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 5, May 2019

TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud

Miss. Namrata Kakuste[1], Prof. M. D. Ingle[2]

PG Student, Department of Computer Engineering, JSPM's JSCOE, Hadapsar, Pune, India[1]

Assistant Professor, Department of Computer Engineering, JSPM's JSCOE, Hadapsar, Pune, India [2]

ABSTRACT: Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. In proposed system, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time and save the energy consumption on file retrieval, meanwhile the network traffics during the file retrievals are also significantly reduced.

KEYWORDS: Mobile cloud storage, searchable data encryption, energy efficiency, traffic efficiency

I. INTRODUCTION

Cloud storage system is a service model in which data are maintained, managed and backup remotely on the cloud side, and meanwhile data keeps available to the users over a network. Mobile Cloud Storage (MCS) denotes a family of increasingly popular on-line services, and even acts as the primary file storage for the mobile devices. MCS enables the mobile device users to store and retrieve files or data on the cloud through wireless communication, which improves the data availability and facilitates the file sharing process without draining the local mobile device resources. The data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme. However, mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration of the limited computing and battery capacities of mobile device, as well as data sharing and accessing approaches through wireless communication. Therefore, a suitable and efficient encrypted search scheme is necessary for MCS. Generally speaking, the mobile cloud storage is in great need of the bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable traffic fee. Therefore, we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and the network traffic, while keep meeting the data security requirements through wireless communication channels. To this end, we introduce TEES (Traffic and Energy saving Encrypted Search) architecture for mobile cloud storage applications. TEES achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in cloud storage systems. By careful redesign of ranked keyword search procedure, TEES offloads the security calculation to the cloud side to save the energy consumption of mobile devices, and TEES also simplify the encrypted search procedure to reduce the traffic amount for retrieving data from encrypted cloud storage.

II. LITERATURE SURVEY

N. Cao, C. Wang, firstly Authors describe and resolve the difficult of multi-keyword ranked search over encrypted cloud data, and create a variety of privacy requirements. Between numerous multi-keyword semantics, it select the effective similarity measure of “coordinate matching”, i.e., as various matches as likely, to effectively capture the relevance of outsourced documents to the query communication. For convention the challenge of supportive multi-keyword semantic without privacy breaks, Authors proposed a basic idea of MRSE. Then they give two better MRSE outlines to realize many stringent privacy requirements in two dissimilar threat models. Detailed analysis studying privacy and efficiency guarantees of presented schemes is given, and experiments on the real-world data set show that systems introduce low overhead on both computation and communication. [1]

B. Wang, S. Yu, W. Lou, and Y. T. Hou, authors tackled the challenging multi-keyword fuzzy search problem over the encrypted data. Authors presented and integrated several innovative designs to solve the multiple keywords search and the fuzzy search problems simultaneously with high efficiency. Our approach of leveraging LSH functions in the Bloom filter to construct the file index is novel and provides an efficient solution to the secure fuzzy search of multiple keywords. In addition, the Euclidean distance is adopted to capture the similarity between the keywords and the secure inner product computation is used to calculate the similarity score so as to enable result ranking. Authors presented a basic scheme as well as an improved scheme in order to meet different security requirements. Thorough theoretical security analysis and experimental evaluation using real-world dataset were carried out to demonstrate the suitability of this presented scheme for the practice usage. [2]

M. Li, S. Yu, K. Ren, W. Lou, as an initial attempt to achieve practical and effective multi-key word text search over encrypted cloud data, authors make contributions in two major aspects, supporting similarity-based ranking for more accurate search result and a tree-based search algorithm that achieves better-than linear search efficiency. For the accuracy aspect, they first exploit the popular similarity measure, i.e., vector space model with cosine measure, to effectively procure the accurate search result. Authors presented two secure index schemes to meet various privacy requirements in the two threat models. Eventually, the leakage of sensitive frequency information can be avoided. To boost search efficiency, Authors present a tree based index structure for the whole document set. From the utilization of the prototype of secure search system, it identifies three essential efficiency-related factors, by which the efficiency of the search algorithm upon our index tree can be significantly improved. Finally, thorough analysis on the real-world document set demonstrates the performance of BMTS and EMTS in terms of search effectiveness, efficiency and privacy. [3]

W. Sun, B. Wang, N. Cao, an analytical tool to support the organizations in assessing whether the use of private or public storage solution will result in a cost-efficient solution has been introduced. It has been shown analytically that the use of a public storage is likely to be cost-efficient whenever the organization’s acquisition cycles are relatively long, e.g. once per year. On the other hand, should the organization have a possibility to re-assess its storage needs and acquire additional storage often say, every second month - the use of the private storage capacity is likely to prove less expensive. Since the acquisition interval is determined by the organization’s ability to foresee the growth of storage demand, by the provisioning schedules of storage equipment providers, and by internal practices of the organization, among other factors, the organization owning a private storage solution may want to control some of these factors in order to attain a shorter acquisition interval and thus make the private storage (more) cost-efficient. [4]

III. EXISTING SYSTEM

Traditional file search and retrieval schemes, such as TRS, can provide data security but at the cost of more complicated procedures than Plain Text Search.

- TRS has been widely employed in cloud storage systems, but the encryption and the ranking incur the heavy calculation cost on a mobile device, and thus introduce the new challenges in efficiency for MCS traffic and energy consumption.

- It is necessary to rethink the design of the whole procedure with a careful consideration of the energy consumption and of the traffic efficiency. We analyze the model and indicate several possible optimizations.

IV. SYSTEM ARCHITECTURE

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

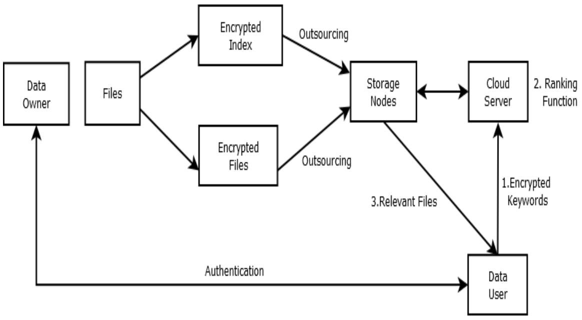


Fig 1: System Architecture

ALGORITHM

Algorithm: Build Index
Input: K, F
Output: I

```
Extract the terms $T = (t_{1,} t_{2,} t_{3, \dots ,} t_m)$ from the file set F.
for $t_i$ Ɛ T do
    Get the encrypted term     $(t_i)$ and hash it to get its entry (     $(t_i)$) in the TF table.
end for
for ti Ɛ T and $1 \leq j \leq |F|$ do
    Calculate the term frequency $t f_{ij}$ and get $\sim t f_{ij} = |(S/= | f_{ij}|)* t f_{ij} |$
end for
Compute $(\sim t f_{ij})$, and store it in the index I.
return I
```

V. RESULTS

We have considered the following two parameters as performance metrics:

- Time Complexity: The record inquiry and recovery time relies upon the document size and system data transmission. Significance score estimation offload and Multiple Keyword Ranked Search.
- Battery Consumption: We have determined the vitality utilization of cell phone by taking the distinction between the battery level of gadget amid looking and battery rate subsequent to downloading. This is improved the situation both single catchphrase and numerous watchwords.

The results are supported by graph of time complexity and battery consumption. The service provider can view these graphs through Service provider account.

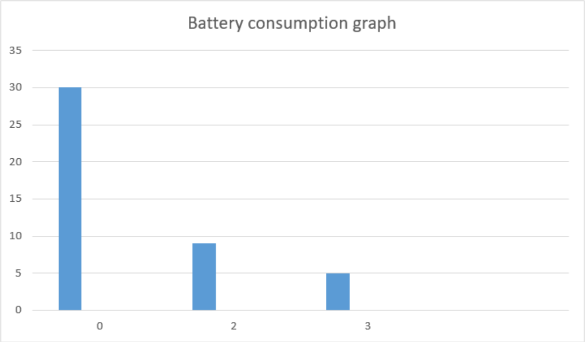


Fig 2: Battery Consumption Graph

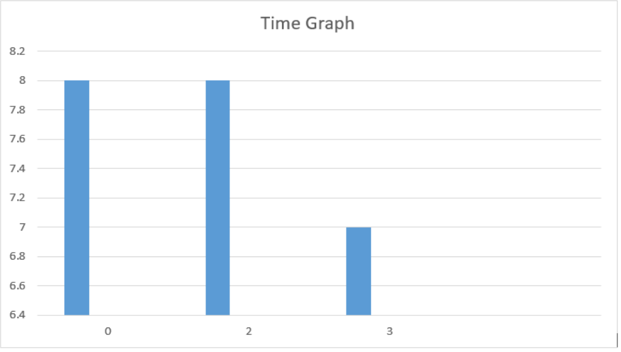
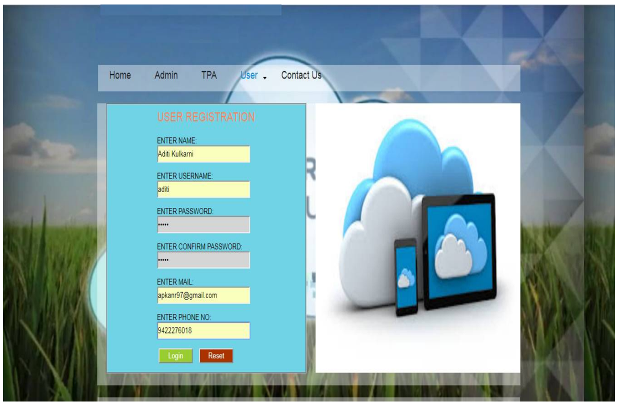


Fig 3: Time Graph



USER REGISTRATION

ENTER NAME:
Aditi Kulkarni

ENTER USERNAME:
aditi

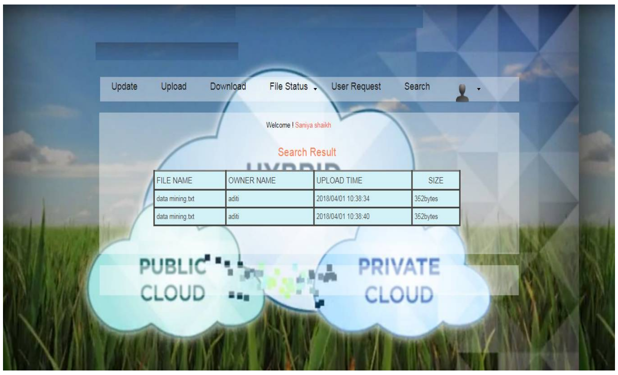
ENTER PASSWORD:
•••••

ENTER CONFIRM PASSWORD:
•••••

ENTER MAIL:
apkanr97@gmail.com

ENTER PHONE NO:
9422276018

Fig 4: User Registration

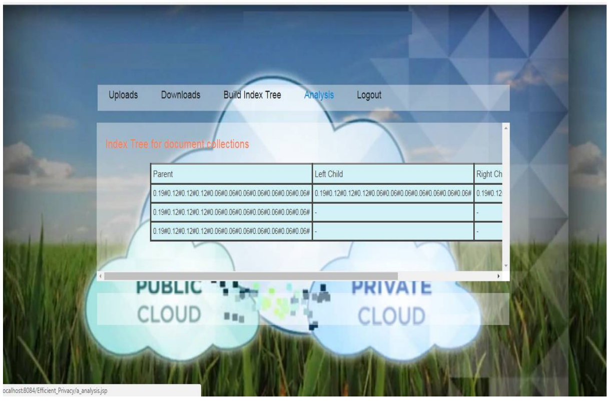


Welcome ! Saniya shaikh

Search Result

FILE NAME	OWNER NAME	UPLOAD TIME	SIZE
data mining.txt	aditi	2018/04/01 10:38:34	352bytes
data mining.txt	aditi	2018/04/01 10:38:40	352bytes

Fig 5: Show Result



Index Tree for document collections

Parent	Left Child	Right Ch
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-

ocalhost:8084/Efficient_Privacy/a_analysis.jsp

Fig 6: Analysis

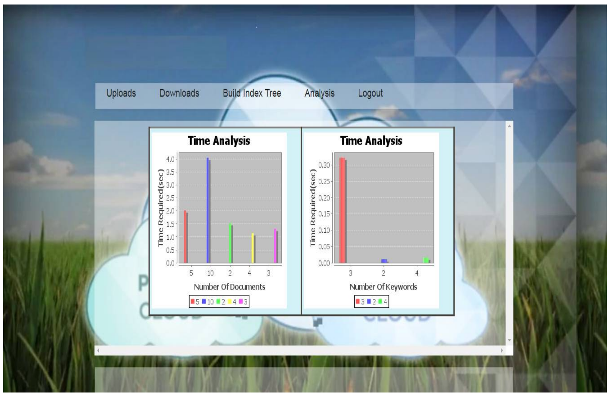


Fig 7: Time Analysis Ratio

ADVANTAGES

- User store the file on secure cloud
- Better speed for the searching.
- It is a reliable.
- It has more efficiency.
- Less latency time.

DOI: 10.15680/IJIRCCE.2019. 0705050

VI. CONCLUSION AND FUTURE WORK

In this paper, we developed an efficient implementation to achieve an encrypted search in a mobile cloud. The security study of proposed system showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. It saves significant energy compared to traditional strategies featuring a similar security level. Based on proposed system, this work can be extended to more other novel implementations. We have proposed a multi keyword search scheme to make encrypted data search efficient. To increase the searching efficiency and searching speed current work can be extend by adding some sorting algorithm to sort the files with the number of occurrences of keyword searched in past. It will avoid the extra time required to search same keywords again in same file.

REFERENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data”, Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222233, 2014.

[2] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud”, in INFOCOM, Proceedings IEEE, 2014.

[3] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, “Toward privacy assured and searchable cloud data storage services”, Network, IEEE, vol. 27, no. 4, pp. 5662, 2013.

[4] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Privacy preserving multi-keyword text search in the cloud supporting similarity-based ranking”, in Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ser. ASIA CCS 13. New York, NY, USA: ACM, 2013.

[5] C. Orencik and E. Savas, “Efficient and secure ranked multi-keyword search on encrypted cloud data”, in Proceedings of the 2012 Joint EDBT/ICDT Workshops. ACM, 2012.

[6] 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.

[7] 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, 2012.

[8] Q. Chai and G. Gong, ``Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers", in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012.

[9] 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.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multi-keyword ranked search over encrypted cloud data", in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.