International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Cloud Data retrieval process by Trapdoor Using indexes of Document

A.Mounika [1]& Ms. L. Sunitha Rani[2]

[1]M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

[2]Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

Abstract:

In a mobile cloud computing system, the outsourced data need to be encrypted due to the privacy and confidentiality concerns of their owners. Encrypted data should be accurately searchable and retrievable without any privacy leaks, concretely for the mobile client. The challenges imposed by wireless networks, such as latency sensitivity, poor connectivity, and low transmission rates. This leads to a long search time and extra network traffic costs when utilizing traditional search schemes. In this, a traffic and energy preserving encrypted search scheme is utilized for simplified search and retrieval process that reduces the network traffic reduced by engendering lightweight trapdoor i.e. .encrypted keyword compression technique utilizing mermer hashing technique and Ranked Serial Binary Search (RSBS) algorithm that reduces search time. In additament, we provide an authentic world application of the proposed scheme and verify the theoretical results with empirical observations on an authentic dataset.

Keywords: - Mapping Table, Compression, Ranking Search, Encrypted Search, Mobile Cloud.

1. INTRODUCTION

In today's data environment, cloud computing plays a major role in storing the data cloud computing becomes mundane due to the fact that it abstracts the load of astronomically immense scale data management in a cost efficacious manner. Hence there is a substantial amount of data like personal health records to data in the mobile, at the same time to transfer all these personal data to the cloud server might lead to an security issues such servers are called as un trusted cloud servers hence the users are more concern about the privacy to store their personal documents in the cloud server. To mitigate these quandary researchers came up with an encryption mechanism. To bulwark data security in the documents of cloud our project provides encryption system which surmounts the disadvantages of traditional encryption system, here our system is going to encrypt the documents and each document will have a unique keyword, index value afore it is uploaded to

the server these two are calculated and the keywords and indexes of the documents are encrypted afore uploading to the cloud server. When utilizer request certain documents from the cloud server they first send keywords to the pristine provider the provider will encrypt the keyword and index. And utilizing this keywords and index the utilizer will make a request to the cloud server and the server will return the top k documents to the utilizer utilizing a private key provided by the provider the utilizer can decrypt the documents.

2. RELATED WORK

Subsisting system

Here the FAH encryption algorithm for document indexes is employed in antecedent literature . Utilizing this FAH algorithm, we encrypt slices of each index. detailed encryption process for one slice Slicec of the index Ic is that encrypting l-bit term t in Slicec is utilized by the hash function , and mapping l-bit encrypted term into r-bit optimized term is by the mapping function, where and then accumulating all the r-bit optimized terms together. Conclusively we get the encrypted slice Slice . In this way, we can encrypt the index Ic by accumulating all the slices (s slices), and obtain the encrypted index I\ c equals accumulatin all the optimized terms in this document.

Proposed system

The ranked keyword search will return documents to the pertinence score. Zero et al. proposed a novel technique that makes the server side carry out the search operation. However, it should send many unrelated documents back and let the utilizer filter them. This is a waste of traffic, which is unsuitable for the mobile cloud. Bowers et al. proposed a distributed cryptographic system that preserved the security of the document retrieval process and the high availability of The system, but this system suffers from two network round trips and calculation involution for target documents. Wang et al. proposed a single round trip encrypted search scheme, but their system is not secure enough, as it leaks the keyword and associated document information from multiple keyword searches. Li et al. Proposed a single-keyword encryption search scheme utilizing ranked keyword search, which network communication between the utilizer and the cloud by transferring the computing burden from the utilizer to the cloud.

Advantages

We proposed a novel encrypted search system EnDAS over the mobile cloud, which ameliorates network traffic and search time efficiency compared with the

traditional system. We commenced with an exhaustive analysis of the traditional encrypted search system and. analyzed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is congruous for the mobile cloud to address these issues, where we utilized the TMT module. RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Determinately our evaluation study experimentally demonstrates the performance advantages of EnDAS

3. IMPLEMENTATION

Documents and indexes uploading process

Here providers are the one who is responsible for encrypting the index and keyword afore storing to the cloud. And these terms must be retained and each and every term which is encrypted keyword is treated as an index. The encryption algorithm can utilize here classic symmetric-key cryptography algorithm. The index here is calculated for a particular document predicated on the frequency of the each word count; determinately provider will upload the documents and corresponding indexes, keywords to the cloud.

Trapdoor generation process

To perform a search request utilizer has to authenticate with the provider first then here providers sends the secrete key to the utilizer to decrypt the documents stored in cloud. Once if authentication is prosperous the utilizer can request the documents if it is invalid utilizer can request the documents. On valid authenticate provider going to compute the trapdoors for the documents.

Document retrieval process

In this process, utilizer which he received a trapdoor from the provider, utilizing this trapdoors the utilizer requests a cloud server then cloud will abstract a noise in the trapdoor and searches for the documents then predicated on the keyword and index value the cloud sever will retrieve a top k documents to the utilizer

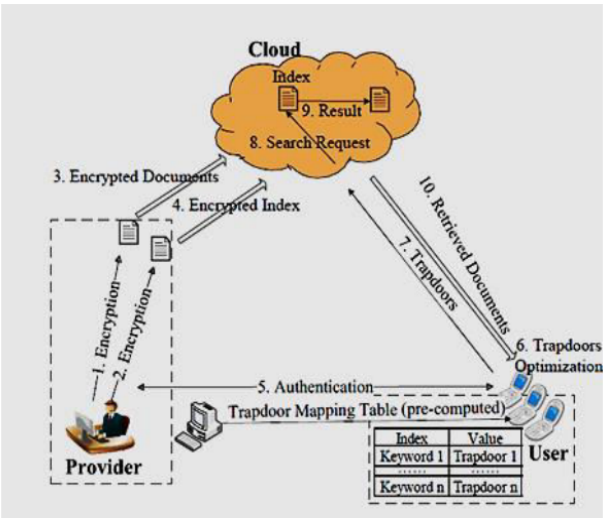

Fig:-1 Project Architecture

4. EXPERIMENTAL RESULTS

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

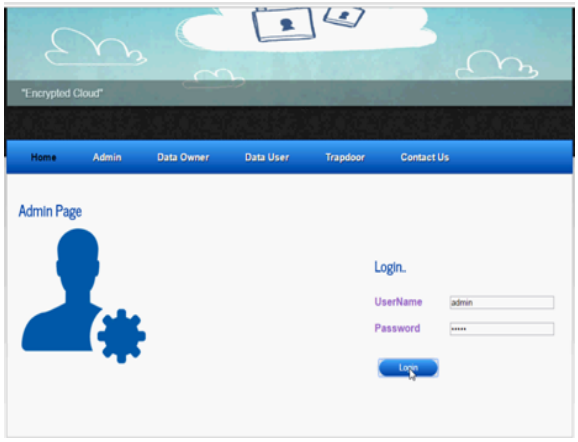

Fig:-2 Admin Login

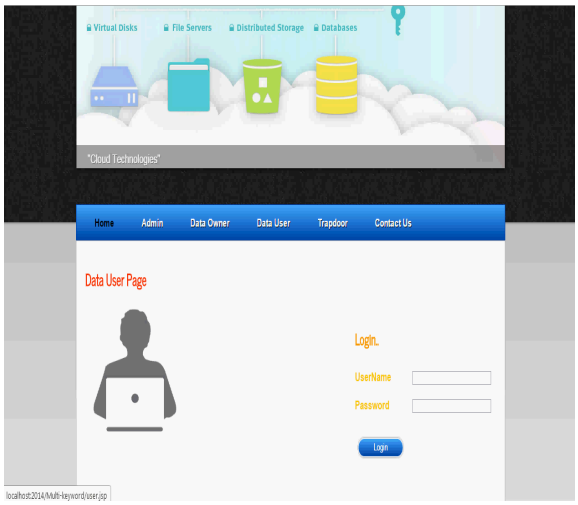

Fig:-3 Data User

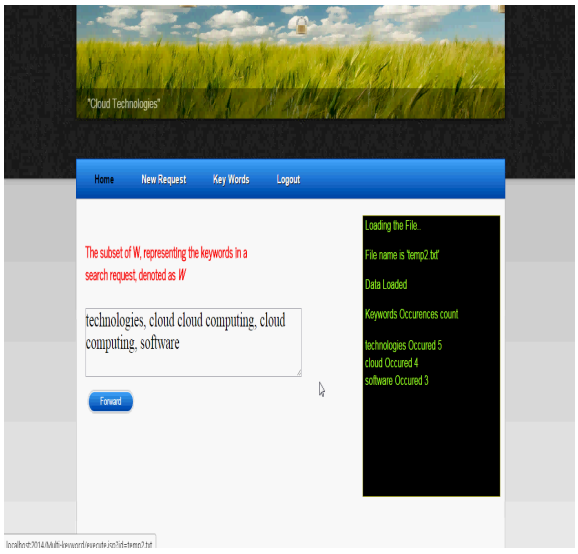

Fig:-4 Trapdoor Keys generation

Fig:-5 Symmetric Key generation

5. CONCLUSION

In this paper a novel encryption method has been proposed which enable decrease in search delay and ameliorated efficiency of network traffic over the cloud compared to traditional system initially we analyzed a traditional systems and what are the bottlenecks for the traditional system and endeavored to solve some of those circumscription by adopting a trapdoor compression method and RSBS algorithm(ranked serial binary search) these to enforced to a decremented cost and efficiency in the network traffic as well as decremented delay in search.

6. REFERENCES

[1] Ruhui Ma, Jian Li, Haibing Guan, Mingyuan Xia and Xue Liu EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service Volume: 3 Issue: ,2016, 8 Issn: 2321-8169 5303 – 530456

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manag. Data (COMAD), Jun. 2014, pp. 563–574.

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[4] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M.Wu, and D.W. Oard, "Confidentiality-preserving rank-ordered search," in Proc. ACM Workshop Storage Secure. Survivability (StorageSS), Oct. 2007, pp. 7–12.

[5] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order preserving symmetric encryption," in Advances in Cryptology-EUROCRYPT 2009, 2009, pp. 224–241.

[6] J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Trans. Cloud Comput., Feb. 2015.

[7] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in Proc. Int. Conf. Comput. Commun. (INFOCOM), Apr. 2014, pp. 2112– 2120.

[8] P. Wang, H. Wang, and J. Pieprzyk, "An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data," pp. 145–159, 2009.

[9] J. S. Culpepper, G. Navarro, S. J. Puglisi, and A. Turpin, "Top-k ranked document search in general text databases," in Proc. Annu. Euro. Conf. Algorithms (ESA), Sep. 2010, pp. 194–205.

[10] X. Lai, "On the design and security of block ciphers," Ph.D. dissertation, Diss. Techn. Wiss ETH Z¨ urich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. B¨ uhlmann, 1992.