International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 1 – APRIL 2016.

AN ENERGY EFFICIENT AND TRAFFIC REDUCIBLE MULTI-KEYWORD ENCRYPTED SEARCH SCHEME IN CLOUD

Mathumathi.M[#1] ,Shenaaz. A[*2], Priyadharsini. R[*3]

[#]*Master of Engineering in Computer Science and Engineering, K. Ramakrishnan College of Technology, Trichy, India*
[*]*Bachelor of Engineering in Computer Science and Engineering, K. Ramakrishnan College of Technology, Trichy, India*

fcpmathu@gmail.com
shenaazshynu@gmail.com
ravidharshini10@gmail.com

***Abstract*-Increasingly more and more companies are now using cloud computing. Cloud is growing technology in worldwide. Using cloud computing users can outsource the data and retrieve it in any locations. It is very convenient to all users. But the security of the technology is low. Because the user uploads file to the unknown and low trustworthy CSP (cloud service provider). So it leads to encrypt data and index. Due to encryption of index the retrieving process is very complicated. In existing system the retrieval process is done in searchable data encryption. It is reduce the network traffic efficiency and energy efficiency. Unfortunately the keyword failure probability is very high. They can't remember the apt index in all time. So it makes file retrieval complication. To overcome this problem we propose An energy efficient and Traffic reducible multi-keyword encrypted search scheme in cloud. In this scheme user just know only one keyword for the file to retrieve it from Cloud. Network traffic, energy, keyword failure all of those get reduced and the performance is high.**

I. INTRODUCTION

Cloud computing is a service model in which the data are backup and securely handled in cloud. The cloud is nothing but the remote storage and meanwhile the data’s are available in worldwide. Mobile Cloud Storage (MCS) are increasingly popular on-line services and the MCS works like a primary storage of mobile devices [1], [2]. Using MCS a normal user can upload data and retrieve the data to cloud by wireless communications, MCS leads to improve the data availability and shared resource [4]. User can get the data’s in anywhere without any other local devices resource

The data privacy is a very issue in cloud storage system, to avoid those issues the valuable data and valuable documents are encrypted by the data owner before uploading onto the cloud and data users downloads the interested data or documents by encrypted keyword search scheme [5], [6]. However, the MCS is have more difficult to handle the encrypted keyword search in cloud computing, in consideration of mobile battery and computing technologies for encryption by using in cloud computing the MCS need a suitable and efficient encrypted search scheme for mobile devices.

Due to the limited energy of mobile phones and payable network traffic fee. Therefore, we need to provide importance on the design of a mobile cloud storage scheme that is efficient in reduce energy consumption and the network traffic, through wireless communication channels in cloud computing

In existing system of Encrypted Search scheme are used for mobile cloud computing applications. It’s achieves high efficiencies by using and modifying the ranked encrypted keyword search scheme. The ranked keyword search gives the high scores to represent the relevance a file to the searched encrypted keyword and identifies the top-k relevant files are match with client and sends to client. It will be a more efficient scheme for cloud storage than the Boolean keyword search approaches [8], [9], [10]. Because the Boolean keyword search approaches send all the matching files to the clients, they not identify the top-k relevant files. it will produce a larger amount of network traffic for the mobile devices.

By using traffic reducible scheme the network traffic and the energy is reduced highly. Unfortunately the encrypted keyword search only provides score to files that keywords are matched with file index. In this keyword search scheme the user must know the file index. But if user has multiple no of files the users can’t remember the file indexes. In some urgent situation the user can't remember the file correct index they can't get a file. Due to overcome this problem we propose a multi-keyword encrypted search scheme. In this scheme the data owner creates the keyword set for each file and encrypts the keywords set and set the keyword set to file index and upload it. Ifuser wants to get the file they just give a only one keyword from the keyword set. If cloud identifies the keyword set easily provide the file to user. This scheme is very high efficiency and will reduce the traffic and energy from user mobile in MCS.

II. RELATED WORK

2.1 Encrypted Search over Cloud Computing

In Traditional cloud storage system is the basic system for cloud storage and processing data shown in Fig1. It haves file/index encryption process by data owner, uploading the encrypted data to the cloud storage servers, and encrypted data search/retrieval procedure of users in cloud computing technology.

2.1.1 File and Index Encryption Techniques

The data owner begins the process by preprocessing and indexing work in this process data owner selects the file to upload and find it from text search engines [18]. The

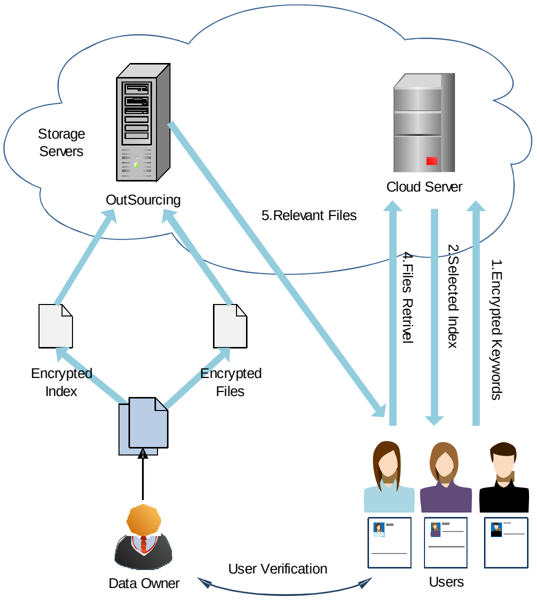

Figure1

File Indexis important to the encryption process. After this step, the data owner encrypts data and fixes its entry in the selectedfile index. The indexes are created by the data owner. Finally, the data owner encrypts the same file indexes and uploads it into the cloud storage server, together with the encrypted files. In existing systems are under use the Order Preserving Encryption [19] (OPE) to encrypt the file and its file index. This encrypted file index is often a TF (Term Frequency) table composed of TF (Term Frequency) values. The TF-IDF table could be used to identify the word relevance in file indexes [21], [22], [23].

2.1.2 Data Search, Download and Retrieval after Verification

A data user can only access file after finishing the successful verification to data owner. At the end of verification process, the data owner identifies the user identity. The data owner sends the encrypted keys back if the user is a verified user.

In the process of search and retrieval, the cloud server finds the related files to the keyword and provide to the user without encrypting it. Searches incur following the steps

1. An verified user encrypts the index to be queried, encrypts it with the same keys which encrypted used as a encrypted keyword and hashes it to get its entry in the index. Then the encrypted keyword sent with file request to cloud server.
2. When the cloud server receiving the file request from the data user. It selects the keyword and searches from the index list and has sent the all related files. The cloud server give some score to with are relevant to keyword. Cloud server only gives the score only which file relevant to the keyword.
3. When the user get the relevant files from the cloud server. The user searched file with in this relevant file list. The data user sends the file details to the cloud. May be it in a file name or important keyword for the file.
4. When cloud server gets the second request it searches with that keyword in the file stored location.
5. The data user decrypts the files with the keys get from the data owner and recovers the plain text.

The process computational components for these steps are showed in Figure 1 and with clear details, which uses the traditional two-round-trip schemes for a file search and encrypted keyword retrieval process invoked by an verified user. We call this encrypted file retrieval methods abbreviated as TRS (Two Round trip Search) [11]. In this method the process to get file is too long. For example, if data owner uploads the file to cloud in encrypted manner. If user wants the file. After verificationthe data user first get the decryption keys from data owner. The second process he send the keyword to cloud. Third he get the file list and selects one file from that. Fourth downloads the file from server in encrypted form. Finally he decrypts the file to get original text.

This process will take the more time finish all process. When the process is done 5 mini processes so the network traffic between the clouds to user is high. When the network traffic is high the computational time will be increased. When the energy consumption to get one file is going high it may leads to user battery dead. The process will be fully collapsed and make some internal problems to get the file difficult situation.

III. DATA RETRIEVAL IN CLOUD

3.1 Multi Keyword Encrypted Search over Cloud Data

Data owner creates the keyword set for file and File, index, keyword set encryption are done by the data owner, outsourcing those encrypted data to the cloud servers, the data owner first executes the creating keyword set, preprocessing and indexing work. Data owner creates the keyword set by the file index the keywords are in the file index because it will be very useful to user can remain the keyword. Data owner creates the set of keywords and encrypt those keywords. Because cloud can identify the file using that keywords. Finally, the data owner encrypts the user file index and uploads it into the cloud server, together with the encrypted file set. Most of the existing systems use the Order Preserving Encryption to encrypt the file and file index.

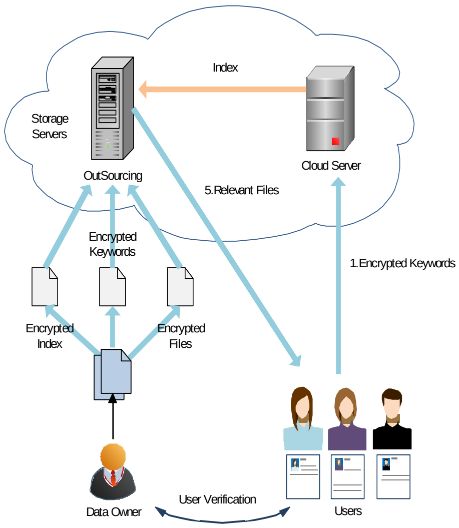

Figure 2

3.2 Data Search and Retrieval after verification

User can access the file details only after finishing successful user verification. In the process of user verification, the data user only identify that he is a verified user. The data owner provides the encryption keys back if the data user is a verified user.

In the process of encrypted search and retrieval, the cloud server gets the keys and search with keyword set and provides the file. These following steps are easily understood the search:

When cloud server get the keyword from data user. Their first search from it in the keyword set if the keyword is available in the keyword set it easily identifies the encrypted file index. If the keyword is not available in the keyword set it sends a message to the user to try other keyword. Then the index related to the file sent back to the data user.

The data user gets the encrypted file from the cloud server. If the user want get plain text the user must send the keyword request to the data owner. The data owner first identifies the user is valid or not. If the user is verified data owner provide the decryption keys to user. If the user is not verified the data owner not respond to him.

3.3 Encryption techniques

In past years, encrypted search provide the very high security to share user data [8]. But it makes some problem in keyword searches and looking for make it efficient in encrypted search. In encryption each of word of the file is encrypted and can't identify. Uses the different type of keyword search [11].

Algorithm 1 Order Preserving Encryption

```
Input: $tf1$
Output: $E(tf1)$
for $ti€T$ and $1 \le j \le |F|$ do
    Get $E(tf1ij)$, $E(tf1ij) \leftarrow \{ R\ G(tf1ij), G(tf1ij)+1, ..., H(tf1ij)\}$.
end for
return $E(tf1)$.
```

In data Retrieval, TF-IDF (Term Frequency-Inverse Document Frequency) is a statistic which converts the all word from the encrypted document in a collection or corpus. It is often used as a important factor in keyword-based decryption and text mining. The TF-IDF algorithm proposed by Salton and McGill's book is one of the most popular schemes. From start to end, encrypted keyword search scheme includes Boolean keyword search and ranked keyword search [8], [9], [10]. In existing Boolean keyword search the server sends back files to data user only based on the existence or credits of the encrypted keywords, without looking at their keyword relevance.

IV. THE BASIC IDEA OF MULTI KEYWORD ENCRYPTED SEARCH

4.1 Encrypted keyword search

The Figure 2 will explains our new multi-keyword encrypted keyword search scheme. The basic idea behind encrypted keyword search is to give score to the relevant files the higher scored files are taken as a requested file. It perfectly designed for the applications to reduce the energy and the network traffic in mobile cloud computing. Cloud service providers only provide the computing cycles, and it will helpful for user to reduce the computation of the application and user side energy consumption. However the offloaded applications not reduce the computation cycles and the transmission energy. These application will increase the file retrieval process in high efficient. There are three main processes to retrieve the data and get higher performance.

- The user verification process is used by the data owner to verify and identify the data users.
- The sensitive documents, file index and file keyword set are uploaded to the cloud after being encrypted by the data owner.
- After finishing successful user verification the data user send a file request with encrypted keyword in download and data retrieval process.

4.2 Power and Traffic Efficiency Improvements Schemes

The existing technologies are cannot directly apply to cloud computing for, achieve low energy consumption to get a file from mobile cloud is very helpful to overcome the mobile cloud issues. Now a days many OPE [11], [19], or fully homomorphism encryption techniques have been used. These technologies are high secured and accurately used by the encrypted keyword search. However, its high cost compared to many computing resources. The energy consumption of the algorithm is high, when it used from the mobile devices it been complicated. Therefore we choose the very simple encryption algorithm but high efficient to the encrypted keyword search raises the question in importance of the performance and energy in mobile cloud. They used four basic techniques to save energy in mobile devices can be considered. It can identify and analyze the factors that affect the mobile energy in mobile cloud computing. Provided some results related to their important characteristics of contemporary mobile devices that shows the integration balance between local and remote mobile cloud computing. That also presents very detailed information of the energy consumption of mobile phone, in testing the power usage and battery lifetime were validated under a number of usage search. They analyzed the most promising areas to focus on for improve the energy management. Theseare techniques are very helpful to reduce the network traffic and energy consumption. Without any decrease in the performance.

V. PERFORMANCE EFFICIENCY

The overall architecture of the multi keyword search is shown in Figure 1, in which the relevance scores given is helpful retrieve file from the cloud, it a very complicated and high efficient process. The process of file is one round trip process and a very simple process, the encrypted file search and retrieval steps are as follows:

i) When the data user finishes their verification process to data owner. They will provide the secret keys to data user.

ii) An verified user stems the keyword to be send, encrypt the keywords with the secret keys and hashes it to get its entry in keyword set. The user sent a file request with the keyword.

iii) When cloud server receives the encrypted keyword, it searches the keyword from the keyword set and identifies the index for the file. When cloud server identifies the index easily sends the file to data user.

iv) The data user decrypts the files using the secret keys and recovers the original data from decryption process.

VI. RUNTIME PERFORMANCE EVOLUTION

6.1 Experimental Environment

We used the scheme practically, we use data as a of 1000 files with different sizes in the cloud with Dual vCPUs at 2.27GHz. An windows smart phone with a CPU at 1GHz sends the queries as the mobile client multi-keyword encrypted search through an about 8M wireless network.

In user side receives the user's input keyword and encrypts it before getting the hash valueand sent to the mobile cloud server. Another important feature ofthis program is to retrieve the files back from the mobile cloud server and decrypt the file. When the user using the decryption processthey can easily get the original text of the file.

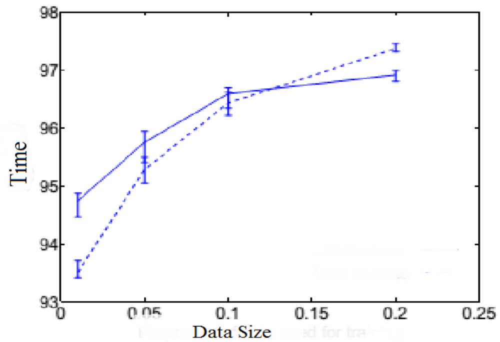

Figure 3

6.2Throughput

An experimental results that shown figure 3. The data size and the time are plotted in a graph. As energy consumption for encrypted search is critical for mobile devices, we estimate that energy efficiency in this subsection. Observe that the energy consumption is reduced when searching and retrieving files of size 100KB, this meansthat the scheme saves 55% energy compared to existing OPS encryption technique system. When searching and retrieving files of 1MB size, the energy consumption is reduced from 200 seconds to 96 seconds, that means a 35% energy saving in encrypted search and it very higher efficient.

VII. CONCLUSION

This is a new system for traffic and energy reducible multi-keyword encrypted search scheme in cloud computing. In previous systems the efficiency of the encrypted search in cloud computing is very low Compared to our new scheme. The basic problem is to energy and network traffic in multi keyword searching cloud computing. To overcome the energy and traffic problem we developed a high performance implementation to achieve an encrypted search in a mobile cloud. Our proposed system is high secured enough architecture. This system is slightly more time but the efficiency and the security of the data is very high compared to existing systems. This system will be easily handled by user. This work can be extended to more other novel implementations.

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] X. 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 MobileComputing Systems & Applications*. ACM, 2010, pp. 43–48.

[7] A. A. Moffat, T. C. Bell *et al.*, *Managing gigabytes: compressing andindexing documents and images*. Morgan Kaufmann Pub, 1999.

[8] 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.

[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] Jian li, Rahui Ma, Haibing Guan “TEES: An efficient search scheme over encrypted data on mobile cloud.

[12] Y. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in *Applied Cryptography andNetwork Security*. Springer, 2005, pp. 391–421.

[13] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, “Zerber+ r: Topk retrieval from a confidential index,” in *Proceedings of the 12thInternational Conference on Extending Database Technology: Advancesin Database Technology*. ACM, 2009, pp. 439–449.

[14] 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.

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

[16] 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.

[17] 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*.

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

[19] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in *Proceedings of the 2004 ACMSIGMOD international conference on Management of data*. ACM, 2004, pp. 563–574.1022, 2003.

[20] J. Ramos, “Using tf-idf to determine word relevance in documentqueries,” *Technical report,Department of Computer Science, RutgersUniversity*, 2003.

[21] D. M. Blei, A. Y. Ng, and M. I. Jordan, “Latent dirichlet allocation,”*the Journal of machine Learning research*, vol. 3, pp. 993–

[22] D. Hiemstra, “A probabilistic justification for using tf× idf term weighting in information retrieval,” *International Journal on DigitalLibraries*, vol. 3, no. 2, pp. 131–139, 2000.

[23] K. Jones, “Index term weighting,”*Information storage and retrieval*, vol. 9, no. 11, pp. 619–633, 1973.

[24] 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, pp. 917– 922.

[25] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in*Financial Cryptography and Data Security*. Springer, 2010, pp. 136– 149.

[26] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, “Toward privacyassured and searchable cloud data storage services,” *Network,IEEE*, vol. 27, no. 4, pp. 56–62, 2013.