International Journal For Technological Research In Engineering
Volume 3, Issue 12, August-2016 *ISSN (Online): 2347 - 4718*

REMODELING EFFICIENT ENCRYPTED DATA SEARCH OVER REMOTE MOBILE CLOUD SERVICES

Sangeetha. K[1], Ms. ABARNA.N[2]
[1]Research Scholar, [2]Assistant Professor
[1]Department of Computer Science, [2]PG & RESEARCH Department of Computer Science and Information Technology
Arcot Sri Mahalakshmi Women's College, Villapakam, Tamil Nadu, India

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, particularly 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 using traditional search schemes. In this, a traffic and energy saving encrypted search scheme is used for simplified search and retrieval process that reduces the network traffic reduced by generating lightweight trapdoor i.e. .encrypted keyword compression technique using mermer hashing technique and Ranked Serial Binary Search (RSBS) algorithm that reduces search time. In addition, we provide a real world application of the proposed scheme and verify the theoretical results with empirical observations on a real dataset.
Keywords: Mapping Table, Compression, Ranking Search, Encrypted Search, Mobile Cloud.

I. INTRODUCTION

Mobile cloud computing (MCC) provides a easy way to access many applications. It reduces the hardware requirement and provides many on-demand services and resources for these services to the user. In MCC, mobile users typically outsource their data to external cloud servers, e.g., Mobile Emails and mobile APPs, to access Anywhere, Any Time and Any How. However, as outsourced data typically contain sensitive confidentiality information, such as personal photos, emails, etc., which would lead to severe confidentiality and confidentiality violations, if without efficient protections. It is therefore necessary to encrypt the sensitive data before outsourcing them to the cloud. The data encryption, however, would result in salient difficulties when other users need to access interested data with search, due to the difficulties of search over encrypted data. This fundamental issue in mobile cloud computing accordingly motivates an extensive body of research in the recent years on the investigation of searchable encryption technique to achieve efficient searching over outsourced encrypted data.

In this, a traffic and energy saving encrypted search scheme is used for simplified search and retrieval process that reduces the network traffic for the communication of the selected index and reduces the file retrieval time.

Scope of the Work

To protect data security, the documents and their indexes are usually encrypted before outsourcing to the cloud for searches. Encrypted data should be effectively searchable and retrievable without any privacy leaks, particularly for the mobile client.

Motivation

In Mobile Cloud Apps Search an efficient Encrypted DAta Search (EnDAS) scheme are used to a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency.

Objectives

In Mobile Cloud Services 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 using traditional search schemes. This study addresses these issues by proposing an efficient Encrypted DAta Search (EnDAS) scheme as a mobile cloud service

II. EXISTING SYSTEM

When users need to query certain documents, they first send keywords to the original data provider. The provider then generates encrypted keywords (also called trapdoors) and returns the trapdoors to the user. The user then sends these trapdoors to the cloud. Upon receiving the trapdoors, the Cloud uses a special search algorithm to select a set of desired documents (encrypted) based on the encrypted indexes and given trapdoors. Finally, the user receives these encrypted search results and uses the private key from the provider to decrypt documents.

Disadvantages

Mobile devices are heavily utilized to request document search services which connects to internet by wireless network which incurs some challenges

1) Latency sensitivity
2) Poor connectivity
3) Low network transmission rate

III. PROPOSED SYSTEM

An efficient Encrypted Data Search (EnDAS) scheme as a mobile cloud service to tackle traffic and search time

inefficiency issues over the mobile cloud is proposed. It supports multi-keyword privacy-preserving search and greatly reduces network traffic and search delays. For network traffic, EnDAS pre-computes trapdoors for common search keywords and avoids one network round trip for recomputing trapdoor per request. Several mechanisms to compress trap-doors and could be effectively stored and loaded in mobile device memory is proposed. Ranked Serial Binary Search (RSBS) algorithm, which could reduce query time in the cloud is used.

Advantages

- Network traffic is reduced by a single round trip information exchange and the trapdoor compression method
- The search time is reduced by the RSBS algorithm and the Trapdoor Mapping Table (TMT) module
- The computing burden for generating trapdoors is also offloaded by the TMT module.

IV. METHODOLOGY

This section introduces the design of the EnDAS system and retrofitted trapdoor generation process in EnDAS. Compared the EnDAS system (Figure 3) with traditional system (Figure 1), the main difference is that (1) network traffic is reduced by a single round trip information exchange and the trapdoor compression method; and (2) the search time is reduced by the RSBS algorithm and the TMT module; and (3) the computing burden for generating trapdoors is also offloaded by the TMT module

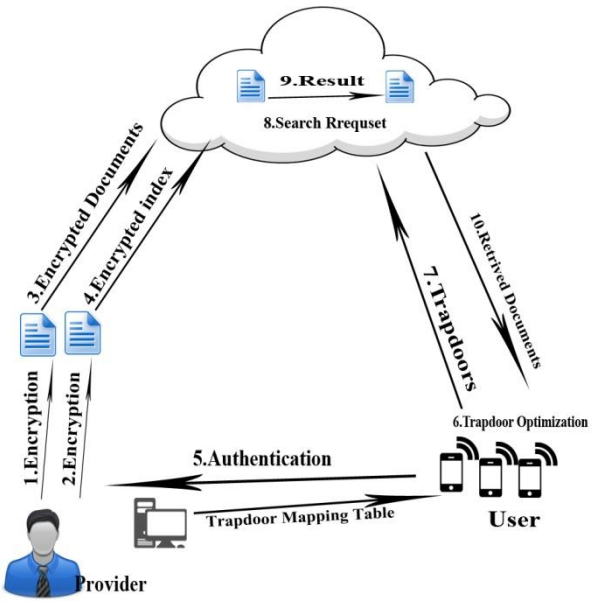

Figure 1: EnDAS Architecture

There are normally three main processes:

- The process of authentication is used by the data owner to authenticate the data users.
- The file set and its index are stored in the cloud after being encrypted by the data owner during the preprocessing and indexing stages.
- The data user searches the files corresponding to a keyword by sending a request to the cloud server in the search and retrieval processes.

Modified Process of Search and Retrieval

i) If a data user wants to retrieve the top-k relevant files based on a keyword, he first obtains authentication from the data owner and then receives the keys to encrypt the keyword.

ii) The data user stems the keyword to be queried and encrypts it using the keys.

iii) The data user wraps the encrypted keyword into a tuple, adding some noise to avoid statistic information leak; this tuple is used to perform the retrieval. Then, it is sent to the cloud server together with the number k. The wrap method renders the keywords indistinguishable for an attacker, which will be introduced.

iv) On receiving the wrapped keyword, the cloud server first makes sure that it is accessed by a legal user. If the server is notified by the data owner that this user is to become invalid in a near future, the search is performed but a warning is also issued. If this is a legal user, the server unwraps the tuple to recover the entry of the keyword and searches for it in the index. After calculating the relevance scores, the position of the files corresponding to the keyword is picked and the top k relevant files are sent back to the data user's mobile clients without performing any decryption on these files

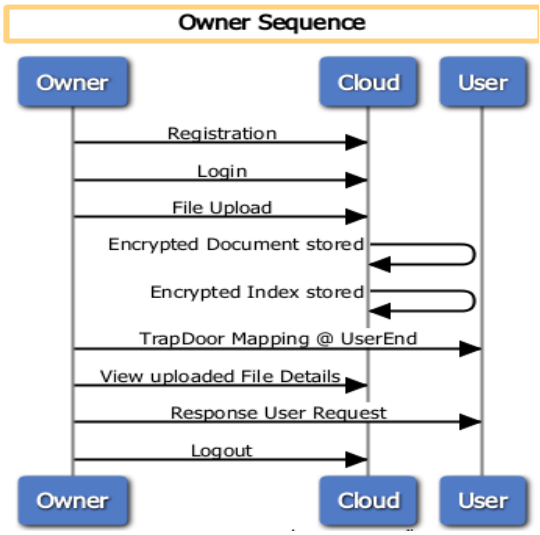

Figure 2- Owner Sequence Diagram

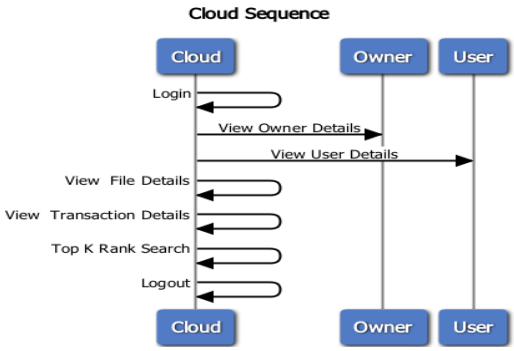

Figure 3- Cloud Sequence Diagram

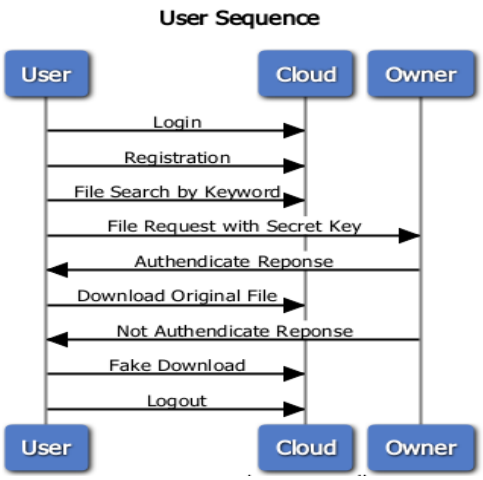

Figure 4- User Sequence Diagram

V. RESULTS

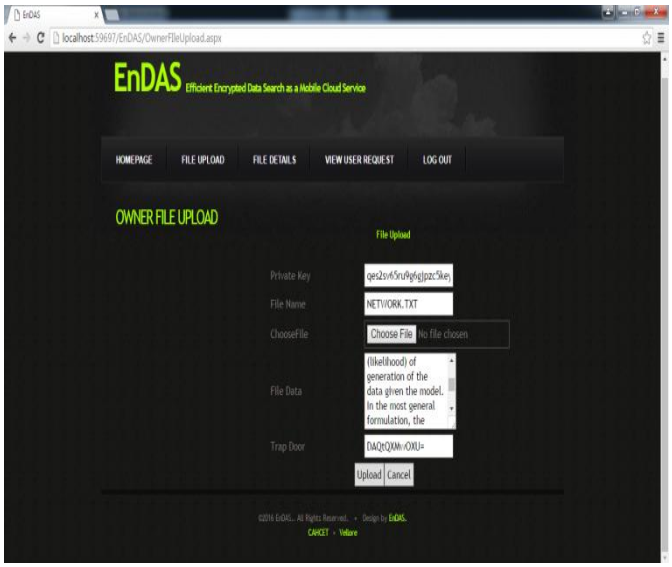

Figure 5 - TRAPDOOR GENERATOR AND FILE ENCRYPT

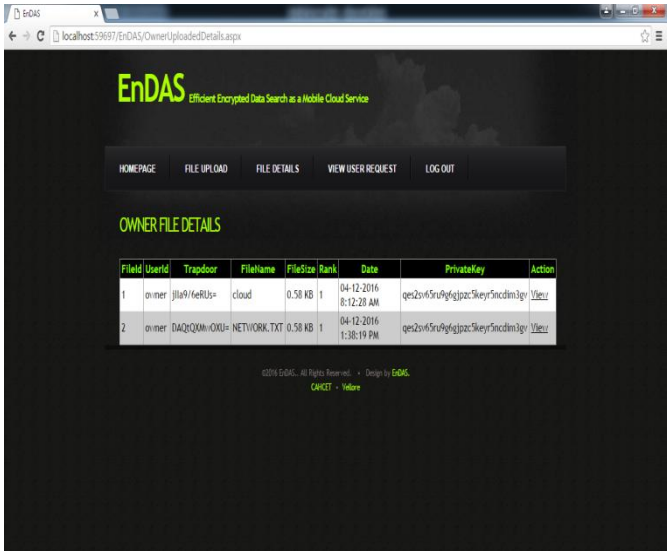

Figure 6- VIEW OWNER FILE DETAILS

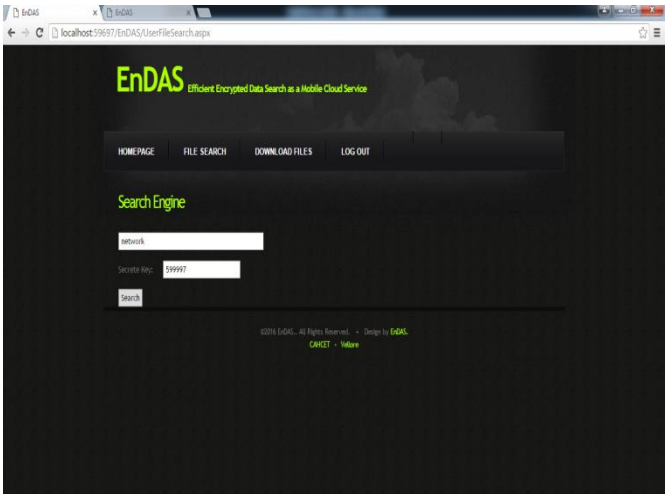

Figure 7- User File Search

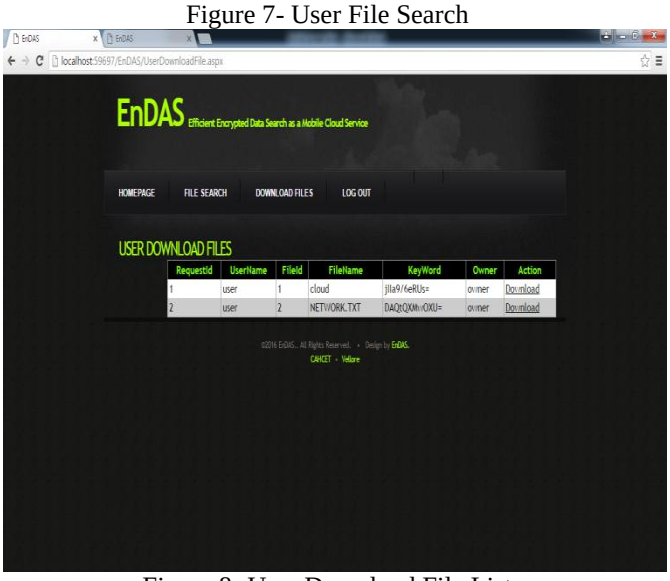

Figure 8- User Download File List

VI. CONCLUSIONS

A novel encrypted search system EnDAS over the mobile cloud is proposed here, which improves network traffic and search time efficiency compared with the traditional system. A thorough analysis of the traditional encrypted search system is done and also analyzed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module and the RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Finally evaluation study experimentally demonstrates the performance advantages of EnDAS.

VII. FUTURE ENHANCEMENT

This application enables keyword search which is tolerant to the typographical errors both in the queries and the data sources. Finally, we illustrated the performance of the proposed scheme with empirical analysis on a real data.

REFERENCES

[1] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Commun. Tech. Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27–31, 2011.
[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc.Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 829–837.
[3] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure andefficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Systems, vol. 23, no. 8, pp. 1467–1479, 2012.
[4] 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.
[5] C. Gentry and S. Halevi, "Implementing gentrys fully- homomorphic encryption scheme," in Advances in Cryptology–EUROCRYPT 2011, 2011, pp. 129–148.
[6] C. ¨ Orencik and E. Savas¸, "Efficient and secure ranked multi- keyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.
[7] Gartner, "Worldwide traditional pc, tablet, ultramobile and mobile phone shipments on pace to grow 7.6 percent in 2014," http://www.gartner.com/newsroom/id/2645115.
[8] Trellian, "Keywords number," http://www.keyworddiscovery.com/keyword-stats.html?date=2014-03-01.
[9] V. Rijmen and J. Daemen, "Advanced encryption standard," Federal Information Processing Standard, pp. 19–22, 2001.

