ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

# IMPLEMENTING FLEXIBLE ACCESS CONTROL SCHEME FOR OUTSOURCED MEDICAL RECORDS

**P.S.K Gayathri**
*B.Tech, Department of Computer Science &Engineering, Narayana Engineering College Gudur*
*gaiprincess89@gmail.com*

**Ch.D.Sunil Kumar**
*Asso.Professor,Department of Computer Science &Engineering, Narayana Engineering College Gudur*
*cassunil@gmail.com*

**V.Lakshmi Lahari**

*B.Tech ,Department of Computer Science &Engineering, Narayana Engineering College Gudur*
*laharivayugundla24@gmail.com*

**P.Amulya**
B.Tech ,Department of Computer Science & Engineering, Narayana Engineering College Gudur
amulyavarshik@gmail.com

## *Abstract*

Electronic medical records (EMRs) play an important role in healthcare networks. Since these records always contain considerable sensitive information regarding patients, privacy preservation for the EMR system is critical. Current schemes usually authorize a user to read one's EMR if and only if his/her role satisfies the defined access policy. However, these existing schemes allow an adversary to link patients' identities to their doctors. Therefore, classifications of patients' diseases are leaked without adversaries actually seeing patients' EMRs. To address this problem, we present two anonymous schemes. They not only achieve data confidentiality but also realize anonymity for individuals. The first scheme achieves moderate security, where adversaries choose attack targets before obtaining information from the EMR system. The second scheme achieves full security, where adversaries adaptively choose attack targets after interaction with the EMR system. We provide rigorous proof showing the security and anonymity of our schemes. In addition, we propose an approach in which EMR owners can search for their EMRs in an anonymous system. For a better user experience, we apply the "online/offline" approach to speed up data processing.

**Index Terms** – E**lectronic medical record, privacy preservation, security.**

## I.INTRODUCTION

Currently, electronic medical records (EMRs) are very prominent in healthcare networks. It enables users to share their health information in a flexible and easy way[11]. For example, to receive a single diagnostic report, the patient or his physician only needs to retrieve this information from the database rather than looking for multiple identifiable documents. Health data is highly sensitive, and the biggest challenge is to safely secure and access EMRs in modern EMR systems. As most EMRs are deployed in the cloud, they are easily exposed to potential

 

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

threats and are vulnerable to leaks, loss and theft.[4] To prevent EMRs from unauthorized access, the standard solution is to perform encryption before uploading to the cloud.

General information is maintained in the form of files access is controlled by its device OS. But this restriction can be Pass through when the attacker receives a physical entry into the empty storage. Physical access to the file system is possible when removing the storage device and inserting it into another computer just by logging in, or simply bypassing the app from a variable source such as CD, pen drive having OS.[7]

Specifically, the EMR owner encrypts the EMR using the measurement key, and only authorized medical personnel are authorized to access and delete it. However, data sharing has not changed in this case. Two potential problems are to handle complex keys and duplicate encryption[2]: as patients often do not know who is allowed to access their EMRs, they encrypt multiple pieces with different session keys and distribute the keys of various members of the medical staff.

The cryptographic system is said to be safe if the ciphertext does not have enough information to get the same cryptography. In fact, one can generate an immortalized zipher by assigning a random key to each of the mathematical intangible data. Since various random bits or buttons will fail to result in any duplicate patterns.[8]

The approach to accessing users' data needs to be flexible enough to address changes in users' roles[3]. Several schemes adopting attribute-based encryption (ABE) have been presented for fine-grained access contro[1],[10]. Users with attributes satisfying the access policy can decapsulate the EMR data. In addition, some advanced mechanisms, consisting of a multi-authority model in an outsourcing system[5] and a view-based access control[6] that allows patients to specify a list of authorized/unauthorized users, have recently been proposed. Role-based access control schemes (RBACs)[12] also allow fine-grained access control. They define a role-based policy for a hierarchical organization with identity-based broadcast encryption (HIBBE). While the above proposals achieve data confidentiality in the EMR system, privacy preservation for patients is still an unresolved issue.

## II.BACKGROUND WORK

Access control is widely adopted in the EMR system to protect patients' health data. Access control policies are defined by specific pieces of legislation, e.g., health insurance coverage and accountability action (HIPAA) electronic documents , and company rules or regulations. The law regulates who can enter and how EMRs are stored. Two solutions are often used to support flexible access control. One solution is to use an encrypted attribute. Since attributes can be used to define user rights, data owners determine access policies. One solution is to use role-based access control schemes, in which an individual's identity defines a role and another is allowed access permission if his role is a defined policy. However, there is some uncertainty regarding the privacy of EMR owners. Anonymity strategies can be used to ensure the privacy of users.

There are many cryptographic systems that use complex operations including substitution and permissions to produce incompatible kophertext, even if the security level of these cryptosystems is correct, there should be a transaction between security level and operating costs and the increasing physical and mobile infrastructure[9].

In practice, the unmet challenge to real-world distribution remains: healthcare organizations are often organized in the past, and data is shared among multiple users. In previous work, we have identified anonymous controls based on the role of a variety of organizations with a limited security level, where an attacker must issue a targeted identity before interacting with the EMR program. This scheme is represented as RBACAnony in this paper. We are also proposing to add a new system to the current work, defined as RBACAnony-F, in which an attacker releases the intended authorization power after interacting with the EMR program.

## III.PROPOSED METHOD

We describe the general healthcare network in Fig. 1. It includes three components: the TKA-based rating authority (TKA), the patient and the medical staff. TKA is faithful to the system and is responsible for generating and distributing program parameters, rooting master key, and authorizing senior medical staff and patients. The patient is identified by his or her name or identity. The patient and his or her medical staff are responsible for the EMR.

 

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

A senior medical practitioner transfers rights to his subordinates, forming a tree-like organization. Each worker is identified by a role graphic designer composed of charged atomic roles. For example, the role of the pulling-in physician, with the atomic order roles "chief physician, associate physician, center physician", is under the control of a colleague, whose atomic roles are "primary physician, associate physician". Assign a general practitioner, associate physician and internal physician to the same policy for a particular patient. Each user may be able to enter a patient's EMR, but only their role that satisfies the defined access policy or the patient itself can disassemble it. We hide all identity-related information in the system so that opponents can access patients' personal information. Enemies include dishonest internal workers and malicious external attackers.

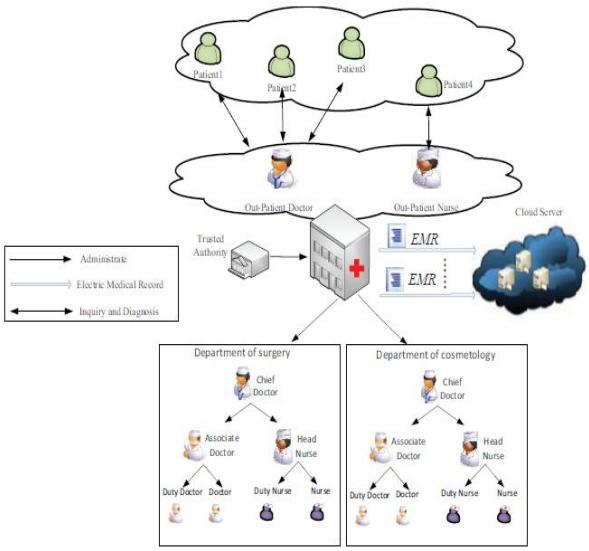


**Fig. 1:** System architecture

We show how to achieve RBACAnony-F completely anonymous rights management. We use an anonymous HIBE concept in our RBAC. The user first selects an access policy, which can be considered as a broadcast group with all permissions. You only need to wrap the EMR once and allow the different medical staff to shrink if their identity belongs to the broadcast team. Note that the function is also defined for an anonymous HIBBE program. The main difference lies in the fact that patients are privately identified in our scheme, while being allowed access to their EMRs. Therefore, we consider patients' identity in addition to an access policy when designing a distribution algorithm.

## IV. RESULTS AND DISCUSSIONS

As shown in Fig.2 the home page which consists of modules like cloud server, service provider, users(department), and trusted authority.


 

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

Fig. 2 .Home page

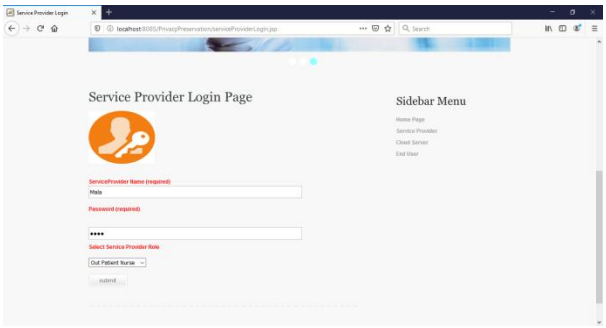


Fig .3 login page of service provider

Fig 3. shows the login page if the service provider is new then “click” on the new register to upload the service provider details or if the service provider is already has registered then they can login to the page by using service provider name and the password .and they perform the operations like updating the patient details, view end user transactions etc.

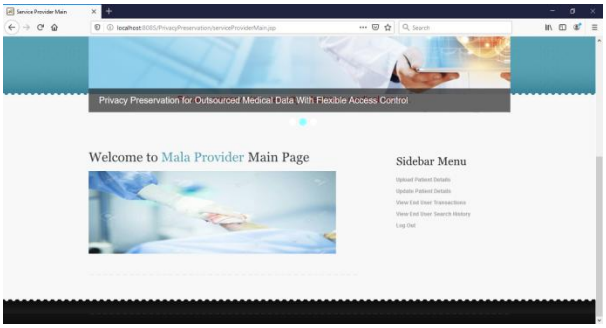


Fig.4 provider main page

In Fig 4. the data owner performs operations such as Upload Patient Details, Update Patient Details, View End User Transactions, View End User Search History

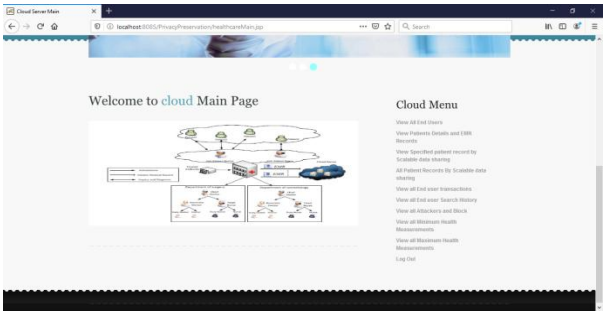


Fig.5 cloud server

 

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

In Fig 5.The Cloud Server manages a server to provide data storage service and can also do the following operations such as View All End Users , View Patients Details and EMR Records, View Specified patient record by Scalable data sharing, All Patient Records By Scalable data sharing , View all End user transactions, View all End user Search History, View all Attackers and Block, View all Minimum Health Measurements, View all Maximum Health Measurements

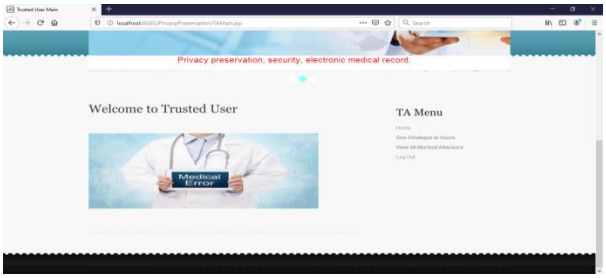


Fig. 6 Trusted users

As shown in Fig 6. In this module, the sector can do following operations such as Give Privileges to Users, View All Blocked Attackers

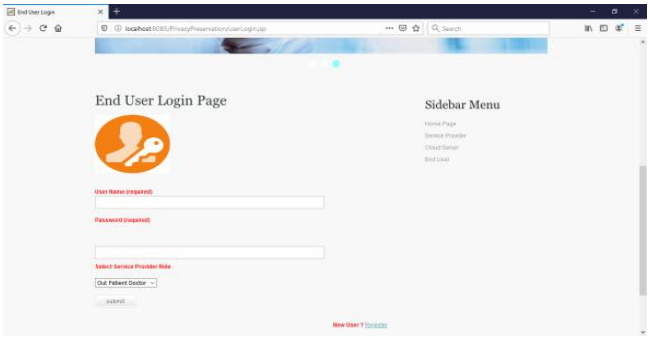


Fig.7 end users login page

In Fig7. In this module, he logs in by using his/her user name and password. After Login receiver will perform operations like View My Profile, Request Permission, Request Response Details, Searches files based on Patient, My Search History, My Transaction

## V.CONCLUSION

In this paper, we propose two anonymous RBAC techniques for the EMR system. We have access to flexible access control such that EMR data can be standardized according to the on demand policy, only users who have their own access policy roles are able to distribute it. Patients' privacy is maintained using a bilinear group, where all information related to the identity is hidden in the subgroup. Based on the estimates of the selected bilinear group, we prove that our proposed models have a place for semantic security and anonymity.

 

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

## REFERENCES

1. 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.

2. J. Huang, M. Sharaf, and C. T. Huang, "A hierarchical framework for secure and scalable 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. M. J. Atallah, M. Blanton, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, 2009
5. 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.
6. Rajasekar, P., and H. Mangalam. "Design and implementation of low power multistage AES S box." International Journal of Applied engineering Research 10 (2015): 40535-40540.

7. P Penchalaiah, M Vijay Kumar etl, "A Research Threshold Efficient Hybrid Encryption Schema for Secure File System", International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, (Volume-8, Issue-2S3, Page 888 – 891,July 2019
8. Penchalaiah P, Ramesh Reddy K, "Random Multiple Key Streams for Encryption with Added CBC Mode of Operation*", Perspectives in Science (ISSN: 2213-0209),* Volume 8, pp.57-62, April 2016.
9. Penchalaiah P, Ramesh Reddy K, "Secure and Cost Effective Cryptosystem Design on Random Multiple Key Streams", *Journal of Information Security Research,(* ISSN: 0976-4143) *DIRF Publisher,* Volume 7, Number 1, pp. 29-40, March 2016.
10. S. Narayan and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in CCSW'10. ACM, 2010, pp. 47–52
11. M.Geetha Bhargava, M.Srinivasa Reddy, Shaik Shahbaz, P. Venkateswara Rao , V.Sucharita "Potential of Big Data Analytics in Bio-Medical and Health Care Arena: An Exploratory Study", Global Journal of Computer Science and Technology: CSoftware & Data Engineering Volume 17 Issue 2 Version 1.0 Year 2017 Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
12. W. Liu, X. Liu, J. Liu, Q. Wu, J. Zhan, and Y. Li, "Auiting and revocation enabled role-based access contrl over outsourced private ehrs," in HPCC 2015. IEEE, 2015, pp. 336–341.
13. M. Sicuranza, A. Esposito, and M. Ciampi, "A view-based acces control model for EHR systems," in IDC 2014. Springer, 2014, pp. 443–452.

 