6 Secured Electronic Medical Record

The patient information will be stored in an Electronic Medical Record (EMR). The required patient information will be rapidly and completely available to the persons who should receive that information, and not be made available to anyone else. To achieve that simple objective many pieces of technology have to work correctly and reliably. Issues of security and privacy are not unique to medical information, but they become more complex in medical records. Part of the work presented in this chapter is published in [GKV2009].

Protection of privacy depends greatly on having a secure system. Security first of all requires that persons accessing the system are properly identified, or authenticated. Once they are authenticated, they can be authorized to read or manipulate specific parts of the EMR.

6.1 Electronic Medical Record

The EMR must serve a very wide variety of purposes. At the same time, medical information cannot be as well structured as, say, banking or merchandising records. Unfortunately, personal identification is essential for many of the purposes in a medical record.
Encryption technology for communication is routinely available, and has only modest effects on system performance and costs. On the other hand, it is not effective to store medical records for the long-term in encrypted form. The variety of accessors is such that means for decryption will have to be provided at many points, adding protection and high costs to assure that access is provided when and where needed.

Within a domain, an authenticated accessor will have certain rights. Rights may pertain to certain files, or certain records. For instance, nurses on a ward should have access to all medical information for patients in the ward, while the physicians will need access to the patients under their care in various localities. The right to append information, as entering orders, is more restricted. Authorization to actually change stored information is rare, since it inhibits the audit trail for decisions that have been made.

Transmission of information, including the passwords or identifications needed for authentication, can be protected through encryption. Encryption causes a message to be transformed according to an encryption key. The encryption key can direct shuffles, boolean transforms, reversible multiplications, and the like. Cryptography can provide an arbitrarily high level of protection by lengthening the key. The difficulty of breaking encrypted information increases proportionally to the power of the size of the encryption key. Still, the information to be gained by breaking into an EMR rarely warrants even that effort.
Cryptographic procedures with much longer keys are now becoming available. Existing and developing capabilities seem to be adequate for Medical records.

Managing the keys is still a problem. The key used for encryption has to be made available to the destination, so that decryption can be performed. Loss of the key makes all of the information inaccessible, and stealing a copy of the key makes encryption meaningless. Key losses can be dealt with by depositing copies of the keys with a responsible party, an escrow agent. Law enforcement agencies have been favoring schemes where keys would always be deposited with an escrow agent, so that encrypted files could be decoded when a legal search warrant is issued.

The HEC encryption uses two keys to overcome the problem of key management. Data to be transmitted are encrypted with two keys, one supplied by the sender and one by the receiver. A private version of the key is retained locally and derived keys are made publicly available. Encryption uses the local private and the remote public keys. Decryption requires the remote public and the local private keys. Public-key encryption is effective for modest data volumes, for sharing keys used to encrypt larger quantities of data, and to authenticate remote accessors.

Although cryptography is an essential tool in protecting information from intruders, it only provides protection for well-defined tasks, and cannot distinguish among the many types of accessors that
need to get to an EMR. All legitimate accessors to a record would need the same encryption key, and could not be distinguished.

In the Medical sector doctors and patients need to have access to the medical records efficiently and in a secure manner. As information technology gets increasingly deployed in the medical sectors it becomes eminent that the medical records are stored electronically. Secured Electronic Medical Records (SEMR), which aims at providing a set of services which will provide secure and efficient access of the EMR. The set of services that are provided by SEMR include Authentication, Authorization and Secure communication. This chapter suggests that the implementation of a digital envelope combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve Cryptography (HECC). The result illustrates that the best alternative digital envelope hybrid cryptosystem for EMR.

In the medical sector, the EMRs are of utmost importance. It is important that apart from the patient, no one else should have complete control over the EMR of a particular patient. Also, such EMRs should be readily accessible to the doctors and patients. In order to create a secure environment for such a sector, the minimum set of services that need to be implemented should provide Authentication, Authorization and Secure Communication [RKH2004].
i) Authentication involves identifying whether the user is a valid entity of the system. In order to access any resource in the system, the user has to be authenticated. One of the ways to implement the authentication service would be to ask for user identification in terms of username and password. Additional factors like an RSA token or fingerprint reading can be used to improve the security.

ii) Authorization involves identifying the rights of the users. Authenticated users should access only those resources to which they have access to. Also, the type of access (read, write, execute) determine the capability of the user to access that resource. This functionality can be implemented by creating access control list for the resources. These ACLs identify the type of access the user has to the resource.

iii) In a medical system, messages are distributed in nature and data needs to be communicated amongst the different services. It is important that the communication takes place securely. Such secure communications can be implemented by encrypting the data that is sent over the transmission media.

Apart from these basic services, auditing of all the events are also important components of the system. This auditing event provide the administrators to analyze the past events and make changes to the system if required. They can also be used to trace a user’s intrusive activity.
6.2 Architecture of SEMR

The SEMR system uses two-factor authentication method for authenticating the users. Further, roles assigned to each user are used to identify the privileges he has for accessing the resources. This system implemented a role-based access control for user authorization. This chapter describes and implements the architecture of the system [GKV2009]. Finally, further improvements are discussed that can be done in the system.

The proposed Digital Envelope system has 3 major components –

i. MD5 Hashing Algorithm for secret key integrity checking.

ii. Encrypt the Patient History using AES Algorithm (Symmetric Cryptography)

iii. Encrypt the AES key using HECC Algorithm (Asymmetric Cryptography) (Secrecy and Authentication) [STA2003].
Figure 6.1: Architecture of SEMR
From the diagram there are basically six interactions that take place in the system for one complete cycle from authentication to accessing an EMR. These interactions are as follows:

i. Client Machine (representing the Doctor) to generate the secret key for encrypts of the Patient history.

ii. Client Machine (representing the Doctor) to digest the secret key using MD5.

iii. Client Machine (representing the Doctor) to encrypt AES key using the doctor's private key and patient's public key (Asymmetric Encryption). Doctor will send the Digital Envelope including the Cipher text of patient history, Cipher message of AES key and Message digest of the AES key to the patient.

iv. Client Machine (representing the Patient) to decrypt digital envelope using the patient's private key and Doctor's public key for the AES key.

v. The Client Machine (representing the Doctor) decrypts the cipher text of patient history using the AES key.
vi. Message digest of the AES key is obtained and compared with digital envelope message digest to check whether the patient history is correct or not.

Additionally, on all the other events, logged into log files which can be further analyzed by the administrator.

This System used Java for implementing the architecture described above. Communication channels used the Java extensions to provide the encryption and Message digest. The Java Cryptography Extensions (JCE) is used to implement the encryption and decryption of tokens.

At this moment, all the certificates that are used in the EMR system are assumed to be trusted. There is no central Certifying Authority (CA) in place. One of the further improvements would be to provide a CA so that the certificates of users can also be trusted.

The SEMR system implementation provides a secured way to access the EMR. Additional security has been provided by the use of two-factor authentication method [GKV2009]. This method takes into consideration the location of the user. The implementation of the system provides an insight into developing a distributed system which is secure, robust and user friendly. It has also provided a deeper understanding of the role based access control model.