SCRIBBLE LEGALIZATION CRYPTOGRAPHIC ASPECT BASED ON DATA ACCESS CONTROL FOR STEAM COUNT

Yerragudipadu, Subba Rayudu, R M Noorullah and C Praveen Kumar
Department of Computer Science and Engineering, Institute of Aeronautical Engineering, Jawaharlal Nehru Technological University, Hyderabad, India
G-Mail: Subbu.iare@gmail.com

ABSTRACT

Recently, healthcare applications adopt the advents of cloud technologies. Electronic Health Records (EHR) plays a vital role in healthcare environments. Thus, the proper usage and protection of EHR systems enabled the growth of cloud based healthcare applications which implies the patients-safety of their sensitive information. However, the data owner should be online in order to send the PRE keys to the CSP in a timely fashion, to prevent the revoked user from accessing the future data. The delay of issuing the PRE keys may cause potential security risks in this paper, we have proposed cryptographic Aspect Based access control system for EHR systems which uses time and location based user's authentication process. A defined set of attributes embedded with time period T to access the data by its intended users. Experimental results have shown the efficacy of our proposed work in terms of decryption key compromised, role expiration and lessened key complexity have been studied.

Keywords: healthcare applications, electronic health records, cloud technologies, user's authentication, time period, location and data access control.

1. INTRODUCTION

The developments achieved in the cloud system have convoluted the traditional healthcare systems. Most of the cloud technologies have been applied in every aspect of the real-time applications. A variant of analysis have been carried out in the healthcare applications. With the advents of cloud technologies, the availability rate of medical services is increased. Henceforth, it is coined as 'e-health cloud'. The Personal Health Record (PHR) is transferred to Electronic Health Records (EHR) in order to prevent medical data errors, time consumption and security enhancements. Since PHR and EHR are the electronic versions, the PHRs are handled by patients and the EHRs are handled by healthcare service providers [2]. The cloud health databases management system with reasonable cost is being adopted by several countries. The traditional healthcare system is re-invented and termed as 'e-health cloud'.

In the view of service providers, the electronic records are offered with reasonable cost and also variant finance companies are developed. In real time systems, the patients may experienced different roles like physician, specialist, therapist etc. In some cases, the patients may engages into different insurance schemes [3]. Hence, the sensitive information of the patients may resides anywhere in the healthcare networks. In the aspect of clinicians, the information should be updated periodically. Thus, the demand for sharing and integrating the medical records from variant service providers should be balanced and protected. Storage requirement of cloud computing systems in healthcare networks is a troublesome and demanding issue.

The technology innovation made in the healthcare process has to achieve an efficient, less expensive and of higher quality [4]. Digital era on healthcare data has revolutionized the field of healthcare management system. Henceforth, this novel field is more vulnerable to the exploitation of cyber crime [5]. Though, several schemes are introduced by the financial and retail sectors, the current era on EHR transition requires a devised cryptographic model. Owing to the integration of the technology into our lives, the need for advancement of technologies in the medical domain has been explored by different researchers.

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

2. RELATED WORK

This section presents the basic primitives in e-heath data and existing security schemes suggested by other researchers.

A. Basic primitives of e-health data

a) User revocation

User revocation is a frivolous task. With the help of previous keys, the revoked users may access the sensitive data and the adversaries can also modifies those sensitive information. In order to eliminate the tasks performed by revoked users, the concepts of re-keying and re-encryption were introduced. Let us consider an example, the data is encrypted using Attribute based Encryption systems (ABE) where the data owner should update the private keys for its authenticated users in periodic manner. By incorporating so, the ABE model incurs higher storage space, data overhead and time consumption. To overcome from this drawback, the concept of third-party authenticator is introduced which concurrently reduces the intensive computational tasks [6]. And then the proxy re-encryption concept is introduced for better communication systems. The demerits of these systems are the PRE keys supply from CSP blocks the revoked users from data access.

b) Proxy re-encryption

One of the cryptosystems is the proxy re-encryption [7] that works on ciphertext without any knowledge of its plaintext. It is a semi-trusted server. Consider a communication between Alice (the delegator) and Bob (the delegatee), the Alice sends the encrypted message with its secret keys to the bob.

c) Searchable encryption

Searchable encryption is the recent concept enabled in the proxy re-encryption schemes. It operates over the indices generation of the files [8]. The role of searchable index is to protect the data resides at cloud servers and thus validating whether the authorized users access the data. The function is to obtain the relevant keywords from user's petition. Thus, it necessitates several search operations in the server side where the search complexity is proportional to the number of semantically closed keywords.

B. Prior works

Generally, the traditional encryption schemes like Public Key Encryption (PKE) and Symmetric Key Encryption (SKE) are used for storing and protecting the data. These primary schemes were undergone some researches and different enhanced model was introduced. From the analysis, it is inferred public key system performed less than the symmetric schemes. This was further enhanced to SKE where symmetric keys are used for encrypting the data and PKE is used for protecting the private keys. The security schemes like ECC, RSA [9] etc were used for protecting the systems. The hybrid approaches are discussed below:

A reference model based data management system over untrusted cloud was introduced in [10]. In order to prevent the anonymity's actions, patient oriented model was suggested. Then the authentication process between two users was verified by their signatures. The similar study is extended to the Group systems where every member in the groups is identified by their validated signatures. Henceforth, the medical logs research was studied by variant researchers. Similar study was performed by [11] where the patient provides privileges to the content from the unauthorized modifications. They specifically introduce the Digital Rights Management (DRM) [12] that specifically focused on the e-health records. Before outsourcing, the data is encrypted and it is further decrypted by owner [13]. It is termed as 'Content Key Encryption (CKE)' [14]. Content key is used for opening the content. In this case, the patients and physicians have possessed the public and private keys for encryption and decryption.

A security protocol from aspects of patients is introduced by [15]. The concept of data access control layer was used for storing efficiently and preserving the sensitive data. A survey of electronic records generated to cloud centers did by [16]. They stated importance of e-health data and prior methods for data maintenances using hash values [17]. Universal Designated Verifier Signatures (UDVS) [18] is introduced to ensure the usage of record. And also, it is verified that the designated verifier receives the designated signatures. If such information is disclosed, then the monitoring system would not be able to effectively manage the access control. The author in [19] proposed a framework, Online Referral and Appointment Planner (ORAP) that supported the efficient transmission of the secured data to different aspects of healthcare environment. Amazon S3 cloud framework was also recently used as temporary storage which is in encrypted form. However, the ORAP lacks in integration of patient centric functions that makes it less flexible in providing Aspect Based access.

Then, the study was extended to the Aspect Based and time based access control model [20]. This approach makes encrypted EHRs over the untrusted clouds and resolves the key management issues. Based on the roles, the data accessing is permitted over stipulated period of time [21]. This was further extended to the multiple roles using multiple keys.

3. PROPOSED WORK

This section depicts an enhanced cryptographic based timing enabled proxy re-encryption model is explained.

A. Problem definition

Security is a significant metric that has to be focused over the outsourced e-health data. Most of the healthcare networks get attracted by the cloud technologies. The transition over EHRs is a demanding issue with affordable costs. Thus, the deployment of cryptographic model is employed over the e-health records. The EHR model contains multiple EHR owners and multiple EHR users. In this model, patients are referred by 'owners' that has different control over data. The data users comprises of different roles like staff member, nurse etc. of e-health environment. Generally, the EHRs files are structured in hierarchical way. Prior works have been focused on storing and protecting the medical records in secured and authenticated manner. Even though, the security requirements of e-health cloud is not yet achieved. The attackers act like normal users and steal the personal records. Thus, timing based search has been proposed.

B. System model

Let us consider system model which comprises of three roles, namely, data owner, data user and data center. Using the third party databases, the data owners stores and manages their sensitive data. Each file obtains a keywords and it is in encrypted form. Thus, the encrypted keywords acts as searchable indices for file retrieval process. The EHR files are encrypted and then outsourced to the cloud servers. In this model, the cloud server contains two systems, namely, EHR storage provider and search server. When the user enters their keywords, the data is searched and retrieved using those two models. Then, the users perform search over the cloud centers, where the matched results will be returned based on the validated user's private key. Considering the above similar scenario, we highlight the timing enabled proxy-re-encryption searchable encryption model. In specific to, we contribute Aspect Based time controlled function over the searched data. The searching operations are carried out by similarity cum conjunctive keyword search process.

C. Proposed timing enabled searchable encryption model

a) Design goals

The target of the proposed framework is to eliminate the activities performed by unauthorized users to view the EHR files. The following are the design objectives:

a) **Fine grained access control:** Enforcing the secure mechanism those different users can read/ write the data over variant *set of files.*

b) **User revocation:** Accord to the privileges, the user's access over data is invoked/ revoked.

c) **Efficiency:** The security system should be scalable in nature i.e support of voluminous users.

d) **Time based revocation:** Timing is set to different users in order to prevent the usage of unauthorized users. Identity based timing controlled function is defined for each delegates and delegator.

b) Proposed algorithm

Consider a set of attributes (R, T and M) be the set of role space, time space and message space respectively. The proposed steps are as follows:

a) **Setup:** With security parameter k and the no.of users U, the public parameters mpk and master secret key msk are generated. An empty revocation list (RL) is maintained.

b) **KeyGen:** Using the msk, the private key is generated for the intended users. Along with user identity ID € I, the private key for the user is given as Sk_{id} and update its states st.

c) **Tokenup:** For every role r and msk, the time period T_i € T is allocated for intended users and outputs the token t_i where i € [1, poly (1^k)].

d) **Dekeygen:** The decryption key is generated from the inputs sk_{id} and T_i and depicts the decryption key $Sk_{id, i}$

e) **Rekeygen:** The re-encryption process is as follows:

- Input: $Sk_{id, i}$, msk, T_i and $T_i^{'}$
- Output: Re-encryption key, where $1 \leq i < i^{'}$
- Re-keytoken: With the above given inputs, the re-key token is generated as $\Psi_{i \rightarrow i'}$
- Reenc-key: With the re-keytoken and $Sk_{id, i,}$ the re-encryption key is given as $rk_{id, i \rightarrow i'}$

f) **Encryption:** The ciphertext C is generated from the inputs role r, T_i and message m.

g) **Re-Encryption:** With the inputs $rk_{id, i \rightarrow i'}$ and Ciphertext C, the re-encrypted ciphertext C is formulated under (r, $T_i^{'}$) and C is not valid, then it notifies as indicator $^{\theta}$.

h) **Decryption:** Similarly, it takes the input $Sk_{id, i,}$ and Ciphertext C, the message m is decrypted and in case C is not valid, then it notifies as indicator $^{\theta}$.

i) **Revoke:** The revocation process executes by the role ID and its revoked time period Ti, current state of the users and outputs the updated Revocation list (RL) .

Thus, our proposed algorithm has simplified and stronger security functions than the prior searchable encryption schemes.

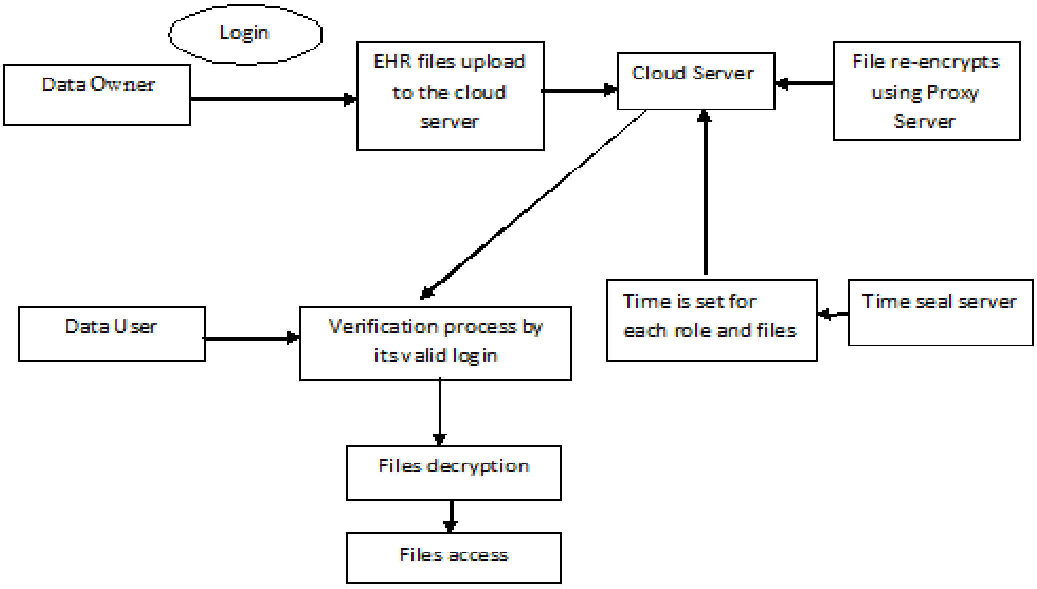
Login
Data Owner
EHR files upload to the cloud server
Cloud Server
File re-encrypts using Proxy Server
Data User
Verification process by its valid login
Time is set for each role and files
Time seal server
Files decryption
Files access

Figure-1. Workflow of the proposed algorithm.

4. PERFORMANCE ANALYSIS

This section depicts the performance analysis of our proposed scheme in terms of security. The security analysis like decryption key compromised, role expiration and lessened key complexity have been studied.

A. Decryption key compromised

In case any adversary tries to modify the records, the decryption key $sk_{id,\ i}$ for the intended role r and time period $T_{i,}$ the user ID updates the sensitive data to its cloud environment. By doing so, re-encryption process is invoked and eliminates the activities of unauthorized users. Under certain time period T, the re-encryption key is generated implicitly and makes the stronger e-health cloud environment.

B. Expiration of identity

The user's role is expired after certain time period T and its also updated to its cloud environment. For every time period T, the re-encryption key is generated which eliminates the data access using prior knowledge. The ciphertext C under (r, T_i) to the ciphertext C under (r, T_j) are processed with the newly arrived re-encryption key. If not, the revocation list consists of revoked users based on valid period of token.

C. Lessened complexity of key update phase

The key update phase is linearly depends upon the availability of users. The secret key is generated only for the users who are not listed in Revocation List (RL). The Token Up algorithm depicts that user's role r will not participate in the token T_i. This is in further helps to identify the revocable and non-revocable users. This is applied to decryption key generation, message encryption and decryption.

Table-1. Files and its keywords.

No. of files	Keywords
200	1500
400	2600
500	1356
700	2631
1000	1652

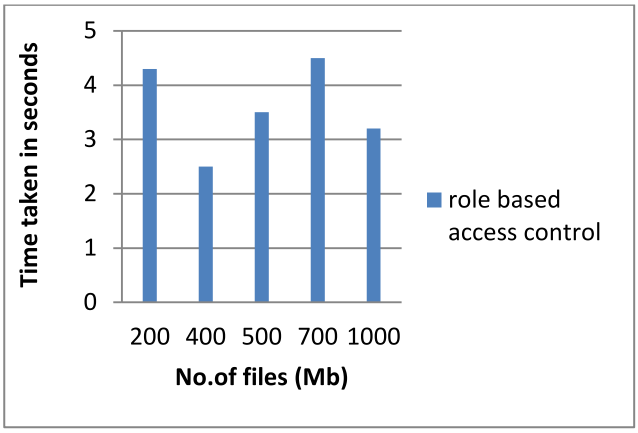

Figure-2. Total time taken to search and retrieve the similar files under cryptographic aspect based time-enabled proxy-re-encryption system.

5. CONCLUSIONS

The recent developments in the cloud technologies has re-innovated the healthcare systems. The objective of the system is to assist the medical service providers and ensures patients-safety. In this paper, we have explored a cryptographic Aspect Based timing enabled proxy re-encryption systems which embeds keywords with certain time period T. The outsourced e-health records contain sensitive information which is uploaded to the cloud in encrypted form. A time controlled function is used for eliminating the adversary's action. Similarly, the privilege settings for different roles are provided. Any users can access the data within stipulated period of time with security analysis in terms of decryption key compromised, role expiration, and lessened complexity of key update phase. The main purpose is to devise the data structure with the qualities of lessened storage space and rapid search functionalities.

REFERENCES

[1] Yang Yang *et al*. 2016. Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds. IEEE transaction on Information forensics and security. 11(4).

[2] 2012. Federal Health IT Initiatives. http://www.hhs.gov, accessed December 24.

[3] Canada Health Infoway. 2012. http://www.infoway-inforoute.ca, accessed December 24.

[4] J. Dzenowagis and G. Kernen. 2005. Connecting for health: Global vision, local insight. World Health Organization Press, Report for the World Summit on the Information Society. pp. 1-36.

[5] H. J. Cheong, N. Y. Shin, and Y. B. Joeng. 2009. Improving Korean service delivery system in health

care: focusing on national e-health system. in IEEE International conference on e-Health, Telemedicine and Social Medicine (TELEMED '09). pp. 263-268.

[6] L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson and D. Bell. 2011. DACAR platform for e-Health services cloud. in 4th IEEE International Conference on Cloud Computing. pp. 219-226.

[7] P. G. Goldschmidt. 2005. HIT and MIS: Implications of health information technology and medical information system. Communication of the ACM. 48(10): 69-74.

[8] E. Davidson and D. Heslinga. 2007. Bridging the IT adoption gap for small physician practices: An action research study on electronic health records. ACM Journal of Information Systems Management. 24(1): 15-28.

[9] E. AbuKhousa, N. Mohamed and J. Al-Jaroodi. 2012. E-Health Cloud: Opportunities and challenges. Future Internet. 4(3): 621-645.

[10] R. Zhang and L. Liu. 2010. Security models and requirements for healthcare application clouds. 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA. pp. 268-275.

[11] R. Wu, G.-J. Ahn, and H. Hu. 2012. Secure sharing of electronic health records in clouds. In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom). pp. 711-718.

[12] S. P. Ahuja, S. Mani, and J. Zambrano1. 2012. A survey of the state of cloud computing in healthcare. Network and Communication Technologies. 1(2): 12-19.

[13] P. Mell and T. Grance. 2012. The NIST definition of cloud computing. NIST special publication, 2011, http://predeveloper.att.com/home/learn/enablingtechnologies/The_NIST_Definition_of_Cloud_Computing.pdf, accessed December 14.

[14] S. Yu, C. Wang, K. Ren, and W. Lou. 2010. Achieving secure, scalable and fine-grained data access control in cloud computing. IEEE INFOCOM Proceedings. pp. 1-9.

[15] B. Horowitz. 2012. Cloud Computing Brings Challenges for Health Care Data Storage, Privacy, http://www.eweek.com/c/a/Health-Care-IT, accessed December 20.

[16] G. Ahn, H. Hu, J. Lee, and Y. Meng. 2010. Representing and reasoning about web access control policies. 34th IEEE Annual Conference on Computer Software and Applications, (COMPSAC '10). pp. 137-146.

[17] H. Takabi, J. Joshi, and G. Ahn. 2010. Security and privacy challenges in cloud computing environments. Security & Privacy, IEEE. 8(6): 24-31.

[18] R. Wu, G.J. Ahn, H. Hu, and M. Singhal. 2010. Information flow control in cloud computing. 6th International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom '10). pp. 1-7.

[19] R. Wu, G. Ahn, and H. Hu. 2013. Secure Sharing of Electronic Health Records in Clouds. http://www.public.asu.edu/~hongxinh/papers/TrustCol12.pdf, accessed December 14.

[20] M. Johnson. 2009. Data hemorrhages in the health-care sector. Financial Cryptography and Data Security. pp. 71-89.

[21] Z. Xiao and Y. Xiao. 2012. Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials. pp. 1-17