Privacy Preservation for Outsourced Medical Data with Flexible Access Control

[1]Ms. Gayatri Naik, [2] Miss. Apurva Malgaonkar, [3]Mr. Shriraj Tarkar, [4] Mr. Vishal Badgujar
[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.
[1]krishnagita123@gmail.com,[2]badgujarvishal097@gmail.com,[3]shrirajtarkar1404@gmail.com,
[4]apurvam61@gmail.com

Abstract- In current health care network, Electronic medical records (EMR) play a very vital role. As the records contains personal and sensitive information regarding patients, the system's privacy preservation is necessary. The current scheme which is available permits the user to read EMR only if it satisfies the set policies. But the currently existing system links the identities of the patients with their particular doctors. Hence, the classified data of the concerned patients are shared without the third party actually identifying the patient. To address this problem, it requires of present of two anonymous schemes. This scheme helps user to confidentially store and process data preserving it's anonymity. The proposed first scheme provides moderate security, where the attacker targets individuals without prior getting information from the EMR systems.

Keywords-- privacy preservation, security, electronic medical record.

I. INTRODUCTION

Currently, electronic medical records (EMRs) are very prominent in healthcare networks. It enables users to share their health data in a flexible and convenient way. For example, to find one's diagnostic report, a patient or doctor needs only to retrieve the information from a database rather than having to search through numerous physical documents. Health data is very sensitive, and it is a major challenge to securely store and access EMRs in modern EMR systems. As most EMRs are projected to the cloud, as it is easily exposed to potential threats and vulnerable to leakage, loss, and theft.[1]To prevent EMRs from unauthorized access, a standard solution is to perform an encryption before uploading it to the cloud. Specifically, an EMR owner encrypts an EMR using a symmetric key, and only authorized medical staff are authorized to access and decrypt it.

However, data sharing becomes inflexible in this case. As patients usually do not know who is allowed to access the EMRs, it encrypt many pieces with distinct session keys and distribute the keys to different medical staff members. The approach to accessing users' data needs to be flexible enough to address changes in user's roles Several schemes adopting attribute based encryption (ABE) have been presented for fine-grained access control[4],[5].Users with the one of attributes satisfying the access policy can decapsulate the EMR data. In addition, some advanced mechanisms, consisting of a multi-authority model in an out of the projecting system and view based access control that allows patients to specify a list of authorized/unauthorized users, have recently been proposed. RBACs also allow fine-grained access control.

II. AIMS AND OBJECTIVE

a) Aim

In current worlds modern health care system Electronic form of health record play a very vital role. The components present in EMR normally provide a large variety of spectrum and fundamental security. During data exchange of patients record a structure is needed which will provide the needed security. To achieve security and privacy-preservation for information exchange, it proposes a consent-based access control (CBAC) mechanism for healthcare systems.

b) Objective

The main objective of the proposed system is to propose a framework for electronic health record systems where data providers offer the original health information (encrypted for privacy preservation) to the center where data is stored; which is supposed to be trustworthy and authenticate.

III. LITERATURE SURVEY

The literature survey deals with the topics and the researches that would help to understand the existing systems that are similar to Privacy Preservation for Outsourced Medical Data with Flexible Access Control.

 DOI : 10.35291/2454-9150.2020.0228

The objective of this literature survey is to analyze the related work to this project and mechanisms used in previous studies.

Paper 1: Dynamic and efficient key management for access hierarchies.

In the context of access control hierarchies arise whenever the user population can be modeled as per the set of partially ordered classes. A user who has privileges to access a class also obtains access to objects stored at that particular class and all descendant classes in the hierarchy. The problem of key management for such hierarchies arises which then consists of assigning a key to each class in the hierarchy so that keys for descendant classes can be obtained via efficient key derivation. Whereas many previous schemes had some of these properties, the project is the first that satisfies all of them. The security of the project scheme is based on pseudo random functions, without reliance on the Random Oracle Model.

Paper 2: A hierarchical framework for secure and scalable EHR sharing and access control in multi- cloud.

Electronic Health Records (EHRs) is a efficient and preferred method to store patients' health records. The emergence of cloud computing services allows flexible access, large storage capability and low costs, which motivate EHR maintainers to consider migrating EHR data from their own storage to the cloud. However, securing EHRs in cloud is a challenge that appears to be major. Several security properties need to be satisfied for this, such as data privacy, fine-grained access control and scalable access between different clouds. In this paper, system proposes a secure and scalable framework for EHR data sharing which combines IBE and ABE together to enforce access control policies.

Paper 3: A flexible role- based secure messaging service: Exploiting IBE technology for privacy in health care.

The management of private and confidential information is a main problem that exists for dynamic organizations. Secure solutions are the need to exchange confidential documents and to protect them from unauthorized accesses and cope with changes of people's roles and permissions. This paper describes an innovative technical solution in the area of secure messaging that exploits (IBE) technology. Thus this paper deals with IBE technology for privacy in health care.

IV. EXISTING SYSTEM

An EMR owner encrypts an EMR using a symmetric key, and only authorized medical staff are authorized to access and decrypt it. Two potential issues are raised here. They are the complicated key management and repetitive encryption. The current existing system links the patients information with doctors. Hence, the classified data of patients diseases are shared without the third party having actual access to the patients EMR file. To gain fine-grained access control this system represents several scheme supporting attribute-based encryption (ABE). So now the above said proposed system can achieve data confidentiality but the issue related privacy preservation is not ye solved. However, data sharing becomes inflexible in this existing schemes.

V. COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	Technology	ADVANTAGE	DISADVANTAGE
1.	Privacy preservation for outsourced medical data with flexible access control	Zhou, Xingguang, et al	RBAC, ABE	Only users who satisfy the role based policy can access the data	If only the role is satisfied the user can access the data otherwise access is denied.
2.	Dynamic and efficient key management for access hierarchies. ACM Transactions on Information and System Security.	Atallah, M. J., Blanton, M., Fazio, N., & Frikken, K. B.	Key Generation	1. Data is stored in collaborative manner so it is easy to access any information required. 2. A user who can access a class also gets to access the objects of that class and all the lower classes in its hierarchy.	1. Space complexity and Time Complexity arises minute details of every person are stored in the database. 2. To execute and complete tasks particular set of instructions are required.
3.	A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud	Huang, Jie, Mohamed Sharaf, and Chin-Tser Huang.	Identity-based Encryption and Attribute based Encryption	1.System proposes a secure and scalable framework for EHR data sharing 2. Secure and scalable framework for HER data is available in the system.	1. Security of Data stored on cloud is not guaranteed. 2. Several security properties need to be satisfied.

 DOI : 10.35291/2454-9150.2020.0228

4	A flexible rolebased secure messaging service: Exploiting IBE technology for privacy in health care	Mont, Marco Casassa, Pete Bramhall, and Keith Harrison	IBE identifier based encryption Technology	1. Innovative technical solution in the area of secure messaging that exploits (IBE). 2. To exchange confidential documents secure solutions are needed.	Currently used in a trial with a UK health service organization so not sure if it works properly. 2. Traditional cryptographic solutions are the limitations.

VI. PROBLEM STATEMENT

In Reality, an EMR System is vulnerable to attacks by outside entities. A dishonest party may try to obtain useful information from encrypted data that it is not authorized to access or to divert instructions from the system regarding benefits (e.g., with false information in medical disputes). Many attacker with ill intentions may together collide to attack the system. Hence, according to the above content of attacks, it is necessary for the system to meet some following mentioned security requirements. Data Confidentiality. Personal data needs to be encrypted before being uploaded and securely stored on the cloud until an entitled recipient downloads and decrypts it. Specifically, only the users whose roles satisfy the associated access policy have the privilege to access the data, with all other unauthorized entities not able to obtain any useful information from the encrypted data, even if they collude with each other.

VII. PROPOSED SYSTEM

This system presents two anonymous schemes. It not only achieves data confidentiality but also helps to provide anonymity to the system users. The first mentioned above scheme achieves moderate security, where the attacker attacks without obtaining any information. The second scheme helps achieves full security, where attacker adaptively choose attack individuals after gathering information from the EMR system. In addition, it proposes an approach in which EMR owners can search for their EMRs in an anonymous system. EMR data can be encapsulated according to an on-demand access policy, with only users whose roles satisfy the access policy being a ble to decapsulate it. Patient 's privacy is preserved using a bilinear group, where all the identity-related information is hidden in a subgroup. Based on the chosen bilinear group assumptions, it is that proposed models have the property of semantic security and anonymity. It applies the "online/ offline" approach to achieve a better user experience[3].

VIII. ALGORITHM

Role- based access control (RBAC) Algorithm also known as role based security is used in computer system security. It helps to restrict the access of the system only to the authorized users. RBAC's flexibility allows it to implement mandatory access control (MAC) and discretionary access control (DAC). Even though the framework of DAC and MAC is different it can implement without creating any complications. Systems implementing RBAC Algorithm are popularly used in organizations have large number of systems or comparatively bigger employee crowd.

Role-Based Access Control (RBAC) Role Classification Algorithm

Step 1 :Audit log record:

X1,X2,,,Xn,Ri

where…

X1,X2,,Xn-n attributes of the audit log Ri role held by user who created the log record assumption.

Every user can hold only one role

X1,X2,,,Xn,Rj

X1,X2,,,Xn,Ri

No records of the form with Ri?Rj

Step 2 :Classification Phase

Calculate distance between the newly produced audit record Recnew of a user U and each existing cluster

a) Find cluster Cmin closer to Recnew

b) Find cluster Ccur closest to Recnew

c) If role represented by Ccur role of Recnew then U is a normal user else U is an intruder and an alarm is raise.

IX. MATHEMATICAL MODEL

KeyGenM (PK,MSK,→− R). For any medical staff member associated with role →R = (R1,...,Rd), denote I = {i :R i ∈ S→R}. When a medical staff member wants to join the system, he should first be authenticated by the TKA. Next, if he is a top-level medical staff member, the TKA generates a secret key SK→− R for him. The TKA picks random exponents r1, r2,s1,s2,t1,t2 R ← ZN satisfying s1 · t2 − s2 · t1 6=0 mod pands1·t2−s2·t1 6= 0 mod q. If the equations do not hold, the TKA picks other random exponents and repeats the procedure. It outputs the secrets key SK→− R, which consists of two sub keys: the sub key

SK→− R d is used for decryption and delegation, and the sub key SK→− R r is used for re-randomization.

 DOI : 10.35291/2454-9150.2020.0228

SK→ Rd ={{w(∏ hi Ri i∈I)r1fr2,gr1,gr2,gr1 h ,{hr1 j }} SK→ Rr ={(∏ hi Ri iCI)s1fs2,gs1,gs2,gs1 h ,{hs1 j },

(u∏ $hiRi$ i i∈)t1ft2,gt1,gt2,gt1 h ,{ht1 j }}

In the above equations, j ∈ [1, n]\I. Finally, the TKA outputs SK −→R = n SK −→R d , SK −→R r o for the medical staff.

KeyGenP(PK,MSK,ID). When a patient with identity ID wants to access his own EMR, the TKA first authorizes him and then assigns him a secret key.

The TKA picks a random exponent r0 1,r0 2 R ←ZN and outputs SKID = {$d1$ ′ ,$d2$ ′ ,$d3$ ′ {dj ′}j∈[1,n]} =

{ω(ugh ID)$r1$ ′ f$r2$ ′ , g$r1$ ′ , g$r2$ ′ ,{h$r1$ ′ }j∈[1,n] }

In conclusion, by running KeyDelegM, the delegated secret key is well formed, appearing as if it was generated directly by the TKA using KeyGenM.

X. SYSTEM ARCHITECTURE

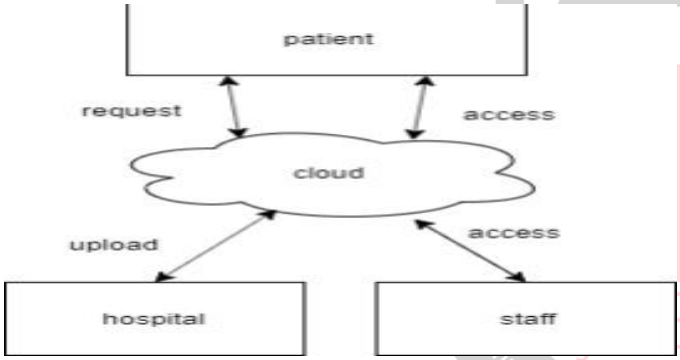

Fig.1: Current System Architecture

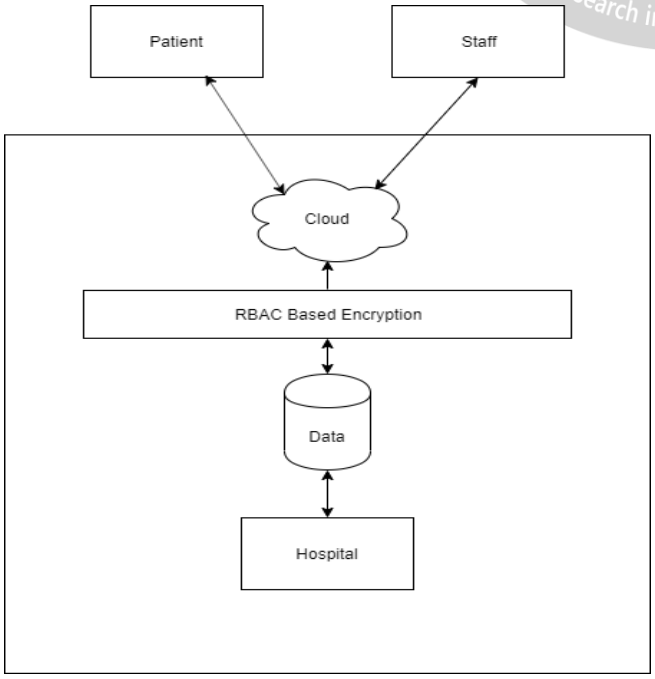

Fig no.2: Proposed system architecture

XI. ADVANATGES

- Data is stored in collaborative manner so it is easy to access any information required.
- Patient's privacy is preserved using a bilinear group, where all the identity-related information is hidden in a subgroup.
- It achieves flexible access control such that the EMR data can be encapsulated.
- According to an on-demand access policy, with only users whose roles satisfy the access policy being able to decapsulate it.
- Proposed models have the property of semantic security and anonymity.

XII. DESIGN DETAILS

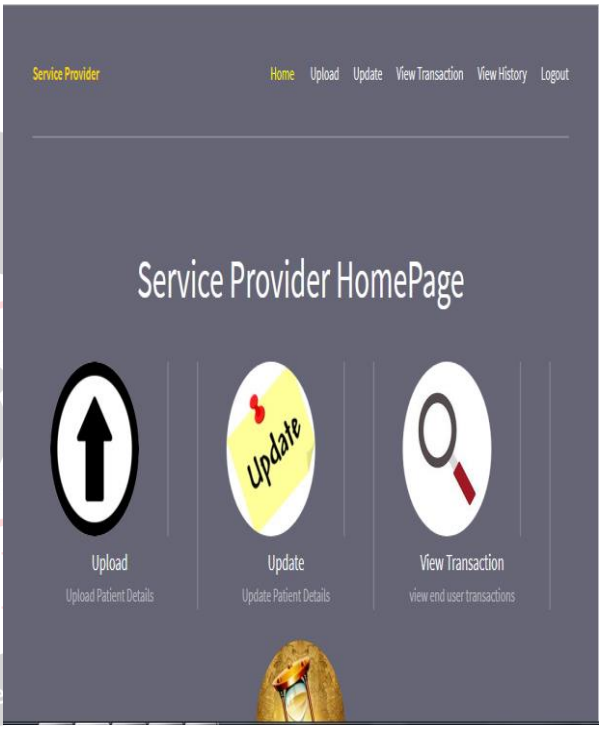

Fig 2: Service Provider Homepage

XIII. CONCLUSION

Thus, we have tried to implement the paper "Xingguang Zhou, Jianwei Liu, Qianhong WU, And Zongyang Zhang.", "*Privacy preservation for outsourced medical data with flexible access control"*. IEEE 2016 and according to the implementation the conclusion is as follows. In this paper, it is proposed that two anonymous RBAC schemes for the EMR system.

It helps achieve flexible access control such that the EMR data can be encapsulated on the basis of an on-demand access policy, with only users whose roles satisfy the access policy which can be able to decapsulate it.

Patients' privacy is preserved using a bilinear group, where the entire information of identity related content is hidden in a particular sub-group. As it has been applied

 DOI : 10.35291/2454-9150.2020.0228

to achieve a better user experience whether online or offline. Because it is based on the selected bilinear group assumptions, it is proved that the proposed models currently have the semantic security and anonymity property.

REFERENCE

[1] M. J. Atallah, M. Blanton, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," ACM Trans. Inf. Syst. Secure., vol. 12, no. 3, 2009.

[2] J. Huang, M. Sharaf, and C. T. Huang, "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud," in ICPPW 2012. IEEE,2012, pp. 279–287.

[3] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploting ibe technology for privacy in health care," IEEE Computer Society, vol. 432, 2003.

[4] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in SPSM 2011. ACM, 2011, pp. 75–86.

[5] S. Narayan and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," in CCSW'10. ACM, 2010, pp. 47–52.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE .Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[7]Holland, Christopher P., and Gordon D. Mandry. "Online search and buying behaviour in consumer markets." 2013 46th Hawaii International Conference on System Sciences. IEEE, 2013.

[8]Jiao, Ming-hai, et al. "Research on personalized recommendation optimization of E-commerce system based on customer trade behaviour data." 2016 Chinese Control and Decision Conference (CCDC). IEEE, 2016.

[9]Hernandez, Sergio, et al. "Analysis of users' behavior in structured e-commerce websites." IEEE Access 5 (2017). Q. Su and L. Chen, "A method for discovering clusters of e-commerce interest patterns using click-stream data," Electronic Commerce Research and Applications, vol. 14, no. 1, pp. 1 – 13, 2018.

[10]Gordon D. Mandry. "Online search and buying behaviour in consumer markets." 2013 46th Hawaii International Conference on System Sciences. IEEE, 2013

 DOI : 10.35291/2454-9150.2020.0228