ANALYSIS OF AN EFFICIENT ENCRYPTED DATA ON MOBILE CLOUD

1. BATTU CHIRANJEEVI 2.BOMMINENI MADHAVARAO

[1]Asst Professor, CSE Department, Narsimha Reddy Engineering College

[2]Assoc Professor, CSE Department, Narsimha Reddy Engineering College

[1]chiru516@gmail.com,[2]bommineni6170@gmail.com

ABSTRACT

Cloud storage provides a convenient and more storage at low cost, but data security is a main concept that prevents users from storing documents on the cloud. One of the methods for improving security from the data owner point of view is to encrypt the document before outsourcing them onto the cloud and decrypt the documents after downloading them. In this paper there is some limitation as follows,(1)data encryption is a heavy overhead for the mobile devices, and(2) data recovery process incurs a difficult communication between the data user and cloud. (3)Typically with limited bandwidth capacity and limited battery life, these issues, established heavy overhead to computing and communication with mobile device users in which makes very difficult for encrypted search over mobile cloud. Now, we have proposed TEES (Traffic and Energy saving Encrypted Search), in which with more bandwidth and better energy efficient encrypted search architecture over mobile cloud.

1. INTRODUCTION

Cloud storage system is a service model in which data are maintained, managed and backup remotely on the cloudy side, and for now the data keeps accessible to the users over a network. Mobile Cloud Storage (MCS), denotes a family of more and more popular on-line services, and even acts as the primary file storage for the mobile devices [1]. MCSenables the mobile device users to store and recover files or information on the cloud through wireless communication, which improves the data accessibility and facilitates the file sharing process without difficult using local mobile device resources. The data privacy issue is supreme in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users recover the interested data by encrypted search scheme. In MCS, the recent mobile devices are confronted with many of the same security threats as PCs, and a variety of traditional data encryption methods are imported in MCS, but it incurs latest challenges over the traditional encrypted search schemes, in concern 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 essential for MCS. Finally, we establish 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 stage basis, which has been broadly employed in cloud storage systems.

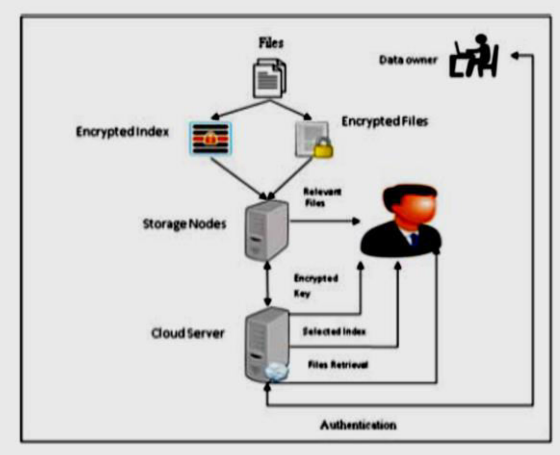


Figure 1: Traditional Encrypted Search Architecture

Mobile devices have become so integrated in the cloud environments that people are really talking about helping business people to get their work done easily. It is the fact that the Mobile Cloud Services are taken up by customers rather than enterprises rushing to use them up for their own needs. Mobile Cloud Computing can be considered by its unique advantages found in mobile computing. At present, there is a wide range of mobile cloud applications available. These applications fall into different areas such as image processing, natural language processing, shared GPS, shared Internet access, sensor data applications, querying, crowd computing and multimedia search. Even though there are plenty of benefits, there are some issues to be addressed and solved. Figure 1 shows data protection risks to regulate data. Network connection dependency, data sharing and integrating applications and security are some of the challenges in MCC environment. Another key challenge for Mobile Cloud Computing is intermittency and network availability.

2. RELATED WORK

2.1 ENCRYPTED SEARCH SCHEMES

Over the past latest years, encrypted search has evolved to the facility data sharing with the protection of users ‘privacies. Song et al. [2] proposed a scheme in which encrypted each word of a document individually. So its not suitable to existing file encryption schemes but it cannot deal with compressed data. In Information recovery, TF-IDF (term frequency-inverse document frequency) is a statistic which reflects how important a word is to a document in a collection or quantity. It is frequently used as a weighting factor in keyword-based recovery and text mining. Until now encrypted search includes Boolean keyword search and ranked keyword search. In Boolean keyword search [2],[3], [4], the server sends back files only based on the existence or absence of the keywords, without looking at their importance.

Ranked keyword Search: Chang et. al., [5] provided scheme of keyword search, but it does not send back the most important files. In ranked encrypted search, the server sends back the top-k ranked files. In previous work, **Agrawal et al. [8]** proposed a one-to-one mapping OPE which will lead to Statistics Information Leak Control. Wang et al. [7] presented a secure ranked keyword search over encrypted cloud data. though, in

their work the terms are directly related to the documents, which could lead to potential information leak. Wang et al. [6] proposed a one-to-many mapping OPE(order preserving encryption)technique to produced secure those sensitive score information; They implemented a complicate algorithm for security protection.

2.2 POWER EFFICIENT AND TRAFFIC EFFICIENCYIMPROVEMENTS SCHEMES

The previous schemes cannot directly apply to mobile cloud, for achieving efficient energy consumption to address the important issue for mobile cloud. In recent years many OPE [8] methods have been proposed. They proved themselves secure and accurate enough for searching encrypted data purpose. However, they will cost many computing resources. The consumption is becoming important factor, a complicated algorithm isnot suitable in mobile devices. Therefore we choose simple order preserving encryption method in our TEES.

Miettinen et al. provided an analysis of the critical factors affecting the energy consumption of a mobile client in cloud computing. They also present some measurements related to the central characteristics of existing mobile devices that define the basic stability between local and remote computing. Carroll et al. also presented a complete analysis of the power utilization of mobile phone, in which the energy convention and battery lifetime were tested below a number of convention patterns.

2.2 PRIVACY PRESERVING RANK SEARCH

Privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and established a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi keyword semantics. The efficient principle of ―coordinate matching‖, is choosed.i.e. as many matches as possible, to capture the similarity between search query and data documents, and further to use ―inner product similarity‖ to quantitatively formalize such principle for similarity measurement. Here a basic MRSE scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Overall analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication. Privacy protection ranking operation, should not leak any keyword related information. On the other hand, to improve search result accuracy as well as enhance user searching experience. It is also crucial for such ranking system to support multiple keywords search, as single keyword search often yields far more result. As a common practice indicated by today’s web search engines (e.g., Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. And each keyword in the search request is able to help narrow down the search result further. ―Coordinate matching‖, i.e., as many matches as possible, is an efficient principle among such multi-keyword semantics to refine the result relevance, and has been widely used in the plaintext information retrieval (IR) community. However, to apply it in the encrypted cloud data search system remains a very challenging task because of inherent security and privacy obstacles, including various strict requirements like data privacy, index privacy, keyword privacy, and many others. privacy, and many others.

3. TEES SYSTEM DESIGN

To well support an encrypted search scheme with a high security level over cloud data, we have to introduced anew architecture that we name TEES. Now we are provided to the design of secure encrypted search over mobile cloud storage .Our scheme achieves the security and efficiency goals mentioned.

3.1 THE BASIC IDEA OF TEES

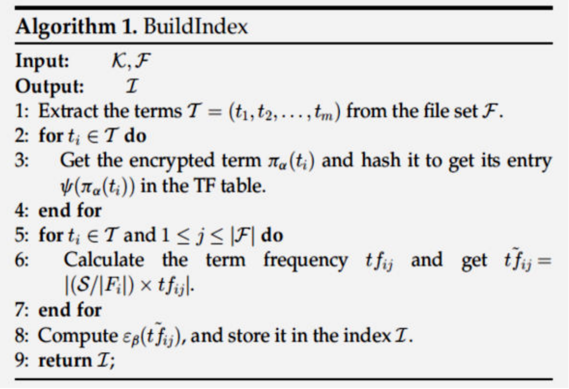
The basic idea at the back TEES is to pass on the computation and the ranking load of the importance scores to the cloud. Cloud providers can give computing cycles, and users can apply these cycles to decrease the amounts of computation on mobile systems and save energy. Though, simultaneously offloaded applications intend to increase the communication amount and thus raise the energy used from an additional aspect.Thereare usually three major processes: (i)The process of confirmation issued by the data owner to confirm the data users.(ii)The file set and its index are stored in the cloud once being encrypted by the data owner for the duration of the preprocessing and indexing stages.(iii)The data user searches the files consequent to a keyword by sending are quest to the cloud server in the search and recovery processes.

3.2 MODIFIED PROCESS OF SEARCHING AND RETRIEVAL:

In the preprocessing and indexing stages, the data owner gets a TF table like index and uses Order Preserving Encryption (OPE) to encrypt it. As a outcome, the cloud server is capable to evaluate the relevance scores an drank them with no decrypting the index. This renders the offloading of the computational load secure and possible. Presently, many researches focused on developing the encrypted search efficiency with multi-keywords ranking. Wang et al. [6] implemented a one - round trip search scheme which could observe 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 [9]. Multi-keyword is probably the future main stream encrypted search scheme with greater searching accuracy, but presently on-going research cannot give an authentic method.

4. TEES IMPLEMENTATION FOR SECURITYENHANCEMENT FOR MOBILE 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 leak, we implement our one-to-manrope in the data owner module (Section 4.1). We also wrap the keywords to be searched by adding some noise in the data user module to help controlling the keywords-files association leak. In order to get top-k relevant files, we implemental ranking function to calculate the relevant score on the cloud. Given a keyword in ORS, the cloud server is in charge of calculating the relevance scores for the data user to get the corresponding top-k relevant files. Therefore, we implement both the unwrap and rank functions in the cloud server module (Section 4.3). Hence these modules are modified compared with the traditional ones.



```
Algorithm 1. BuildIndex
Input:    $\mathcal{K}, \mathcal{F}$
Output:   $\mathcal{I}$
Extract the terms $\mathcal{T} = (t_1, t_2, \ldots, t_m)$ from the file set $\mathcal{F}$.
for $t_i \in \mathcal{T}$ do
    Get the encrypted term $\pi_\alpha(t_i)$ and hash it to get its entry $\psi(\pi_\alpha(t_i))$ in the TF table.
end for
for $t_i \in \mathcal{T}$ and $1 \leq j \leq |\mathcal{F}|$ do
    Calculate the term frequency $tf_{ij}$ and get $\tilde{tf}_{ij} = |(\mathcal{S}/|F_i|) \times tf_{ij}|$.
end for
Compute $\varepsilon_\beta(\tilde{tf}_{ij})$, and store it in the index $\mathcal{I}$.
return $\mathcal{I}$;
```

ADVANTAGES:

- The traditional encrypted search architecture focuses on network traffic and search time and conventional approach is not applicable in mobile-cloud environments.
- An efficient encrypted data search scheme to address these challenges.
- This architecture includes a trapdoor compression method to reduce traffic costs, as well as a Trapdoor Mapping Table (TMT) module and RSBS algorithm to reduce search time. Save computing and battery capacities of mobile device.

Bandwidth and energy efficiency for data encrypted search scheme, due to the save battery life and payable traffic fee

CONCLUSION

In this paper, we developed a new architecture, TEES as an original challenge to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. TEES is a little more time and energy overriding than keyword search over plain-text, but simultaneously it saves important energy compared to usual strategies featuring a like security level. Based on TEES, this work can be unlimited to more new novel implementations. We have to proposed a single keyword search method to make encrypted data search well-organized. However, there are still some possible extensions of our recent work remaining. In future we would like to proposed a multi-keyword search method to perform encrypted data search over mobile cloud. Since our OPE algorithm is a simple one, another expansion is to find a great algorithm which will not spoil the efficiency.

REFERENCES

[1] Bowers.K, Juels.A, and Oprea.A, ―Hail: a high-availability andintegrity layer for cloud storage,‖ in Proceedings of the 16th ACMconference on Computer and communications security. ACM, 2009,pp. 187–198.

[2] Cao.N, Wang.C, M. Li, Ren.K, and Lou.W, ―Privacy-preserving multi-keyword ranked search over encrypted cloud data,‖ Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[3] Carroll.A and Heiser.G, ―An analysis of power consumption ina smartphone,‖ in of the 2010 USENIX conference onUSENIX annual technical conference. USENIX Association, 2010,pp. 271–284

[4] Chai.Q and Gong.G, ―Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,‖ in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922

[5] Gentry.C and Halevi.S, ―Implementing gentry´s fully homomorphic encryption scheme,‖ Advances in Cryptology–EUROCRYPT 2011, pp. 129–148, 2011

[6] Gentry.C, ―A fully homomorphic encryption scheme,‖ Ph.D. dissertation, Stanford University, 2009

[7] Huang.D,―Mobile cloud computing,‖ IEEE COMSOC Multimedia Communications Technical Committee (MMTC) ELetter, 2011.

[8] Hou.S,Uehara.T, Yiu.S, Hui.L.C, and Chow.K, ―Privacy preserving multiple keyword search for confidential investigation of remote forensics,‖ in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on. IEEE, 2011, pp. 595–599.