# Ensuring Privacy of EHR system using access control mechanism in Public Cloud

[1]O.Kiran Kumar,[2]J.Raja Ratnam,[3]V.Raghavendra Kumar,[4]P.Hari Krishna Reddy
Assistant Professor, St. Joseph's Degree College, Kurnool

***Abstract:*** **-**Huge volume of continuity generated data or record sharing at will have constrained most of the physicians to approve EHR (Electronic Health Record) for record-keeping of patients. It also makes convenient to the other stake holders of healthcare ecosystem such as nurses, specialists and patient. Due to lower costs and scalability of application, the cloud is becoming the infrastructure for most of the EHR but without comprising the privacy of data. In this paper we have proposed Secure Access Control Mechanism for Ensuring Privacy of EHR in Public Cloud In this case, cloud computing helps users to effectively manage health information, increase storage capacity, and secure access to information through access control systems. Access control to protect patient data in health information systems is a primary security barrier. Access control ensures that content is available to content owners. With the help of an access control mechanism supported by authentication, patient privacy can be achieved in health information systems.

***Keywords***—Public Cloud, Security, Electronic Health Records, Role based Access Control

## 1. INTRODUCTION

Security and privacy protection of patient's records in the cloud-based healthcare system. It is a unconditional importance and involves various requirements. First, the creation and maintenance of cloud-based healthcare e-records of any type should preserve content authenticity, integrity and privacy. Next, all healthcare data should be guarded in secure storage with protective access mechanisms and secure transmissions. The PHR empowers patients to deal with their medical records; previously putting away the reports on the server they can utilize appropriate access control instruments which guarantee the patient's full control over their PHRs. The PHRs may contain diverse sorts of information seeing sensitivity, for example, very sensitive, confidential, and typical information. PHRs might be sensitive by thinking about the person's situation in the workplace or society, and it might be case sensitive in term of malady and test. However, there are some PHRs, which can be dealt with as standard and can be presented to the specialists, pharmaceutical organizations, understudies for the examination and instructive purposes. By considering the person and case we arrange the information in various sensitivity levels and feel to provide security as per these levels.

If we need to secure the information we have to provide security to the data utilizing diverse security systems, for example, advanced mark, encryption, get to control and so forth. The purpose of the characterization is, we need to provide security by considering the sensitivity levels of the information, and this prompts the execution upgrade of the framework.


Figure 1. Health Information flow

The EHR, also called the electronic medical record, refers to a structure in digital format of patients' health data that is maintained throughout their life and is stored accurately in a repository [2]. Health care providers use EHRs, whose data can vary greatly and can include vital signs (such as body temperature, pulse, respiration, and blood pressure), age, weight, medications, allergies, medical examination results, and radiology images that are used to diagnose conditions [2,4]. The EHR is used to support health care professionals and health organizations (eg, hospitals, laboratories, or clinics) for the improved management of patient health data. However, these health records are usually not stored with the same structure in different health organizations. These factors hinder the interoperability of health information among hospitals, clinics, and laboratories. To address some of these problems, the PHR concept was proposed in 2006 [4] and was defined as an ISO (International Organization for Standardization) standard (ISO/TR 14292) in 2012 [10].

## 2. RELATED WORK

The Szolovits et. al. in 1994 introduced the concept of patient-centered health record to be stored in web based system. For sharing and authentication, Hu et al. (2010)presented the use of public key infrastructure (PKI) in order to maintain the confidentiality of the health records. A similar work has also been presented in Yu and Chekhanovskiy (2007). In order to provide the security and privacy of EHR, cryptographic key management has been discussed in Lee and Lee (2008). In particular, hierarchical identity-based encryption and privacy preserving EHR system based on cloud is used in Benaloh et al. (2009). The trade-off between real time performance and security levels has been considered in Takabi et al. (2010) for cloud based EHR systems.

The trust is one of the main concerns of the users Shen et al. (2010) and it requires the complexity of the security mechanism be at a minimum so that it will not be difficult for the users to use the system. The various vulnerabilities have been examined in Li et al. (2010). To analyze the risk in third party clouds, Popovic and Hocenski (2010)discuss challenges, security issues and requirements that Cloud Service Providers (CSP) face during cloud engineering. Few critical concerns of Cloud computing have been identified by Xiao and Xiao in Xiao and Xiao, 2013. The requirements for achieving privacy and security for data sharing in cloud have been discussed by Chen and Zhao (2012).

A survey focusing on how privacy laws should also take into consideration Cloud computing and to prevent security and privacy breaches of one's personal data in the Cloud what work can be done is provided by Zhou et al. (2010). Factors affecting management of information security in Cloud computing has been explored by Wang et al. (2011). To understand the dynamics of information security in the Cloud the necessary security needs for enterprises are explained by it. Among enterprises through pilot testing privacy/security compliance a study on privacy and security compliance of Software-As-A-Service (SaaS) is carried out by Wang (2011). To determine the user experience of Cloud computing a survey is carried out on a number of users by Oza et al. (2010) and found that the trust and how to choose between different Cloud Service Providers was the main issue of all users.

In most of the existing methods, the security has been considered at data level without considering the data networking and data storage separately. This gives the two hackers two places where data can be hacked comprising security and privacy of EHR. To overcome this problem, we considered double encryption system, separately for data communication and data storage. Doing so, even if at all data are hacked while data in communication channel, theft doesn't get propagated to cloud.

## 3. PROPOSED FRAMEWORK

A secure framework for patient-centric information with a suite of security mechanisms for data access control to EHRs has been proposed in this section.

### 3.1 EHR System Architecture

One of the templates of the integrated health care system has been considered here to give an example of EHR, where cryptography can be used to secure the access of data stored in the cloud. The proposed architecture with hierarchy and cloud connectivity of the EHR network is shown in Fig. 2

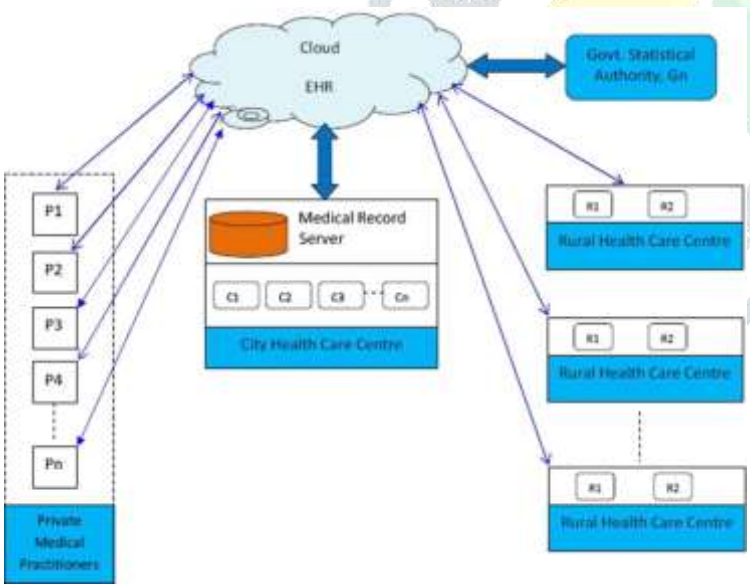


Figure 2. Source from the EHR access network on cloud in Indian context.

The health care services are divided as city health care centers, Health Service Centers, and Rural Health Service Centers. As compared to City health services, rural health services will be very basic and less advanced. The treatment with specialized health services in physician and equipment point of view will not be available in most parts of the rural area. Rural health care units and Private medical practitioners are directly connected to the cloud-EHR. City health service center will have its own server and thus, any

member of cloud-EHR from the city health center will access the data from cloud via medical server. The need of having medical server is that the city health center will have normally many health departments and medical and nursing college co-located with it. Thus, access management to the staff members or students of city health care center will put extra burden on the cloud management. In order to avoid this burden, access control in city health care center can be isolated using dedicated server. The multiple level of access management associated with hierarchical member entities can be an approach to achieve the key management for medical server. Thus, most of the requests from members of city health care will be verified and authorized for particular operations at server level and only after validating request positively; it will be forwarded to the cloud-EHR. The essential set of primitives, namely, encryption and decryption, while writing and reading the data.

### 3.2 Secure Key Access Management System

The patient chooses to give the authority to one physician to access his/her medical record on the cloud any time. This is done by pairing the secret keys of both into the key access management scheme. This is expected to be done at the time registration of patient. Pairing is static and stored in key access management.

### 3.3 Attribute Based Access Policy:

When there is patient data is accessible by the doctors, lab Technician, Nurse and some other Researchers for data analyses, then system should provide access policy to restrict from the unauthorized access control mechanism. In this connection system should construct role based access policies i.e Doctors, Physician, Nurse, Scientist, along with read and write operations.

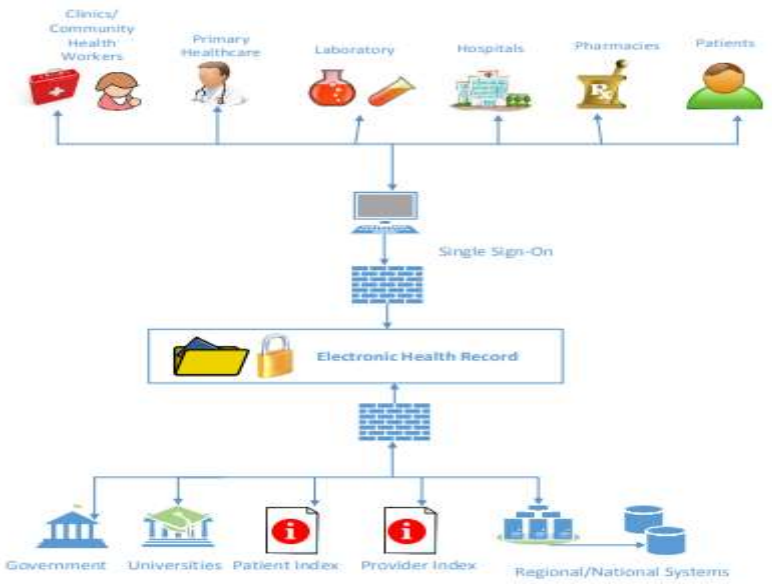


Figure 3. HER network system.

This basic architecture can be implemented for a single entity such as a hospital, doctor's office, or clinic to produce an Electronic Health Record that could be then shared in a national/regional Public Health System. Use of extensible markup language (XML) and resource description framework (RDF) standards are the current choice of consolidating World Wide Web technology and data structuring in attempting to enforce global Internet standards. This will allow clinical ontology's better querying and information transmission, considering clinical information technology is still not yet refined or a top priority among the medical profession.

### 3.4 Access control

Access Control has been described as "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner" . Access Control can allow not only a person admittance to secure data, but also the type of access granted as well. Access control comes in three major favors – Administrative, Logical, and Physical. Administrative deals with policies and procedures intended to administer rules for security.

**Types of Access Control**

In the world of security models for Access Control there are typically types of traditional policies and some new models and types. Access control mechanisms can be grouped into four main classes: discretionary, mandatory, role-based and attribute based. [1] An access control scheme outlines rubrics for users retrieving data, profiles or information.

**Discretionary Access Control (DAC)**

DAC is based on the characteristics of users and/or links to defined groups. Right of entry is normally based on the authentication approved 13 to the user based on the classifications they presented at the time of validation and the identity of the control to elect whether to authorize or decline an request for access.

**Role based Access Control**

Role-Based Access Control access to data is based on a user's roles and position within an organization or company. Role-based access control (RBAC) is a framework for controlling user access to resources based on roles and it can significantly reduce the cost of access control policy administration and is increasingly widely used in large organizations. An example for the Electronic Health Record would be the roles of users that may include nurse, doctor, patient, and administrative clerk. These users necessitate separate levels of access in order to carry out their duties[12]. RBAC structure should provide application security administrators with the knowledge to detect who can perform what tasks, when, from what area, and in what order of sequence. RBAC has five major elements. The user or the person trying to gain access, role that configures what permissions the user has, the permissions themselves that grant access to objects, operations such as read, write, update and delete, and finally the objects which are the data or information that are needed to be accessed. The following attributes can be found for a RBAC model:

## 4 SECURITY REQUIREMENTS

In the following, we introduce four characteristics of the main security requirements in the EHR cloud system.

**Data Confidentiality:** When electronic health record of data owner stores in the cloud, it couldn't be arbitrarily consulted if someone doesn't own private key and possess patients' authorization. Thus, the EHR has to be encrypted before uploading to the cloud server. Owing to encrypt data though patients' attribute, only someone obtains the private key that has been authorized[13].

**Authenticity:** Data owner reserves their information in the EHR system, which implements varieties of operation in the third cloud platform. Patients don't permit their valuable and sensitive record to be compromised and distorted by malicious attackers. Hence, the cloud server has to guarantee the authenticity of data for data provider. Similarity, we can ensure the authenticity of data for verifying the information and

improving access control in especial scheme, such as, respectively. For another approach, the user accesses data used to study or treat other patients. If the patient's EHR is not reliable, this will be big hidden dangers.

**Privacy protection for patients:** The number of access control population should be confined by the purpose of the visitor. According to the user's attribute differences, he has different access permissions. For instance, doctor, nurse and researcher, they have possession of authority to access data based on their usage purpose in the EHR system[14].

**Revocation:** If a user wants to revoke his attribute, after that immediately the user will not be available to access EHR using that attribute, known as attribute revocation. There is another situation user's can no longer use corresponding private key

## 5 CONCLUSIONS

Securing EHR system is prim concern in public cloud while storing and sharing among the network. In this paper we proposed secure access control mechanism with degree of security such that privacy of patients cannot be compromised. Moreover we proposed four characteristics of the main security requirements in the EHR cloud system.

## 6 REFERENCES

1. Benaloh, Josh, Chase, Melissa, Horvitz, Eric, Lauter, Kristin, 2009. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security. ACM, pp. 103–114.
2. Butler, Declan, 2007. Data sharing threatens privacy. Nat. News 449 (7163), 644–645. Chen, Deyan, Zhao, Hong, 2012. Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1. IEEE, pp. 647–651.
3. Domingo-Ferrer, Josep, 2002. A provably secure additive and multiplicative privacy homomorphism. In: Proc. 5th International Conference on Information Security. Feldman, Lindsay, Patel, Deesha, Ortmann, Leonard, Robinson, Kara, Popovic, Tanja, 2012. Educating for the future: another important benefit of data sharing. Lancet 379 (9829), 1877–1878.
4. Geoghegan, S., 2012. The latest on data sharing and secure cloud computing. Law Order, 24–26. Hu, Jiankun, Chen, Hsiao-Hwa, Hou, Ting-Wei, 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Comput. Stand. Interfaces 32 (5), 274–280.
5. Hu, Haibo, Xu, Jianliang, Ren, Chushi, Choi, Byron, 2011. Processing private queries over untrusted data cloud through privacy homomorphism. In: 2011 IEEE 27th International Conference on Data Engineering (ICDE), pp. 601–612.
6. Lee, Wei-Bin, Lee, Chien-Ding, 2008. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans. Inf. Technol. Biomed. 12 (1), 34–41.
7. Li, Huan-Chung, Liang, Po-Huei, Yang, Jiann-Min, Chen, ShiangJiun, 2010. Analysis on cloud-based security vulnerability assessment. In: 2010 IEEE 7th International Conference on e-Business Engineering (ICEBE). IEEE, pp. 490–494.
8. Mitchley, M., 2006. Data sharing: progress or not. Credit Manage., 10–11
9. Oza, Nilay, Karppinen, Kaarina, Savola, Reijo, 2010. User experience and security in the cloud – An empirical study in the finnish cloud consortium. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, pp. 621–628.
10. Popovic, Kresimir, Hocenski, Zeljko, 2010. Cloud computing security issues and challenges. In: MIPRO, 2010 Proceedings of the 33rd International Convention. IEEE, pp. 344–349.

11. K.Samunnisa, Bhavsingh Maloth," Privacy-Preserving Scalar Product Computation over Personal Health Records". International Journal of Computer Engineering In Research Trends, Volume 3, Issue 2, February-2016, pp. 42-27.
12. Allam Jyothi,G.Somasekhar and Dr S.Prem Kumar," A Secure Multi-Owner Data Sharing Scheme for Dynamic Group in Public Cloud." International Journal of Computer Engineering in Research Trends., vol.2, no.8, pp. 475-480, 2015.
13. A.Shekinah Prema Sunaina," Study on Competent and Revocable Data Access Control Scheme for MultiAuthority Cloud Storage Systems." International Journal of Computer Engineering in Research Trends., vol.2, no.5, pp. 365-368, 2015.
14. R.Srinivas and Ajay Kumar," Attribute-Based Encryption for Reliable and Secure Sharing of PHR in Cloud Computing." International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 679- 682, 2015.