International Journal of Research
Available at https://edupediapublications.org/journals
Special Issue on Conference Papers
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 06
March 2018

TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud TEES (Traffic and Energy saving Encrypted Search)

Mr.A.Mahesh, Mr. R. Uttham Sai
Assistant Professor, DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING , visvesvaraya college of engineering and technology
maheshakuthota@gmail.com

Abstract: Cloud storage provides a convenient and more storage at low cost, but data privacy is a major concept that prevents users from storing files on the cloud. One way of improving the data privacy is to encrypt the files before sending them onto the cloud and decrypt the files when they are downloaded. However, data encryption is a difficult task for the mobile devices, and data retrieval process is a complicated communication between the data user and cloud. With limited capacity and a limited battery life of mobile phones, these issues may introduce heavy overhead to computing and more power consumption for mobile device users, which makes the encrypted search over mobile cloud very difficult and as a challenge task for the user. In this paper, we have proposed, TEES, in which with more bandwidth and better energy efficient encrypted search over a mobile cloud. The proposed architecture removes the computation from mobile devices to the cloud, and hence we further can optimize the communications of the mobile clients and the cloud.

Keywords: Mobile Cloud Storage, Searchable Data Encryption, Energy Efficiency, Traffic Efficiency.

I. INTRODUCTION

Cloud storage system is a model in which data are maintained, managed and backup remotely on the cloud side, and mean while data is kept available for the users over network. Mobile Cloud Storage [1], [2] denotes as a huge amount of data that can be stored, and even acts as the primary file storage for the mobile devices [3]. Mobile Cloud Storage enables the mobile device users to store and recover files or data on the cloud through a wireless communication, which improves the data availability of the file sharing process without draining the local mobile device resources [4].

The data privacy issue is preeminent in cloud storage system, so the sensitive data is encrypted by the owner before sending onto the cloud, and data users recovers the important data by encrypted search scheme. In Mobile Cloud Storage, the modern mobile devices face with many of the same security threats as PCs, and various traditional data encryption methods are used in MCS [5], [6]. However, mobile cloud storage system provokes new challenges over the encrypted search schemes, in application of the limited computing and battery capacity of mobile device. Therefore, an efficient encrypted search scheme for MCS.

Hence, we came up with TEES (Traffic and Energy saving Encrypted Search) as an architecture for mobile cloud storage applications. TEES fulfils the capability, through modifying the ranked keyword search as the encrypted search platform, which has been invoked in cloud storage systems.

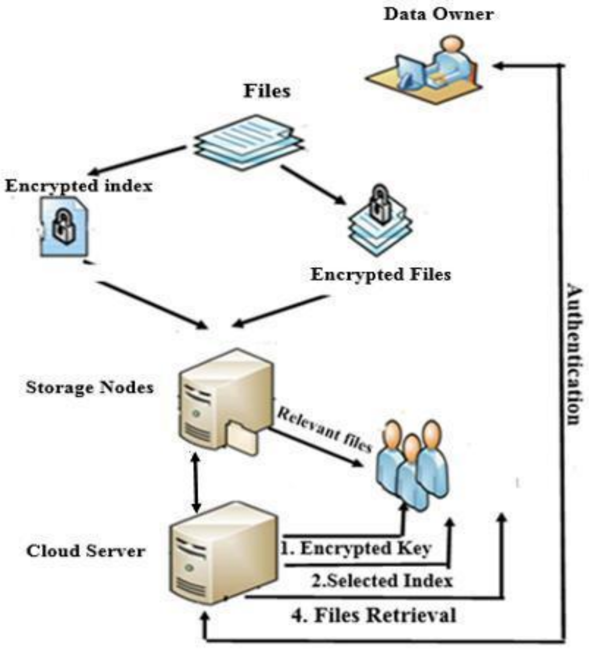

Fig. 1. Traditional Encrypted Search Architecture

II. RELATED WORK

1. Encrypted Search Schemes

In last recent years, encrypted search has expanded towards data sharing with protection of user‟s privacies. A scheme was proposed [7], which encrypted each word of a document separately. So, it is not adaptable with existing file encryption schemes and it does not deal with shrinked We now introduce the design how TEES addresses the data. After that many methods of Encrypted search power efficiency and the security challenges in modifying schemes were derived such as, In Information Retrieval, these processes. Term Frequency-Inverse Document Frequency [8].

i. Modified Process of Search and Retrieval

Up to now, encrypted search consists of Boolean keyword During the Preprocessing and indexing stages, the data search and ranked keyword search. In Boolean keyword owner receives a TF table as an index and uses OPS search, [7], [9], [10] the server sends back files based on (Order Preserving Encryption) to encrypt it. As a result, the presence or nonappearance of the keywords, without the cloud server is able to calculate the applicable scores looking at their importance.

2. Ranked keyword Search

Chang et al. [11] implemented a scheme of keyword search, but it cannot send back the most importance files. The earlier schemes used OPE to encrypt the file set. In the last work, Agrawal et al. [12] implemented one-to-one mapping OPE which will lead to Statistics Information Loss. Control. Wang et al, [13] implemented a one-to-many mapping OPE. They developed a complicate algorithm for security protection. However, their working and energy consumption would be a problem since their algorithm was complex and needed much computing resource.

III. TEES SYSTEM DESIGN

To adequately support an encrypted search scheme with a more security level on to the cloud data, we propose a new architecture that we named as TEES. According to some of the threats, we aimed is to design a solution for secured encrypted search over a mobile cloud storage. We firstly introduced the design idea, and then introduced development of our own protocols of file search and betterment for the cloud data. Our scheme attains the security and goals.

IV. THE BASIC IDEA OF TEES

The idea behind TEES is to offload the calculation and the ranking load of the appropriateness scores to the cloud. It has been noticed that offloading computation applications onto the cloud can be an efficient low power design philosophy [14]. Cloud providers can provide computing cycles, and users can use these cycles to diminish the amounts of calculation on mobile systems and save energy. However, offloaded applications aim to increase the transmission amount and thus increase the energy consumption from another aspect.

There are normally three main processes:

and rank them without decrypting the index. This deliver‟s the offloading of the estimate load secure and possible. Thus, the modified search and retrieval processes of TEES shown in Figure 2 follow the steps:

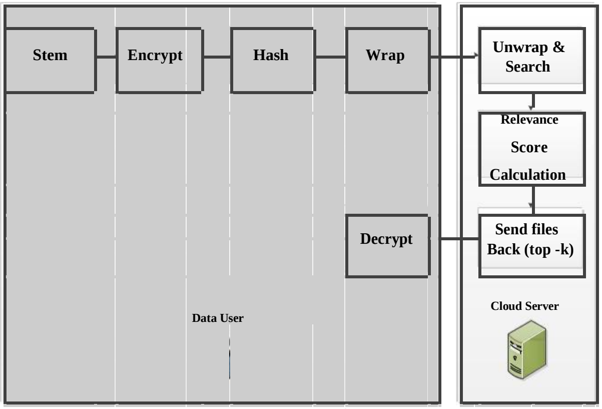

Fig. 2. ORS: Novel Process of Search and Retrieval

i) If a data user wants to receive the top-k related files based on a keyword then, they first obtain authentication from the data owner and then receives the key to encrypt the keywords.

ii) The data user branch the keywords to be inquire and encrypts it using the keys.

iii) The data user wraps the encrypted keyword into a tuple, including some noise to remove statistic information loss. Then, it is send to the cloud server together with the number k. The wrap method delivers the keyword identity for an attacker.

iv) On receiving the wrapped keywords, the cloud server first assures that it is accessed by an authorized user. If the server is identified by the data owner, the search is performed and a warning is also shown. The data user decrypts these files in the mobile client and recovers the original data.

V. POWER AND TRAFIC EFFECIENCE IMPROVEMENT SCHEME

The early schemes didn‟t directly apply to mobile clouds,

- The process of verification is used by the data owner to for gaining efficient energy consumption to address the verification the data users. particular issue for mobile cloud. In previous years, [12],
- The file sets and its index are stored in the cloud after [15], [16] OPE or fully homomorphic encryption being encrypted by the data owner during the techniques [17], [18] were recommended. They proved preprocessing and indexing stages. themselves secure and right enough for searching
- The data user searches the files according to a keyword encrypted data purpose. As energy consumption is by sending a request to the cloud server in the search becoming necessary, a complex algorithm is not suitable and retrieval processes. in mobile devices.

Hence, we choose a simple order preserving encryption method in our TEES. Kumar et al. [14] came up with a question of the importance of the energy and performance in mobile cloud computing. They concluded four basic approaches to saving energy and expanding mobile devices battery lifetime that can be considered.

VI. APPLICATION

A. TEES Implementation for Enhancement of Security Cloud

In order to achieve security enhancement with energy and traffic efficiency, we implement the modules in TEES using modified routines and new algorithms. Our system will be introduced in three parts.

As previously mentioned, the data owner should build a TF table as index and encrypt it using OPE in order to offload the calculation and ranking load of the relevance scores to the cloud. So as to control the statistics information loss, we enforced our one-to-many OPE in the data owner module. We also wrapped the keywords to be searched by including some noise in the data module to help handling the keywords-files loss. In order to get top-k important files, we achieved a ranking function to calculate the importance score on the cloud.

B. Redesign of the Data Owner Module

We customized the way of constructing the index to support the ORS scheme by one-to-many OPE and achieved it to control the statistics information loss. The authentication between the data owner and the data user is also enhanced in order to ensure the security of TEES.

VII. PROPOSED SYSTEM

Currently, many researches focused on developing the encrypted search efficiency with multi-keywords ranking. Wang et al. implemented a one - round trip search scheme which could examine the encrypted data. It was worth noticing that multi-keyword ranked search may acquire more serious Keywords-files Association Loss problem.

If attackers observed the keywords and returned files to learn some relationships between keywords and files, through wireless communication channels for mobile cloud. Cao et al. implemented privacy conserve method for multi-keyword encrypted search with a way to control the „double key loss”. In a fuzzy multi-keyword, fuzzy search scheme was granted, but it goes through from faulty search time with two round-trip communications [19].

Multi-keyword is probably the future main stream encrypted search scheme with greater searching accuracy, but presently on-going research cannot provide an authentic method. Hence, we will apply the single keyword with OPE TF-IDF encryption method to establish a more powerful and traffic efficient encrypted data search architecture [19].

VIII. GENERAL MODEL FOR PROPOSED SYSTEM

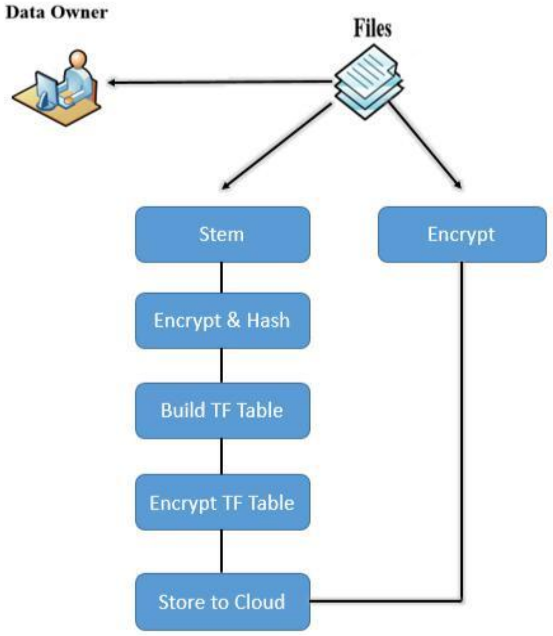

Fig 3. Process of Preprocessing and Indexing

File/Index Encryption: -

a. The data owner first executes the **preprocessing and indexing** work as shown on Figure 3. The owner should convert files that are selected to store on the cloud, for text search engines [20].

b. Every word in these files goes through stemming to retain the word stem. Next, the data owner encrypts and hashes every term to fix its entry in the index.

c. The index is then created by the data owner. Finally, the data owner encrypts the index and stores it into the cloud server, together with the encrypted file set.

IX. CONCLUSION AND FUTURE WORK

In this paper, we evolved a new architecture, TEES as a basic attempt to create a traffic and energy efficient encrypted keyword search tool on to mobile cloud storages. We began with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and we presented their inefficiency in a mobile cloud conditions.

TEES is more time and energy consuming than keyword search over plain-text, but simultaneously it saves significant energy related to traditional strategies promoting a similar security level. Based on TEES, this work can be expanded for more other novel implementations.

We have proposed a single keyword search scheme to make encrypted data search capable. However, there are possible extensions of our present work remaining. We would like to introduce a multi-keyword search scheme to implement encrypted data search on to mobile cloud in future.

[16] J. Zhang, B. Deng, and X. Li, "Additive order preserving encryption based encrypted documents ranking in secure cloud storage," Advances in Swarm Intelligence, pp. 58–65, 2012.

[17] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[18] Stehle and R. Steinfeld, "Faster fully homomorphic encryp-´ tion," Advances in Cryptology-ASIACRYPT 2010, pp. 377–394, 2010.

[19] Ma, R.; Guan, H. Li, J. "TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud" IEEE/ACM Transactions on

REFERENCES

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[3] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[6] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[7] D. 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] 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.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in CryptologyEurocrypt 2004. Springer, 2004, pp. 506–522.

[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] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.

[12] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[13] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[14] K. Kumar and Y. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" Computer, vol. 43, no. 4, pp. 51–56, 2010.

[15] A. Boldyreva, N. Chenette, Y. Lee, and A. O´ neill, "Order preserving symmetric encryption," Advances in Cryptology EUROCRYPT 2009, pp. 224–241, 2009.

Cloud Computing Volume PP, Issue 99 FEBRUARY 2015.

[20] J. Zobel and A. Moffat, "Inverted files for text search engines," ACM Computing Surveys (CSUR), vol. 38, no. 2, p. 6, 2006.