International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

SECURE DATACOMMUNICATION IN CLOUD USING TEES

Smita Kulkarni[1] ,Amrit Pannu[2] , Swapna Shrikhande[3] , Piyush Tambe[4]
[1] Assistant Professor of Terna Engineering College,Nerul, Navi Mumbai
[2,3,4]Terna Engineering College, Nerul, Navi Mumbai

ABSTRACT
Cloud storage allows a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way to increase privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data recapture process incurs a complicated communication between the data user and cloud. Normally with restricted bandwidth capacity and restricted 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.
We have implemented TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture unloads the computation from mobile devices to the cloud, and we further enhance the communication between the mobile clients and the cloud. Our experiments show that TEES reduces the computation time significantly.
Keywords—Mobile Cloud Storage, Searchable Data Encryption, Energy Efficiency, Traffic Efficiency.

I. INTRODUCTION

Cloud storage system is a service model in which data are managed,maintained, and backed up remotely on the cloud side, and simultaneously keeps data available to the users over a network. Popular online services and a primary file storage for the mobile devices[4] is represented by Mobile Cloud Storage(MCS)[2][3].The data availability and the file sharing process without drawing off the local mobile device resources [5] has been improved as mobile device users store and retrieve files or data on the cloud through wireless communication and this has been achieved with the help of MCS.The data privacy issue is a main concern in cloud storagesystem, so the sensitive data is encrypted By the ownerbefore outsourcing onto the cloud, and data users regain the interested data by encrypted search scheme.

The situation is that there is limited battery life and payable traffic fee and due to which there is need of bandwidth and energy efficiency for mobile cloud storage for data encrypted search scheme. Hence, primarily focus is given on design of mobile cloud scheme which will be efficient and can provide both energy consumption and network traffic, while keeping into consideration the data security requirements throughwireless communication channels.

So, we implementedTEES[1](Traffic and Energy saving Encrypted Search) architecture for mobilecloud storage applications. TEES achieves the efficiencies by employing and modifying the ranked keyword search(ORS- One way Round search) as the encrypted search platform basis, which has been widely used in cloud storage systems. Traditionally, two categories of encrypted search methods exist,that will help the cloud server to perform search viz. ranked keyword search and Boolean keyword search over the encrypted data.

The ranked keyword search functionality is as follows:

1) To represent the relevance of a file with regards to searched keyword, it takes up the relevance score[8] and it sends the top-k relevant files to the client.

2) The drawback of boolean keyword search is that it need to send all the matching files to client which results in incur imposing a larger amount of network traffic and heavier post processing overhead for the mobile devices and this is the reason why ranked keyword is more suitable for cloud storage.[9]

TEES perform following features:

i) To avoid statistics information leak, TEES redistributes the encrypted index.

ii) It wraps keywords so that it will add noise which will protect from attackers.
iii) Security level of TEES is guaranteed and enhanced for MCS wireless communication

The encryption on data is an effectual way to protectthe confidentiality of data in cloud. But when it comes to searching, efficiency gets low. In literature many research works are inefficient in searching specially for complex queries. This inefficiency may lead to leakage of valuableinformation to unauthorized peoples or intruders.

Song, for the firsttime proposed the practical consistent searchable method based on cryptography. In this scheme the file is encryptedword by word. To search for a keyword user sends thekeyword with same key to the cloud. The limitation of this scheme is that it reveals the word frequency .[9]

channels and it has been proved by the security analysis. [1]

II. LITERATURE SURVEY

Gohtried to overcome the drawback of Song's scheme byconstructing secure index table using pseudorandomfunctions and unique document identifier randomizedbloom filters. [11]Bosch worked on the concept given byGohand introduced the concept of wild card searches.The drawback of this scheme is that bloom filters mayintroduce false positives. [13]

In Chang's proposed scheme,an list is built for each document. The scheme is moresecured compared to Goh's scheme since number of wordsin a file is not disclosed. The drawback of this scheme isthat it is less efficient and does not support random updateswith new words. Golle scheme allows multiplekeyword searches with one encryptedquery.

Table 2.1 Summary of Literature survey

Sr. No.	Author	Year	Paper Title	Objective
1	AnkathaSamuyelu Raja Vasanthi	2012	Secured Multikeyword Ranked Search over Encrypted Cloud Data	Main focus is on the solution of multi-keywordranked searchover encrypted cloud data (MRSE) while preserving strict system-wise privacyin the cloud computing paradigm.[9]
2	Larry A. Dunning, Ray Kresman	2013	Privacy Preserving Data Sharing With Anonymous ID Assignment	Main objective is to assign user an anonymous ID[10]
3	Jian Wang, Yan Zhao , ShuoJaing, and Jaijin Le	2010	Providing Privacy Preserving in Cloud Computing.	The main idea isprotecting individuals privacy in cloudcomputing and provides some privacy preserving technologies used in cloud computing services.[11]
4	Y.Prasanna, Ramesh	2012.	Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data.	This paper has defined and solved the problem of effectual yet secureranked keyword search over encrypted cloud data.[12]
5	Y.-C. Chang and M. Mitzenmacher	2005	Privacy Preserving Keyword Searches on Remote Encrypted Data.	Main objective is to get the access to user's data whichis storedremotelyfrom anywhere accordingto user's ease.[13]

III. PROBLEM STATEMENT

In the proposed system one way round search is proposed for the Encrypted data. And for the systematic searching here coordinate matching is proposed in which as many matches as possible to give search result. The main objective is to provide ORS for fast retrieval of data and
AES algorithm and to achieve efficient search.Methodology in the proposed system is the data is encrypted using AES algorithm for security

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

and stored in cloud. User can request for the files with multiple keywords, and get ranked result.

IV. METHODOLOGY:

4.1 Existing System:

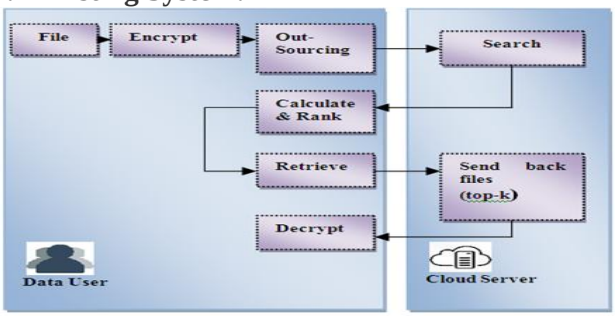

Figure: Existing System

A data user can only access a file after being authenticatedby the data owner. In the process of authentication,the user sends his recognition to the data owner. The data owner sends the encrypted keys back if the user is a legal user. In the process of search and recapture, the cloud server helps the users to find the top-k relevant files for a given keyword without decrypting it. Searches incur following the steps, as illustrated in Figure 1:

1) An authenticated user stems the keyword to be queried, encrypts it with the keys and hashes it to get its entry in the list. Then the encrypted keyword is sent to the cloud server.

2) On receiving the encrypted keyword, the cloud server first searches for it in the index. Then the index associated to this keyword is sent back to the data user.

3) The data user calculates the relevant scores withthe selected index to find the top-k relevant files and sends a follow-up request to the cloud server in order to retrieve the files.

4) The position of these files is selected and they aresent back to the data user from the cloud server.

5) The data user decrypts the files and recovers the original data.

The related estimated components for these stepsare illustrated in Figure 3, which indicate the traditional two-round-trip scheme for a file search and retrieval process invoked by an authenticated user. We call this file retrieval scheme abbreviated as TRS (Two Round trip Search). This scheme provides privacy protection through a complicated file retrieval process compared to a simple PlainText Search scheme (PTS) where searching and retrieving a file is done in only one round without security service.

4.2Proposed System:

We define and solve the difficult problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of authorized privacy requirements for such a secure cloud data implementation system to become a reality. We use One way Round Search key (ORS) and AES for Efficient search of data which would not only reduce search time but also reduce the load on the device. This will increase the device performance by 15 to 20 percent and decrease time by 10 to 15 percent.

Advantage:

- ORS(Search completes in one round)
- Coordinate matching by inner product similarity.

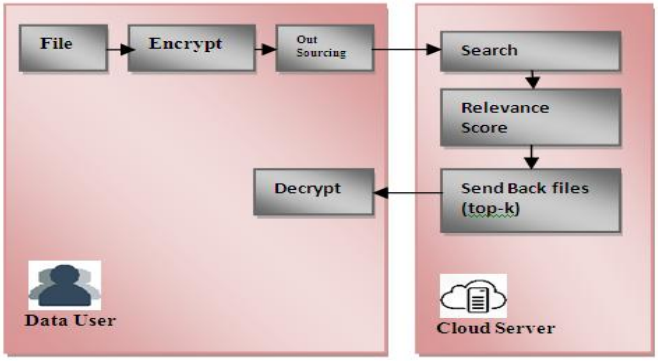

Figure4.2: Proposed System

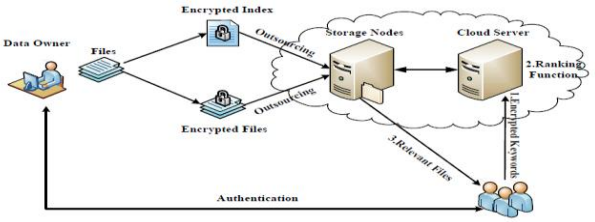

Figure4.3: Proposed architecture of the search over encrypted cloud data

MODULES

1. Encrypt Module
2. Client Module
3. Admin Module

Encrypt Module:

This content is used to help the server to encrypt the document using RSA Algorithm and to change the encrypted document to the Zip file with stimulation code and then activation code send to the user for download.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

Client Module:

This content is used to help the client to search the file using the multiple key words concept and get the precise result list based on the user query. The user is going to select the required file and register the user information and get activation code in mail from the "customerservice404" email before enter the stimulation code. After user can download the Zip file and extract that file.

Admin Module:

This content is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading features and the counting of file request details on flowchart. The admin can upload the file after the exchange of the Zip file format.

Figure: required output for the home page

Figure:user registration form

V. REQUIREMENT ANALYSIS

Minimum hardware requirement specification forProcessor isIntel Pentium IV, Clock speedis1.8 GHz, RAM should be 256 MB, HDD is 80 GB, FDD is 1.44 MB,CD Driveis 52x Reader, Pointing device is Scroll Mouse, Keyboard is 101 Standard Key-board.

Software requirement specification of System Architecture is Java.Required Core Languages are Jspand Servlet. Operating System required for the systemisWindowsXp. Database MySql and Apache Tomcat serveris required.

VI. CONCLUSION

We implemented a new architecture TEES as an first attempt to create an One way Round search scheme to perform encrypted data search over mobile cloud. In cloud computing, the outsourced data of data owners is shared with a number of users, who might want to only retrieve the data files they are interested in. To do so the most preferred way is through keyword-based retrieval. Using a new searchable encryption scheme, in which novel technologies in cryptography community are employed, including AES encryption.

In the proposed scheme, the data owner encrypts the searchable index with AES encryption. When the cloud server receives a query consisting of multi key words, it computes the scores from the encrypted index stored on cloud and then returns the encrypted result of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest- scoring files recognizer to request to the cloud server. The rehabillitation takes a two-round communication between the cloud server and the data user. By security analysis, we show that the proposed scheme guarantees data privacy.

In the future it is expected that to maximize the security and to avoid the attacks, there is need to check whether the authorized user is logging or hackers is logging, so one new technique is used to keep away from attacks by using color values technique, each user will have one color values and key color values. Also if same score is calculated for two queries, our technique finalizes one particular query by using the constant calculation method at some particular time.

REFERENCES

[1]JianLi,Ruhui Ma, HaibingGaun, "TEES: An Efficient Search Scheme over Encrypted data on Mobile Cloud" IEEE Transactions onCloud Computing, TCC 2015

[2] 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.

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

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

[5] 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.

[6] 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.

[7] 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.

[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]AnkathaSamuyeluandRaja Vasanthi,"Secured Multikeyword Ranked Search over Encrypted Cloud Data",, IEEE Conference Publicationspp. 104 – 110,2012

[10]Larry A. Dunning and Ray Kresman,"Privacy PreservingData Sharing With Anonymous ID Assignment",IEEE Transactions on Information Forensics and Security ,2013Vol. 8, pp 402 - 413,

[11]Jian Wang, Yan Zhao ,ShuoJaing, and Jaijin Le," Providing Privacy Preserving in Cloud Computing,3rd International Conference on Human System Interaction,pp. 472 - 475,2010

[12]Y.Prasanna, Ramesh,"Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data",2012 International Conference on Cloud and Service Computing,2012

[13]Y.-C. Chang and M. Mitzenmacher,"Privacy Preserving Keyword Searches on Remote Encrypted Data",IEEE International Technology Management Conference (ICE),2005