International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 455~466
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp455-466

Security framework for cloud based Electronic Health Record (EHR) system

Raghavendra Ganiga[1], Radhika M. Pai[2], Manohara Pai M. M.[3], Rajesh Kumar Sinha[4]
[1,2,3]Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education (MAHE), India
[4]Department of Health Information Management, Manipal College of Health Professions, Manipal Academy of Higher Education (MAHE), India

Article Info

Article history:

Received Mar 9, 2019
Revised Jul 24, 2019
Accepted Aug 29, 2019

Keywords:

Electronic health records
Healthcare
Risk
Security framework
Threat modeling

ABSTRACT

Health records are an integral aspect of any Hospital Management System. With newer innovations in technology, there has been a shift in the way of recording health information. Medical records which used to be managed using various paper charts have now become easier to organize and maintain, thereby increasing the efficiency of medical staff. The Electronic Health Records (EHR) System is becoming a high-tech medical management technology developed for the economic or emerging economic countries like India. In a national health system, the EHR integrates the Electronic Medical Records (EMR) in all collaborating hospitals through different networks. EHR gives healthcare professionals a way to share and manage patient data quickly and effectively. Due to the mass storage of confidential patient data, healthcare organizations are considered as one of the most targeted sectors by intruders. This paper proposes a security framework for EHR system, which takes into consideration the integrity, availability, and confidentiality of health records. The threats posed to the EHR system are modeled by STRIDE modeling tool, and the amount of risk is calculated using DREAD. The paper also suggests the security mechanism and countermeasures based on security standards, which can be utilized in an EHR environment. The paper shows that the utilization of the proposed methods effectively addresses security concerns such as breach of sensitive medical information.

Corresponding Author:

Radhika M. Pai,
Department of Information & Communication Technology,
Manipal Institute of Technology, Manipal Academy of Higher Education,
Madhav Nagar, Manipal 576104, Karnataka, India.
Email: radhika.pai@manipal.edu

1. INTRODUCTION

Healthcare system of India is one of the largest and most complex in terms of providing quality services to the population. Approximately 1.26 billion people across a wide range of geographic and socioeconomic settings are getting benefitted with the services offered from competent healthcare professionals. The system involves a complex network of public and private service providers, ranging from a single doctor in rural healthcare centers to specialized tertiary care institutions [1]. Indian healthcare system is a three-tier system, i.e., Primary Health Care (PHC), Secondary Health Care (SHC), and Tertiary Health Care (THC) [2]. These institutions are functioning under the aegis of the Central and State Government. The private sector institutions, along with the public sector, equally participate in the provision of quality services to the needy population [3]. The primary health centers are the first point of contact between a healthcare institution and community. Hence, the focus is more towards maternal, and child healthcare services for the rural community, whereas secondary and tertiary care institution services are more open to

the urban population. The secondary and tertiary care center also acts as a referral institution for primary health centers. When the patient gets referred from primary to secondary or tertiary care centers, it is always expected that the referral center should accept the case and provide quality services. But, to provide such services, the healthcare professionals expect the instant availability of the patient's complete information, as it allows them to understand the case and achieve the quality outcome. This study is an attempt to integrate the three level of the healthcare system through a secure cloud-based EHR system.

The paper-based medical records is a conventional approach in maintaining health information of the patient in chronological order [4]. In this traditional approach, the patient records are housed in a clinical record room under lock and key. In India, the primary health centers follow the conventional method in maintaining patient information on paper due to the lack of resources and qualified workforce [5, 6]. The secondary health centers maintain a hybrid record, a combination of both paper-based and electronic medical record. Some of the tertiary health centers have moved from the paper-based medical records to the electronic repository, which connects different departments of tertiary health centers to a centralized warehouse. This electronic repository allows healthcare professionals to access the patient information irrespective of geographical boundaries. This system assists the healthcare professionals in receiving and sending patient information in real-time and also controlling the flow of information at the point of care.

There are several digital health initiatives taken by Government of India as a part of 'Digital India movement' where the healthcare applications are developed to streamline the process of health information system and to maintain the patient data in a digital form [7]. Presently, the healthcare centers are equipped with Electronic Medical Records (EMR), but it only limited to a few institutions. The EMR does not support the healthcare professionals at the referral level to get patient data as it is only maintained, and access is limited to the facility level it is maintained. This limitation calls for an Electronic Health Record (EHR) system. EHR plays a vital role to enable physicians and other healthcare professionals to access the patient's data anytime and anywhere irrespective of geographical region. To provide such accessibility of patient data in real-time, without any restriction, it is always suggested that the healthcare institutions incorporate cloud-based approach during the implementation of EHR across all the level of the healthcare system.

Cloud-based EHR system helps the healthcare professionals and providers in sharing patient information at all levels of the healthcare system. Cloud is useful to the healthcare ecosystem by connecting healthcare centers with laboratory, pharmacy, medical billing, etc. [8]. Based on the assessment of the present healthcare system of India, a cloud-enabled architecture is developed, including the features for sharing patient data without any restriction across multiple geographical location as shown in Figure 1. This EHR consists of a global database to store the health data available in the form of text, image, and videos from the healthcare facility at all level of the present healthcare system. The provision of services at all the levels of the healthcare system for a single patient through an EHR is also a security concern, as the data moves across the network. The challenges in maintaining data security are due to the large population size across the wide geographical landscape and lack of IT infrastructure in the country.

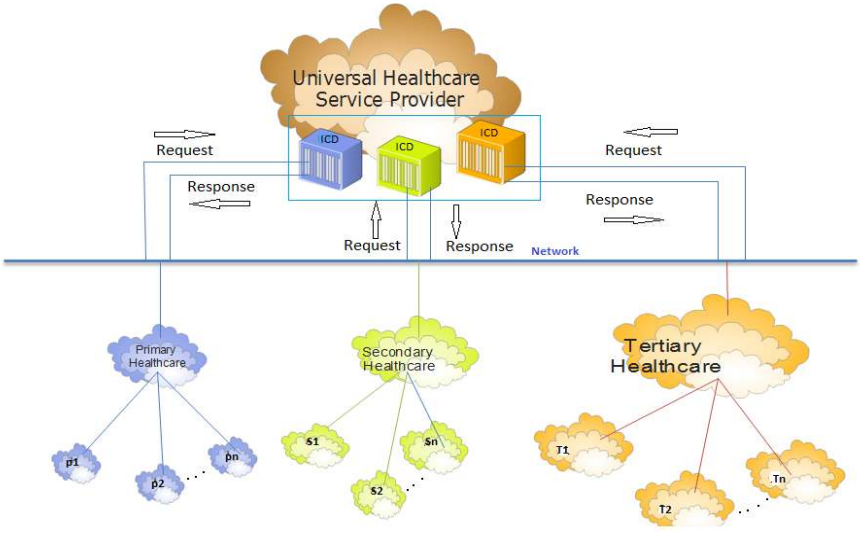

Figure 1. Cloud-based architecture for EHR System

There are few guidelines suggested under the Health Insurance Portability and Accountability Act (HIPAA), 1996 to protect the patient data that are available and maintained using Electronic Health Record.

To make the healthcare system to run smoothly, HIPAA has suggested a set of valuable security and privacy guidelines within the purview of federal law [9-11]. The essential guidelines related to privacy, confidentiality, and security are presented in Table 1.

Table 1. Security and privacy requirement as recommended by HIPAA

Requirement	Description
Patient's understanding	This indicates that patients have the right to know about their sensitive and private personal health information are recorded and used by healthcare provider.
Patient's control	The control permits patients to given permission about their own record with the access policy.
Confidentiality	Confidentiality of the patient information should be maintained and kept away from unauthorized access.
Data integrity	The data integrity ensures that shared or stored information should be a true representation of original information without any form of alteration or modification.
Consent Exception	Patient's health information can be accessed only during emergency cases without his consent.
Non-repudiation	All the patients' health information recorded and stored with supported evidence to avoid dispute or distrust.
Auditing	The health data of the patient should be monitored all the time to ensure the data on transit and rest both are secure and protected.

The aim of the hospital health information system is to maintain patient data in a secure manner, considering the privacy rights of the patient and their caregivers. When the records are maintained electronically using EHR, where it has to be shared among multiple healthcare providers at a different level of the healthcare system, chances of the breach in privacy and confidentiality of patient data becomes more, which creates a threat for a healthcare institution. As the medical records contain sensitive information about the patient, the breach in privacy and confidentiality lead to defamation, discrimination, and stressful conditions to the patient and caregivers. The privacy and confidentiality of the medical records can be ensured by providing authorized access to the Electronic Health Record of the patient. Providing integrity of Electronic Health Records is essential because records are more prone to destruction or modification by an unauthorized intruder. Due to the sensitive nature of the information contained in Electronic Health Records, the need for advanced security safeguard techniques has been prompted, to put these worries at ease. This paper deals with the architecture of a security framework tool to build a secure, dynamic, and dependable EHR system.

This section describes the current research work in the area of EHR and various aspects of security. Clemens Scott Kruse *et al* [12] have given descriptive investigation on security of Electronic Health Records and its limitations. They have mentioned about the specific security methods and techniques to protect the sensitive nature of the health care system. The method and techniques are categorized as Administrative, Physical, and Technical safeguard. In addition, authors have suggested the need for advanced security technique for a sensitive EHR system. In their study, the authors failed to specify facility specific security technique which is required for the future healthcare organization.

Amer K [13] presented a conceptual framework which illustrates the complex issues in the healthcare information system. The security concept used for the current healthcare system is variable in nature because different hospitals follow different set of standards. The main goal of the framework is the safe and ethical use of Electronic Medical Records in all levels of healthcare system.

Choi, Young B., *et al*. [14] have assessed the security challenges associated with the health information based on HIPAA and security rule. They have done a detailed study on various techniques of creating, receiving, maintaining, or transmitting health information in the modern healthcare system and suggested all healthcare organizations to comply with HIPAA security rule and regulations to secure the data.

Almulhem *et al* [15] proposed client server model of healthcare system to analyze the attacks inside the healthcare organization. In their study attack tree tools are used to analyze the attack which affect the healthcare system. Authors also performed qualitative and quantitative analysis for security countermeasures which greatly reduces the attack on the system.

Fernandez Aleman *et al* [16] mainly focuses on privacy and security issues in healthcare data when it is in transit. Healthcare data is prone to attack when sharing outside the hospital premises. Authors suggested the use of the following standards and regulations. The regulations such as HIPAA and European Data Protection Directive 95/46/EC for protecting the health-care data is defined. Additionally, authors suggested the use of a symmetric key, asymmetric key, digital signature, role-based access, and audit log for preventing unauthorized access of the EHR system.

Ardagna, Claudio A., *et al*. [17] have proposed an access control solution which aims to regulate the "break-the-glass" exemptions that efficiently arise in all levels of healthcare systems. Break-the-glass is an approach by which a person can gain access to certain restricted data during emergencies. However, this allows malicious users to gain access to the privileged information by manipulating the security

principle. The main aim is to introduce policy spaces, a language, and a composition algebra solution to control the possible breaches in the patient's privacy.

Anitha K *et al* [18] have proposed a Data storage Lock algorithm to maintain confidentiality of patient data when it moves to cloud storage. They use private key (pk) cryptographic standard to gain access to the storage resources. All the cryptographic keys and index tables are maintained and managed by the cloud service provider and patient data gets accessed only by authorized users with assigned private key.

Jieun Eom *et al*. [19] mainly focuses on patient controlled attribute-based encryption, in which patient (data owner) has complete control over the health record. In their method, patient has complete rights to give access to any healthcare professional. The model enables the patients to control access to their health data stored in the database. When a patient moves to another hospital, sharing data becomes easy and eliminates redundant work. Additionally, the authors have also implemented services during emergency situation, where patient health data is available to the doctor with special permission.

2. THE PROPOSED SYSTEM

The security of EHR system is the main concern in all levels of healthcare system. In this paper a security framework for cloud based EHR system is proposed. The threats posed to the EHR system are modeled by STRIDE modeling tool, and the amount of risk is calculated using DREAD. Various attacks and vulnerability have been identified and mitigation techniques have been discussed.

2.1. Security framework

The proposed security framework for EHR system is based on threat modeling and is depicted in Figure 2. The proposed system protects the health information created, stored, and maintained in the cloud-based EHR database. It provides structured security process for the healthcare application developers and enables them to evaluate security threats and identify appropriate counter-measures. The framework also incorporates security rules such as administrative, physical, and technical safeguards which ensure confidentiality, integrity, and security of the EHR system. Different components of the security framework for an EHR system are discussed in the following sections.

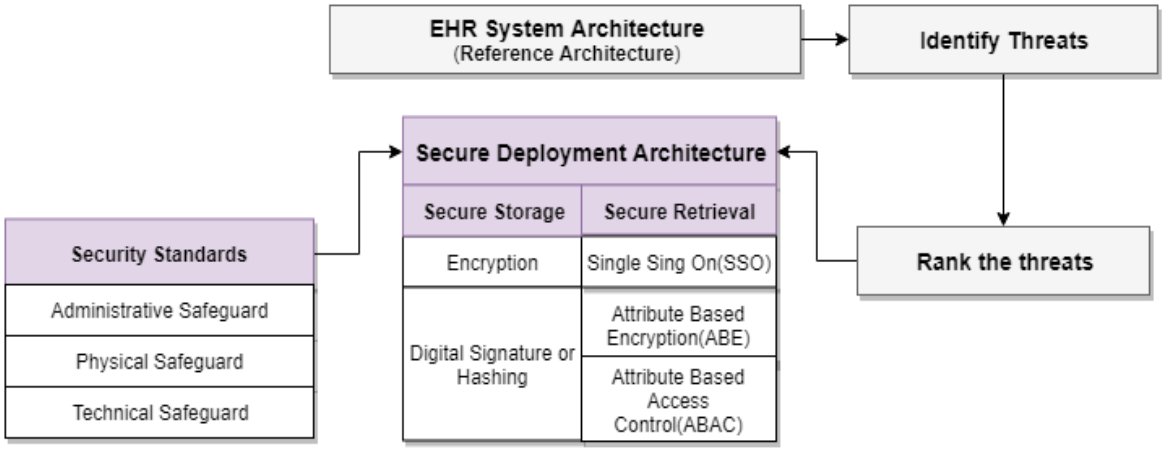

Figure 2. Proposed Security Framework for EHR system

2.1.1. EHR system architecture

Electronic Health Record (EHR) has the potential to provide real-time data of the patient and the population by connecting all the levels of the public health system, irrespective of their geographical boundaries. The security of the EHR is the major concern when sharing health information at various healthcare levels. Figure 3 shows the architecture of the EHR system, which is the reference architecture for identifying threats in the system.

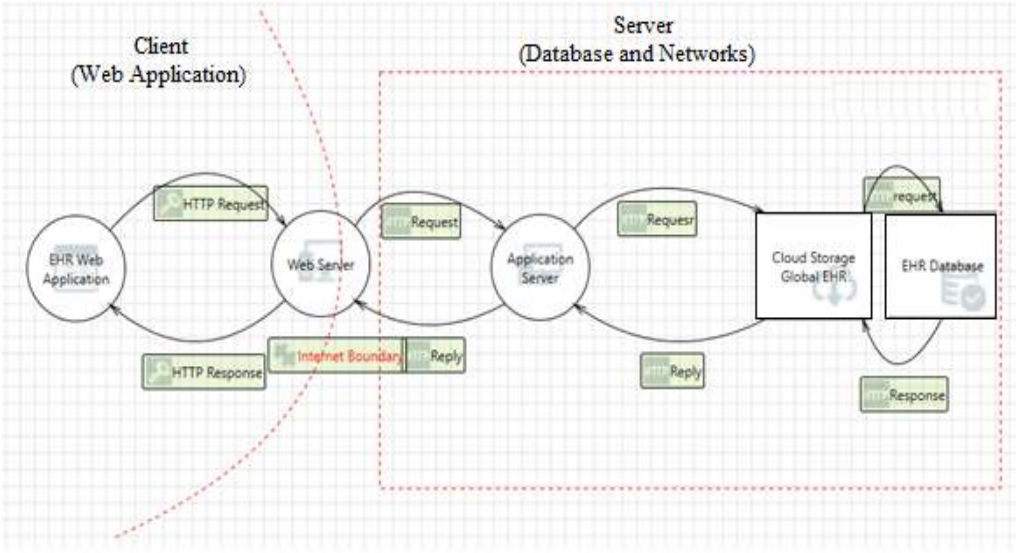

Figure 3. EHR System architecture

The architecture follows three-tier model, which is divided into three major parts such as client (Web application), Server (Applications and Database), and networks. The first visible part of an EHR system is the client. It plays a key role for viewing, entering and modifying health information. This component is thus expected to be attacked the most. The second most visible part of the system is the server. The compromising server gives complete control to the attacker. The server attacks include exposing, altering and/or destroying health information which completely damages the system. A compromise in the network results in eavesdropping, altering and more when data is in transit mode. The attacker's main goal is to target the visible component of the system including client, server, and networks. Compromising any one of them result in compromising the entire system.

2.1.2. Identifying threats

The Threat Modeling Tool [20] is used by software architects to identify and mitigate potential security issues. It is a core component of the Microsoft Security Development Lifecycle (SDLC). It provides cost-effective way of developing a system with the minimum number of security errors. Threat modeling(TM) is the process that improves application and network security by identifying and rating the potential threats and vulnerabilities in the EHR system. TM is especially important during the design phase. TM allows experts to determine the possible threats that could affect the system. The reference architecture designed for EHR system is given as input to the threat model to identify threats. Identifying threats helps to develop meaningful security model for cloud-based EHR. Threats exist due to weaknesses in design, implementation or configuration. These threats are identified by a systematic review of the system and identifying the intruder access points to eliminate the threats. The Microsoft STRIDE model is used to identify security threats in the proposed EHR system. The possible threat category list for the EHR system is shown in Table 2.

Table 2. STRIDE model threat category list for the EHR system

Sl.No	Threat Category	Description
1	Spoofing(S)	With other user identities, the attacker successfully impersonates the account in the EHR system
2	Tampering(T)	Performing improper alteration in the EHR record
3	Repudiation(R)	Users who repudiate performing an action without having any way to prove
4	Information Disclosure(I)	Sensitive patient information is exposed.
5	Denial Of Service(D)	The required resources are inaccessible to its intended users of the EHR system.
6	Elevation Of Privilege (E)	Attacker gets additional permission to access the content of EHR system

2.1.3. Threat ranking

The identified threats are ranked using DREAD. The DREAD is acronym formed from the first letter of each category of threat namely Damage Potential, Reproducibility, Exploitability, Affected users, Discoverability. The risks are rated over DREAD scheme with numerical values of 3, 2, and 1. The threat rating scheme is shown in Table 3.

Table 3. Threat rating scheme

Threat Rating	Description
Damage Potential(D)	1 = Nothing 2 = Individual Users' Data 3 = Complete System.
Reproducibility(R)	1 = The attack is very difficult to reproduce.
	2 = The attack can be reproduced during certain time intervals.
	3 = The attack can be reproduced very easily.
Exploitability(E)	1 = Attacker need in-depth knowledge about the system.
	2 = A skilled programmer can make attack.
	3 = A person who is new to the system can exploit
Affected Users(A)	1 = Very small percentage of the users. 2 = Some users 3 = All users
Discoverability(D)	1 = Required controls do not exist 2 = Insufficient log management
	3 = Full control over system

The DREAD equation used to compute a risk value, which is the mean of all five categories is shown in (1).

$$Risk = (D+R+E+A+D) / 5 \quad (1)$$

The computed risk value is categorized as low (0 to 6), medium (7 to 11) or high (12 to 15) based on the impact the threat possesses to the EHR system. DREAD uses the standard scale for computing High, Medium and Low to rate the threat. When threat is high, it means it needs to be resolved by implementing appropriate counter-measures. If the identified risk is medium, it also needs to be addressed. If identified risk is low, it does not pose any significant damage to the system. The computed risk for the identified threats for the proposed system is shown in Table 4.

Table 4. Risk computation for EHR using DREAD

Threat (T)	D	R	E	A	D	Total	Rating
T1. Attacker monitors the network and obtains authentication credentials	3	3	2	2	2	12	HIGH
T2. Theft and replay of authentication cookies	2	2	2	2	2	10	MEDIUM
T3. Links to sites that use cookie less session state	2	1	2	2	1	8	MEDIUM
T4. Attacker possible way of predictable session IDs	1	1	1	1	1	5	LOW
T5. The attacker obtains Sensitive patient data on cloud database	3	3	2	3	2	13	HIGH
T6. An attacker with inadequate authorization is able to see other patient data and possibly access other restricted data.	3	3	2	2	2	12	HIGH

The result indicated the high possible threats associated with user authentication and authorization whereas theft and replay of authentication cookies and link to the site of those cookies are found with medium threats. The result also indicated that prohibited users can gain unauthorized access to the EHR system by spoofing the login credentials. This threat may lead to the sharing of patient's personal and health-related data in an unauthorized manner that may result in information misuse, information disclosure, and altering information. To enhance the features for the secure access and storage of patient data, Administrative, Physical, and Technical security standards are included in the proposed system. These security standards are discussed in Section 2.1.4.

2.1.4. Security standards

The health record system in India necessarily is safeguarded by the privacy and security standards. These standards guarantee that, health data is secure during its storage, retrieval, and transmission. For adopting security standards, the health organization must consider various aspects such as the size of the organization, complexity of the system, healthcare IT infrastructure, and application security capabilities. Administrative, physical, and technical are the three main safeguards for security standards used in the health information system which ensures the confidentiality, integrity, and availability of EHR system [21].

2.1.4.1. Technical safeguard

The developed EHR system must comply with technical safeguard to protect its security plan. Technical safeguards are technology, policy, and the procedures for the protection of the EHR by controlling access to it. Hence, the implementation need to address the following standards, focusing on the functionalities as shown in Table 5.

Table 5. Technical safeguard for EHR system

Sl.No	Type	Purpose
1	User Authentication and authorization	Privilege Management and Role based Access Policy
2	Audit Trail and Logs	All activities performed by the user must be recorded
3	Data Integrity	Secure Hash Algorithm (SHA), recommended to use SHA-256 or higher
4	Data Encryption	Encryption key-Minimum 256-bits key length Encrypted connection- HTTPS, SSL v3.0, and TLS v1.2
5	Digital Certificate	Digital certificates use and management

2.1.4.2. Administrative safeguard

Administrative Safeguards requires to develop and implement security processes that mainly focus on internal organization, policies, procedures, and security measures that safeguard health information of the patient. To ensure security measures and to protect patient information, it is necessary to update the organizational policies. Frequent changes to policies will ensure that intruders get less time to adapt and find possible vulnerabilities. Training the employees to follow security procedures increases their awareness and allows them to take the appropriate actions and follow the established contingency plans. Administrative policies should also clearly mention the access control policies and role to access health data [22].

2.1.4.3. Physical safeguards

To protect the EHR system from physical damage or theft mainly requires physical safeguard techniques such as installing closed-circuit television (CCTV) cameras. Implementing biometric authentication schemes such as fingerprint login or iris scans can further enhance security. Integrating physical safeguards with the cloud EHR system reduces unauthorized intrusion and can limit remote attacks on the network. For instance, if a policy is implemented which allows the generation of a valid login key only after successful biometric authentication, it can narrow down the intruder's reach. Physical safeguards should also include the entities which are authorized to grant access to physical resources and their maintenance.

2.1.5. Mitigation techniques for secure storage and retrieval of EHR

Some of the mitigation techniques to address the attacks identified earlier are described in this section.

2.1.5.1. Authentication model for EHR

Single Sign-On (SSO) is user authentication service that permits EHR users to access multiple health services after signing in only once [23]. When the user signs in, their identity is recognized and they need not sign in multiple times to access different types of health services. Figure 4 depicts the proposed SAML-SSO based authentication model. Implementation of SSO is based on security assertion markup language (SAML). It is an XML based communication protocol for exchanging authentication information between the service provider and identity provider (IdP). If a user from PHC, SHC, and THC tries to access the EHR service, a small request is generated and redirected to the IdP. IdP contacts active directory present in the hospital and parses the request and authenticates the user for access. A small token is generated and returned to the user. Using this token, the user of the hospital can access the EHR service, which improves the security and increases the access speed.

In addition to the authentication model, the salting technique which is a random data is used as an additional input to the hash function. Without salting technique, an intruder can precompute the rainbow tables of common password hashes and easily compare them to a database and see who used which common password. With rainbow table attack output of a hash function is always the same when the input remains the same. To make each hash password unique, random data is added to the input of the hash function. Figure 5 shows user interaction with the EHR database with salting technique [24].

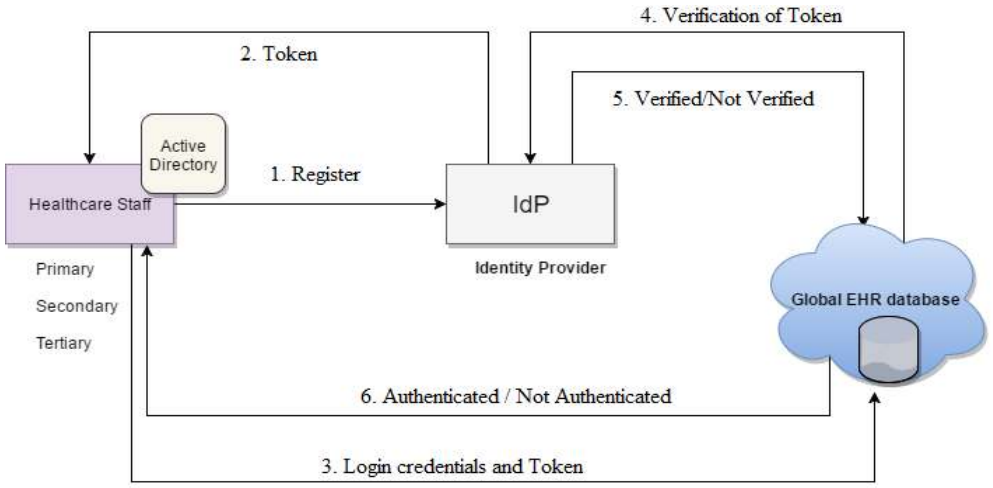

Figure 4. Single sign-on (SSO) authentication model for cloud-based EHR

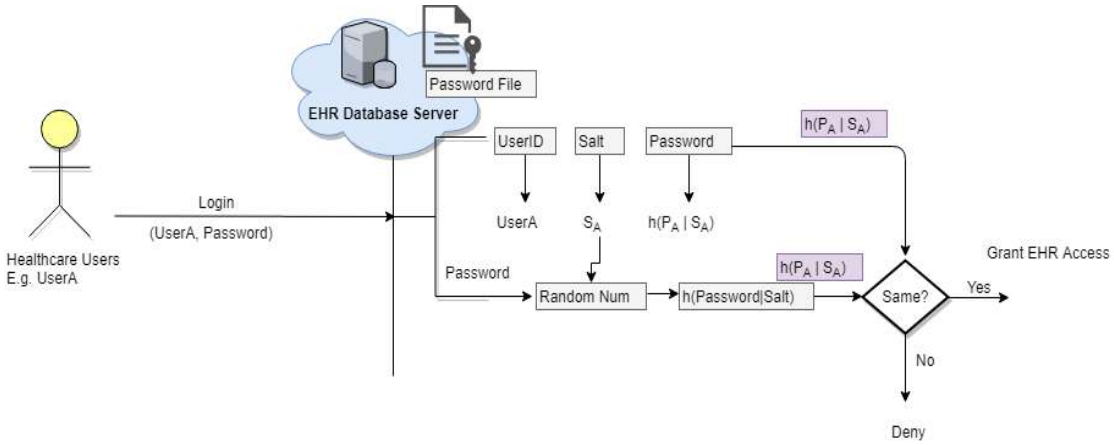

Figure 5. Salting method for authentication

In this model, the healthcare user logs into the system with his username and password to access the services. The cloud service before giving access will verify the user name and password of the user for authentication. Initially, all the user credentials are recorded in the password file. The salt (random data) is saved with the password for additional security of the EHR system. The salting value is the random data that is unique to each user. The salt is added to the password before it is hashed and stored in the database.

If the user tries to access the EHR services, the user credentials are matched with the previously stored user credentials with salt value. If the match is found, a user is granted access to the service; otherwise access to the services is denied. If an attacker compares the salted password hash with the list of common password hashes, then none of the hashes would match in effect. Since the output of the hash function is changed completely due to the addition of the salt, the attacker would have to use brute force to try gaining access thereby eliminating the benefit of a rainbow table thus making it more difficult for the attacker to break in.

2.1.5.2. Attribute-based encryption

EHR is a health record repository to store patient health information. As more sensitive data is shared and stored on the third party platform on the cloud, there is a need to protect the data from the unauthorized access. To achieve this attribute-based encryption (ABE) is used as the main encryption technique to encrypt each patient's EHR data [25]. The proposed framework for patient-centric, secure and scalable EHR sharing on cloud storage is depicted in Figure 6.

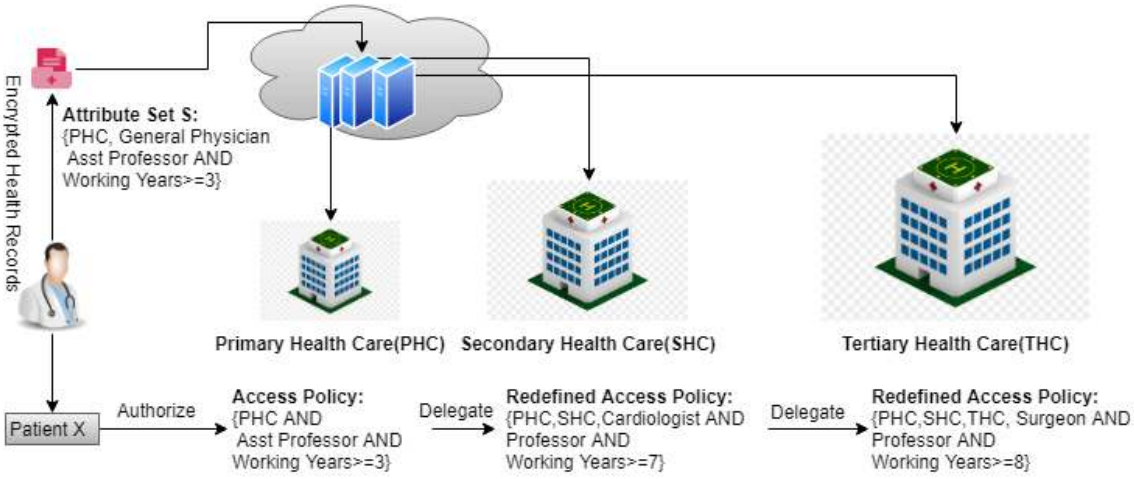

Figure 6. Attribute-based encryption for EHR system

To protect the privacy of the patient data, all health records must be encrypted. The attributes such as Healthcare Institute Name, Health Department, Doctor Designation, Work Experience, etc can be considered. Assume that patient health record from the PHC is encrypted with the following attributes Primary healthcare, General medicine, Professor, Working Years ≥ 3, which is denoted by A. If the same patient needs consultation by a Senior doctor of cardiology department of SHC, then instead of sharing secret key with all health care professionals, current doctor can give access policies having following attributes Primary health Care, Secondary Health Care AND Cardiologist AND Professor AND Working Years ≥ 7 denoted by A^{I} and further generates a secret key S_{KA} using it. With this key pair A and S_{KA}, higher level health-care professional can access patient data. This process of allowing access to other health-care center doctors is referred as redefining access policy. Similarly, when the same patient needs to be referred to a surgeon working in a higher level hospital such as THC, current doctor in SHC can give access policies having following attributes Primary health Care, Secondary Health Care AND Surgon AND Professor AND Working Years ≥ 8 denoted by A^{II} and further generates a secret key S_{KA} using it. Atribute based encryption ensures that security and privacy of sensitve patient data is protected from unauthorized users.

2.1.5.3. Attribute-based access control

Attribute-Based Access Control (ABAC), also known as Policy Based Access Control (PBAC) refers to defining access policies and authorizing access to resources and data based on certain attributes defined by the organizations [26, 27]. Attributes can vary from organization to organization. In contrast to Role Based Access Control (RBAC) which provides access based on predefined roles, ABAC allows organizations to set a complex set of Boolean logic and conditions to ensure that access is provided if and only if all the conditions have been satisfied.

When it comes to healthcare organizations, various factors can be considered as attributes. For demonstration, this paper has considered a few of them such as patient consent, attendance timestamps (login and log out), role hierarchy, and work experience. Figure 7 illustrates a sample workflow demonstrating ABAC in healthcare organizations. The Pseudocode 1 summarizes the workflow of a user who wants to update cardiac patients' records.

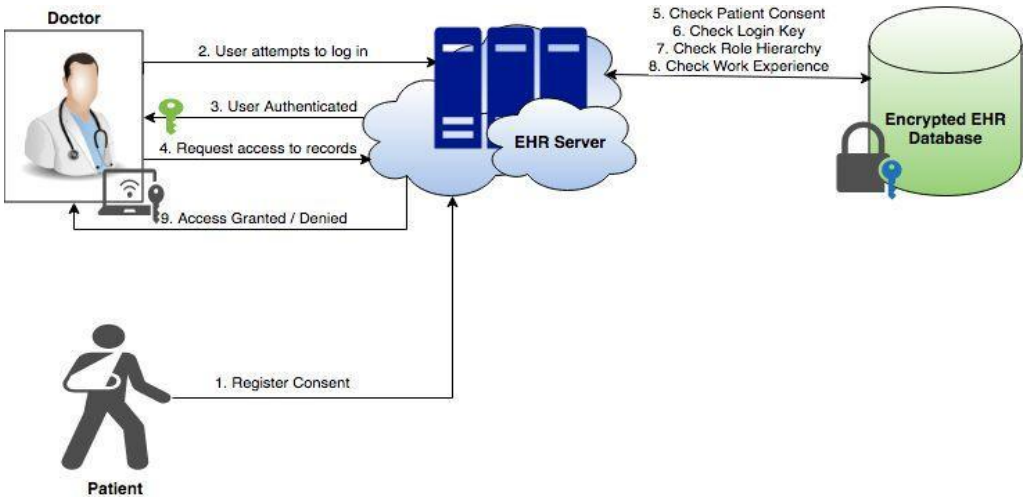

Figure 7. Sample workflow of access control

Pseudocode 1 - Employee Access for Updating Cardiac Patients' Records

```
IF (user.getHospital ().getPatientConsent () == 'YES') THEN
        IF (user.getLoginKey ().isValid ()) THEN
        IF (user.getDepartment () == 'CARDIOLOGY') THEN
                IF (user.getRoleHierarchy () >= min (task.getAuthorizedRoleHierarchies ()) &&
user.getWorkExperience () >= task.getRequiredWorkExperience ()) THEN
                Access Granted – Update patient records
            ELSE
                        Access denied – Contact Supervisor
                END IF
            ELSE
                Access denied – Contact the concerned department
            END IF
        ELSE
            Access denied – Validity of login key has expired
ELSE
        Access denied – Contact concerned patient for the hospital authorization
END IF
```

In a multi-healthcare collaboration in the cloud, a user from a particular hospital is granted access to a patient's records if and only if the patient or his family has registered and given their consent and has authorized that hospital to do so. Once a hospital has been authorized, the hospital policies come into play. If a user satisfies all the conditions and policies set by the healthcare organization that they are working in, then they are granted access to that patient's records. In the above algorithm, role hierarchy is a numeric value that refers to their position in the organization as shown in Table 6. Work experience is also a numeric value that refers to the number of months the user has worked in the organization. In addition to the attributes as mentioned earlier, other company attributes can also be taken into consideration, such as trust factors, performance reviews, and other key performance indicators (KPIs). The mitigation techniques are incorporated into the system, and the EHR solution is proposed for secure access and storage of patient data. The proposed solution is described in Section 3.

Table 6. Role and role hierarchy

Role Hierarchy	1	2	3	4	5	6	7
Role	Chief of Medical Staff	Department Chief	Sr Resident Doctor	Jr Resident Doctor	On Call Doctor	Medical Interns	Medical Students

3. PROPOSED SOLUTION

Figure 8 shows the proposed secure solution for Electronic Health Record System. The first tier is user interface, is also called a presentation tier. With this level, healthcare professional gets access to the healthcare system. In order to provide security, authentication model SSO and salting methods can be implemented in presentation tier. The SSO and salting methods in user interface improves the security and making it more difficult for attacker to access the system. The second one is the functional process or business logic which can be secured using secure access protocol such as HTTPS and SSL. Third one consists of data storage and data access and is developed and maintained as independent modules. Implementing authorization module OAuth ensures that the patient's data can be accessed securely without compromising the patient's or the user's account credentials. As more sensitive data is shared and stored by third-party sites on the cloud, there will be a need to encrypt data stored at these sites. To achieve fine-grained and scalable data access control for Electronic Health Record, attribute-based encryption (ABE) is used as the main encryption technique to encrypt each patient's EHR data. ABAC ensures that access is provided if and only if all the conditions set in the algorithms. The final proposed architecture ensures the EHR system with confidentiality, integrity, and availability of the data.

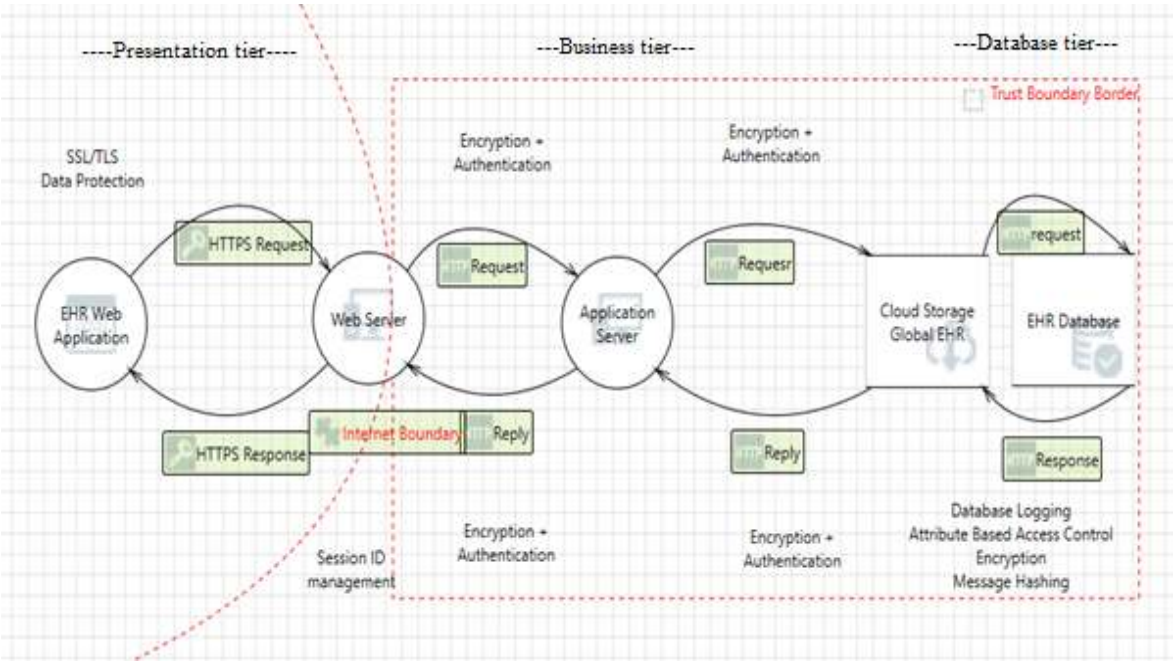

Figure 8. Proposed solution model for electronic healthcare

4. CONCLUSION

Healthcare organizations are considered as one of the most targeted sectors by intruders to gain sensitive information for malicious uses. To share the data among multiple healthcare providers in a secure manner, EHR reference architecture is developed and various attacks and vulnerabilities have been identified. Potential threats are identified in the EHR system by using STRIDE Microsoft threat modeling tool and the amount of risk posed to the system are calculated using DREAD. Also a solution is proposed to mitigate the threats which includes authentication, authorization, attribute-based encryption and access control to provide a safe EHR system.

REFERENCES

[1] S. Davey, *et al*., "A comparative evaluation of public health centers with private health training centers on primary healthcare parameters in India: a study by data envelopment analysis technique," *Indian journal of community medicine*, vol. 40, pp. 252-257, 2016.

[2] Ministry of Health and Family Welfare, Government of India, "Electronic Health Record Standards for India," 2013. Available: https://www.nhp.gov.in/NHPfiles/ehr_2013.pdf.

[3] A. L. Terry, *et al*., "Implementing electronic health records: Key factors in primary care," *Canadian Family Physician*, vol. 54, pp. 730-736, 2008.

[4] M. A. Musen and J. H. van Bemmel, "Handbook of medical informatics," 2018. Available: http://www2.hawaii.edu/~nreed/ics691BMI2/discpapers/handbookMICh7.pdf.
[5] G. D. Mogli, "Managing Medical Records," Channel publishing Publications Company, USA, 1996.
[6] E. K. Huffman, "Medical Record Management," Physician's Record Company, 7th edition, 1981.
[7] Ministry of Health and Family Welfare, National Health Policy, Government of India, "Electronic Health Record Standards for India," 2017. Available: https://mohfw.gov.in/sites/default/files/17739294021483341357_1.pdf.
[8] C. S. Sindhu and N. P. Hegde, "A Novel Integrated Framework to Ensure Better Data Quality in Big Data Analytics over Cloud Environment," *International Journal of Electrical & Computer Engineering*, vol. 7, pp. 2798-2805, 2017.
[9] B. Yüksel, *et al*., "Research issues for privacy and security of electronic health services," *Future Generation Computer Systems*, vol. 68, pp. 1-13, 2017.
[10] D. Ramesh and B. Rama, "Secure Privacy Implications for Clients and End-users through Key Assortment Crypto Techniques Implicated Algorithm," *International Journal of Electrical and Computer Engineering*, vol. 8, pp. 25443-5448, 2018.
[11] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal*, 2018.
[12] C. S. Kruse, *et al*., "Security techniques for the electronic health records," *Journal of medical systems*, vol. 41, pp. 127, 2017.
[13] K. Amer, "Informatics: Ethical use of genomic information and electronic medical records," *The Online Journal of Issues in Nursing*, vol. 20, 2015.
[14] Y. B. Choi, *et al*., "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules," *Journal of Medical Systems*, vol. 30, pp. 57-64, 2006.
[15] A. Almulhem, "Threat modeling for electronic health record systems," *Journal of medical systems*, vol. 36, pp. 2921-2926, 2012.
[16] F. Alemán, *et al*., "Security and privacy in electronic health records: A systematic literature review," *Journal of biomedical informatics*, vol. 46, pp. 541-562, 2013.
[17] C. A. Ardagna, *et al*., "Access control for smarter healthcare using policy spaces," *Computers & Security*, vol. 29, pp. 848-858, 2010.
[18] Anitha K. L and T. R. Gopalakrishnan N., "Data storage lock algorithm with cryptographic techniques," *International Journal of Electrical & Computer Engineering*, vol. 9, pp. 3843-3849, 2019.
[19] J. Eom, *et al*., "Patient-controlled attribute- based encryption for secure electronic health records system," *Journal of medical systems*, vol. 40, pp. 253, 2016.
[20] A. Shostack, "Threat modeling designing for security," 2017. Available: https://the-eye.eu /public/ Books/ HumbleBundle/ threat_modeling_designing_for_security.pdf.
[21] Bahga, Arshdeep, *et al*. "A cloud-based approach for interoperable electronic health records (EHRs)," *IEEE Journal of Biomedical and Health Informatics*, Vol. 17, No. 5, pp. 894-906, 2013.
[22] Murtaza, Mirza B. "Risk management for health information security and privacy," *American Journal of Health Sciences*, Vol. 3, No. 2, pp. 125-134, 2012.
[23] V. Beltran, "Characterization of web single sign-on protocols," *IEEE Communications Magazine*, vol. 54, pp. 24-30, 2016.
[24] W. Stallings, "Cryptography and network security: Principles and Practice," Pearson Education, 5th Edition, 2012.
[25] M. Li, *et al*., "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, pp. 131-143, 2012.
[26] Y. Zhang, *et al*., "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, pp. 2130-2145, 2018.
[27] Seol. Kwangsoo, *et al*. "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, Vol. 7, pp. 9114-9128, 2018.