Project Design Phase -Part 1

Proposed Solution

Team Id	NM2023TMID04415
Project Name	Block chain Technology For Electronic Health Records

Cloud-based architecture for EHR 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.

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.

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:

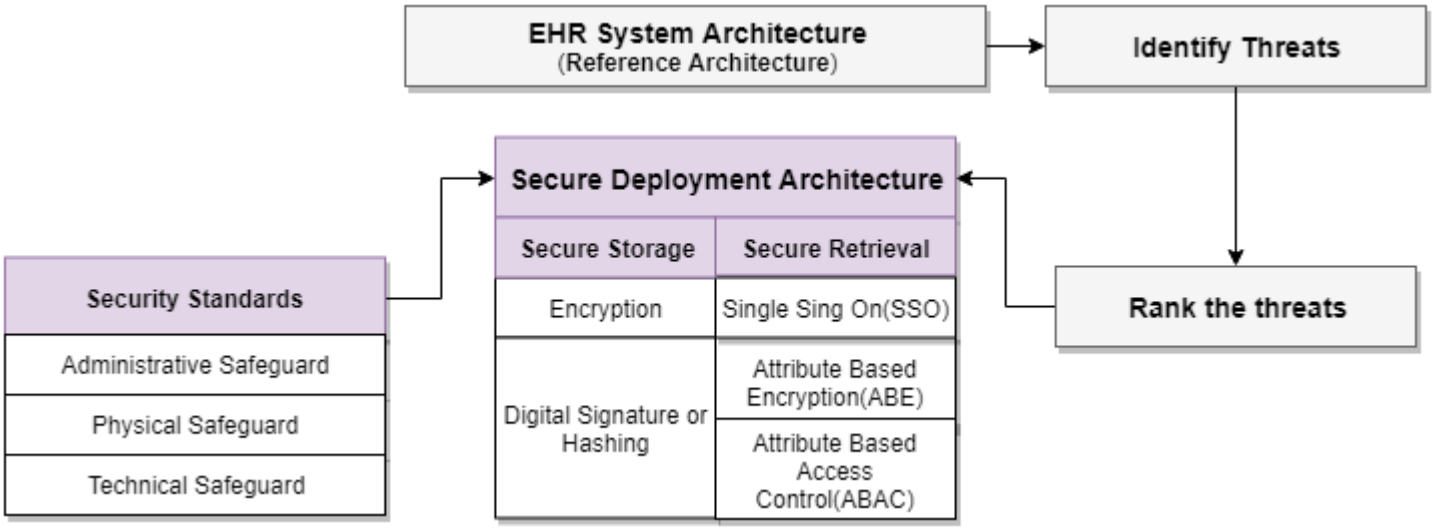


Figure 2:Proposed Security Framework for EHR system

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 3shows the architecture of the EHR system, which is the reference architecture for identifying threats in the system.

Figure 3:

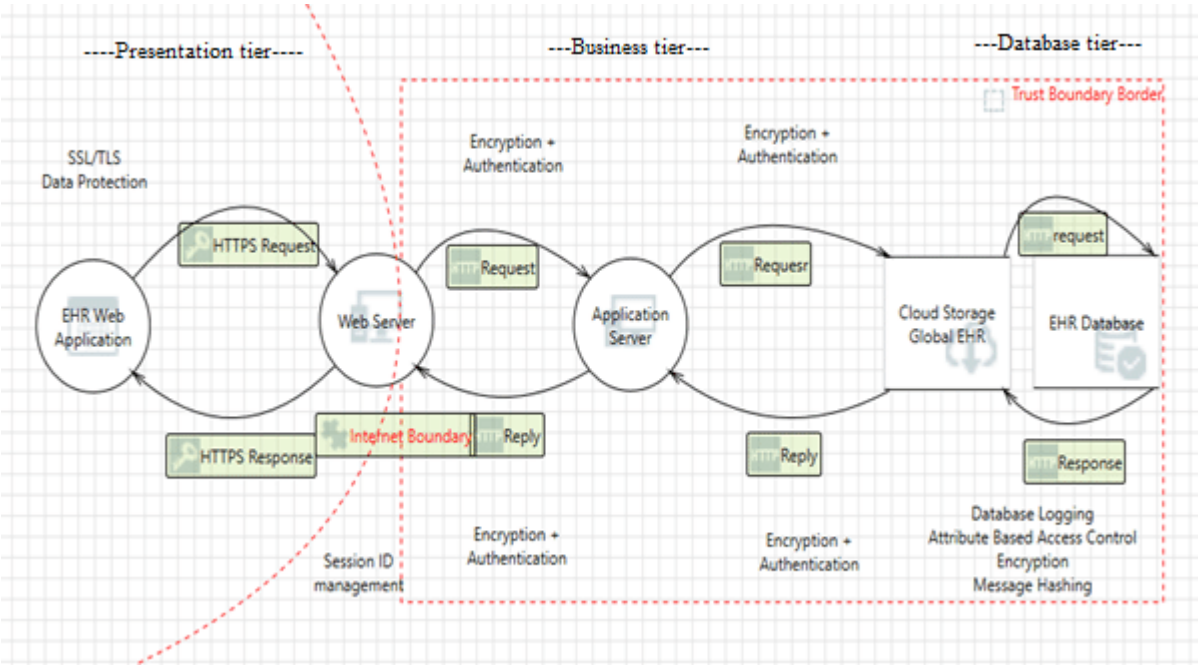


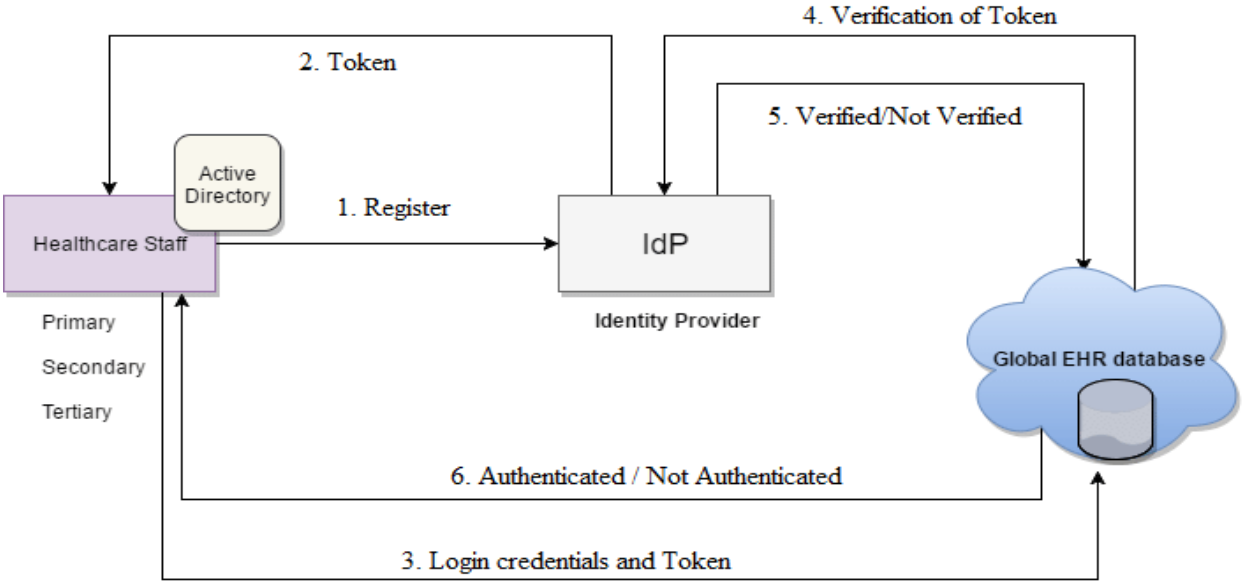
Figure 3. EHR System architecture

Authentication model for EHRs:

- 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.

Figure 4:

Figure 4. Single sign-on (SSO)



authentication model for cloud-based HER