International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 7 – APRIL 2017 (SPECIAL ISSUE)

AN ENHANCED RESILIENT CLOUD SECURITY SCHEME AGAINST OFF-LINE KEYWORD GUESSING ATTACK

Thanapriya.J [#1]

[#] *B.E.(Final year), CSE,IFET College Of Engineering, Villupuram, India*

***Abstract*— Nowadays, larger group of people make use of cloud computing systems. It acts centralized data repository system for social users and organizations. Since the users are inspired to outsource their confidential data to the cloud, the security and privacy are the major concern of the cloud security model. In this paper, we have proposed a timing enabled proxy re-encryption scheme that allows the users to search and retrieve the data in timely events. Simulated results demonstrate that it provides fast and efficient conjunctive search for unstructured data in original documents on cloud server. The proposed technique reduces the overhead of decryption thereby minimizing the adversary's events to a considerable extent.**

***Index Terms*— Cloud computing, confidential data, time-dependent, conjunctive search and unstructured data.**

I. INTRODUCTION

Recently, cloud storage plays an important role towards on-demand access to huge amounts of data shared over the internet. Inspired by the benefits of cloud storages, most of the business users make use of the cloud systems. The social user's shares sensitive information, photos, videos etc over the internet. Social user relies on the cloud infrastructure to store and share their data using the cloud platforms [1]. The cloud infrastructure may reveal personal data due to misbehaving events. The revealing may do by any opponent or mischievous cloud operator. In order to avoid these threatening issues, data owners are encouraged to perform encryption before outsourcing their data to the cloud system. The spatio-temporal DBMS and Raster data management system are transferred from local server to the cloud server for its easiness, availability, scalability and giving better performance in lesser cost [2].

In general, the cloud computing is defined as the "a model that works on-demand network access to the shared pool of the configurable computing resources with minimized cost and effort. Security and privacy are the major parameter to be focused on cloud computing systems. In the recent days, the cloud introduces different level of security to the cloud users [3]. To overcome from these issues, several encryption and decryption techniques are introduced. A prior encryption and decryption technique poses several hypothetical questions and time consuming process. The study on performing linear search over unstructured data has not yet furnished perfectly. In this paper, we focus on enhancing the cloud security even in the case of off-line keyword guessing attacks. Our proposed scheme exhibits secure, efficient and accurate.

Due to the significance of effective storage and computational models available in the cloud, number of cloud service users is increasing day by day. As a result of this, bulks of information are being getting added into the cloud servers. In such environment, searching and retrieving the required file is like finding needle onto the sand beach. Sometimes, due to encrypted forms of data on cloud may also force us to have to search through it, in encrypted form only. This makes the retrieving problem a challenging task. Retrieving files without relevance makes wastage of computational cost and unreliable way to access files [4]. Thus, the use of efficient search technique gains a very high importance nowadays. As user stores the encrypted data at cloud side, traditional searching will not be effective as well. To meet the effective searching on the encrypted cloud data, multi-keyword query can be formed so as to get the top relevant data of user interest [5].

The rest of the paper is organized as follows: Section II describes the related work; Section III presents the proposed work; Section IV depicts the performance analysis of the proposed work and concludes in Section V.

II. RELATED WORK

This section depicts the earlier work processed in Searchable encryption systems.

Searchable encryption is the system that allows users to securely search the encrypted data via keywords. It makes use of Boolean search without capturing any relevant data. The author in [6] made a comparative study between cloud computing and traditional computing systems. They clearly depicted the functional and non-functional opportunities of the cloud storage with its merits and demerits. The author in [7] depicted a model for efficient ranked keyword search that effectively utilizes encrypted data. They introduced order based mapping function in ranked search. The IDF is measured for searching the data at the earliest. They also adopted the multi-user settings using attribute based encryption model.

The author in [8] framed the model for extracting the

secret query from secret keyword. Their intention was to provide simple and efficient searching algorithm in order to eliminate the overhead. The outsourced data is stored in encrypted form to reduce security and privacy overhead. To avoid overhead the scheme provides provable secrecy for encryption so that the server which is not trustworthy can't learn anything about plain text the controlled searching is provided. Without the user's authorization, an arbitrary word can't be searched by a untrusted server.

The author in [9] studied about the searchable symmetric encryption that resolved all existing security issues. They introduced two effective searchable encryption and adaptive searchable encryption that supported multi-user and multi-key SSE schemes. They utilized heavy key sizes for encrypting the keywords. The author in [10] studied about the Boolean keyword search technique was proposed. They focused on the SSE technique over encrypted data. Further, the encrypted data is ranked by term frequency and identity factors.

The author in [11] studied about the keyword privacy and fuzzy keyword search over encrypted data. They introduced Decisional Diffie Hellman assumption model for the keyword privacy. The keywords are predefined for approaching the fuzzy models. They have analyzed and achieved better file retrieval system. The author in [12] focused on the most challenging scenario where the outsourced dataset distributed to multiple users from multiple owners. In this paper, authors describe attribute-based keyword search scheme. Efficient user revocation scheme was proposed to enable scalable fine level search authorization. The major concerns about privacy needs are the semantic security of keywords and unlinkability of Trapdoors. This systems drawback is security which not provided to the access pattern because of its high level of complexity. Fine level search and scalability are achieved by this scheme.

III. PROPOSED WORK

This section depicts the proposed security scheme to eliminate the offline keyword guessing attack. Prior works throw some issues like:

a) Expensive communication and computation costs.
b) Leakage of the information when trapdoor is generated.
c) If any adversaries find that generated trapdoors possess low entropies then there is higher possible risk of keyword guessing attacks.

In order to overcome from all above mentioned issues, we have proposed efficient conjunctive keyword search that works on time dependent searchable encryption scheme. The proposed algorithm contains five phases, namely,

A. *Delegator owner module:*

Delegator owner is the first process in our proposed scheme. It is characterized by the proxy re-encryption mechanism. Re-encryption key is used for protecting the ciphertext using delegator's public key. This encrypted data can further opened by the delegatee's private key.

B. *Delegate module:*

With the help of searching authority, delegate performs the search operations until the time expires. With the re-encrypted ciphertext and its timestamp, the user can access the data. If not then the search query of the delegatee will be rejected by the data server if the current time beyond the preset time.

C. *Conjunctive keyword search:*

In order to obtain better search data, conjunctive keyword search is used. It is wise to use for obtaining the accurate search results. When the user's types the keywords, the intersected words are retrieved. Here, we have used delegation function to easily retrieve the searched keywords. By doing so, we achieved better security level.

D. *Proxy re-encryption:*

The Electronic Health Records (EHR) is persevered in the proxy re-encryption system. It assists the patients to protect their sensitive information. The access right is restricted according to the entity's role.

E. *Time controlled revocation:*

Time controlled revocation is the major part of our proposed security scheme. When the search keywords extend beyond the preset time, then the authorized user, itself will not able to search the data. Every action in this system is a time dependent. Hence, it is known as time-dependent scheme.

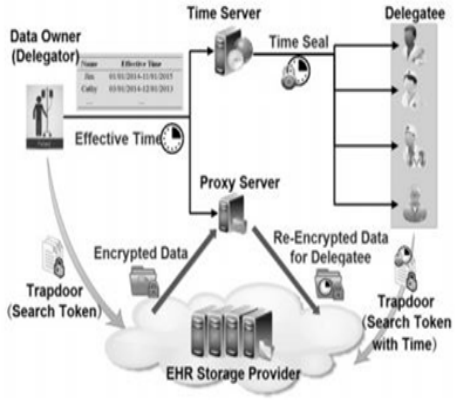

Fig.1. Proposed architecture

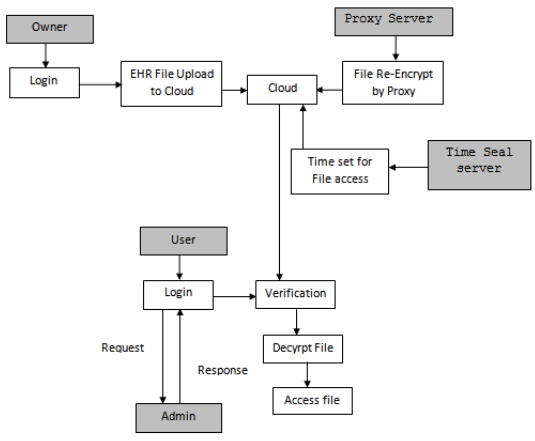

Fig.2. Proposed scheme- Block diagram

IV. EXPERIMENTAL RESULTS

This section depicts the experimental analysis of the

proposed cloud security scheme. The proposed algorithm is experimented via Java programming language. It is explained as follows:

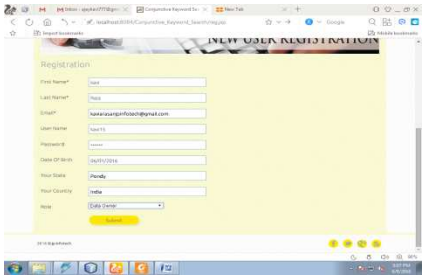

Fig.3. Registration of the new users.

Fig.4. Viewing the owner and user details

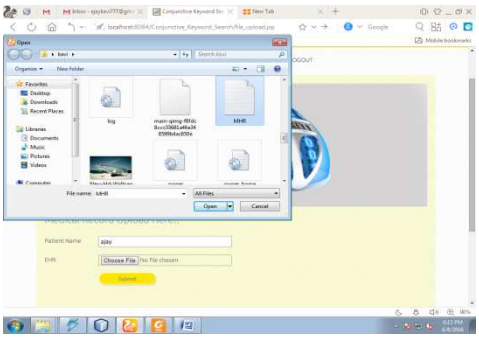

Fig.5. File uploaded from owner's login

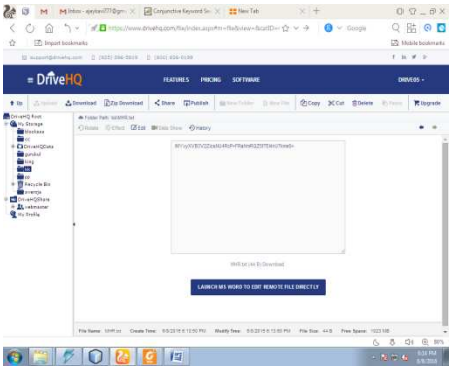

Fig.6. File is uploaded from cloud drive.

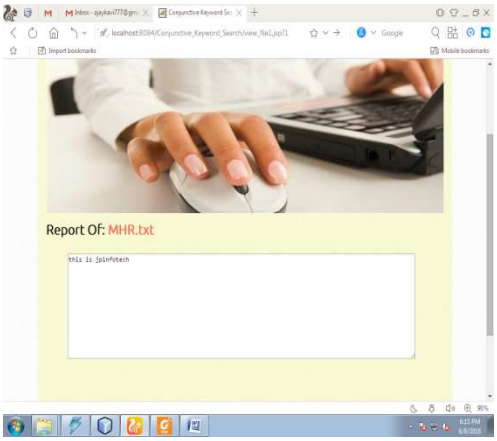

Fig.7. Viewing the uploaded file

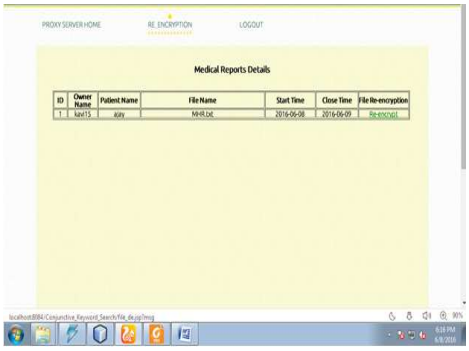

Fig.8. Medical records viewed from proxy's login

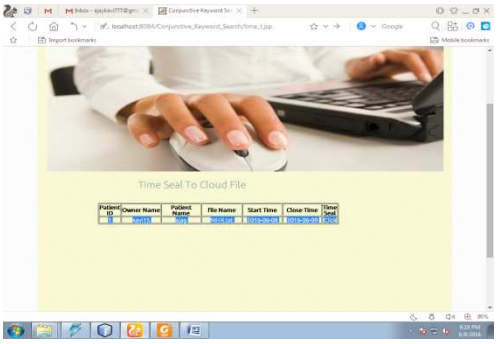

Fig.9. Enabling time seal for every medical record.

Fig.10. Setting log out time for each user.

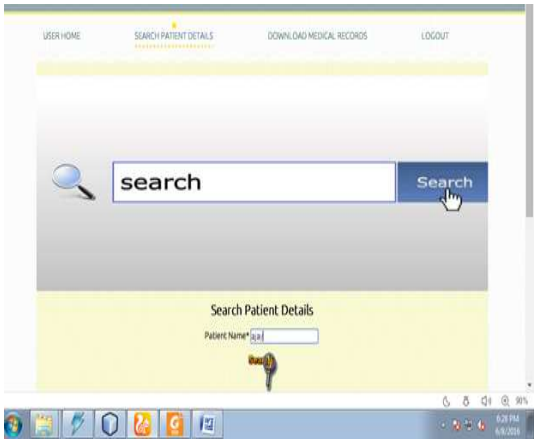

Fig.11. Searching for patient records.

Fig.12. Downloading the patient details under time seal server

V. CONCLUSION

This paper concentrates on safe and secure searching of unstructured data in cloud. To accommodate secure encryption on cloud, a novel method of searching encrypted data on cloud is proposed. Thus, user does not need to hesitate about security issues and shall be willing to place more data on cloud. In this paper, we have proposed a timing enabled proxy re-encryption scheme that allows the users to search and retrieve the data in timely events. Simulated results demonstrate that it provides fast and efficient conjunctive search for unstructured data in original documents on cloud server. The proposed technique reduces the overhead of decryption thereby minimizing the adversary's events to a considerable extent.

REFERENCES

[1] Rongmao Chen et al, "Server-Aided Public Key Encryption with Keyword Search", IEEE Transactions on Information Forensics and Security, 2016.
[2] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.
[3] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.
[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.
[5] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE Transactions On Parallel And Distributed Systems, VOL., NO.1,2015.
[6] Bing Wang, Wei Song, Wenjing Lou, and Y. Thomas Hou "Inverted Index Based Multi-Keyword Public-key Searchable Encryption with Strong Privacy Guarantee" IEEE Conference on Computer Communications (INFOCOM), 2015.
[7] Yanzhi Ren, Yingying Chen, Jie Yang, Bin Xie " Privacy-preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing" Globecom Communication and Information System Security Symposium 2014.
[8] Hongwei Li, Dongxiao Liu,Yuanshun Dai, Tom H. Luan, And Xuemin (Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", December 2014.
[9] Mikhail Strizhov and Indrajit Ray "Multi-keyword Similarity Search Over Encrypted Cloud Data" International Conference on Pervasive Computing (ICPC), 2012.
[10] E.-J. Goh, "Bloom filters in order to construct the indexes for the data files" IEEE Conference on Computer Communications, 2016.
[11] Jun Zhou, Zhenfu Cao, Xiaolei Dong and Xiaodong Lin "More Efficient Verifiable Outsourced Computation from Any One way Trapdoor Function" IEEE ICC - Communication and Information Systems Security Symposium, 2015.
[12] Fanyu Bu, Yu Ma, Zhikui Chen and Han Xu "Privacy Preserving Back-Propagation Based on BGV on Cloud" 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015.