I J C T A, 9(13) 2016, pp. 5987-5994

Efficient Content Search for Preserving Energy over Mobile Cloud

Smriti Vardhan* **and Pallabi Malakar***

ABSTRACT

In this paper, we intend TEES (Traffic and Energy saving Encrypted Search), a bandwidth and vitality efficient encoded search design over mobile cloud. Cloud storage provides a suitable, massive, and accessible storage at low cost, but data privacy is a major distress that averts users from storing files on the cloud suspiciously. One way of improving isolation from data owner point of view is to encrypt the files before farm out them onto the cloud and decrypt the files after transferring them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a difficult communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy above to computing and communication as well as a higher power feasting for mobile device users, which makes the encrypted search over mobile cloud very stimulating. The proposed architecture offloads the totaling from mobile devices to the cloud, and we further augment the communication between the mobile clients and the cloud. It is monstrated that the data secrecy does not degrade when the performance improvement methods are adapted. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval, temporarily the network traffics during the file retrievals are also significantly reduced.

I. INTRODUCTION

Cloud storage system is a facility model in which data are preserved, accomplished and backup distantly on the cloud side, and temporarily data saves available to the users over a network. Mobile Cloud Storage (MCS) denotes a family of progressively popular on-line services, and even acts as the primary file storage for the mobile devices. MCS permits the mobile device users to collection and regain files or data on the cloud through wireless communication, which advances the data availability and enables the file sharing process without demanding the local mobile device resources. The data privacy issue is paramount in cloud storage system, so the delicate data is encrypted by the owner before farm out onto the cloud, and data users recover the interested data by encrypted search scheme. In MCS, the modern mobile devices are challenged with many of the same security threats as PCs, and various outdated data encryption methods are imported in MCS. However, mobile cloud storage system incurs new challenges over the traditional scrambled search schemes, in consideration of the limited calculating and battery capacities of mobile device, as well as data sharing and retrieving methods through wireless communication.

II. RELATED WORK

Dawn Xiao dong Song David Wagner Adrian Perrig proposed Practical Techniques for Searches on Encrypted Data. In his paper, he describe his cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. His techniques have a number of crucial advantages. They are provably secure; they provide provable isolation for encryption, in the sense that the entrusted server cannot learn anything about the plaintext when only given the cipher text; he

* Department of Information Technology, Sathyabama University, Chennai, Tamilnadu
E-mail: smritivardhan@gmail.com; pallavimalakar25@gmail.com

provided query isolation for searches, meaning that the entrusted server cannot learn anything more about the plaintext than the search result; he provided controlled searching, so that the entrusted server cannot search for an artery word without the user's authorization; he also support hidden queries, so that the user may ask the entrusted server to search for a secret word without revealing the word to the server. The algorithms he present are light, fast (for a document of length, the encryption and search algorithms only need flow cipher and block cipher operations), and introduce almost no space and connection overhead, and hence are practical to use today.

Dan Boneh, Giovanni Di Crescenzo proposed Public Key Encryption with keyword Search. In his paper he described the problem of searching on data that is uncorrupted using a public key system. Considering user Bob who sends email to user Alice uncorrupted under Alice's public key. An email entrance wants to test whether the email contains the keyword immediate so that it could track the email accordingly. Alice, on the other hand does not wish to give the entrance the ability to decrypt all her messages. He spout and construct a mechanism that enables Alice to provide a key to the entrance that enables the entrance to test whether the word urgent" is a keyword in the email without studying everything else about the email.

He refer to this mechanism as Public Key Encryption with keyword inquiry. As another example, consider a mail server that stock various messages publicly uncorrupted for Alice by others. Using his mechanism Alice can send the mail server a key that will permit the server to identify all messages containing some specie keyword, but learn nothing else. He spout the concept of public key encryption with keyword search and give several constructions.

Cong Wang, Ning Cao proposed Enabling Secure and Efficient Ranked Keyword Search over expanded Cloud Data. Cloud computing economically enables the pairing of data service expanding. However, to protect data isolation, delicate cloud data has to be uncorrupted before outsourced to the commercial public cloud, which makes useful data utilization service a very confronting task. Although traditional salable encryption techniques allow users to securely search over uncorrupted data through keywords, he support only Boolean search and are not yet sufficient to meet the useful data utilization need that is naturally demanded by large number of users and huge amount of data files in cloud. In his paper, he define and solve the problem of secure ranked keyword search over uncorrupted cloud data. Ranked search greatly build up system usability by permissive search result relevancy ranking instead of sending identical results, and further ensures the file betterment accuracy. Specifically, he explore the statistical measure approach, i.e. relevancy score, from information betterment to build a potect salable index, and develop a one-to-many order-preserving scaling technique to properly assure those sensitive score information. The resulting pattern is able to forward efficient server-side ranking without losing password privacy. Thorough analysis shows that his proposed solution enjoys "as-strong-as-possible" security assurance compared to previous salable encryption schemes, while correctly performing the goal of ranked keyword search. Comprehensive experimental results determined the ability of the proposed solution.

Cong Wang and Wenjing Lou proposed Secure Ranked Keyword Search over Encrypted Cloud Data. Coud Computing becomes frequent, sensitive information are being increasingly stylized into the cloud. For the protection of data privacy, sensitive data has to be uncorrupted before expanding, which makes effective data usage a very challenging task. Although popular searchable encryption schemes allow users to securely search over uncorrupted data through keywords, these techniques hold only Boolean search, without grab any relevancy of data files. This approach suffers from two main difficulty when directly applied in the situation of Cloud Computing. On the one hand, users, who do not positively have pre-knowledge of the uncorrupted cloud data, have to disclose process every retrieved file in order to find ones most duplicate their interest; On the other hand, customarily retrieving all files containing the examine keyword further acquire unnecessary network traffic, which is absolutely unpopular in today's pay-as-you-use cloud paradigm.

Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou proposed Privacy-Preserving Multi-keyword Ranked Search over uncorrupted Cloud Data. With the approach of cloud computing, data owners are motivated to expand his complicated data management systems from local sites to the financial public cloud for great complaint and economic savings. But for protecting data privacy, delicate data has to be uncorrupted before expanding, which obsoletes traditional data usage based on plaintext keyword search. Thus, permissive an encrypted cloud data search service is of outstanding importance. Considering the large number of data users and script in the cloud, it is necessary to allow multiple keywords in the search appeal and arrival script in the order of their purpose to these keywords. Related works on salable encryption focus on single keyword search or Boolean keyword search, and seldom sort the search results. In his paper, for the first time, he define and solve the confronting problem of privacy preserving multi-keyword ranked search over uncorrupted cloud data (MRSE).He establish a set of strict privacy essential for such a secure cloud data utilization system. Among various multi keyword defination, he choose the efficient similarity measure of "coordinate dual", i.e., as frequent examining as feasible, to gain the relevance of data documents to the inspection query. He another need "inner stock affiliation" to intuitively cost such similarity reassure. He first propose a basic idea for the MRSE based on secure inner product estimation, and then gave two significantly improved MRSE schemes to achieve various drawing privacy requirements in two different threat models. Thorough analysis inspecting privacy and efficiency guarantees of proposed schemes is given. Undertaking on the real-world dataset further showed proposed schemes indeed introduce low overhead on estimation and communication.

Bing Wang, Shucheng Yu, Wenjing Lou and Y. Thomas Hou proposed Privacy-Preserving Multi-Keyword Fuzzy Search over uncorrupted Data in the Cloud able keyword search directly over encrypted data is a desirable technique for powerful utilization of encrypted data expand to the cloud. Existing solutions provide multi keyword exact enquiry that does not bear keyword spelling error, or original keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search outline rely on building an expanded index that covers available keyword misprint, which lead to significantly bigger ratio file size and higher search complication. In his paper, he proposed a novel multi keyword fuzzy search scheme by abusing the locality-sensitive hashing technique. His proposed scheme achieves fuzzy matching through algorithmic layout rather than expanding the index file. It also eliminates the use of a predefined dictionary and forcefully supports multiple keyword flossy search without increasing the index or search complication. Extensive analysis and experiments on real-world data show that his proposed scheme is secure, efficient and accurate. To the best of our ability, this is the first work that archives multi-keyword fuzzy search over encrypted cloud data.

In the above described model the data confidentiality issue is supreme in cloud storage system, so the delicate data is encrypted by the owner before subcontracting onto the cloud, and data users retrieve the keen data by encrypted search scheme. Current mobile devices are opposed with many of the same security risk as PCs , and various outdated data encryption methods are imported in MCS Mobile cloud storage system incurs new experiments over the traditional encrypted search schemes, in deliberation of the limited computing and battery dimensions of mobile device, as well as data distribution and accessing approaches through wireless

III. SEARCHING METHODOLOGY OVER MOBILE CLOUD

TEES decreases the energy consumption by 35%_55% by unburdening the calculation of the relevance scores to the cloud server. With a simplified search and retrieval process, TEES decreases the network traffic for the connection of the selected index, and reduces the file rescue time by 23%_46% in our experiments. In implementing the upgrade encrypted search procedure, TEES reallocates the encrypted index to avoid statistics information leak, and wraps keywords adding noise in order to furnish them in unique to the attacker.

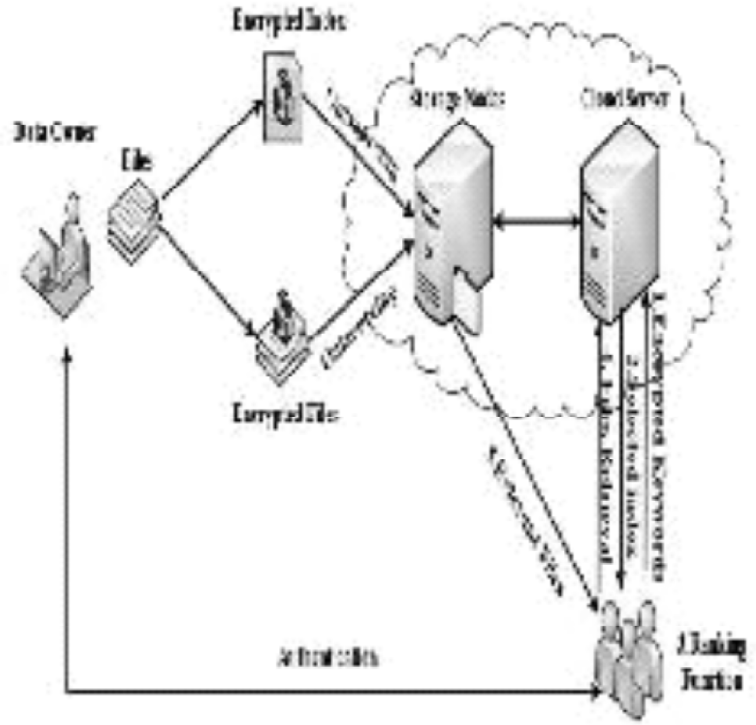


Figure 1: Traditional Encrypted Search Architecture

File Update

In this scheme data owner upload the multimedia files in the cloud server. Each service has different set of files. Data owner collect several file from the local path and stored in the Cloud Server. This cloud server has collection of server cluster which uniquely connected with the cloud server.

Select stem

The admin select the stem word from the uploaded file and to update the file to the cloud server. And this stem word always matches with the file. Whenever the user finds the file into the cloud the stem word refers dynamically to the respective file.

File outsource

After the completion of the wrapping the file has to be encrypted before the expanding process. Each and every time cloud owner has to encrypt the file before outsource into cloud. This is for security reasons in the cloud server.

Keyword search

The user after the successful login goes to view the Searching page. In that category contains could request the file into cloud server. During the Process the keyword has to be encrypted and that could be wrapped to the cloud server.

Requesting File

In this phase the authenticated users view the multimedia services. The user wants to see the particular category of files then they have to access the category and they can generate a request. Once the Request is generated the Resource managers assign the task to the cloud server.

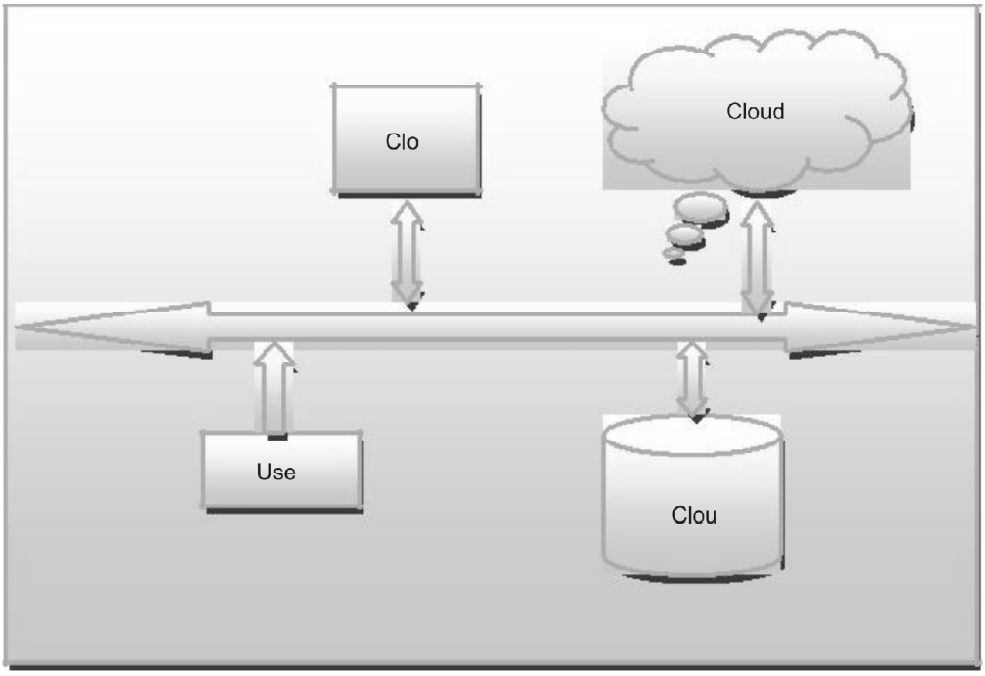


Figure 2: Searching methodology

Retrieve file

In this module the user will get a response file for the corresponding request. The request is initially generated by the user now the cloud server responds that request are developing datasets is LIC based datasets and work out the trained datasets.

Algorithm : Key Generation

Input: TF Table
Output: ~ G(TF); ~H (TF)

1: Get the distribution histogram of the TF table and get TFx as all TF values occur in .
2: for tfi 2 TFx **do**
3: Get the occurrence ci.
4: end for
5: Get C =
PjTFxj i=1 ci.
6: for tfi 2 TFx **do**
7: Calculate pi = ci=C.
8: end for
9: for tfi 2 TFx **do**
10: if i==1 **then**
11: Get G(tfi)=1 and H(tfi) = floor(2B _ pi).
12: else
13: Get G(tfi)=H(tfi 1) + 1 and H(tfi) = H(tfi 1) + floor(2B _ pi).
14: end if
15: end for
16: return ~ G(TF); ~H (TF).

Algorithm: Order Preserving Encryption

Input: tf

Output: E(tf)

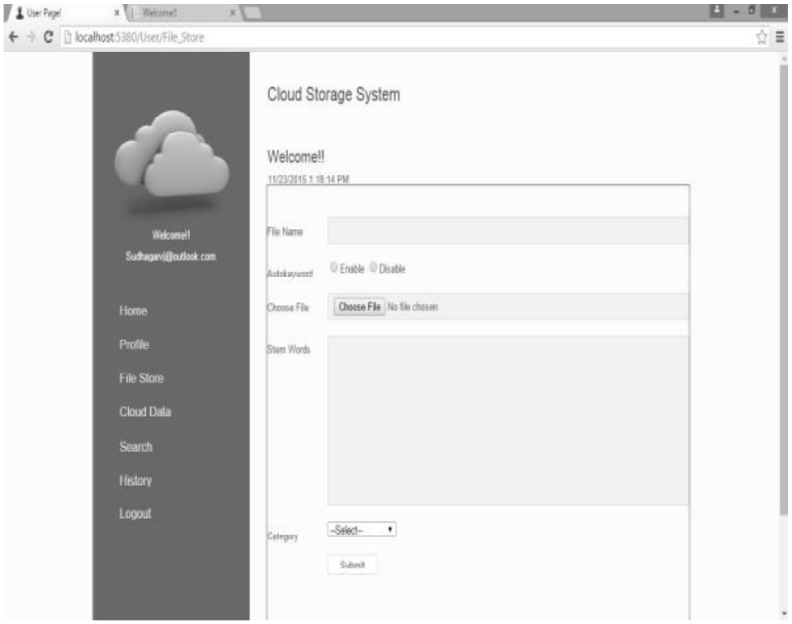
1: for ti 2 T and 1 _ j _ jFj **do**

2: Get E(tfij), E(tfij) R fG(tfij);G(tfij)+1; :::;H(tfij)g.

3: end for

4: return E(tf).

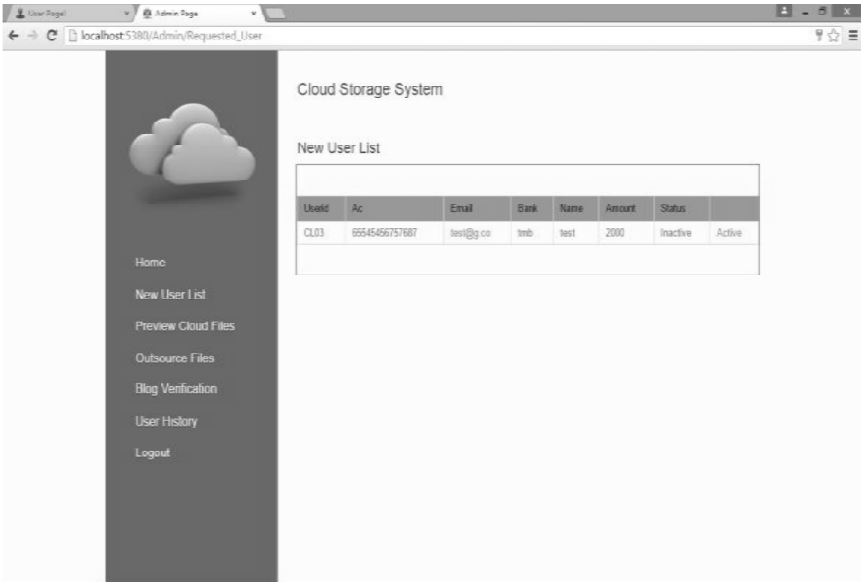
IV. RESULT AND DISCUSSION FILE UPDATION



The above fig shows the design of User file upload and add the stem word of file.

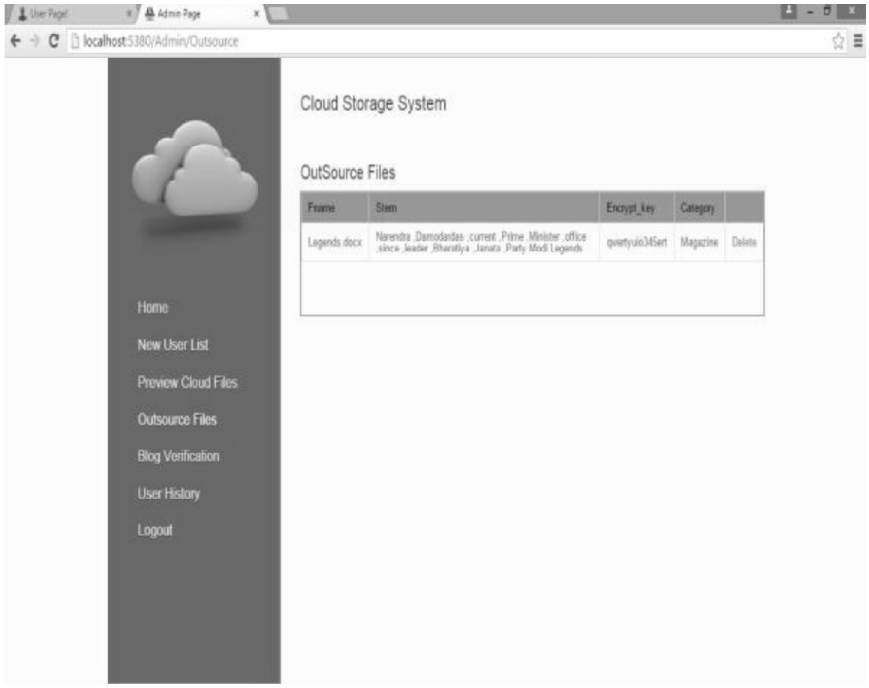
Output: File will be encrypted by cloud owner and it will be stored in the cloud.

USER ACTIVATIION



The above fig shows the design for new user information. Once the owner approved then the new user able to access the cloud

FILEOUTSOURCE



The above fig shows the design Outsource file description.

Input: User updates their files into the Cloud Server.

Output: It will be encrypted and then updated into the cloud server.

V. CONCLUSION

Input: User has to upload their personal documents and other documents into the cloud server.

We have planned a single keyword search scheme to make encrypted data search well-organized. However, there are still some possible delays of our current work remaining.

We would like to propose a multi-keyword search pattern to achieve encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another distention is to find a powerful algorithmic which will not harm the efficiency.

REFERENCES

[1] D. Song, D. Wagner, and A. Perrig, “Practical techniques for Searches on encrypted data,” in Security and Privacy, 2000. S&P2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,”Publickey encryption with keyword search,” in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

[3] 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.

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[5] 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. 222–233, 2014.

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

[7] 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.

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

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

[10] 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.