International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

Enhanced Traffic and Energy saving Encrypted Search

Dr. S. Sharavanan [1], Dr. T. Buvaneswari [2], M.Vigenesh [3], M. Saranya [4]

[1] *Vice Principal, Annapoorana Engineering College, Salem*
[2,3] *Assistant Professor, Department of Computer Science Engineering, Annapoorana Engineering College, Salem*
[4] *P. G Scholar, Department of Computer Science Engineering, Annapoorana Engineering College, Salem*

Abstract - *Cloud storage and its application enhancing continuously due to its convenient, huge and scalable storage at low cost. However its advantages increases one of the major concerns is data privacy. One of the common ways to increase privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud. Then the respective receiver can decrypt and download the files respectively. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. hence a new approach has been proposed represented as ETEES(Enhanced Traffic and Energy Saving Encrypted Search). Initially, shortest path is selected between sources to destination using ACO (Ant Colony Optimization). Therefore shortest path has been selected and it is a multipath transmission when hurdles occurs alternative shortest path will be available to attain reliable communication. Then traffic will be analyzed through tees and data are searched efficiently through our approach.*

Key Words **:** Mobile Cloud Storage, Searchable Data Encryption, Energy Effiiency, Traffic Efficiency

1. INTRODUCTION

Cloud storage system is a service model in which data are maintained, managed and backuped remotely on the cloud side, and meanwhile data keeps available to the users over a network. Mobile Cloud Storage (MCS) denotes a family of increasingly popular on-line services, and even acts as the primary file storage for the mobile devices. MCS enables the mobile device users to store and retrieve files or data on the cloud through wireless communication, which improves the data availability and facilitates the file sharing process without draining the local mobile device resources. The data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme.In MCS, the modern mobile devices are confronted with many of the same security threats as PCs, and various traditional data encryption methods are imported in MCS. However, mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration 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 necessary for MCS.Generally speaking, the mobile cloud storage is in great need of the bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable traffic fee. Therefore, we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and the network traffic, while keep meeting the data security requirements through wireless communication channels.To this end, we introduce 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 platform basis, which has been widely employed in cloud storage systems. 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 to represent the relevance of a file to the searched keyword and sends the top-k relevant files to the client. It is more suitable for cloud storage than the boolean keyword search approaches, since boolean keyword search approaches need to send all the matching files to the clients, and therefore incur a larger amount of network traffic and a heavier post-processing overhead for the mobile devices.By careful redesign of ranked keyword search procedure, TEES offloads the security calculation to the cloud side to save the energy consumption of mobile devices, and TEES also simplify the encrypted search procedure to reduce the traffic amount for retrieving data from encrypted cloud storage. Besides the energy and traffic efficiencies, TEES is implemented with security enhancement in consideration of the modified encrypted search procedure in order to mitigate statistics information leak and keywords-files association leak for MCS, by adding noise in Term Frequency distribution function and keeping the Order Preserving Encryption attributes.

2. RELATED WORK

The concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature has been discussed. More than 20 definitions have been studied

allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches[1]. The cloud storage owns advantages in pay for use and elastic scalability. However, the data security risk destroys the trust relation between the cloud service provider and user. A direct method to avoid this problem is to encrypt data before data stored in the cloud. [2]. The volume of worldwide digital content has increased nine-fold within the last five years, and this immense growth is predicted to continue in foreseeable future reaching 8ZB already by 2015. [3].

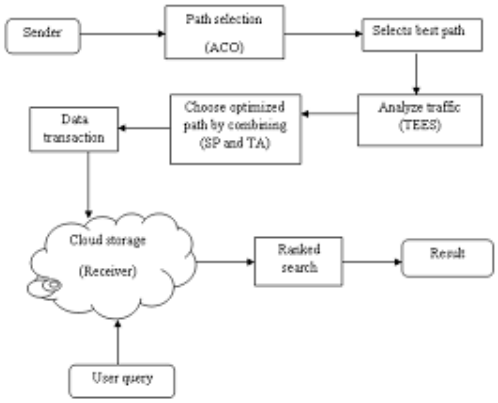
Modern mobile devices continue to approach the capabilities and extensibility of standard desktop PCs. Unfortunately, these devices are also beginning to face many of the same security threats as desktops. [4]. It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. [5].

An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. [6], Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. [7]. is proposed a framework that duplicates the information stream on more than one association connect misusing the assorted variety of numerous WiFi joins.

The following problem: a user U wants to store his files in an encrypted form on a remote file server S has been considered. Later the user U wants to efficiently retrieve some of the encrypted files Containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. [13]. Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data has to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. [14], [15], or [16], to content driven systems administration [17], [18], to cooperative streaming through cell phones [19], [20]. It is likewise essential to take note of the work by Zhang et al. [21], where the investigation distinctive reception apparatus designs in regards to television Void area. The method of reasoning is that a large portion of the proposition endeavor to figure the system conditions, and select to it.

3. MOTIVATION AND SYSTEM MODEL

In the proposed system here used an (Ranked serial binary search) RSBS. This innovative scheme uses a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency. Here propose two optimization methods for document search, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm to speed the search time. RSBS Algorithm upon receiving a trapdoor (encrypted form of search keywords), the cloud would perform a privacy preserving search from the indexes provided by the provider. All this process is done during transaction where initially path has been selected through ACO and traffic is analyzed by dint of TEES. Hence our approach transmits the data with minimum energy consumption and attains minimum data loss due to analysing Here propose two optimization methods for document search, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm to speed the search time. RSBS Algorithm upon receiving a trapdoor (encrypted form of search keywords),



3.1 Architecture diagram for ETEES

Then it selects top-k documents that contain the given search keywords. This process is achieved by using the RSBS algorithm. The RSBS algorithm aims to find the top-k documents that best match the search keywords provided by the user. To this end, it maintains a score array for each document.

4. SYSTEM STUDY

4.1 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out.

This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.
Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

4.2 ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

4.3 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

4.4 SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

5. SYSTEM ANALYSIS

5.1 EXISTING SCHEME

In the existing system involve many methods of keyword search. In Information Retrieval, uses a TF-IDF (term frequency-inverse document frequency).TF-IDF (term frequency-inverse document frequency) is a statistic which reflects how important a word is to a document in a collection or corpus. Data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme. In MCS, the modern mobile devices are confronted with many of the same security threats as PCs, and various traditional data encryption methods are imported in MCS.

The demerits in mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration of the limited computing and battery capacities of mobile device, as well as data sharing and accessing approaches through wireless and also unused as a weighting factor in keyword-based retrieval and text mining. To overcome the problem in traditional data encryption methods, here use an Efficient Encrypted Data Search as a Mobile Cloud Service. This architecture faces many challenges offloads the computation from mobile devices to the cloud and optimize the communication between the mobile clients and the cloud. This innovative scheme uses a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency. However performance enhancement is an problem in efficient encrypted data search.

5.2 PROPOSED SCHEME

In the proposed system here used an (Ranked serial binary search) RSBS. This innovative scheme uses a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency. Here propose two optimization methods for document search, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm to speed the search time. RSBS Algorithm upon receiving a trapdoor (encrypted form of search keywords), the cloud would perform a privacy preserving search from the indexes provided by the provider. All this process is done during transaction where initially path has been selected through ACO and traffic is analyzed by dint of TEES. Hence our approach transmits the data with minimum energy consumption and attains minimum data loss due to analyzing the traffic and transmitting data in efficient way.

Then it selects top-k documents that contain the given search keywords. This process is achieved by using the RSBS algorithm. The RSBS algorithm aims to find the top-k documents that best match the search keywords provided by the user. To this end, it maintains a score array for each document.

6. CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper, we developed a new architecture, TEES as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. In addition ETEES has been implemented to enhance the performance of the system through constructing shortest path between source and destination which is a key idea to reduce the energy consumption of the system thereby it increases the lifetime of the network. Through selecting minimum path between source and destination by ACO reliability could be achieved and it is a multipath transmission process hence it ensures data reliability and availability. Once path is selected traffic is analyzed through TEES and data was initiated to transmit hence without traffic data transmitted and it ensures minimum data loss in the transaction. Hence it concludes that the proposed approach attains reliability and minimum data loss in transaction thereby it increases the performance of the system.

However, there are still some possible extensions of our current work remaining. We would like to propose a multi-keyword search scheme to perform encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency.

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 Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[7] A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing 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&P 2000. 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 Cryptology- Eurocrypt 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] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.

[12] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Topk retrieval from a confidential index," in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

[18] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[19] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent dirichlet allocation," the Journal of machine Learning research, vol. 3, pp. 993–1022, 2003.

[20] J. Ramos, "Using tf-idf to determine word relevance in document queries," Technical report,Department of Computer Science, Rutgers University, 2003.

[21] D. Hiemstra, "A probabilistic justification for using tf idf term weighting in information retrieval," International Journal on Digital Libraries, vol. 3, no. 2, pp. 131–139, 2000.

[22] K. Jones, "Index term weighting," Information storage and retrieval, vol. 9, no. 11, pp. 619–633, 1973.

[23] 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.

[24] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136–149.

[25] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward privacy assured and searchable cloud data storage services," Network, IEEE, vol. 27, no. 4, pp. 56–62, 2013.

[26] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li,"Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 71–82.

[27] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 829–837.

[28] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "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.