Medical Cyber - Physical System; A Digital Healthcare Solution

Dr .N. Sowri Raja Pillai [1], Jesintha Mary.D[2], Ezhilarasi .R[3], Yazhini. K[4]
[2,3,4]Student, Department of Information Technology
[2]Head of the Department, Department of Information Technology
[1, 2,3,4] RAAK College of Engineering and Technology

Abstract- *Several advanced countries are working to develop an efficient architecture and mechanism for Electronic Health Record (EHR) which is gradually eliminating the use of paper and becoming more popular in healthcare organizations. Online accessing of patient record and transaction related to diagnosis have many benefits for patients as well as healthcare organization and professionals. But it also raises serious privacy issues related to private data of patient e.g. any patient would not like to expose some health information which may defame her/him or may create problem for her/his professional career as well as personal life. Internet based EHR systems allow patients remote access to their entire medical history anytime. Hence security and privacy comes in the picture. For adaptation of the EHR, the key factors are financial incentives and barriers, laws and regulations, the state of technology, and organizational influences. EHR systems are highly desired for efficient integration of all relevant medical information of a person and to represent a lifelong documentation of medical history. Several threats to confidentiality of healthcare information from inside the healthcare institution, outsider intrusion into medical information systems is crucial. This proposed EHRCHAIN system can provide a convenient, simple, privacy preserving, secure mechanism. It can ensure availability of patient's health information to any healthcare entity at any time with consent of patient. In this proposed work and prototype implementation, we have simulated some basic healthcare activities. There are still more activities related with the security of EHR and the privacy of patients, which are needed to be known how these activities can be compatible with existing functions in the implementation. Data management becomes difficult because of the growing numbers of patients' data and information hence concept of Big Data and Cloud computing is required. In future, Blockchain technology and smart contracts seems to be more appealing in the field of healthcare. This proposed solution provides a huge possibility for medical research on particular disease. It can provide anonymous health data which will not have any identifiable information of patient, to researchers.*

Keywords- EHR, Security, Sub Carrier, Data Leak Reduction.

I. INTRODUCTION

Electronic Health Record (EHR) is gradually eliminating the use of paper and becoming more popular in healthcare organizations. Online accessing of patient record and transaction related to diagnosis have many benefits for patients as well as healthcare organization and professionals. But it also raises serious privacy issues related to private data of patient e.g. any patient would not like to expose some health information which may defame her/him or may create problem for her/his professional career [1]. Internet based EHR systems allow patient to remote access their entire medical history anytime. Hence security and privacy comes in the picture. For adaptation of the EHR, the key factors are financial incentives and barriers, laws and regulations, the state of technology, and organizational influences [2].

There are three correlated records in healthcare information system:.

Personal Health Record (PHR) is typically a record that is maintained by patient. It includes complete summary of medical history by gathering information from many sources including EMR and EHR.Several threats to confidentiality of healthcare information from inside the patient care institution, from within secondary user setting, outsider intrusion into medical information systems is crucial. Inside patient care institution accidental disclosure, insider curiosity, insider subornation could be the possible threat to confidentiality.

Electronic Health Record (EHR) is a subset of EMR cord maintained by each CDO and is created and owned by the patient. EHR has patient input and can be used across multiple healthcare delivery organizations within a community. [2] EHR systems are highly desired for efficient integration of all relevant medical information of a person and to represent a lifelong documentation of medical history.

Three general classes of technological interventions to improve system security are deterrents, obstacles and system management precautions [4]. Deterrents depend upon

the ethical behavior of people and provide reminders and oversight to reinforce those standards. Obstacles directly control the ability of a user to get information with the goal of constraining access only to information for which they have a need or right to know. System management precautions involve proactively surveying an information system to ensure that vulnerability is eliminated through known sources.

II. SECURITY AND PRIVACY ISSUES

Due to risk associated to EHR it is vital to assure privacy of the patients. The following security issues should be handled properly in any healthcare entity while accessing or transacting EHR. User Authentication: When any user is trying to access the health record then only authorized user will be able to access the record. Smart card based several solutions have been proposed [6]. Biometric based system is also in use for ensuring the authorized access of records Confidentiality & Integrity: It is related to the accuracy and reliability of healthcare record and integrity and reliability of physical computer and network systems. Hacking incidents on EHR systems may lead to altering patient data or destruction of clinical systems. [10] Access Control: It is a fundamental security issue in shared computing environments where medical records stored in databases and exchanged through heterogeneous file system. As roles and privileges vary depending on the nature of the system and organization, so it requires controlling of user's right to use certain resources by granting or rejecting access to resources. It is easy for an unidentified user to access the network if the remote connection is not secure [12] Electronic systems should enable the core security features of role-based access, passwords, and audit trails. There are serious privacy issues related to genetic testing. Individuals are faced with a fear of employment loss and life insurance. Hence the refusal to use effective genetic tests hurts individuals, researchers, and physicians [12].

III. DATA OWNERSHIP:

It is also important when delegation of power Access of patient record is considered. Who will own which data, delegation of authority over data? Also duties and responsibilities of data ownership should be handled transparently.

IV. DATA PROTECTION POLICIES:

As several entities are involved in healthcare diagnosis system, crossing organizational and functional boundaries, so acceptable and consistent protection are required. Organizations require strict policies and procedures the use of physical media and portable devices to prevent theft or loss.

EHR systems require continued development of functionality to manage security ,add levels of security, and block access to specific notes or results, track versioning, and mask sensitive entries for release of information [4]. User Profiles: Several entities are involved in healthcare system like patient, practitioners, healthcare organization, trusted third party, pharmacist etc. Hence issues related to defining user types and roles needed to distinguish the functional requirements and security levels of users[4]. There is great variability and incompatibility of patient identification systems in healthcare facilities, making it difficult to uniquely identify patients within one facility or between entities. A system of identifying patients between entities must exist for interoperability to occur. Currently, there is no record-to-record matching standard in the industry[5]

Misuse of Health Record: Some of the websites offering EHRs, mostly the ones that offer storage space for free are not concerned with privacy. They may sell the data to other companies, or advertise on the same page as the content uploaded by the patient [9]. In a multispecialty environment, security of health records can be challenging. Organizations must have the ability to segregate any records related to treatment of substance abuse, as treatment of these patients can encompass multiple medical specialties and document types[9].

V. REALTED WORKS

After going through many research papers, we selected several relevant papers for our literature review on healthcare information security issues. Basic concepts and problems, models, and architecture for theelectronic health record have been reviewed which is discussed in [1][2][4]. We found following directions for the review work.

- Electronic Health record (EHR) systems are highly desired for efficient integration of all relevant medical information of a person and to represents a lifelong documentation of the medical history. Internet based EHR systems allow to patient remote access to their entire medical history anytime. Hence an efficient protocol and architecture is required which is not standardized yet[3][11][12].
- Anonymization is the important approach in healthcare information security, hence Hashing of medical data for privacy issues in healthcare is central issue but an efficient and acceptable approach is not available yet. Several approaches have been proposed for the assuring security issues related to healthcare security by this mechanism.

- Access control mechanism and application related to e-prescription system and other consumer related healthcare services requires a secure mechanism [5][6][14][15][17]. The above categories are different dimension of research in healthcare information security but still interrelated. Pseudonimazation concept can be used partially in e-prescription system and EHR database security and architecture solution.
- **E-health transformation model in Serbia: Design, Architecture and developing**

  In Serbia, The architecture of healthcare system is hybrid smart card based solution [4]. The organization of database and two model one online and second offline is briefly outlined here. In this system, hybrid smartcard (RFID and IC) have been used as part of a starting point in the strategic planning of this national level project. This smart card is a plastic card having standard format with RFID antenna and microchip. Microchip can receive sufficient amount of information. Chip card is a kind of small computing machine which can perform calculations and exchange information to/from system. RFID part of the smart card manages procedures for registration, authentication as well as treatment .

  Basic component of this proposed system are:

  1. HIS Healthcare information system – it ensures accessing of health information by authorized entities only.
  2. EHR – it is patient's all health relatedrecord.
  3. EHR applications – this application manages creation of patient's record, all history of activity like scheduling proposal, patient's visits to doctors, treatment done by doctor, otherservices.
  4. approaches a PHR – it is a combination of several online tools which will be responsible for allowing patients to access their own health record.
  5. Card for Patient Doctor – this electronic card is an alternative for traditional health booklet used in hospitals, but it is different in form and functionality. These cared are capable to store and transmit health information..

VI. ANONYMOUS E-PRESCRIPTIONS

From the security point of view, healthcare systems have several characteristics for consideration. Healthcare system includes heterogeneous set of institutions and hence sometimes has conflicting goals. The whole patient's experience of medical care is private. Hence providing confidentiality of medicine prescriptions is important one [5]. In the case of particularly, doctor's medical prescriptions to patient, more interaction is needed. Pharmacist collects the information and often stored in large database owned by hospitals or businesre often computationally intensive,enterprises known as "Pharmacy benefits management system (PBMs)". There is no federal law for privacy of patient's health records maintained by pharmacies. Hence privacy of patients is compromised. Some example of misuse of patient data has been felt. Medicine prescription defined as both entities-"a token signed by a doctor and as a process".

A smart-card-enabled privacy preserving E-prescriptions system.

This e-prescription system addresses "issues pertaining to the privacy protection in the process of drug prescription"[6]. Smart card play crucial role in this prescription system. 25 | P a g e In our research paper the whole process is described as follows [24]. "The smart cards are implemented to be portable repositories carrying up-to-date personal medical records and insurance information, providing doctors instant data access crucial to diagnosis process. A number of parties involved in the health care provision such as hospitals, General Practitioners (GP) business associates like insurance companies, Billing agencies, Pharmacists. This solution concentrates on smart card based portable personal information repository to simplify the process of drug prescription, enabling the doctor to bypass several bureaucratic procedures. Smart card not only work as repository device but also some intelligent task, like digital signature signing capability to sign the electronic pads, patient authorization. An extension in smart card role is to include the delegation of prescription signing capability among users, which they referred as Delegated signing. It is intended for a designated person who uses his own smart card to sign the prescription on behalf of the patient in collecting the medicine. It provides flexibility to be carried by someone else than the owner himself. Moreover it does not complicate the system. Advantage of this smart card enabled solution are-(a) Authenticity of the patients is automatically ensured by holding cards. (b)It prevents multiple prescriptions from different practitioners. (c)It can be used as a tool for tracking public health initiatives".

VII. RESEARCH OBJECTIVES

The research objectives (RO) are:
RO1: To study several available Hashing based solutions for Electronic Health Record (EHR).
RO2: To study requirements of access control mechanisms for healthcare.

RO3: To develop prototype architecture for integrated approach of Hashing and Encryption mechanism to ensure Privacy of Electronic Health Record (EHR). This prototype will be developed to demonstrate the effectiveness of the proposed work which includes following entities:- Patient Healthcare Information System - allows only authorized entities to access information Electronic health record (EHR) EHR applications Access control module

RO4: To propose an efficient Hashing based mechanism to achieve following goals:- User Authentication Confidentiality & Integrity Access Control Avoidance of Misuse of Health Record.

VIII. METHODOLOGY

We have developed prototype implementation of EHRCHAIN system. This prototype implementation has following features:

- In this EHRCHAIN system, in India Aadhaar number is used whereas in other country any national level biometric identification ID can be used, for registration to avoid forgery to own healthcare information in database.
- Unique pseudonym number which will be generated by patient by passing some secret information. This pseudonym will be used to store patient's healthcare information to preserve privacy.
- In Hashing process all identifiers/quasi-identifiers from patient's health record is removed so that if intruders get access to database, he will not be able to determine owner of particular health record, hence privacy is ensured
- In this prototype implementation of EHRCHAIN system, simIn Hashing process all identifiers/quasi-identifiers from patient's health record is removed so that if intruders get access to database, he will not be able to determine owner of particular health record, hence privacy is ensuredulations of some basic healthcare activities have been done.
- As identifiers/quasi-identifiers is not stored in EHRCHAIN health records database, this proposed solution provides a huge possibility for medical research on particular disease.
- Patient can update his/her access control policy at any time.

For prescription or any other purpose, any third party will be able to access the data after revealing his identity.

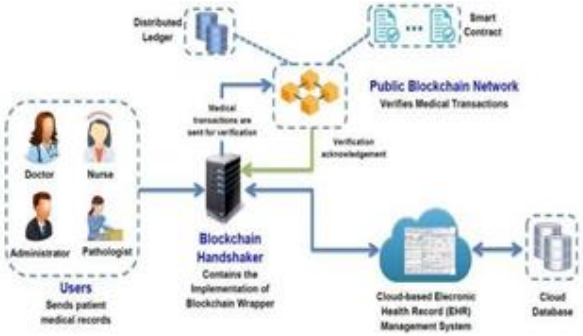

Figure 1. Proposed Architecture

Different countries have different choice according to need of the community but most of the popular EHR solution argue for patient-centered as it gives total access right to the patient [4][13][14][26][27][34]. This EHRCHAIN system is patient-centered. We have combined the Hashing techniques and encryption mechanism to provide an efficient mechanism for security and privacy of healthcare information system. In figure 4.1, it is shown that pseudonym is used to provide privacy to the patient. This pseudonym will be generated by patient. Access control policy controlled by patient will decide what and to whom the portion of his data may be accessed. 55 | P a g e Hashing of the sensitive data records supports both privacy- preserving primary and secondary usage as long as the records are depersonalized. The Architecture of EHRCHAIN system consists of two separate databases.

EHRCHAIN:

Health Records database and EHRCHAIN Patient Profile database, an Hashing module, Access control Module for Patients and Access control Module for Doctor/healthcare authority, and data access policy and sharing management as shown in figure .1. In following section functionality of each have been described.

EHRCHAIN DATABASES:

If any intruder become successful in accessing database then patient's privacy may be compromised hence to ensure strong privacy EHRCHAIN maintain two separate databases one for identifiable information in encrypted form and another for pseudonymised health records: i. EHRCHAIN Health Records database which contains patient's health records after Hashing ii. EHRCHAIN Patient Profile database which contains encrypted patient's profile and encrypted patients' pseudonym.

HASHING MODULE

Before storing health records from patient/healthcare center into EHRCHAIN Health Records database, Hashing module removes all identifiers and quasi-identifiers from patient's health record so that if intruder gets access to database, he will not be able to determine the owner of a particular health record. Each patient can create a unique pseudonym (digital long random number) using Pseudonym Generation mechanism. Pseudonym can be generated locally in her own environment without any information exchange between EHRCHAIN and Patient. Pseudonyms can not be guessed from patient's information and need not to remember. Pseudonym is

PATIENT'S PROFILE AND HASH ENCRYPTION

Patient's pseudonym is encrypted by his public key (using public key cryptography technique). There are several fields which have been identified as personally identifiable information e.g. name, date of birth, age, mobile number, AADHAR Number, email etc. These identifiable information is needed when patient visit new healthcare center first time. All these identifiable information are encrypted by a shared key (using symmetric key cryptography technique) shown in figure 4.3. Encrypted profile and encrypted pseudonym are stored in secure EHRCHAIN Patient Profile database. For addition of a new record, pseudonym is decrypted by patient's private key which is known to patients only.

ACCESS CONTROL MODULE

several access control models have been discussed. RBAC is the most frequently used model with some variations. Every entity of healthcare system has different access requirements which should be handled by the access control module without compromising privacy of patient. Each entity of healthcare system i.e. patient, doctor, and health centers/health authority will register in the EHRCHAIN system. AADHAR Number will be used for verification of the each entity. Hence identity of the accessing applicant is verified. Patient can access all the health records containing his pseudonym. Firstly patient needs to decrypt his pseudonym using his private key. this private key is known only to patient. hence privacy is maintained.

Doctors/healthcare authorities have limited access rights. They can access only those health records or some fields of the health records which are allowed by the patients. Firstly patient needs to decrypt her/his pseudonym using her/his private key. This private key is known only to patient. Then the doctor/healthcare authority will pass his pseudonym by following same step of decryption. With both pseudonym of patient and pseudonym of doctor/healthcare authority, access control module will permit to access those health records. Hence it will be validated that who accessed the health records.

IX. CONCLUSION AND FUTURE WORK

Most of available healthcare solutions and services don't provide full control to the patients as well as are not strongly privacy preserving as anyone can access patient's information from health card without his consent. . Different countries have different choice according to need of the community but most of the popular EHR solution argue for patient-centered as it gives total access right to the patient. So we developed patient- centered EHRCHAIN system to provide a convenient, simple, privacy preserving, secure mechanism. It will enable availability of patient's health information to any healthcare entity at any time with consent of patient. . Hashing of the sensitive data records supports both privacy-preserving primary and secondary usage as long as the records are depersonalized. It is highly recommended for healthcare information system . Hence in EHRCHAIN, Hashing techniques and encryption mechanism have been combined to provide an efficient healthcare for security and privacy of healthcare information system. Access control policy controlled by patient will decide what and to whom the portion of his data may be accessed. It is recommended by several solutions to adopt smart health cards in the implementation to improve the performance in healthcare activities. In prototype implementation of EHRCHAIN healthcare system, we have simulated some basic healthcare activities. By Hashing process all identifiers and quasi-identifiers from patient's health record are removed so that if intruder gets access to database, he will not be able to determine the owner of a particular health record. There are still more activities related with the security of EHR and the privacy of patients, to examine whether these activities can be supported by our pseudonym solution or not. This proposed solution provides a huge possibility for medical research on particular disease by using anonymous health data. It can provide anonymous health data which will not have any identifiable information of patient, to researchers. Hence without compromising privacy, anonymous health data will be available for the researchers..

REFERENCES

[1] Al-Hamdani, Wasim A. "Cryptography based access control in healthcare web systems." 2010 Information Security Curriculum Development Conference. ACM, 2010.

[2] Zhang, Rui, and Ling Liu. "Security models and requirements for healthcare application clouds." 2010 IEEE 3rd International Conference on cloud Computing. IEEE, 2010.
[3] Huda, MD Nurul, Noboru Sonehara, and Shigeki Yamada. "A privacy management architecture for patient-controlled personal health record system." J. Engineering Science and Technology 4.2 (2009): 154-170.
[4] Vucetic, Miljan, Ana Uzelac, and Nenad Gligoric. "E-Health Transformation Model in Serbia: Design, Architecture and Developing." 2011 International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery. IEEE, 2011
[5] Ateniese, Giuseppe, and Breno de Medeiros. "Anonymous eprescriptions." Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society. ACM, 2002.
[6] Yang, Yanjiang, et al. "A smart-card-enabled privacy preserving E-prescription system." IEEE Transactions on Information Technology in Biomedicine 8.1 (2004): 47-58.
[7] Riedl, Bernhard, et al. "A secure architecture for the Hashing of medical data." The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007.
[8] Poag, Stephen, and Xiaodong Deng. "Information security and privacy concerns of online prescription systems." refereed research paper, okland University.
[9] Slamanig, Daniel, and Christian Stingl. "Privacy aspects of e-health." 2008 Third International Conference on Availability, Reliability and Security. IEEE, 2008.
[10] 10. Riedl, Bernhard, and Veronika Grascher. "Assuring integrity and confidentiality for pseudonymized health data." ECTI-CON2010: The 2010 ECTI International Confernce on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology. IEEE, 2010.
[11] Alhaqbani, Bandar, and Colin Fidge. "Privacy-preserving electronic health record linkage using pseudonym identifiers." Health Com 2008-10th International Conference on e-health Networking, Applications and Services. IEEE, 2008.
[12] Addas, Rima, and Ning Zhang. "Support access to distributed EPRs with three levels of identity privacy preservation." 2011 Sixth International Conference on Availability, Reliability and Security. IEEE, 2011.