemented using MATLAB and tested over 5000 documents of RFC data set .The correctness of the results is found by comparing the results of the proposed approach with a naive method, which guarantees the 100% accurate results.

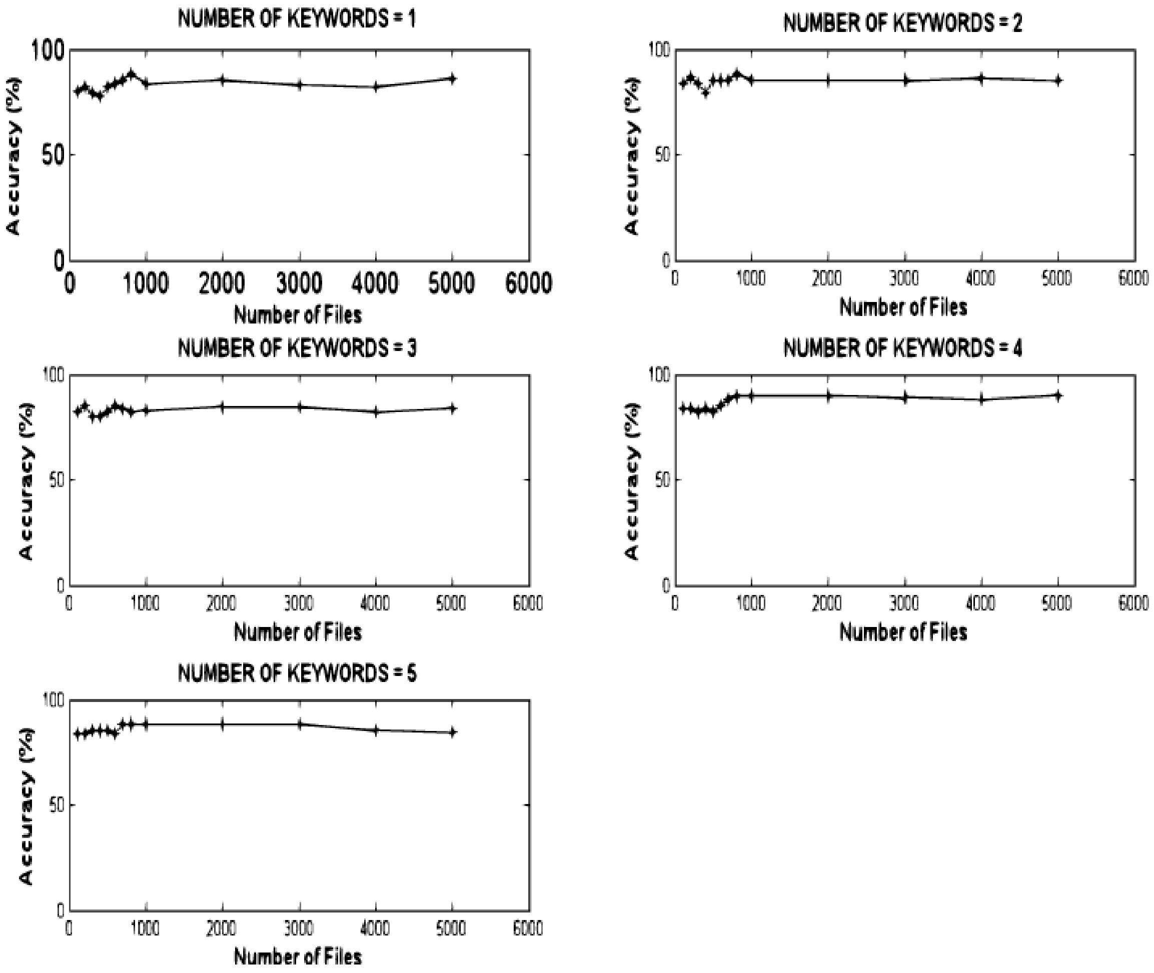
Naive Method:

1. The number of data owners is fixed and the data users are restricted to be one of the data owners.

2. Data users are authorized to access only certain documents and the index maintains this information. Each data owner/user has both private key and a public key.

3. Each document has its own index. For every unique keyword in the document, the index has one column for each data owner to store the encryption of the keyword done using the public key of that data owner. The TF-IDF score for each keyword is calculated and stored in the index.

4. During search operation, query is encrypted using query initiators public key.



NUMBER OF KEYWORDS = 1

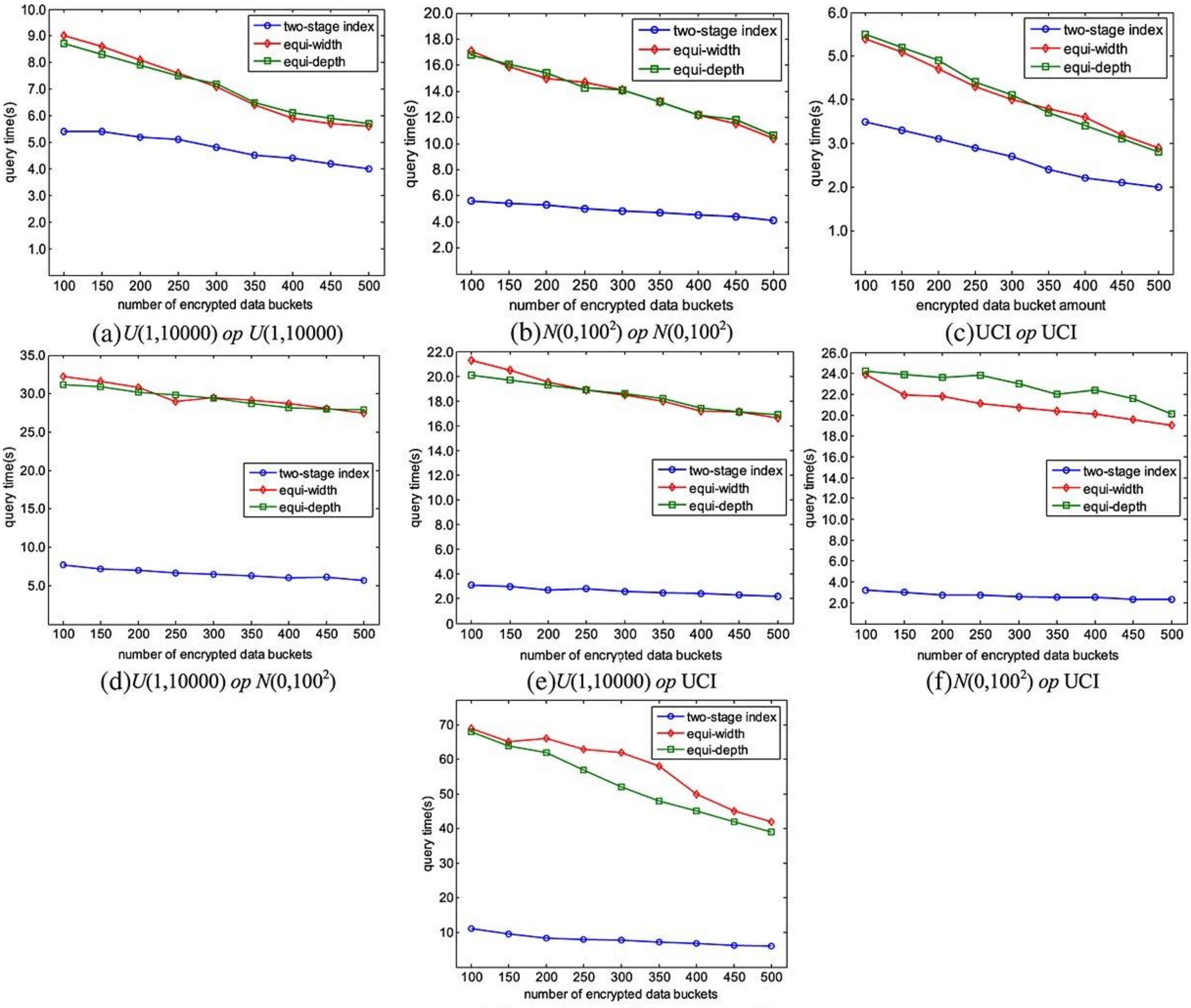
NUMBER OF KEYWORDS = 2

NUMBER OF KEYWORDS = 3

NUMBER OF KEYWORDS = 4

NUMBER OF KEYWORDS = 5

Fig 2: Searching time and comparison of method and proposed



(a)U(1,10000) *op* U(1,10000)

(b)N(0,100^2) *op* N(0,100^2)

(c)UCI *op* UCI

(d)U(1,10000) *op* N(0,100^2)

(e)U(1,10000) *op* UCI

(f)N(0,100^2) *op* UCI

(g)*t_student.stu_id=t_score.stu_id*

Fig 3: Efficient privacy preserved data query over ciphertext in cloud

V. Conclusion

A Proxy server based approach for supporting search operation over the data of multiple owners is proposed. Different from the existing approaches, the data user’s query in this approach can be used to search over the multiple owners’ data without transforming the query. In order to bypass the query transformation, the idea of partial encryption is used, i.e., half of each of the both index keyword and query keyword are encrypted by using the secret key of the data owner and the data user respectively and the other half of the index keyword and query keyword is encrypted by using common secret key of the proxy server. The experimental results confirm that the proposed approach is efficient. Future work could be to include a module for addition and revocation of data users and also to enhance the security functionalities of the proposed approach.

References:

1. 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.
2. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2004, pp. 506–522.
3. J. Lotspiech, “12 - broadcast encryption,” in Multimedia Security Tech- nologies for Digital Rights Management, W. Zeng, H. Yu, and C.-Y. Lin, Eds. Burlington: Academic Press, 2006, pp. 303 – 322.
4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryp- tion for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS ’06. New York, NY, USA: ACM, 2006, pp. 89–98.
5. W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, “Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing,”IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566–1577, 2016.
6. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” CCS- 2006:ACM conference on Computers and Communications Secu- rity, pp. 79–88, 2006.
7. Q. Wang, Y. Zhu, and X. Luo, “Multi-user searchable encryption with fine-grained access control without key sharing,” in 2014 3rd International Conference on Advanced Computer Science Applications and Technologies, Dec 2014, pp. 145–150.
8. Z. Deng, K. Li, K. Li, and J. Zhou, “A multi-user searchable encryption scheme with keyword authorization in a cloud storage,” Future Gener- ation Computer Systems, vol. 72, pp. 208–218, 2017.
9. T. Korenius, J. Laurikkala, and M. Juhola, “On principal component analysis, cosine and euclidean measures in information retrieval,” Infor- mation Sciences, vol. 177, no. 22, pp. 4893 – 4905, 2007.
10. RFC, “Request for comments database,” https://www.rfc- editor.org/retrieve/bulk/.

Author’s Profiles:

Dr. P Penchalaiah received Ph.D (Aug-2017) in Computer Science & Applications from Vikrama Simhapuri University, A.P State Govt. University, India. He qualified the UGC-NET & AP-SET exams that ensure minimum standards in teaching profession and research exams for Indian National. He has more than 12 years of experience in Academic and Industry (Software Engineer) as well. His research papers are indexed in international renowned indexing database like SCOPUS, WoS and he authored three books. His research areas of interest are Cryptology, Information Security, Cyber Security, Cyber Forensics, and Data Sciences.

V.Deepthi has received her degree in B.Sc Computers from S.V Arts &Science College-Gudur which is affiliated to SVU Nellore. Now persuing MCA at Narayana Engineering College-Gudur which is affiliated to JNTU Anantapuram.