ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Mobile Cloud over Encrypted Data in Traffic and Energy Saving

Bhanushree S V[1], Nagamani P H[2], Chaithra G[3], Dr. K S Jagadeesh Gowda[4]

U.G Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[1,2]

Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[3]

Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[4]

ABSTRACT: Cloud storage is presently a trending era thanks to huge storage supplied at negligible price. Cloud offerings are vulnerable to attacks due to loss of centralized control. To keep information safety and privacy, statistics must be saved in an encrypted format on cloud garage. Cellular Cloud garage (MCS) presents storage solutions to cell tool users by means of allowing storage and retrieval of information on cloud through Wi-Fi conversation.MCS incurs new demanding situations due to trouble of cellular devices in phrases of bandwidth, computational functionality and payable site visitor's rate. Encrypted seek on cell cloud outcomes in massive processing overhead. To conquer the aforementioned drawbacks, we proposed a visitors and energy efficient encrypted a couple of keywords ranked look for cellular tool users. The proposed structure offloads computation from cellular devices to cloud server and optimizes the communique ride. more than one key-word search narrows down the result set offering the maximum applicable records. We've got testified the outcomes with the aid of graphical analysis in phrases of time complexity and battery consumption and observed multiple keywords ranked search approach efficient and consumer friendly.

I. INTRODUCTION

Cloud storage is a garage model in which large records may be saved on the cloud and it could be accessed each time, anywhere by means of a consumer across a network. Cellular Cloud storage (MCS) is a form of cloud storage that allows the mobile device customers to shop and retrieve data on the cloud through Wi-Fi communique [1]. The information privateness problem is paramount in cloud storage device, so the touchy statistics is encrypted by means of proprietor earlier than outsourcing onto the cloud, and statistics customers retrieve the involved facts through encrypted seek scheme. These conventional records encryption methods can't be imported directly in MCS due to confined computing and battery capacities of cellular gadgets. Consequently, MCS is in need of an efficient encrypted search scheme that specializes in bandwidth and strength efficiency. TEES (traffic and strength Saving Encrypted search) architecture was brought to fulfil the MCS necessities. This approach makes use of Ranked key-word seek as a records encrypted search scheme [2].

II. EXISTING SYSTEM

Historically, classes of encrypted seek techniques exist, that can allow the cloud server to perform the search over the encrypted data: ranked key-word search and Boolean keyword search. The ranked keyword seek adopts the relevance ratings to represent the relevance of a document to the searched key-word and sends the pinnacle-ok applicable documents to the patron. it is extra suitable for cloud garage than the boolean key-word search approaches, due to the fact boolean key-word search techniques need to ship all the matching files to the customers, and consequently incur a larger amount of network traffic and a heavier publish-processing overhead for the cellular gadgets.
Existing System has the following disadvantages:

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

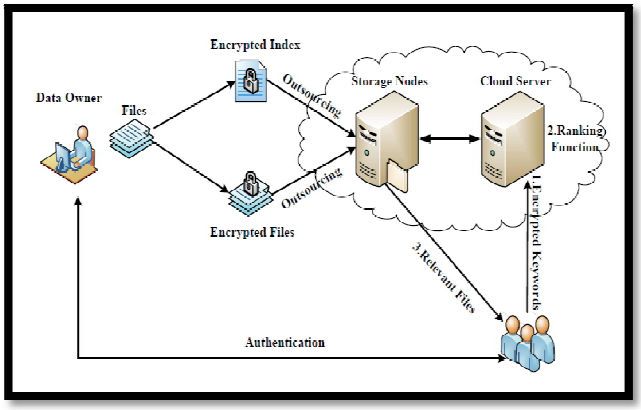
i) Mobile cloud garage device incurs new demanding situations over the traditional encrypted search schemes, in consideration of the restrained computing and battery capacities of cellular device, as well as records sharing and getting access to procedures via Wi-Fi communique. Consequently, a suitable and efficient encrypted search scheme is essential for MCS.
ii) In the present machine, the phrases are intently related to the documents, that could cause ability information leak Present machine suffers from heavy electricity intake due complicated algorithms Current machine is low inperformance due to heavy computations Heavy network visitors increases record retrieval time.

III. PROPOSED SYSTEM

We introduce site visitors and energy saving Encrypted seek architecture for cell cloud garage applications. It achieves the efficiencies thru employing and modifying the ranked keyword search because the encrypted seek platform foundation, which has been extensively employed in cloud storage structures. It's miles carried out with security enhancement based totally on popular TF-IDF, however the vital safety defects of this encryption technique cannot be completely resolved. To the great of our expertise, there is no unbreakable security scheme, however the architecture is widespread sufficient to host and decorate diverse encrypted seek schemes. Furthermore, we propose that a cloud storage provider is semi-sincere and will now not collude with attacker in TEES, as maximum of the related works. TEES employs the structure redecorate over conventional encrypted search process.
Proposed System has the following advantages:
i) TEES reduces the electricity consumption of cellular devices by using offloading the security computation of the relevance scores to the cloud server.
ii) It simplifies the encrypted search process to reduce the visitor's quantity for retrieving records from encrypted cloud storage. except the energy and site visitors efficiencies, TEES is carried out with security enhancement in consideration of the modified encrypted search process as a way to mitigate statistics data leak and keywords-documents affiliation leak for MCS, by using including noise in time period Frequency distribution characteristic in an effort to render them indistinguishable to the attackers and preserving the Order retaining Encryption attributes.
iii) It improves overall performance through reducing network site visitors& optimizing computations.

IV. SYSTEM ARCHITECTURE

The general structure of TEES is shown in figure, wherein the relevance ratings calculation is offloaded to the cloud, which eases the heavy burden on cellular customers. Moreover, TEES functions simplest one round-journey communications for each seek. In this scheme, the file seek and retrieval steps are as follows:



i) The data user sends his identification to the data proprietor and get the name of the game keys if authenticated.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

ii) An authenticated user stems the keyword to be queried, encrypts it with the keys and hashes it to get its entry in the index. Then the encrypted keyword is dispatched to the cloud server.
iii) On receiving the encrypted key-word, the cloud server will use the feature of relevance rating calculation to locate the pinnacle-okay applicable files and dispatched back to the information user in which the top-k is configured by means of the users.
iv) The statistics consumer decrypts the documents and recovers the authentic statistics. Thus, the blessings of TEES are without difficulty located, and we complicated and quantify them.

V. RESULTS

Fig (a)Home Page of TEES

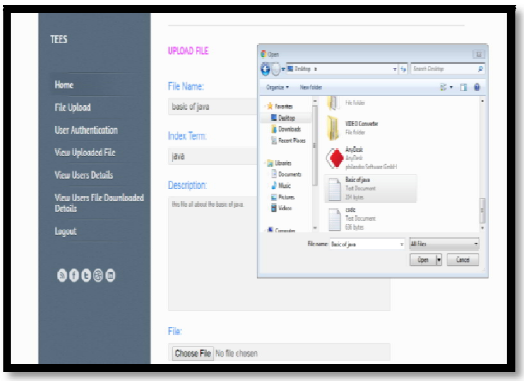


Fig (b)Data Owner Uploading the File

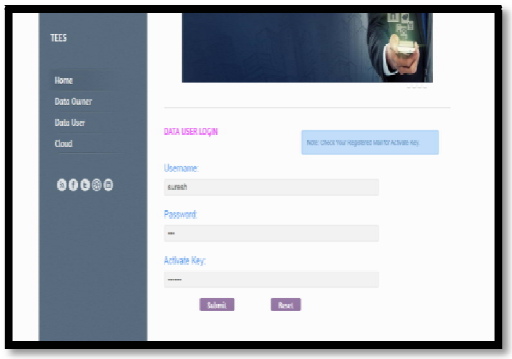


Fig (c) Data User Login Page

Fig (d) Data User Decrypting and Downloading Files

Fig (a) shows the Home Page ofTEES consisting of 3 modules – Data Owner, Data Userand Cloud. The Data Owner has to click on the Data owner link in the Home Page to do his tasks. Similarly, the Data User has to click on the Data User link to login and search files.

Fig (b) shows the Data Owner Uploading the files to the cloud with File Name, Index Term and Description. This is the Home Page of Data Owner.

Fig (c) shows the Data User Login Page. Data User has to login with username, password and the Activation key.

Fig (d) shows Data User Decrypting and Downloading the Files after authentication from the Data Owner.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

V. CONCLUSION

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. We started with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and showed their inefficiency in a mobile cloud context. Then we developed an efficient implementation to achieve an encrypted search in a mobile cloud. The security study of TEES showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. TEES is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Based on TEES, this work can be extended to more other novel implementations. We have proposed a single keyword search scheme to make encrypted data search efficient. 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, "Abreak in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.
[2] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.
[3] 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.
[4] 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
[5] 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.
[6] A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.
[7] 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.
[8] 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.
[9] 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.
[10] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.