A Framework for Secured and Privacy Preserving eHealth System

By

Mahmuda Begum

A dissertation submitted for the degree of
Bachelor of Information Technology (Honours)
of Charles Sturt University

October 2014
DECLARATION

I declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgment is made in the dissertation. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged.

I agree that the dissertation be accessible for the purpose of study and research in accordance with the normal conditions established by the University Librarian for the care, loan and reproduction of the thesis.

( Mahmuda Begum)
ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor Dr. Quazi Mamun for being a constant support throughout my entire period of research work and also for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this dissertation.

Besides my supervisor, I would like to thank my course coordinator Maumita Bhattacharya for her encouragement and support during my whole study period.

Last but not the least, I would like to thank my beloved family for supporting me in my life.
ABSTRACT

eHealth, the future of health care system, is gaining popularity in quick succession in the context of Australia. The core of eHealth is the Electronic Health Record (eHR) system which functions to record patient health information. In the era of the current communication networks, healthcare systems should utilise the advantages of storing, fetching and distributing the information between different healthcare stakeholders efficiently. To make the system secure in respect to the access to eHRs, the Personally Controlled Electronic Health Record (PCEHR) has recently been proposed. Despite the claim of PCEHR being controlled by the patients, vulnerabilities of disclosing credentials by the healthcare professionals and system operators are still present in the system. Other threats include, but not limited to, sensitive data in wrong hands, vulnerable authentication, and confidentiality. Moreover, an uninterrupted application of the security principle of electronic data files necessitates encrypted databases. So far, many research works have been progressed to confirm the patient’s privacy. In most of them, the healthcare authority can get the consent to retrieve the patient’s eHRs. These vulnerabilities may impact the patients and warrant the necessity of emerging robust and effective authentication and access control schemes for eHRs.

In this dissertation we introduce a patient centric cloud-based PCEHR framework, which utilises the homomorphic encryption technique in storing the eHRs. The proposed system guarantees the control of both access and privacy of eHRs stored in the cloud environment.

Moreover, we propose a robust authentication scheme and a hybrid access control model to enhance the security and privacy of eHRs. Various methods of authentication are available using passwords, secret keys, tokens, and bio-metric features are the ones. An authentication system is required be elementary, fast and protected against unlawful use. In this dissertation, we propose multi-factor, multi-channel based authentication system which overcomes most of the drawbacks of existing the authentication system. Moreover, due to the simplicity of the proposed method, it is user friendly while ensures the strong security of the
system, at the same time the proposed authentication method is quick, convenient, and resistant to compromises.

For security requirements and protection of medical data it is necessary to implement access control policy in health care. Access control in eHealth solution which is right can ensure authorised access to sensitive records to keep privacy of her. In the traditional models, access control depends on specific attributes of the users and the objects. But the fact is that these access control models in these traditional models missing the notion of “context” which is part and parcel of the health care system. In this dissertation, we propose a new access control model combining with Role Based Access Control with context-constraint and Discretionary Access Control model, which restricts the access control and preserve the privacy of the records. We show that the PCEHR framework with the proposed access control method successfully satisfies various security and privacy requirements of the health care system.
Table of Contents

Chapter 1 .................................................................................................................. 7
1. Introduction ........................................................................................................... 7
   1.1. What is eHealth .................................................................................................. 7
   1.2. Importance of eHRs .......................................................................................... 7
   1.3. Evolution of eHRs: ............................................................................................ 8
   1.4. The Start of the PCEHR .................................................................................... 8
   1.5. Motivation of Research: .................................................................................... 9
   1.6. Contribution of the Research ............................................................................ 10
   1.7. Organisation of the Dissertation ...................................................................... 10

Chapter 2 .................................................................................................................... 11
2. Related Work on Existing Models of an eHealth System ........................................ 11
   2.1. Existing Models for Preserving Privacy in eHealth ........................................... 11
   2.2. Authentication .................................................................................................. 14
   2.3. Access Control ................................................................................................. 17
   2.4. Data structure of the eHRs .............................................................................. 23

Journal Paper .............................................................................................................. 27

Conclusion ..................................................................................................................... 51

References ................................................................................................................... 56

Appendix ....................................................................................................................... 61
Chapter 1

1. Introduction

1.1. What is eHealth

The World Health Organisation (WHO) states eHealth as \textit{the combined use of electronic communication and information technology in the health sector} (Eysenbach, 2001). In more practical terms, eHealth is the means of ensuring that the right health information is provided to the right person at the right place and time in a secure, electronic form for the purpose of optimising the quality and efficiency of health care delivery.

Electronic healthcare record (eHR) which integrates all relevant medical data of a patient and represents ultimate records of the medical history is the central aspect of eHealth. Thus eHR is not owned by any particular healthcare provider and comprises whole records of encounters of a patient throughout the visited healthcare organisations for that particular encounter.

1.2. Importance of eHRs

The following features of eHRs makes the eHealth a better solution for the healthcare system (IOM 2003):

- Simplicity: eHRs is a unique system which uses no paper for the patient’s medical records and treatment. In addition to that the online system enables easy backup procedures thus enhances the duration of the record system which helps to minimize the cost of record system for the patients.
- Effective in complex environments: eHRs exhibits efficiency in large scale system with many different components of the healthcare system thus it improvises the workflow in between the organizations.
- Better patient care: eHR system enables sharing of patient clinical records among the different clinics hence enable to provide better care by accessing the information in a very short period of time.
- Improve quality of care: eHR reduces the reporting time.
A Framework for Secured and Privacy Preserving eHealth System

- Reduce Healthcare Delivery Costs: eHR reduces the redundant medical examination cost by eliminating the repetitive costly test.
- Accelerates research and helps building effective medical practices: Due to eHR’s large database in one location helps disease surveillance and discovery of new drug.
- Better safety: Due to the structural framework i.e access control mechanism eHR offer better safety in contrast to the paper based system.

1.3. Evolution of eHRs:

Discrepancies among the residents of rural and city dweller’s in terms of health services have been a long issue which was addressed in 1990 by implementing the national eHealth policy. With a view to provide better health services the Establishment of National Health Information Management Advisory Council (NHIMAC) in 1999 was a step forward with some specific task to implementing the eHealth in Australia(NHIMAC, 2001). Later the implantation of HealthConnect by Australian Government was a bit step forward in the eHealth eliminating the difficulty of retrieving medical record data among the stakeholders thus improving the gap between public and private health system(Australian Government Department of Health and Ageing, 2008). During emergencies health professionals can access diagnoses, contacts and a medication list (HealthConnect, 2005). In the later stage which is in 2009, the National Health and Hospitals Reform Commission recommended the introduction of a personally controlled electronic health record (PCEHR) for each Australian to improve the quality safety and efficiency of healthcare.

1.4. The Start of the PCEHR

The PCHER is a shared electronic health summary by the Australian government which was implemented by the National Electronic Health Transition Authority (NEHTA).PCEHR is introduced to improve the privacy of sharing individual’s medical history (NEHTA, 2013). The introduction of PCEHR for a common platform by the Australian government with an aim to provide patients medical records obviously with the past and the present situations in a nutshell to facilitate the sharing the medical records among the stakeholders for the wellbeing of the patients but not to forget that the accessibility of the data controlled by the patient. In PCEHR, patient’s location does not matter for the treatment as patient’s records are shared
A Framework for Secured and Privacy Preserving eHealth System

electronically (Spriggs et al., 2012). As part of the 2010/11 Australian federal budget the Hon. Nicola Roxon (Minister for Health and Aging) announced the PCEHR as a "key building block of the National Health and Hospitals Network" (Department of Health and Ageing, 2011).

In April 2011 the draft concept and architecture of PCEHR was released and in the coming year i.e in 2012 the PCEHR was introduced by a government owned web based portal. It’s worthwhile to mention that the National eHealth Transition Authority constructed the main structure for the PCEHR but not limited to healthcare identifiers (for individuals, providers and provider organisations), secure messaging, the national security and access framework and national clinical terminologies (for example Australian medicines terminology) (NEHTA, 2011).

1.5. Motivation of Research:

So far, many research works have been developed to ensure the patient’s privacy. In most of them, the healthcare authority can get the permission to access the patient’s eHRs. Another thing is that, most of them don’t use the encrypted data when collecting and working with them. As a result, they are easily readable to everyone and hence vulnerable to different types of attacks. In this paper, we try to overcome those limitations and give the main concentration into the patient’s priority to access the control of eHRs for ensuring highest privacy.

In our research, we introduce a privacy oriented access control model for electronic health record systems. In our model, we provide full access control of eHRs to the patients only except the emergency situations. Sometimes professionals may intentionally leak out patient information for revenge, spite, profit, or other purposes. The proposed model ensures more privacy and security as well. In doing so, the proposed model suggests to encrypt data in all levels. Homomorphic encryption is suggested to protect the information privacy. Healthcare authority or any health professional can only get the permission to access the patient’s eHR after granted permissions from the patient. The access control mechanism in our proposed PCEHR model ensures the highest level of privacy for accessing patient’s eHRs.
A Framework for Secured and Privacy Preserving eHealth System

Though the existing PCEHR System enables the secure sharing of health information between an individual’s healthcare providers, whilst enabling the individual to control who can access their PCEHR, but the whole system must trust the system operators. As a result these data are vulnerable to be exploited by the authorised personnel in an immoral/unethical way. Furthermore, issues such as the sheer number of eHRs, their sensitive nature, flexible access, and efficient user revocation have remained the most important challenges towards fine-grained, cryptographically enforced data access control. In this paper we propose a patient centric cloud-based PCEHR framework, which employs a homomorphic encryption technique in storing the eHRs. The proposed system ensures the control of both access and privacy of eHRs stored in the cloud database.

1.6. Contribution of the Research

The major contributions of this research are:

- Proposing a conceptual framework of a privacy preserving eHealth model.
- Introducing a conceptual authentication method to enhance the patient’s privacy using the concept of multiple way authentications.
- Analysing the potential weakness of current RBAC model in healthcare in terms of security and flexibility and proposing a new framework for access control which is a hybrid model of DAC and extension of RBAC model.

1.7. Organisation of the Dissertation

The rest of the dissertation is organised into chapter 2, the Journal Paper and Conclusion. Chapter 2 is about related work on existing models of eHealth system. This chapter presents a thorough literature review on existing models for preserving privacy in eHealth systems, authentication and access control. The proposed framework of PCEHR system along with multi-factor, multi-channel authentication method and a hybrid access control method are described elaborately in the journal paper. proposed methods for enhancing the privacy and security of existing eHealth/PCEHR system. Conclusion includes the main contribution with analysis and the future work.
Chapter 2

2. Related Work on Existing Models of an eHealth System

2.1. Existing Models for Preserving Privacy in eHealth

Researchers have proposed several solutions to solve the security and privacy problems related to eHRs. Existing research work associated with privacy preserving techniques of patient eHRs can be categorized as i) Privacy by access control, and ii) Privacy by cryptographic approaches.

2.1.1. Privacy by Access Control

The key objective of access control mechanisms is to permit the authorised users to manipulate data and thus maintain the privacy of data (Barua, Liang, Lu, & Shen, 2011). However, the progresses are not satisfactory enough to fulfil the privacy requirements for eHRs (Santos-Pereira, Augusto, & Cruz-Correia, 2013).

Different access control mechanisms can be found in the literature (Alhaqabi & Fidge, 2007; Chen et al., 2012). Discretionary access control (DAC), mandatory access control (MAC), role based access control (RBAC), and purpose-based access control (PBAC) are the basic models of the access control principles.

DAC restricts access to objects based on the identity of subjects and/or groups to which they belong. However, in DAC granting read access is transitive and the policies are helpless for Trojan Horse Attack (Ferraiolo, Kuhn, & Chandramouli, 2003, Hu, Ferraiolo, & Kuhn, 2006).

MAC policy can prevent the Trojan Horse that occurs in DAC. MAC is based on access control policy decisions, made by a central authority (Ferraiolo et al., 2003, Sandhu & Samarati 1994). In MAC, the individual owner of an object has no right to control the access. Thus, MAC policy fails to preserve the privacy requirement for eHRs of the patients (Motta & Furuie, 2003).
RBAC (Park & Sandhu, 2002) models use consents and rights based on the assigned roles in groups/institutions to limit access. However, RBAC cannot integrate other access parameters or related data that are significant in allowing access to the user (Evered & Bögeholz, 2004).

PBAC is based on the notion of associating data objects with aims (Byun, Bertino & Li, 2005). PBAC has proven the greater privacy preservation by allocating objects with purposes (Naikuo, Howard & Ning 2007; Li, Yu, Ren & Lou 2010).

However, purpose administration creates a great deal of difficulty at the access control level. In Gajanayake et al. (2012), the authors combine three existing access control models and present a novel access control model for eHRs which satisfies the requirements of eHRs but the processes are more complex to implement.

2.1.2. Privacy by Cryptographic Approach

The cryptographic approach is considered one of the safest ways to preserve the security and the privacy of information in distributed settings. To transmit the data safely in cloud computing, cryptographic solutions are suitable enough by practicing the public key structure (Ding & Klein, 2010). Encrypting the private information before sending it to the cloud is an inherent need to a cloud user. But not all settings may allow that to happen. As mentioned in the previous section, in many systems the user has to trust the operator and gives the authority to their data by default. Many cryptographic solutions have now eliminated this requirement and ensure the full authority of the data is in the hand of its owner.

Here are the basic descriptions of some commonly used cryptographic approaches:

- SKC (Symmetric Key Cryptography)
- AKC (Asymmetric Key Cryptography)
- PKI (Public key Infrastructure)
- HE (Homomorphic Encryption)
- CP-ABE (Ciphertext policy attribute based encryption)
- KP-ABE (Key policy attribute based encryption)
- BACM (Biometric Access Control Method)
In our proposed eHealth model, we choose the fully Homomorphic Encryption (FHE) which is described below:

Homomorphic encryption is a special form of encryption where one can perform a specific algebraic operation on the plain-text by applying the same or different operation on the ciphertext. If \( x \) and \( y \) are two numbers and \( E \) and \( D \) denote encryption and decryption function respectively, then homomorphic encryption holds the following condition for an algebraic operation, such as \( + \):

\[
D[E(x)+E(y)] = D(E(x+y))
\]

Most homomorphic encryption system such as RSA, ElGamal, Benaloh, Paillier etc. are capable of performing only one operation. But the fully homomorphic encryption system can be used for many operations (such as addition, multiplication, division etc.) at the same time. In the area of cryptography, the fully homomorphic encryption (FHE) system proposed by Dijk, Gentry, Halevi & Vaikuntanathan (2010) is considered as a breakthrough work which can be used to solve many cryptographic problems. Key generation, encryption and decryption functions of this FHE are as follows:

\[\text{KeyGen} (\lambda) : \text{Choose a random } n\text{-bit odd integer } p \text{ as the private key. Using the private key, generate the public key as } x_i = pq_i + 2r_i \text{ where } q_i \text{ and } r_i \text{ are chosen randomly, for } i = 0, 1, ..., \tau. \text{ Rearrange } x - i \text{ such that, } x_0 \text{ is the largest.}\]

\[\text{Encrypt} (pk, m \in \{0, 1\}) : \text{Choose a random subset } S \subseteq \{1, 2, \ldots, \tau\} \text{and a random integer } r. m \text{ is encrypted to the cipher-text } c = (m + 2r + 2 \sum_{i \in S} x_i (mod x_0)). \text{ Let us denote this operation as } E_{pk}(m).\]

\[\text{Decrypt}(sk, c) : \text{The message } m \text{ is recovered simply by performing } m = (c mod p) mod 2. \text{ Let us denote this operation as } D_{sk}(c).\]

Further detail of this FHE can be found in Naehrig, Lauter, & Vaikuntanathan (2011).

In our proposed PCEHR framework, we will use this FHE technique to enable the system to perform computation on encrypted data. The patient will be the owner of the secret key therefore none can decrypt his/her health record; whereas, the user might be able to perform some edit or write operations on the record without knowing the content of the record itself. Figure 1 demonstrates how this FHE can be used in such a secure computation.
A Framework for Secured and Privacy Preserving eHealth System

Some text here...

Figure 1: A user can update a patients' record in the secured server without knowing the content of the record.

To deal with the potential risks of such privacy exposure, several eHealth systems (Benaloh Chase, Horvitz & Lauter, 2009; Jin Ahn, Hu, Covington & Zhang, 2009; Li et al., 2010) let patients encrypt their health record before storing it in the cloud. Van der Haak et al. (2003) use digital signatures and public-key authentication (for access control) to satisfy legal requirements for cross-institutional exchange of electronic patient records. Ateniese, Curtmola, de Medeiros & Davis (2002) use the concept of pseudonyms to preserve patient anonymity. Layouni, Verslype, Sandikkaya, De Decker & Vangheluwe (2009) consider communication between health monitoring equipment at a patient's home and the healthcare centre.

All these proposed solutions might preserve some of the privacy issues of a patient. They may require the encrypted data to be downloaded from the cloud to the patients' local machine when a modification or a computation might be necessary. This unreasonable requirement would ruin the sole purpose of using the cloud system. Therefore, these proposed solutions are impractical in PCEHR settings. Hence, an encryption-based practical solution for the PCEHR system is extremely important to ensure the full authority of the private data to its owner.

2.2. Authentication

2.2.1. What is Authentication?

The system by which verification of the user identity or data who wanted to access the system is attested is called Authentication. Authentication process engaged in affirming the identity of the person or the software tracking the root. The whole process is done by the authentication server which involved in affirming at least one form of identification.
The applications that used to authenticate the credentials of the users namely account name and password usually provided by the authentication server. In this authentication process clients entering a correct pair of credentials receive a cryptographic ticket to access to the services.

2.2.2. Existing authentication methods in eHealth

Computer security authentication means verifying the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics can be used to prove the identity of the user to the network.

National Authentication Service for Health (NASH) is responsible for strong security system of HealthConnect program for authentication in eHealth system in Australia. NASH service uses PKI infrastructure and multifactor authentication mechanism for issuing digital identities to the users of the network which is the same infrastructure as CA infrastructure (NEHTA, 2011).

The authors use a signature scheme, called a group signature, to allow a member of a group to anonymously sign an EHR. Authentication in distributed EHR systems has been also considered. Sun (Sun, 2010) proposes cross-domain authentication based on hierarchical identity-based public key infrastructure (HIB-PKI) to take advantage of the benefits of identity-based PKI in entities from the two domains. HIB-PKI avoids certificate-based PKI induced costs such as revocation, storage, distribution, and certificate verification (Al-Riyami and Paterson, 2003) and van der Linden et al. (2009) propose two means of authenticating.

Digital signature scheme based on PKI is mentioned by some authors (Hu, Chen and Hou, 2010; Sun, 2010; Quantin et al., 2011; Alhaqbani and Fidge, 2008; Sucurovic, 2010; Jafari, 2010) for authentication. Also some others access mechanisms depicted here are username/password (Benaloh, 2009; Neubauer and Heurix, 2011; Narayan, Gagné and Safavi-Naini, 2010; Jian, 2011), login/password combined with a digital certificate (Neubauer and Heurix, 2011; Jian, 2011; Lemaire et al., 2006; France, Bangels and De-Clercq, 2007; Alzharani et al., 2007), password and PIN (Ueckert and Prokosch, 2002; Ueckert et al., 2004), a smart card and its PIN (Riedl, Grascher and Neubauer, 2007; Riedl et al., 2007, 2008; France,
A Framework for Secured and Privacy Preserving eHealth System

Bangels and De-Clercq, 2007), a smart card, its PIN and a fingerprint (Hembroff & Muftic, 2010) and access policy spaces (Ardagna, 2010). Combination of username and a key proposed by Daglish and Archer (2009) engages the following methods (1) physical location as part of authentication; (2) the use of the Web and a security certificate of a trusted organization. In other proposed model by (Hu, Chen and Hou, 2010) founded on PKI based authentication protocol but the model could be stronger if biometric authentication system could be added. Some other author like Choe and Yoo (Choe and Yoo, 2008) have proposed different model which contains multi-agent architecture which permits access to authorised users and the safe exchange of patients’ data based on Web services. Zhang and Liu (2010) recommend the use of anonymous digital credentials in healthcare Clouds for authentication.

2.2.3. Research Need for a New Authentication System

Authentication is a necessary requirement in any information system to ensure the availability of information to authorized users only. The authentication mechanisms are developed using passwords, secret keys, tokens, and bio-metric features. The verification is performed based on credentials such as unique knowledge of the person being authenticated, a unique thing that the person has, unique personal features and attributes of the person, the ability of the person to respond, and to do so in a fashion that a machine cannot, and so forth. For this, various authentication methodologies have been developed to verify a party's identity prior to access the eHRs. Unfortunately, prior art methods all have weaknesses that can be exploited or that introduce burdens on users and managing organizations.

Most common form of verification of identity is password even though it’s vulnerable due to the possibility of replicate by means of observing the person typing, trial and error or copying from the communication. The PKI based authentication is provided by the dependable third party is a concern as well. Even though the biometrics can be imitated by means of lifting the fingerprints from glasses, bugged in communication and also recording the voice. In the process the more the robust and sophisticated the authentication system is the more awkward the system is for the user. Therefore the authentication system needed to be a secure, fast and elementary. So the authentication process described below engaged a combination of features which is fast, user friendly and secure.
2.3. Access Control

2.3.1. Existing access control models in eHealth

Based on the assessment by NEHTA in Australian healthcare sector in which they have proposed a model which deals with the privacy issues. Namely the unique healthcare identifiers (UHI) attest the user and provide legal access to the medical database (Privacy Study, 2011). Four kernel fields for identifying a person by NEHTA are name, date-of-birth, address, and sex. In the process of ensuring the identity of the person it engages the Medicare Database. National Registration and Accreditation Scheme (NRAS) is a program which is responsible for Registration and Accreditation of healthcare consumers and providers used by the HealthConnect program. NRAS accredited participants are trustworthy for the eHealth services.

The prominent access control models in eHealth are discretionary access control (DAC), mandatory access control (MAC) and role based access control (RBAC) by which it is defined what information each authenticated user can access described in section 2.2.1.

A DAC mechanism allows users to grant access to any of the objects under their control. MAC is a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity (NCSC, 1987). In its most simplistic view, RBAC – in an enterprise setting – associates users to different roles where every role is granted a proper set of permissions (i.e., operation on objects) necessary and sufficient to perform the job functions of any individual assuming that role (Shandhu et al., 1996). Role-based access control (RBAC) is a promising technology for managing and enforcing security in a large-scale distributed system. In the healthcare industry, RBAC has already been adopted by the Health Level Seven (HL7) organization as a key access control standard (Blobel & Marshall, 2005). Detail description of HL7 is discussed in section 2.4.1.

Although RBAC has been introduced to the latest version of HL7 (version 3) for strengthening the security features, it only includes those basic functions. Due to the complexity of the healthcare process, RBAC with only basic functions may not be sufficient. More context constraints need to be processed in addition to traditional RBAC operations. A context
constraint can help the organization provide more flexible and secure control for the RBAC model.

We propose a combined design for access control in healthcare information systems. As shown in Fig. 1, the access control process initiates with authentication as discussed in the previous section. According to our proposed model, access to medical record database is governed by RBAC, but the final access decision is made after examining pertinent context constraints. For handing delegation of access rights, we use a DAC based approach.

Discretionary access control

Discretionary Access Control uses access restriction set by the owner of the data object to restrict access to the objects. DAC models have some inherent drawbacks. A significant issue is the fact that a user who is allowed to access an object by the owner of the object has the capability to pass on the access right to other users without the involvement of the owner of the object. This will create inevitable privacy issues if the DAC policy is used in an eHR system. Another factor we have to consider is the ownership of the data. In healthcare we cannot clearly identify a single entity as the owner of health data. An initial argument would be that the patients are the owners of their own health data. But patients are not always health professionals and it is likely that the involvement of a health authority of a relevant sort is necessary. Due to these reasons it is difficult to use only a DAC policy and fulfill access and privacy requirements of all healthcare stakeholders.

Role-Based Access control

RBAC has become very popular in both research and industry. RBAC models have been shown to be “policy-neutral” in the sense that by using role hierarchies and constraints (Chandramouli, 2003), a wide range of security policies can be expressed. Security administration is also greatly simplified by the use of roles to organize access privileges. A brief description of basic RBAC model is given below, as well as an advanced model with context constraints.
Basic RBAC Model

The basic components of the RBAC model are user, role, and permission (Chen & Sandhu, 1996). The user is the individual who needs access to the system. Membership to the roles is granted to the user based on his or her obligations and responsibilities within the organization. All the operations that the user can perform should be based on the user’s role.

- Role means a set of functional responsibilities within an organization. The administrator defines roles, a combination of obligation and authority in organization, and assigns them to users. The user-role relationship represents the collection of users and roles.

- Permission is the way for the role to access more than one resource. As shown in Figure 2, the basic RBAC model also includes user assignment (UA) and permission assignment (PA) (INCITS359, 2003).

- The user assignment relationship represents which user is assigned to perform what kind of role in the organization. The administrator decides the user assignment relationship. When a user logs on, the system UA is referenced to decide which role it is assigned to. According to the object that the role wants to access, the permission can be assigned to the role referenced by the permission assignment relationship. The set of permissions (PRMS) is composed of the assignments between operations (OPS) and objects (OBS). UA and PA can provide great flexibility and granularity of assignment of permissions to roles and users to roles (INCITS359, 2003).

![Figure 2: Basic RBAC model](image-url)
The basic RBAC model has clearly illustrated the concept about how role-based access control works within an organization. However, it may not be dynamic enough when the business process becomes very complex. Thus, the idea of context constraints is introduced to make the RBAC model more useful.

RABC Model with context constraints

Traditional RBAC supports the definition of arbitrary constraints on the different parts of a RBAC model (Sandhu et al., 1996). With the increasing interest in RBAC in general and constraint-based RBAC in particular, research for other types of RBAC constraints has gained more attention (Bertino, Bonatt, & Ferrari, 2001). In this section, we describe the context constraints in an RBAC environment.

A context constraint is an abstract concept. It certain conditions in order to permit a specific operation. As authorization decisions are based on the permissions a particular subject/role possesses, context constraints are associated with RBAC permissions (see Figure 3). The context constraint is defined through the terms context attribute, context function, and context condition (Strembeck & Neumann, 2004). A context constraint is a clause containing one or more context conditions. It is satisfied if and only if (iff) all context conditions hold. Otherwise, it returns false.

A context constraint can be used to define conditional permissions. Based on the terms listed above, the conditional permission is a permission associated with one or more context constraints, and grants access iff each corresponding context constraint evaluates as “true.” As we can see, a context constraint can help the organization provide more flexible and securer control for the RBAC model.
2.3.2. Research Need for a new access control model

Access control is one of the basic safeguards against improper data access. Proper access control policies are a necessity for any EHR systems operation (Barua, Liang, Lu, & Shen, 2011). As basic models of access control cannot preserve the privacy of patient’s eHRs, some hybrid models, based on the basic model are proposed in the literature. Access control models that have been developed are insufficient to fulfill the requirements of eHR systems (Santos-Pereira, Augusto, & Cruz-Correia, 2013). This is due to the convoluted nature of the industry and the nature of the information used. To address this issue a specialized access control model has to be designed taking into consideration the different requirements of different users/entities involved.

Gajanayake et al. (2012) proposed a privacy oriented access control model for electronic health records. The model is designed by combining the above mentioned access control models with a purpose-based access control (PBAC) mechanism for data access by authorized users. They identified specific requirements of different healthcare stakeholders and combined the principles behind the DAC, MAC, RBAC and PBAC models to address them. According to their model, patients maintain an ACL of their trusted health professionals which is the
main concern of our research. Moreover, applying these four models to preserve the privacy in a large scale is very complex and less flexible in healthcare domain.

Shen (2009) design a flexible role-based access control model for a healthcare information system based on Health Level Seven version 3. The design utilizes the existing access control feature of Health Level Seven version 3 and integrates context constraints to make the system more secure and more flexible. The main drawback is there is no delegation right for the patient.

The most similar approach to our research is proposed by Khan and Sakamura (2012). They propose a combined access control scheme for healthcare information systems, amalgamating features of discretionary access control (DAC), role-based access control (RBAC) and context-aware access control. In their scheme, they introduce eTRON card for authentication and eTRON’s access control mechanism is based on access control lists. The scheme is dependent on physical device eTRON and for issuing the delegation token they have to rely on a trusted third party.

To overcome the above limitations, a new access control model is required. We propose a framework for access control in combination of DAC and RBAC model with context – constraint. The DAC model is used to capture the access settings for users by patients who maintain the ACL for the users.

The role engineering process in RBAC can be cumbersome, but once the roles are determined, it significantly reduces the complexity of security administration. It also supports review of permissions assigned to users, which aids determining risk exposure (resulting from employee system-access) by organizations which need this facility. The RBAC with context constraint seems to be the best as contextual attribute constraints can only reduce permissions available to user (thus imposing another layer of the desired least privilege principle), and thereby the system retains the RBAC capability to determine the maximum set of permissions that can be obtained by user (Sun, 2010). On the other hand, delegation, by nature, is discretionary and it is simpler to implement it using DAC as compared to approaches that try to retrofit delegation capability into RBAC.
2.4. Data structure of the eHRs

Information stored in an EHR may be clinical or administrative. Clinical information contains tabular records, images, scans, raw text, and so on. Administrative information contains information related to patient identification, demographic, insurance, encounters, financials, legal status, and so on. An EHR should be able to contain both structured and nonstructured data with suitable data types to represent all possible types of clinical information. It should be able to contain the information representation structure specified by various standards, coding systems, and terminologies. It should be possible to translate information in an EHR into any human readable language, keeping faithfulness and reliability of original information.

2.4.1. EHR Standard

Over the past several years, several countries have made efforts to develop electronic health record models and systems to maintain it. ISO/TC 215 is a Technical Committee (TC) of ISO (International Organisation for Standardization) working in the area of Health Informatics. Its primary goal is to standardize health information and achieve interoperability across EHR systems. It has published various standards which include data structures, messaging and communications, privacy and security, devices, and so on. It also published ISO/TS 18308, which defines a common specification for EHR architecture.

The Australian Health Ministry established the National e-Health Transition Authority (NEHTA) Limited, for developing national e-health standards and infrastructure requirements for electronic collection and secure exchange of health. It works with healthcare consumers, providers, decision makers and the entire healthcare industry to enable healthcare delivery through e-health (Williams and Howard 2010). The NEHTA works on identified priority areas in healthcare delivery. It develops reference data specifications for these priority areas. Along with the specification of clinical model, it also addresses like security, privacy, and legal and ethical aspects of eHealth in Australia (NEHTA 2006; NEHTA 2011).

The structural model suggested by the NEHTA adheres to the standard specifications given by Standards Australia, which is a Government of Australia recognized standardization body. The Good Electronic Health Record (GEHR) was in use in Australia since the year 2000. The GEHR later evolved as openEHR. NEHTA used GEHR to evolve Structured Document
Template (SDT) whose data types exactly map with the GEHR data types. SDT describes the specifications for organizing data elements used for storing and retrieving health information.

The NEHTA conducted a research study on evaluating existing interoperability standards[Interoperability Study 2007]. It initially suggested supporting the HL7 v2.x standard. The primary purpose was to speed up the e-transition of healthcare services. Keeping this in mind, it suggested the use of Service Oriented Architecture (SOA) in making healthcare services available to the users. The NEHTA suggested that gradually newer versions of HL7 standards are to be used for exchange of clinical information as and when they are widely accepted. The NEHTA researched various clinical events in healthcare practices and evolved SDT which is analogous to HL7’s CDA standard. This template can be used AS-IS for recording data in healthcare events or can be extended as per requirements. Currently NEHTA suggests using the CDA standard for representing this information.

HL7 HER-S Functional Model provides the functional requirements of an EHR system. It describes the various functional profiles categorized as Direct Care, Supportive Functions and Information Infrastructure that individually enlist the various functions involved in patient care management, clinical decision support, administration and financial management, security, record management, registry and standard terminology and related services. It can be used for analysing and evaluating the functions that should be present in an EHR system.

HL7 v2x standard facilitates exchange of data across healthcare applications. The standard has a notion of information model that is given as message exchange format and not EHR model. The message exchange format is not based on object-oriented development. Though it provides the flexibility of defining one’s own field set in messages, it makes it harder to achieve interoperability.

HL7 v3 was developed to address the shortcomings in HL7 v2.x and is based on object-oriented methodology. It provides a Reference Information Model (RIM) and Vocabulary Domain that describes the contents and content types in an HER for exchange. It uses XML for data exchange. HL7 v3 is widely used for data exchange in recently implemented eHR systems and nationwide HER implementations.
CDA is an XML document based standard that uses the basic components of HL7 v3 RIM. It provides a document structure based on Sections, Headings, and Contents and so on.

NEHTA recommendations in Australia appear to be HL7 standards-specific. However, there are other exchange standards such as NEMA’S DICOM and ASTM CCR, which need to be evaluated. The NEHTA suggested the use of customized version of SSNOMED CT for Australia in healthcare practices.

DICOM is a widely used standard for medical image exchange in medical devices. Hence to integrate data from such systems, adoption of DICOM in HER is a primary step toward achieving interoperability and a uniform device interface mechanism. It is one of the most comprehensive standards in radiology/pathology domain. On the other hand, CCR is helpful in identifying clinical record types in an HER system. The CCR Information Model provides the content structure and types for developing patient transfer and discharge summaries.

Here, HL7 v2x focuses on exchange of clinical data but HL7 v3 covers the specification for the information model. And DICOM gives emphasis on image data transfer.

### 2.4.2. Coding Systems

Different coding terminologies and classifications are included to understand each one’s applicable scope in the development of models for electronic health record. The use of coding systems in electronic health records support semantic interoperability and decision making. Hence, developing data representation structures for each of the coding standards in the electronic health record is important. There should be a single data representation structure that can accommodate values of existing and future code sets. Some existing coding systems are:

- **ICD**: ICD provides the classification and groupings of diseases and related health problems. Lack of details regarding diagnostic procedures in ICD codes made healthcare bodies build expanded versions of ICD codes such as ICD-9-CM, ICD-10-CM for clinical modifications and ICD-10-PCS for supporting procedure codes. ICD can be used in EHR frameworks to incorporate disease names and symptoms from the health problems recorded in an HER.
LOINC: It is universally used to identify laboratory tests, results, and clinical observations. It is adopted in almost all the studied national HER programs.

CPT: It provides standardized code set for medical procedures or services performed during healthcare activities. It is best suited for use in financial transactions and legal considerations in medical procedures that help in managing administrative, financial and legal processes in a healthcare environment.

HCPCS: It extends CPT’s code set to provide codes for standardizing external health services carried out during healthcare service delivery such as supplies, pharmacies, medical equipment, and so on. These codes can be used to interpret insurance-related information in an EHR.

SNOMED CT: It is a comprehensive terminology as compared to other coding systems. Many standards and frameworks such as HL7 v3 and openEHR have provided integration of SNOMED CT. It provides extensive support for technical implementation of coding terminology that facilitates rapid developments of these codes in software applications.

UMLS: It specifically targets mapping between existing coding terminologies. It provides mapping with almost all existing coding systems. Hence, in EHR system design, UMLS can be considered as a framework for proving mapping between coding systems rather than a coding system database.

In a heterogeneous standards-based model of EHR, searching for similar terms and concepts should be provided across different code sets. For example, a search query for a record representing an ICD code should also search for records with similar SNOMED CT code. This task raises the need for providing the mapping between similar terms and concepts represented by different code sets where a framework like UMLS can be used.

The structural details of Data Groups and Data Elements are not available in public domain. But the example available help in understanding the structure of various records types in an EHR.
Journal Paper

The following journal paper was submitted as a requirement of the dissertation. The research work was submitted in the The Electronic Journal of Information Systems (EJISE) which is an ERA Ranked B Journal. Moreover, the Journal is listed as level 1 in the Danish Government bibliometric lists.

A Conceptual Framework of Personally Controlled Electronic Health Record (PCEHR) System to Enhance Security and Privacy

Mahmuda Begum, and Quazi Mamun
Charles Sturt University, Wagga Wagga, NSW, Australia
mbegum@csu.edu.au
qamun@csu.edu.au

Abstract: In recent times, the electronic health record (eHR) system is regarded as one of the biggest developments in healthcare domains. A personally controlled electronic health record (PCEHR) system, offered by the Australian government makes the health system more agile, reliable, and sustainable. Although the existing PCEHR system is fully controlled by the patients, but there is a way for healthcare professionals and database/system operators to reveal the records for corruption as system operators are assumed to be trusted by default. Moreover, as a consequence of increased threats to security of electronic health records, an actual need for a strong and effective authentication and access control methods has raised. In cloud computing, proper authentication technique is the basic of security. So, it is essential to admit that only authorized users are allowed to access the corresponding patients’ records. There are many authentication schemes but they are considered vulnerable techniques in cloud environment. Furthermore, due to the sensitive nature of eHRs, the most important challenges towards fine-grained, cryptographically implemented access control schemes which guarantee data privacy and reliability, verifying that only authorized people can access the corresponding health records. Moreover, an uninterrupted application of the security principle of electronic data files necessitates encrypted databases. In this paper we concentrates the above limitations together by proposing a robust authentication scheme and a hybrid access control model to enhance the security and privacy of eHRs. Homomorphic encryption technique is applied in storing and working with the eHRs in our proposed cloud-based PCEHR framework. The proposed model ensures the control of both security and privacy of eHRs accumulated in the cloud database.

Keywords: e-health, electronic health record, PCEHR, homomorphic encryption, authentication, access control.
1. Introduction

eHealth has recently been considered a precipitately changing segment of the healthcare industry. eHealth is defined in many ways such as the transfer of health resources and healthcare by electronic means. According to The World Health Organisation (WHO), eHealth is defined as the combined use of electronic communication and information technology in the health sector (Eysenbach, 2001). The recently proposed Australian government’s personally controlled electronic health record (PCEHR) system is one of the best examples of eHealth system implementation (National E-Health Transition Authority Australia, 2011).

The electronic healthcare record (eHR) is the principle aspect of an eHealth system such as PCEHR. eHR is the digitally stored healthcare information about an individual’s lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times (Gajanayake, Iannella, & Sahama, 2012). eHRs aid efficient communication of medical data and thus ease organisational disbursements with the help of cloud computing (Muhammad, Zwicker, & Wickramasinghe, 2013, Wu, Ahn, & Hu, 2012).

However, privacy in particular, has always been one of the main concerns in eHealth systems (Petkovic & Ibraimi, 2011, Xanthidis & Aleisa, 2012). According to Richard Rognehaugh, privacy is the right of individuals to keep information about themselves from being disclosed to others (Rognehaugh, 1999). The information that is shared as a result of a clinical relationship is considered confidential and must be protected (Rinehart-Thompson & Harman, 2006). Health credentials such as sexual health, mental health, addictions to drug or alcohol, abortions constitute eHR system which required substantial privacy. To sustain privacy of the patients data it’s necessary to restrict patients control to their private data as patients withholding or trying to delete sensitive medical information from their eHRs (Klitzman, 2006). Although healthcare professionals also poses privacy risk in complex eHR systems by making disclosure of a patient’s information.

On the other hand, a system operator may intentionally leak out patients’ information for revenge, spite, profit, or other ill purposes. Risks from inadvertent or intentional release of infectious, mental health, chronic disease diagnoses, and genetic information are all well recognized both online and in mass media. In the conventional privacy preserving techniques, system operators are assumed to be trusted. But in some cases, they may not be reliable. Therefore, we need to construct such a system to eliminate the above assumption. In addition, an eHR system needs to be able to deal effectively with a very high volume of patients’ sensitive data along with ensuring user authentication, role based access control, and patients’ authorisation. Thus, a multi-level security system is required to protect the privacy of eHRs.

Authentication of users and access control to health information are two most important aspects for maintaining multi-level security in healthcare systems. These two security requirements are also closely interlinked; in fact, the most comprehensive definition of access control includes authentication (i.e., corroborating the identity of the user) as a pre-requisite to making access decision (Karp, Haury and Davis; 2009). Again, Authentication considers a significance element of...
security in healthcare domain, aiming to verify a user’s identity when a user wishes to request services from cloud. Access control includes two primary aspects, namely to deny access to healthcare data to those users who do not have the right of access and, secondly, they need to guarantee access to all relevant data to those database users who exercise their access privilege properly. Focusing on this synergy between authentication and access control, in this paper, we propose a framework for authentication and a hybrid model for access control, using the multi-channel authentication concept and incorporating the context constraint with conventional access control models.

To address all the above mentioned issues, in this paper, we propose a framework to access patients’ eHRs. This patient centric framework employs a homomorphic encryption technique in storing and updating the eHRs. The encryption system allows computation on cipher text, thus eliminates the dependency on trusted third parties or system operators. In this framework, the encrypted eHRs residing in the cloud server are accessed by different users through multi-level security procedures.

2. Related Work

Researchers have proposed several solutions to solve the security and privacy problems related to eHRs.

Existing research work associated with privacy preserving techniques of patient eHRs can be categorized as i) Privacy by access control, and ii) Privacy by cryptographic approaches

2.1 Privacy by Access Control

The key objective of access control mechanisms is to permit the authorised users to manipulate data and thus maintain the privacy of data (Barua, Liang, Lu, & Shen, 2011). However, the progresses are not satisfactory enough to fulfill the privacy requirements for eHRs (Santos-Pereira, Augusto, & Cruz-Correia, 2013).

Different access control mechanisms can be found in the literature (Alhaqebani & Fidge, 2007; Chen et al., 2012). Discretionary access control (DAC), mandatory access control (MAC), role based access control (RBAC), and purpose-based access control (PBAC) are the basic models of the access control principles.

DAC restricts access to objects based on the identity of subjects and/or groups to which they belong. However, in DAC granting read access is transitive and the policies are helpless for Trojan Horse Attack (Ferraiolo, Kuhn, & Chandramouli, 2003, Hu, Ferraiolo, & Kuhn, 2006).

MAC policy can prevent the Trojan Horse that occurs in DAC. MAC is based on access control policy decisions, made by a central authority (Ferraiolo et al., 2003, Sandhu & Samarati 1994). In MAC, the individual owner of an object has no right to control the access. Thus, MAC policy fails to preserve the privacy requirement for eHRs of the patients (Motta & Furuike, 2003).
RBAC (Park & Sandhu, 2002) models use consents and rights based on the assigned roles in groups/institutions to limit access. However, RBAC cannot integrate other access parameters or related data that are significant in allowing access to the user (Evered & Bögeholz, 2004).

PBAC is based on the notion of associating data objects with aims (Byun, Bertino & Li, 2005). PBAC has proven the greater privacy preservation by allocating objects with purposes (Naikuo, Howard & Ning 2007; Li, Yu, Ren & Lou 2010).

However, purpose administration creates a great deal of difficulty at the access control level. In Gajanayake et al. (2012), the authors combine three existing access control models and present a novel access control model for eHRs which satisfies the requirements of eHRs but the processes are more complex to implement.

2.2 Privacy by Cryptographic Approach

The cryptographic approach is considered one of the safest ways to preserve the security and the privacy of information in distributed settings. To transmit the data safely in cloud computing, cryptographic solutions are suitable enough by practicing the public key structure (Ding & Klein, 2010). Encrypting the private information before sending it to the cloud is an inherent need to a cloud user. But not all settings may allow that to happen. As mentioned in the previous section, in many systems the user has to trust the operator and gives the authority to their data by default. Many cryptographic solutions have now eliminated this requirement and ensure the full authority of the data is in the hand of its owner.

To deal with the potential risks of such privacy exposure, several eHealth systems (Benaloh Chase, Horvitz & Lauter, 2009; Jin Ahn, Hu, Covington & Zhang, 2009; Li et al., 2010) let patients encrypt their health record before storing it in the cloud. Van der Haak et al. (2003) use digital signatures and public-key authentication (for access control) to satisfy legal requirements for cross-institutional exchange of electronic patient records. Ateniese, Curtmola, de Medeiros & Davis (2002) use the concept of pseudonyms to preserve patient anonymity. Layouni, Verslype, Sandikkaya, De Decker & Vangheluwe (2009) consider communication between health monitoring equipment at a patient’s home and the health-care centre.

All these proposed solutions might preserve some of the privacy issues of a patient. They may require the encrypted data to be downloaded from the cloud to the patients’ local machine when a modification or a computation might be necessary. This unreasonable requirement would ruin the sole purpose of using the cloud system. Therefore, these proposed solutions are impractical in PCEHR settings.

2.3 Existing Authentication Methods in eHealth

National Authentication Service for Health (NASH) is responsible for strong security system of HealthConnect program for authentication in eHealth system in Australia. NASH service uses PKI
A Framework for Secured and Privacy Preserving eHealth System

infrastructure and multifactor authentication mechanism for issuing digital identities to the users of the network which is the same infrastructure as CA infrastructure (NEHTA, 2011).

The authors use a signature scheme, called a group signature, to allow a member of a group to anonymously sign an EHR. Authentication in distributed EHR systems has been also considered. Sun (Sun, 2010) proposes cross-domain authentication based on hierarchical identity-based public key infrastructure (HIB-PKI) to take advantage of the benefits of identity-based PKI in entities from the two domains. HIB-PKI avoids certificate-based PKI induced costs such as revocation, storage, distribution, and certificate verification (Al-Riyami and Paterson, 2003) and van der Linden et al. (2009) propose two means of authenticating.

Digital signature scheme based on PKI is mentioned by some authors (Hu, Chen and Hou, 2010; Sun, 2010; Quantin et al., 2011; Alhaqabani and Fidge, 2008; Sucurovic, 2010; Jafari, 2010) for authentication. Also some others access mechanisms depicted here are username/password (Benaloh, 2009; Neubauer and Heurix, 2011; Narayan, Gagné and Safavi-Naini, 2010; Jian, 2011), login/password combined with a digital certificate (Neubauer and Heurix, 2011; Jian, 2011; Lemaire et al., 2006; France, Bangels and De-Clercq, 2007; Al-zharani et al., 2007), password and PIN (Ueckert and Prokosch, 2002; Ueckert et al., 2004), a smart card and its PIN (Riedl, Grascher and Neubauer, 2007; Riedl et al., 2007, 2008; France, Bangels and De-Clercq, 2007), a smart card, its PIN and a fingerprint (Hembroff & Muftic, 2010) and access policy spaces (Ardagna, 2010). Combination of username and a key proposed by Daglish and Archer (2009) engages the following methods (1) physical location as part of authentication; (2) the use of the Web and a security certificate of a trusted organization. In other proposed model by (Hu, Chen and Hou, 2010) founded on PKI based authentication protocol but the model could be stronger if biometric authentication system could be added. Some other author like Choe and Yoo (Choe and Yoo, 2008) have proposed different model which contains multi-agent architecture which permits access to authorised users and the safe exchange of patients’ data based on Web services. Zhang and Liu (2010) recommend the use of anonymous digital credentials in healthcare Clouds for authentication.

Authentication is definitely a necessary requirement in any information system to ensure the availability of information to authorized users only. The authentication mechanisms are developed using passwords, secret keys, tokens, and bio-metric features. The verification is performed based on credentials such as unique knowledge of the person being authenticated, a unique thing that the person has, unique personal features and attributes of the person, the ability of the person to respond, and to do so in a fashion that a machine cannot, and so forth. For this, various authentication methodologies have been developed to verify a party's identity prior to access the eHRs. Unfortunately, prior art methods all have weaknesses that can be exploited or that introduce burdens on users and managing organizations which are described below.

Most common form of verification of identity is password even though it’s vulnerable due to the possibility of replicate by means of observing the person typing, trial and error or copying from the communication. The PKI based authentication is provided by the dependable third party is a concern.
as well. Even though the biometrics can be imitated by means of lifting the fingerprints from glasses, bugged in communication and also recording the voice. In the process the more the robust and sophisticated the authentication system is the more awkward the system is for the user. Therefore the authentication system needed to be a secure, fast and elementary. So the authentication process described below engaged a combination of features which is fast, user friendly and secure.

2.4 Existing Access Control Methods in eHealth

Based on the assessment by NEHTA in Australian healthcare sector in which they have proposed a model which deals with the privacy issues. Namely the unique healthcare identifiers (UHI) attest the user and provide legal access to the medical database (Privacy Study, 2011). Four kernel fields for identifying a person by NEHTA are name, date-of-birth, address, and sex. In the process of ensuring the identity of the person it engages the Medicare Database. National Registration and Accreditation Scheme (NRAS) is a program which is responsible for Registration and Accreditation of healthcare consumers and providers used by the HealthConnect program. NRAS accredited participants are trustworthy for the eHealth services.

The prominent access control models in eHealth are discretionary access control (DAC), mandatory access control (MAC) and role based access control (RBAC) by which its defined what information each authenticated user can access.

A DAC mechanism allows users to grant access to any of the objects under their control. MAC is a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity (NCSC, 1987). In its most simplistic view, RBAC – in an enterprise setting – associates users to different roles where every role is granted a proper set of permissions (i.e., operation on objects) necessary and sufficient to perform the job functions of any individual assuming that role (Shandhu et al., 1996). Role-based access control (RBAC) is a promising technology for managing and enforcing security in a large-scale distributed system. In the healthcare industry, RBAC has already been adopted by the Health Level Seven (HL7) organization as a key access control standard (Blobel & Marshall, 2005).

Although RBAC has been introduced to the latest version of HL7 (version 3) for strengthening the security features, it only includes those basic functions. Due to the complexity of the healthcare process, RBAC with only basic functions may not be sufficient. More context constraints need to be processed in addition to traditional RBAC operations. A context constraint can help the organization provide more flexible and securer control for the RBAC model. In the following section, we briefly describe the basic RBAC model and RBAC with context constraint.

Role-Based Access control

RBAC has become very popular in both research and industry. RBAC models have been shown to be “policy-neutral” in the sense that by using role hierarchies and constraints (Chandramouli, 2003), a wide range of security policies can be expressed. Security administration is also greatly simplified by
the use of roles to organize access privileges. A brief description of basic RBAC model is given below, as well as an advanced model with context constraints.

**Basic RBAC Model**

The basic components of the RBAC model are user, role, and permission (Chen & Sandhu, 1996). The user is the individual who needs access to the system. Membership to the roles is granted to the user based on his or her obligations and responsibilities within the organization. All the operations that the user can perform should be based on the user’s role.

- **Role** means a set of functional responsibilities within an organization. The administrator defines roles, a combination of obligation and authority in organization, and assigns them to users. The user-role relationship represents the collection of users and roles.
- **Permission** is the way for the role to access more than one resource. As shown in Figure 1, the basic RBAC model also includes user assignment (UA) and permission assignment (PA) (INCITS359, 2003).
- **The user assignment relationship** represents which user is assigned to perform what kind of role in the organization. The administrator decides the user assignment relationship. When a user logs on, the system UA is referenced to decide which role it is assigned to. According to the object that the role wants to access, the permission can be assigned to the role referenced by the permission assignment relationship. The set of permissions (PRMS) is composed of the assignments between operations (OPS) and objects (OBS). UA and PA can provide great flexibility and granularity of assignment of permissions to roles and users to roles (INCITS359, 2003).

![Basic RBAC Model](image)

**Figure 1. Basic RBAC Model**

The basic RBAC model has clearly illustrated the concept about how role-based access control works within an organization. However it may not be dynamic enough when the business process becomes very complex. Thus the idea of context constraints is introduced to make the RBAC model more useful.
RABC Model with context constraints

Traditional RBAC supports the definition of arbitrary constraints on the different parts of a RBAC model (Sandhu et al., 1996). With the increasing interest in RBAC in general and constraint-based RBAC in particular, research for other types of RBAC constraints has gained more attention (Bertino, Bonatt, & Ferrari, 2001). In this section we describe the context constraints in an RBAC environment.

A context constraint is an abstract concept. It certain condition in order to permit a specific operation. As authorization decisions are based on the permissions a particular subject/role possesses, context constraints are associated with RBAC permissions (see Figure 2). The context constraint is defined through the terms context attribute, context function, and context condition (Strembeck & Neumann, 2004). A context constraint is a clause containing one or more context conditions. It is satisfied if and only if (iff) all context conditions hold. Otherwise it returns false.

A context constraint can be used to define conditional permissions. Based on the terms listed above, the conditional permission is a permission associated with one or more context constraints, and grants access iff each corresponding context constraint evaluates as “true.” As we can see, a context constraint can help the organization provide more flexible and securer control for the RBAC model.

Gajanayake et al. (2012) proposed a privacy oriented access control model for electronic health records. The model is designed by combining the afore mentioned access control models with a purpose based access control (PBAC) mechanism for data access by authorised users. They identified specific requirements of different healthcare stakeholders and combined the principles behind the DAC, MAC, RBAC and PBAC models to address them. According to their model, patients maintain an ACL of their trusted health professionals which is the main concern of our research. Moreover, applying these four models to preserve the privacy in a large scale is very complex and less flexible in healthcare domain.
Shen (2009) design a flexible role-based access control model for a healthcare information system based on Health Level Seven version 3. The design utilizes the existing access control feature of Health Level Seven version 3 and integrates context constraints to make the system more secure and more flexible. The main drawback is there is no delegation right for the patient.

The most similar approach to our research is proposed by Khan and Sakamura (2012). They propose a combined access control scheme for healthcare information systems, amalgamating features of discretionary access control (DAC), role-based access control (RBAC) and context-aware access control. In their scheme, they introduce eTRON card for authentication and eTRON's access control mechanism is based on access control lists. The scheme is dependent on physical device eTRON and for issuing the delegation token they have to rely on a trusted third party.

To overcome the above limitations, a new access control model is required. We propose a framework for access control in combination of DAC and RBAC model with context-constraint. The DAC model is used to capture the access settings for users by patients who maintain the ACL for the users.

The role engineering process in RBAC can be cumbersome, but once the roles are determined, it significantly reduces the complexity of security administration. It also supports review of permissions assigned to users, which aids determining risk exposure (resulting from employee system-access) by organizations which need this facility. The RBAC with context constraint seems to be the best as contextual attribute constraints can only reduce permissions available to user (thus imposing another layer of the desired least privilege principle), and thereby the system retains the RBAC capability to determine the maximum set of permissions that can be obtained by user (Sun, 2010). On the other hand, delegation, by nature, is discretionary and it is simpler to implement it using DAC as compared to approaches that try to retrofit delegation capability into RBAC.

We propose a combined design for access control in healthcare information systems. The access control process initiates with authentication as discussed in the previous section. According to our proposed model, access to medical record database is governed by RBAC, but the final access decision is made after examining pertinent context constraints. For handing delegation of access rights, we use a DAC based approach.

Hence, an encryption-based practical solution with appropriate authentication and access control model for the PCEHR system is extremely important to ensure the full authority of the private data to its owner.
3. The Proposed Overall Model

In this section we describe the proposed cloud-based PCEHR model using homomorphic encryption, which is briefly discussed below.

**Fully Homomorphic Encryption (FHE)**

Homomorphic encryption is a special form of encryption where one can perform a specific algebraic operation on the plain-text by applying the same or different operation on the cipher-text. If \( x \) and \( y \) are two numbers and \( E \) and \( D \) denote encryption and decryption function respectively, then homomorphic encryption holds the following condition for an algebraic operation, such as ‘\( + \)’:

\[
D[E(x)+E(y)] = D[E(x+y)]
\]

Most homomorphic encryption systems such as RSA, ElGamal, Benaloh, Paillier etc. are capable of performing only one operation. But the fully homomorphic encryption system can be used for many operations (such as addition, multiplication, division etc.) at the same time. In the area of cryptography, the fully homomorphic encryption (FHE) system proposed by Dijk, Gentry, Halevi & Vaikuntanathan (2010) is considered as a breakthrough work which can be used to solve many cryptographic problems. Key generation, encryption and decryption functions of this FHE are as follows:

*KeyGen* (\( \lambda \)) : Choose a random \( n \)-bit odd integer \( p \) as the private key. Using the private key, generate the public key as \( x_i = pq_i + 2r_i \) where \( q_i \) and \( r_i \) are chosen randomly, for \( i = 0, 1, ..., \tau \). Rearrange \( x - i \) such that, \( x_0 \) is the largest.

*Encrypt* \((pk, m \in \{0, 1\})\) : Choose a random subset \( S \subseteq \{1, 2, ..., \tau\} \) and a random integer \( r \). \( m \) is encrypted to the cipher-text \( c = (m + 2r + 2 \sum_{i \in S} x_i \mod x_0) \). Let us denote this operation as \( E_{pk}(m) \).

*Decrypt* \((sk, c)\) : The message \( m \) is recovered simply by performing \( m = (c \mod p) \mod 2 \). Let us denote this operation as \( D_{sk}(c) \).

Further detail of this FHE can be found in Naehrig, Lauter, & Vaikuntanathan (2011).

In this proposed PCEHR framework, we will use this FHE technique to enable the system to perform computation on encrypted data. The patient will be the owner of the secret key therefore none can decrypt his/her health record; whereas, the user might be able to perform some edit or write operations on the record without knowing the content of the record itself. Figure 3 demonstrates how this FHE can be used in such a secure computation.
Figure 3. A user can update a patients’ record in the secured server without knowing the content of the record.

3.1 Architecture of the Proposed Model

A simplified architecture of the proposed model is shown in Figure 4. The model consists of several entities. These entities are briefly described below:

a. User of Patients’ eHR: In the proposed model, the user refers to any person/organization that needs to access the patients’ eHRs. Thus, the term ‘user’ includes a general practitioner (GP), specialist, pharmacist, nurse, healthcare provider, provider/health insurance company, diagnostic laboratory, hospital, research personnel, family member or relative of the patient. The purpose of the user may differ according to their role, such that a GP might need to access the previous records for making a prescription, whereas a diagnostic lab may need to store a report against a patient only.

b. Authentication Server: Authentication server ensures legitimate access in to the network of the model. The authentication process is usually based on passwords. However, different types of information such as biometric information, rather than text based information, can also be used in the authentication process. Usually every user needs to be registered in the system by associated authority. Other algorithms such as the challenge response protocol, Kerberos, and public key encryption can be used by the authentication server.

c. Access Control List (ACL) Server: The main purpose of this server is to verify when users want to access a specific sub-profile of eHRs of the patients. After a user is authenticated in the system, the access control list server applies access control policies/rules correlated with the authenticated users. Access policies can be defined as relationships between subjects, objects and actions. For example, a pathology lab technician usually does not need to access a patient’s mental health eHRs, or insurance company personnel does not need to modify patient’s disease history. The ACL list also specifies how a user can access an object class of a patients’ eHRs, in other words, the actions that the user can perform on a sub-profile, e.g. read, write, etc.
A Framework for Secured and Privacy Preserving eHealth System

Figure 4. Simplified architecture of the proposed model

d. **Authorisation Server:** After passing through the authentication and ACL servers, users need to be authorised by a patient through an authorisation server to access specific eHRs of the patient. The ACL server confirms the eHR class (known as sub-profile) accessibility, while authorisation confirms a particular object of that eHR class. If a patient provides permission to a user, the authorisation server will issue a token using the encrypted data which can be retrieved from the database server. The encrypted data can be decrypted by the patient’s private key only.

Figure 5 shows how the ACL and the authorisation servers allow users to access patients’ sub-profiles and eHRs. The figure shows four patients P1, P2, P3 and P4. Each patient owns a profile. A patient’s profile is divided into several sub-profiles, such as mental health, sexual health, physical health, personal information etc. The privacy policy dictates which professionals (known as user in the proposed model) are permitted to access which sub-profiles of the patients. For example, Figure 3 shows that the trainer is authorised via the ACL server to deal with patients’ personal information and
physical health. However, the trainer does not have any privilege to access patients’ sexual health or mental health. After accessing through the ACL server, the user waits for a patient’s exclusive permission to access the eHR of the patient. Figure 3 also shows that the psychiatrist receives permissions to access P1’s mental health, the trainer receives permission to access P2’s physical health. Although verified by the ACL server to access physical health sub-profiles of patients, the trainer cannot access P1’s physical health.

![Figure 5: An overview of the function of the authorisation server](image)

**e. Patient**: The patient may be defined as the owner of his/her medical data and therefore holds full rights on the access control of his/her data. In our proposed model, only the patient has the key to decrypt the data and hence without the patient’s consent no-one can access the eHRs. This means that the patient must be able to access the information about all types of data transfer, its purpose and its user. In addition, the patient must receive all the notifications whenever someone uses or access the records.

**f. Cloud Storage**: Scalability would be one of the challenges of eHR system, because the system needs to handle millions of patients’ electronic health records. For example, body are networks (BANs) are recently been proposed to monitor patients’ health. BANs sense, generate, and send monitoring data to the healthcare system. Indeed, the sampling is performed at high frequency, which increases the amount of collected data. In addition, the frequency of sampling is often increased if the condition of patients being monitored gets worse. The amount, size, and heterogeneity of data drive a need for an increasing storage and processing capacities. Besides scalability issues, medical data could be lifesaving and must be accessible at any time and from everywhere. Existing solutions rely on a
centralized paradigm to store and process sensed data thus cannot tackle the aforementioned challenges. Thus, we need new innovative solutions to meet the great challenges of handling the exponential growth in data. We leverage cloud computing technology to dynamically scale storage resources via on demand provisioning. Cloud service providers can be any type of internet provider or application that lives in the cloud and is accessed online. As encrypted data is used in our model, the providers do not know the original records.

**g. Encrypted Database Server:** A database server can be referred to as the back-up system of a database usage client/server structure. A database server accomplishes several tasks such as data analysis, storage, data handling, archiving, and other non-user specific tasks. In the cloud environment, eHRs are always vulnerable to attacks. Encryption of the database server helps us prevent unauthorised access to information database. Applying the homomorphic encryption technique, we can ensure the privacy of the eHRs of the patient.

**h. System Operators:** According to the PCEHR system, the system operator is the entity that is responsible for generating and operating the PCEHR system. The system operator must respect the instructions and recommendations (if any) during their duties given by the PCEHR Jurisdictional Advisory Committee and the PCEHR Independent Advisory Council (2013).

In general, system operators are either persons or machines who oversee the operation of a large computer network. So, system operators enable access to the database as it is assumed that they are always trusted authority. In our proposed model, we use cryptographic solutions to encrypt the central database. This is done by the encryption mechanism which can support addition and multiplication of the encrypted data. One instance of data access method is depicted in Figure 6.

![Diagram](Image)

**Figure 6:** Accessing patient’s eHR by a user (doctor)
Many encryption techniques support one of these operations, either addition or multiplication like the encryption schemes in Rivest, Shamir & Adleman, 1978; El Gamal, 1985; Goldwasser & Micali, 1984; Paillier, 1999. A cryptosystem which supports both addition and multiplication (homomorphic) can be successful for data security, and supports the creation of programs that accept encrypted input and generate encrypted output. As a result, system operators cannot know the original records of the patient.

3.2 The Proposed Authentication Method

Our proposed authentication process consists of the following four steps:

Step 1: Registration Process

According to our proposed model, every user has to register to the system prior to enter to the system. Only registered users have the right to send the request for authentication. When a user registers for an account, information has to be provided. The information includes a pair of username and password and that username is further correlated with two things. First one is the address of a communication device for the user. Here, communication device can be personal computers (PCs), laptops, cell phones, smart phones and so forth. Devices such as smartphones and tablets have been used all over the world. Each device is unique in terms of the device address (e.g. serial number) embedded. In this case where the username is a string of alphanumeric characters, an e-mail address, or the like, the first device can comprise a keypad, keyboard, touch-sensitive screen, or the like on which the username and password can be entered.

The second one is some secret questions. To enhance security, more personal secret questions are added rather than the general one. For example, ‘What’s yours dream place to visit at the age of twenty?’ is more personal than ‘What’s your favorite place?’ and at least ten secret questions are added per user and to avoid the vulnerability, user need to update the secret questions at regular interval. All the user information is encrypted and stored in the database of eHealth system. These parameters are verified when an access is requested. All the registered information is stored in the authentication server.

Step 2: Authentication through communication channel 1

In this step, a registered user looking for to be authenticated, first need to send access request to the authentication server through username and password using device 1 and the server verify the user information over the communication channel 1. Thus the user is controlled by the authentication server. The Remote Authentication Dial-In User Service (RADIUS) protocol can be used in the authentication server. In this client/server based protocol, the client passes user information to designated RADIUS servers and acts on the response that is returned.
The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. When the RADIUS server receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message indicating the reason for the refusal.

Step 3: Authentication through communication channel 2

After authenticating over channel 1, the server needs to verify the user identity over communication channel 2 using device 2 to enhance the security of the authentication process. In our proposed framework, two different channels of communication between the authentication server and the user are used to authenticate a user. The user sends first access request over the first channel and the server responses over the second channel. In this step, the user asked to answer secret question which is received through an email id of the user given to the registration process.

---

**Figure 7:** Conceptual framework of the proposed authentication model
Figure 7 shows the conceptual framework for the entire authentication system. According to this figure, an authentication system in communication with a first device over a first communication channel, and in communication with a second device over a second communication channel. The authentication system can comprise one or more servers, data storage devices, workstations, and the like, networked together and configured to perform the functions described herein. The authentication system is preferably implemented in a secure environment to prevent both external and internal tampering.

3.3 The Proposed Access Control Model

The combined schematic of the proposed authentication and access control mechanism is shown in Figure 8. According to our system, every user carries unique user-identity information. Any access request by a user in our system starts by authenticating himself to the system through the proposed authentication model. After successful authentication, the access request will be placed to the access control list server and the access control process starts. The access control process composed of the following elements:

Access Control List server: According to the DAC module the patient will specify who can access his eHR. He will populate an Access Control List (ACL) with the users who he prefers to be able to access his eHR. an ACL is used to associate each object with the users who can access it. This association also contains the type of access (Read, Write, and Execute) to the object (Blobel and Marshall, 2005). The patient also has the capability to specify the conditions to restrict the access of his records in the ACL which is done using the constraint database.

The Administration Module: This module is designed to create and maintain the general user role assignment. This module is based on the basic RBAC model and performs the general job function associated with the corresponding role. Generally roles can be created, modified or disabled with evolving system requirements.

Access Control Module: This module consists of access control policies. Access control policies define permissions for users to access specific medical records. On the other hand, access policies can be defined as relationships between subjects, objects and actions. For example, a pathology lab technician usually does not need to access a patient's mental health eHRs, or insurance company personnel does not need to modify patient’s disease history.

Constraint Database: This database stores all the context attributes and context conditions. The context attributes and context conditions can be used for the access restriction which is performed by the patient during the access control decision process. (Strembeck & Neumann, 2004). Though the ACL has already the details of registered users, context attribute and context condition make the access control process more secured and every time patient is able to control the access decision through the constraints and always able to change the ACL as well.
4. Analysis of The Proposed Model

Below we discuss different possibilities of attacks against patients’ eHRs and demonstrate how these attacks would be handled by the proposed model.

4.1 Case I: An Intruder wants to access eHRs

According to our proposed authentication model, we use multi-channel authentication system for authenticating a user. Thus when an intruder wants to access the patient’s record, he/she must be authenticated. For this, a registered user need to authenticate by the both channel and for authenticating through the second communication channel, authentication is done twice by email id and the personalized secret question. According to our proposed authentication method, it is very easy to identify one’s originality for the following three reasons:

i. If username and password are stolen, anyone can not authenticate through communication channel 2 as communication device is also used to authenticate further.

ii. If username and password are stolen with communication device 2, anyone can not authenticate through communication channel 2 because of the user’s email id.
iii. If username and password are stolen with the device 2 and email id as well, anyone can not authenticate through communication channel 2 because of the randomly updated personalized secret question.

And it is completely very difficult for anyone to have all the information of any registered user at a time to authenticate.

4.2 Case II: X tries to masquerade as Y

The function of ACL server In a patient’s eHR to maintain the list of permissions for the object class (for example, sexual health information, neonatal information, drug related information etc.) and also allow access according to the allowable operation to object classes. In a typical entry in the system ACL specifies a subject and an operation for example ACL specifies (Alice, read) this would mean to give Alice to read access. In the proposed model if a subject request for access in the eHR then the operating system engages ACL to decide for allowable entry but if the subject doesn’t have access permission then it would raise an alert and inform accordingly. A key issue in the definition of any ACL-based security model is determining how access control lists are edited, namely which users and processes are granted ACL modification access.

4.3 Case III: The subject X manages to pass through the ACL server and tries to access information of a specific patient’s eHR

Passing through the authentication and ACL server, the subject X needs authorisation from the patient to access his/her eHRS. The authorisation server will generate a key to retrieve a patient’s a particular type of eHR. Thus, if healthcare personnel try to access an eHR, for which she/he is not authorised, the authorisation server will not allow the illegitimate access/retrieval of the patients’ eHRS.

4.4 Case IV: System operators try to abuse patients’ eHRS

This is a crucial part in the proposed model. Homomorphic encryption would be used in the database server of the proposed mode. All eHRS of patients are encrypted in the database server using homomorphic encryption. This encryption technique allows the patients to update their eHRS without letting the system operator know about the content of the modification. Even the system operators will not be able to identify in which sub-profile the modification occurred.

4.5 Case V: One patient tries to access/permit other patients’ eHRS

Each patient, whenever they enter the system, is authenticated by the authentication server. After successful authentication, if the patient wants to hack another patient’s eHRS, he/she will not be successful because only the corresponding patient has the private key to decrypt the eHRSs.

4.6 Case VI: Man in the Middle Attack

In our proposed framework, man in the middle attack is impossible. Let us consider the instances when the e-HR of a patient is updated or used:
• Update in the cloud server: When any e-HR user e.g. lab, wants to update the profile of the
patient then the authentication and access right is ensured by authentication server, ACL server
and the patient’s consent. These servers would maintain a session freshness mechanism to
protect any man in the middle attack.

• Display and update at the doctor’s end: When a doctor or specialist will need to access any e-HR
of a patient, we assume, the patient will be present in the session. The doctor will download the
encrypted relevant part of the record from the server to his local machine. Then he only can
decrypt locally with the help of the key provided by the patient. Again at the end of the session if
the doctor needs to update the e-HR, he will encrypt the relevant part of the profile on his
machine locally with the key provided by the patient and upload to the cloud server. Therefore,
man in the middle attack cannot have access to the e-HR since it is encrypted.

5. Conclusion and Future Work

In this paper we present a PCEHR model to enhance the security and privacy of patients’ eHRs using a
cryptographic technique. Many studies have been performed to ensure the security and privacy of
the system, where the system operators are able to access patient’s eHRs. In our proposed model,
system operators cannot learn about a patient’s eHRs. On the other hand, using our proposed
authentication and access control model gives the strong security and privacy of accessing patient’s
records while highest priority is given to the patients to control their eHRs.

According to the proposed model, only the patient has the key to decrypt the data. As a result, when
a patient is disabled or intellectually impaired or in the case of emergency, it is infeasible for any
medical service to retrieve the eHRs. Our future work will include the access control policy using
which patient’s eHR can be accessed during an emergency while still preserving their privacy. We also
want to implement the proposed model which can be compared with other existing solutions in
terms of efficiency and privacy.

References

A. H. Karp, H. Haury, and M. H. Davis, “From ABAC to ZBAC: The evolution of access control models,” Technical

Proceeding international conference of e-health networking, applications and services healthcom,pp. 108–
17.


information system’, In Proceedings of international digital information management conference, pp. 63–
8.

A Framework for Secured and Privacy Preserving eHealth System


Department of Health and Ageing (2011) ‘Personally Controlled Electronic Health Records for All Australians’


A Framework for Secured and Privacy Preserving eHealth System


National E Health Transition Authority (NEHTA) ‘ Draft Concept of Operations: relating to the introduction of a
A Framework for Secured and Privacy Preserving eHealth System

personally controlled electronic health record (PCEHR) system’, 2011


NEHTA (2013) ‘What is a PCEHR?’


A Framework for Secured and Privacy Preserving eHealth System

Conclusion

In this dissertation, we introduce a new framework for secured and privacy preserving eHealth system. Many studies have been performed to ensure the security and privacy of the system, where the trusted third parties are able to access patients’ eHRs. In some cases, they may not be always reliable. The proposed framework ensures the privacy of patients’ data using homomorphic encryption.

We also present privacy preserving authentication and access control schemes for eHealth system in cloud environment. Our schemes not only provide fine-grained access control but also authenticate users who store information in the cloud. The cloud however does not know the identity of the user who stores information, but only verifies the user’s credentials. We identified certain limitations in the existing eHealth systems for ensuring adequate security and privacy of patient’s eHRs which is crucially important in healthcare industry. Our proposed framework is designed to overcome those limitations that can be proved by analyzing the proposed model.

Analysis of the Proposed Model

Below we discuss different possibilities of attacks against patients’ eHRs and demonstrate how these attacks would be handled by the proposed model and make the system strong enough.

Case I: An Intruder wants to access eHRs

According to our proposed authentication model, we use multi-channel authentication system for authenticating a user. Thus when an intruder wants to access the patient’s record, he/she must be authenticated. For this, a registered user need to authenticate by the both channel and for authenticating through the second communication channel, authentication is done twice by email id and the personalized secret question. According to our proposed authentication method, it is very easy to identify one’s originality for the following three reasons:
i. If username and password are stolen, anyone can not authenticate through communication channel 2 as communication device is also used to authenticate further.

ii. If username and password are stolen with communication device 2, anyone can not authenticate through communication channel 2 because of the user’s email id.

iii. If username and password are stolen with the device 2 and email id as well, anyone can not authenticate through communication channel 2 because of the randomly updated personalized secret question.

And it is completely very difficult for anyone to have all the information of any registered user at a time to authenticate.

Case II: X tries to masquerade as Y

The function of ACL server is to maintain the list of permissions for the object class (for example, sexual health information, neonatal information, drug related information etc.) and also allow access according to the allowable operation to object classes. In a typical entry in the system ACL specifies a subject and an operation for example ACL specifies (Alice, read) this would mean to give Alice to read access. In the proposed model if a subject request for access in the eHR then the operating system engages ACL to decide for allowable entry but if the subject doesn’t have access permission then it would raise an alert and inform accordingly. A key issue in the definition of any ACL-based security model is determining how access control lists are edited, namely which users and processes are granted ACL modification access.

Case III: The subject X manages to pass through the ACL server and tries to access information of a specific patient’s eHR

Passing through the authentication and ACL server, the subject X needs authorisation from the patient to access his/her eHRs. The authorisation server will generate a key to retrieve a patient’s a particular type of eHR. Thus, if healthcare personnel try to access an eHR, for which she/he is not authorised, the authorisation server will not allow the illegitimate access/retrieval of the patients’ eHRs.
Case IV: System operators try to abuse patients’ eHRs

This is a crucial part in the proposed model. Homomorphic encryption would be used in the database server of the proposed model. All eHRs of patients are encrypted in the database server using homomorphic encryption. This encryption technique allows the patients to update their eHRs without letting the system operator know about the content of the modification. Even the system operators will not be able to identify in which sub-profile the modification occurred.

Case V: One patient tries to access/permit other patients’ eHRs

Each patient, whenever they enter the system, is authenticated by the authentication server. After successful authentication, if the patient wants to hack another patient’s eHRs, he/she will not be successful because only the corresponding patient has the private key to decrypt the eHRs.

Case VI: Man in the Middle Attack

In our proposed framework, man in the middle attack is impossible. Let us consider the instances when the eHR of a patient is updated or used:

Update in the cloud server: When any eHR user e.g. lab, wants to update the profile of the patient then the authentication and access right is ensured by authentication server, ACL server and the patient’s consent. This server would maintain a session freshness mechanism to protect any man in the middle attack.

Display and update at the doctor’s end: When a doctor or specialist will need to access any eHR of a patient, we assume, the patient will be present in the session. The doctor will download the encrypted relevant part of the record from the server to his local machine. Then he only can decrypt locally with the help of the key provided by the patient. Again at the end of the session if the doctor needs to update the eHR, he will encrypt the relevant part of the profile on his machine locally with the key provided by the patient and upload to the cloud server. Therefore, man in the middle attack cannot have access to the eHR since it is encrypted.
Result

Based on the security analysis, we show that our scheme meets both the security and privacy of patient’s eHRs while giving the full access control right to the patient. According to the extensive theoretical discussion and security analysis, we show that our proposed model is the perfect solution to overcome the current drawbacks of PCEHR system. In this paper we propose a patient centric cloud-based PCEHR framework, which employs a homomorphic encryption technique in storing the eHRs. Thus the administrator has the right to modify, update or delete any record without knowing the original content of the record. Furthermore, encrypted eHealth database enhance the security for any unusual attack. According to our proposed model, it is totally impossible for anyone even authorized personnel like system operators to disclose the patient’s records without patient’s consent. Thus there is no dependency on trusted third party in our proposed framework which is the main contribution of our research.

Moreover, we propose an effective but simple authentication method to make the system more secured from any unauthorized entry. We propose an authentication system based on multi-channel communication. Our proposed multi-channel multi-factor authentication scheme is able to prevent any unauthorised user by authenticating through both channels. This scheme makes the strong security of the proposed PCEHR system while reducing the dependency on trusted third party comparable to the existing PKI based authentication. Furthermore, the proposed authentication model makes the system simple and cost effective by avoiding any scanner compared to the mostly common biometric authentication methods which is another contribution of this research.

To fulfill the requirements of privacy preserving PCEHR system, we also propose a hybrid access control model using RBAC with context-constraint and DAC model. For healthcare informatics. In the healthcare industry, RBAC has already been adopted by the Health Level Seven (HL7) organization as a key access control standard (Blobel & Marshall, 2005). The proposed hybrid access control model obeys recommendations defined by HIPAA Security and Privacy Rule, for example, network security, access control principle of minimum
disclosure, user consent, etc. Our proposed model also possesses different advantages of RBAC, and the simplicity of DAC for delegation management. We advocate a hybrid approach because retrofitting any particular existing model to meet all the access-control requirements of the healthcare domain is prohibitively difficult. This is another contribution of our research.

**Future work:**

According to the proposed model, only the patient has the key to decrypt the data. As a result, when a patient is disabled or intellectually impaired or in the case of emergency, it is infeasible for any medical service to retrieve the eHRs. Thus it is required to make an access control policy to overcome the above limitation. Moreover, further development and testing is required to investigate how this proposed framework would behave in the complex domain of healthcare.

In our future work we will apply access policies for emergency situation which is the main drawback of our current research while still preserving the privacy. We also want to implement the proposed model which can be compared with other existing solutions in terms of efficiency and privacy.

Again, the major work will be the development of those function modules and applying this model to a real healthcare information system to see how the security and privacy are maintained by the proposed framework which can be compared with other existing solutions in terms of efficiency and privacy. Another scope is to extend this proposed model with a suitable language along with the current Extensible Markup Language (XML).
References


A Framework for Secured and Privacy Preserving eHealth System


Department of Health and Ageing (2011) ‘Personally Controlled Electronic Health Records for All Australians’


A Framework for Secured and Privacy Preserving eHealth System


NEHTA (2013) ‘What is a PCEHR?’


A Framework for Secured and Privacy Preserving eHealth System

no.3, pp. 141–60.

Appendix

Publication

The following paper has been published based on the research outcomes proposed in this dissertation.