Traffic and Energy Efficient Secured Encrypted Data Search and Retrieval Scheme over Mobile Cloud

Sowmya S[1], Leena Giri G[2]
[1]M.Tech Student, Department of Computer Science and Engineering
[2]Associate Professor, Department of Computer Science and Engineering
[1,2]Dr. AIT Bangalore, India

Abstract- *It is desirable to store data on the storage server such as on the cloud in the encrypted form in order to reduce security and privacy threat. Though, encryption of data is a heavy burden for the mobile devices, and retrieval of data from the cloud introduces a complicated communication between user and the cloud server. Generally mobile devices have limited battery life and limited bandwidth, these issues incur heavy overhead to communication, computing as well as greater power consumption for them, it makes the encrypted search in mobile cloud very challenging. To overcome these issues we propose a new architecture that is traffic and energy saving, secure encrypted search and data retrieval scheme for mobile cloud. Traditional searchable encryption strategies supports only Boolean search and aren't enough to satisfy the effective data exploitation needs that is essentially demanded by greater number of variety of users and substantial amount of data documents in cloud. In this paper, we describe and elucidate the complex of ranked key-word search over encrypted cloud data. Ranked search considerably enhances system usability by means of enabling search result relevance ranking in the place of sending undifferentiated results. The proposed mechanism offloads the computation from the mobile devices on to the cloud, after which minimizes the communication between the cloud and the mobile gadgets. In order to mitigate statistics information leak the proposed architecture is also implemented with security enhancement.*

Keywords- Mobile cloud, Encrypted data, Statistical information, Traffic efficient, Energy efficient

I. INTRODUCTION

Cloud computing is a computing paradigm that permits access to shared pool of configurable system resources and high level services that can be provisioned with minimum management effort, usually over the Internet. Cloud computing depends on sharing of resources to achieve economy of scale and coherence, as public utility. The goal of cloud computing is to permit users to have the benefit of all of the technologies, without having the knowledge about underlying technologies. Cloud is based on the pay as you go approach as a meter services to the user. It provides the system resources such as computing, storage, network resources on demand. Virtualization is the most important technology in cloud computing. It separates physical devices into one or more virtual devices. Each virtual devices can be easily managed and used to achieve the computing task. Mobile cloud provides the services to mobile devices. It is a mixture of mobile computing, wireless networks and cloud computing to enable affluent computational resources to mobile device users. To achieve privacy the data owner has to encrypt the files before storing it on cloud and decrypt it after downloading. Though, encryption of data adds more burden to mobile devices, and data retrieval from the cloud introduces a complicated communication between user and the cloud server. In mobile cloud storage, various traditional data encryption schemes are imported and the modern mobile devices are confronted with various security threats as in PCs [1]. Mobile devices have limited battery life and limited bandwidth, these issues incur heavy overhead to communication, computing as well as greater power consumption for them. It makes the encrypted search in mobile cloud very challenging. Therefore efficient encrypted search and retrieval scheme for mobile cloud storage is necessary. Usually, due to payable traffic fee and limited battery life mobile devices are in a greater need of bandwidth and energy efficiency for encrypted search. Therefore we propose a new architecture that is traffic and energy saving, secure encrypted search and data retrieval scheme for mobile cloud. Traditionally, two categories of encrypted search methods exit, that can enable the cloud server to perform the search over the encrypted data ranked keyword search and Boolean Keyword Search. The ranked keyword search adopts the relevance scores [2] to represent the relevance of a file to the searched keyword and sends the top-k relevant files to the client. In order to mitigate or control the statistic information leak [3] the proposed architecture is also implemented with security enhancement.

II. LITERATURE SURVEY

The ability of data sharing with user's privacy protection has improved a lot in encrypted search method from past few years. One of the most popular encrypted search algorithms TF-IDF was proposed by Salton and McGill [4]. The big challenge raised by Song et al., [5] was how keyword search

is implemented efficiently on encrypted data. In the proposed system each word of the document is encrypted separately. It is not suited with previous file encryption strategies because it cannot deal with data compression. The static keyword search scheme Term Frequency-Inverse Document Frequency (TF-IDF) [6] revealed how a word is important to a document in a collection, in information retrieval. This has become a major factor in data mining and keyword based search. There are two categories of searches in encrypted search, 1.BooleanKeyword Search 2.Ranked Keyword Search. Ranked Keyword Search enable the search results in the form of relevance ranking instead of undifferentiated results. In Boolean key word search the server searches the files based on the presence or absence of the exact key word, this will never look for a relevant key words.

- **Ranked Keyword search**

The RankedKeywordSearch scheme was introduced by Chang and Mitzenmacher [7], but this will not search for a relevant files. The top N-ranked relevant files are sent to server in ranked keyword search. Instead of traditional Order Preserving Encryption (OPE) we can use homomorphic encryption method in order to encrypt the file index. In order to avoid statistics information leak, One to One mapping OPE is suggested by Agrawal et Al.,[8] One to Many mapping OPE was introduced by Wang et al.,[9] for security protection they implemented a complicated algorithm. Since the algorithm is complete and in need of much system resources which lead to bad performance and energy consumption. A Confidentiality-Preserving rank-order search is proposed by Swaminathan et al., [10]. In this scheme relevant scores are computed in client side which increases its work load and decreases the performance.

Zerber+R model proposed by Zerr et al., [11] featured with novel technique while maintaining the retrieval accurateness of the server for top-N processing which enables the numbering of requests and relevant score for various words differentiable for the server. The clients decrypt the elements returned by the server and filter those elements for nonqueried words.

The one round trip search (ORS) proposed by Wang et al., [12] which may search the encrypted data. When the hackers try to manipulate the search or detects how the file is returned based on keyword and the relation between the file and the key word, the "multi-keyword ranked search" sustain greater severe key word file connection especially with in the wireless networks and mobile cloud.

- **Energy and Traffic Efficiency Improvement Schemes**

The past plans can't straight forwardly apply to mobile cloud, for accomplishing efficient energy utilization to address the critical issue for mobile cloud. Later numerous Order Preserving Encryption (OPE) or completely homomorphic encryption strategies have been proposed. They substantiated themselves secure and precise enough for looking scrambled information purpose. Though it may, they cost numerous computing assets. As energy utilization getting to be vital, the complicated calculation isn't appropriate for mobile devices. Thus we select a simple order preserving encryption strategy in our proposed system. Miettinen and Nurminen [13] gave an analysis of the basic elements influencing the energy consumption of a mobile device users in cloud computing. They additionally show a few estimations identified with the important attributes of contemporary mobile devices that characterize the essential balance between local and remote computing. Carroll and Heiser [14] presented a detailed analysis of power consumption of mobile phone, in which the energy consumption and battery lifetime were tested under various use designs. To focus on for further improvements of power management they identified the most promising areas. These perspectives underscore the way that offloading the workload to the server is a good procedure to modify the existing encrypted search and render them appropriate to the mobile cloud context.

III. PROPOSED SYSTEM

A) System Architecture

The proposed architecture consist of four modules, such as data owner, cloud serve, end user and Auditor each modules serves specific functions as described in the above figure1.

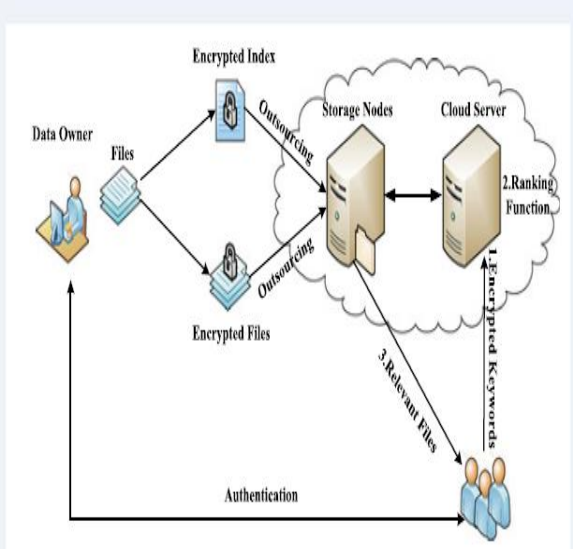

Figure 1: System Architecture

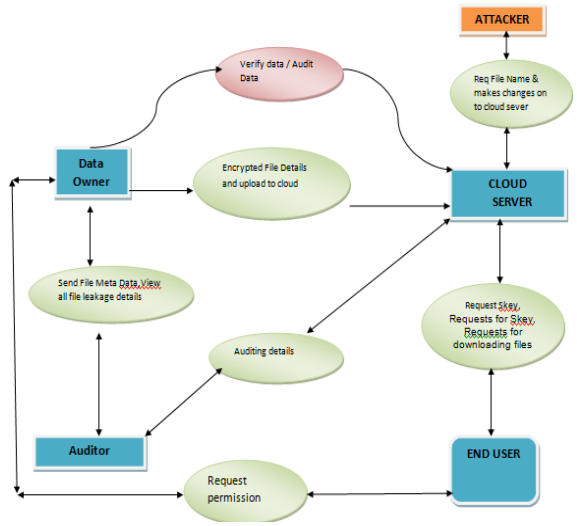

Figure 2: Dataflow Diagram

In order to support encrypted search strategy with greater security level on mobile cloud the new architecture proposed consist of four phases.

1) File encryption and indexing. Upload file and index on to the server
2) Calculate the top-k ranking
3) Retrieve the encrypted file using encrypted index
4) View the statistical information leak

In this scenario, the data owner must first register with cloud server and then encrypt the file and index to be stored on the server. The server calculates the relevance score for the file when user makes a request for the file server sends the top-k ranked files to the user. The user must first take the permission from the data owner to access their file. The data owner sends the secret key and trap door to the user. Using that secrete key and trap door the user is able to download the files from the server. A new module called an auditor is introduced to control the statistical information leak. Auditor audits the files and incase of any information leakage for the file it will notify to the server and user. Some of the algorithms used are described in the next sections.

B) Advanced Encryption Standard

Advanced Encryption Standard (AES) scheme, is a specification for the electronic data encryption. It is based on substitution-permutation network design principle. AES uses key size of 128, 192 or 256 bits and fixed block size of 128 bits. To protect classified information up to secret level the strength and design of all key lengths of the AES algorithm are sufficient. To make the information highly secured it is required to use key length of 192 or 256 bits.

Algorithm: AES

begin

byte state [4,Nb]
AddRoundKey (state, w[0,Nb-1])
for rond = IstepI to Nr-1
SubBytes (state)
ShiftRows (state)
MixColumn (state)
*AddRoundKay (state, w[round * Nb,(round+1)*Nb-1])*
end for
SubBytes (state)
ShiftRows (state)
*AddRoundKey (state, w[Nr * Nb, (Nr+1) * (Nb-1)]*
Out = state

IV. RESULTS

Figure3 and Figure4 are the inferences from the outputs of the proposed work. In the existing traditional encrypted scheme it takes two round trip time to search and retrieve the file, the proposed scheme takes only one round trip time in order to reducing the retrieval time. We observe that the File Search and Retrieval Time (FSRT) of Traditional Search Scheme is more and it does not have to perform any security computation. The FSRT of Traffic Efficient Search is effectively reduced when compared to the one of Traditional Encrypted Search.

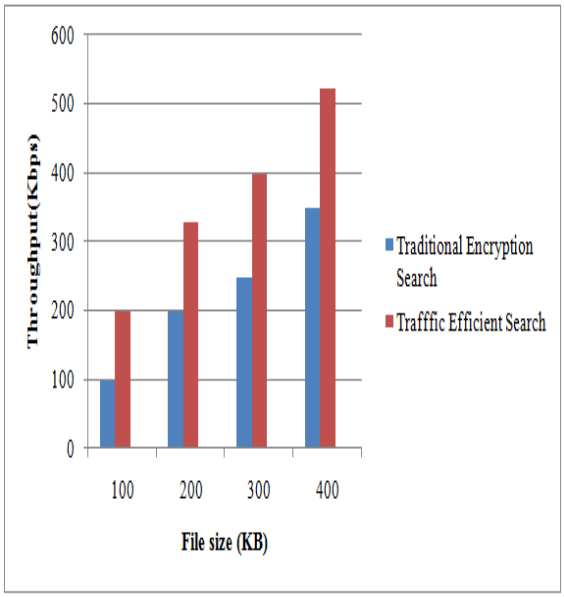

Figure 3: Throughput of Traditional encrypted Search and Traffic Efficient Search

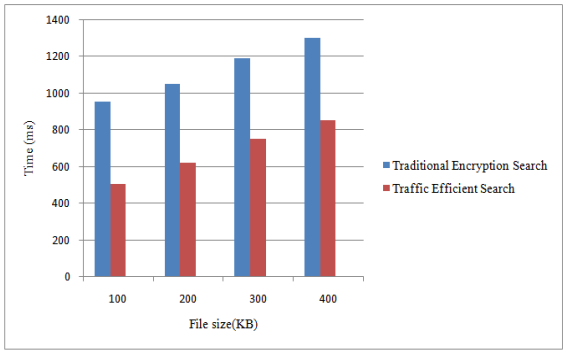

Figure 4: File search retrieval time of Traditional Encrypted Search and Traffic Efficient Search

V. CONCLUSION

The proposed architecture creates energy and traffic efficient encrypted keyword search scheme for the mobile cloud storage. To achieve an efficient encrypted search and retrieval over mobile cloud we propose a new architecture which is an efficient scheme for the mobile cloud context. The security analysis of proposed scheme shows that this approach is secure enough for mobile cloud environment.

REFERENCES

[1] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in Cloud Security Services for Mobile Devices," in Proc. 1st Workshop Virtualization Mobile Comput., 2008, pp. 31–35.

[2] A. A. Moffat, I. H. Witten, and T. C. Bell, "Managing Gigabytes: Compressing and Indexing Documents and Images". San Mateo, CA, USA: Morgan Kaufmann, 1999.

[3] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Top-k Retrieval from a Confidential Index," in Proc. 12th Int. Conf. Extending Database Technol.: Adv. Database Technol., 2009, pp. 439–449.

[4] G. Salton and M. J. McGill, "Introduction to Modern Information Retrieval". New York, NY, USA: McGraw-Hill, 1986.

[5] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[6] A. Aizawa, "An information-Theoretic Perspective of tf-idf Measures," Inf. Process. Manage., vol. 39, pp. 45–65, 2003.

[7] Y. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, pp. 391–421.

[8] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order Preserving Encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[9] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Coud Data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[10] A. Swaminathan, Y. Mao, G. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentiality-Preserving Rank-Ordered Search," in Proc. ACM Workshop Storage Security Survivability, 2007, pp. 7–12.

[11] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Top-k Retrieval from a Confidential Index," in Proc. 12th Int. Conf. Extending Database Technol.: Adv. Database Technol., 2009, pp. 439–449.

[12] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Eloud Data," in Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst., 2010, pp. 253–262.

[13] A. Miettinen and J. Nurminen, "Energy Efficiency of Mobile Mlients in Cloud Computing," in Proc. 2nd USENIX Conf. Hot Topics Cloud Comput., 2010, pp. 21–28.

[14] A. Carroll and G. Heiser, "An Analysis of Power Consumption in a Smartphone," in Proc. USENIX Conf. USENIX Annu. Tech. Conf., 2010, pp. 271–28.