RESEARCH ARTICLE

ACCESSING ELECTRONIC HEALTH RECORDS OF THE UNCONSCIOUS PATIENT

Prachi Gurav, Sanjeev Panandikar

National Institute of Industrial Engineering, Mumbai, India

Correspondence: prachigurav19@gmail.com

ABSTRACT

Electronic Health Records are a digital version of paper-based records. Studying previous treatment, care and medications is important for making diagnosis for the current situation. The aim of this paper relates to the use of EHR as a means of communication between patient and health care provider with a focus on how EHRs communicates health information for unconscious patient to physicians. As accessing records requires credentials of patient and if the patient is not in a condition to enter his credentials, this leads to the scope of dynamic access control. Dynamic access control is provided by dividing EHRs into different levels. The basis for these levels is physician's specialization and patient's health status. This framework is implemented with the help of a WAMP server using PHP and MySQL.

KEYWORDS

Electronic Health Records, Dynamic access control

INTRODUCTION

The aim of this paper is to describe access control to Electronic Health Record (EHR) specifically for the unconscious patient. An EHR is a digital version of patient's records. These records include sensitive information about a patient's health. The majority of the research is aimed at static access control where the access permissions are predefined [2,7] and describes requirements of access control. In their view, patients should have control over their records, grant and revoke access, should delegate control to someone to access certain parts of their health records, also patients should be able to hide certain details. One important requirement of access control is the need-to-know aspect during emergencies. Most of the articles considered static access policies, they considered that patients have predefined permissions to certain doctors, healthcare workers, or hospitals. Defining access permissions is based on a patient's knowledge of the people treating them or an institute to which they get admitted. During emergencies, patients may not be in a condition to remember passwords or security numbers, may be admitted to institutes for which they have not given access permissions. As per Rosenthal [28] article, a model patient's access key may be known by their relatives but at that time relatives may not present or have access. Due to all these possibilities finding the right information at the right time becomes a difficult task. To resolve these issues different levels of EHR are maintained and to access these levels different login credentials are required based on sensitivity of information. To see the records of unconscious patient we used his fingerprints. Also, to track accountability of clinicians viewing the records we used the physician's fingerprint.

RELATED WORK

Several studies have been conducted to examine different situations or scenarios in relation to access control.

1. HEALTH COMMUNICATION:

Berry's [3] health communication is the situation among different players which include doctors, patients, relatives, family friends and carers. The communication may be verbal or non-verbal. Ruben [8] explains the wide nature of health communication ranging from face-to-face to settings outside clinical environment, which include local grocery stores, retail stores, television, billboards, and magazine advertisements. With the expansion of this range health communication has potential to boon or bane. This hampers the quality, security, and applicability of information given in the situation. To make an accurate diagnosis patient-doctor communication is important. [35] The patient's level of consciousness, the amount of physical care given to the patient and the presence of relatives are the factors influencing the communication. [36] Physical examination depends on history but tracking of history is possible only when patient is conscious and carries his/her previous prescriptions. There is possibility that patient is unaware about medical jargons and can't remember medicine names. [38] In case of unconscious patients, history is collected by questioning person who is familiar with the recent history of patient. [34] Personalized care can be achieved by addressing unconscious patients by their preferred names, encouraging family and friends to contribute the sound of familiar voices and discussing subject in which patient has interest. [36,38] strategies to communicate with unconscious patient work only when patient is accompanied with his/her relatives, which is not possible all the time. Arar [5] found that the use of EHR plays important role in information exchange by providing information about medications, prescriptions, renewals and refills. [1] The EHR assists physicians in preparing prescriptions by giving information about their medications. The use of EHR has positive impact on patient-doctor communication.

2. ACCESS CONTROL IN EHR:

Badr [22] proposed an authentication and authorization protocol to manage EHR using a public-key cryptosystem. In this paper, the hospital has access rights on long-term historical EHRs of a targeted patient. When the patients want to transfer their EHR from previous organization to a new one (which may be clinics, hospitals, social organizations), the patient must grant access permission to the new organization. Assigning permissions to new organization is possible when patient is conscious. If patient is unconscious and admitted to new organization then it is difficult to access EHR. [28] proposed a framework in which the patient encrypts personal medical data according to different access policies and stores it in the cloud.

Ming [23] set out that the EHR owner (patient) formulates the access policy, encrypts the data, and uploads it to the cloud server. EHR users (doctor or nurse) who can download data from the cloud server and decrypt it. Rosenthal [28] says to provide accountability this system provides access to only authorized doctors. The patient's key is known to his relatives only. Here patient accompanied by relative who knows the key is mandatory condition, which is not possible every time.

Darnasser [29] focused on system which require coordination among doctors and patients. In this system user of the system has to give a reason for accessing the EHR. Grunwell [27] presents a system in which hospital staff members authorized by a medical institute are allowed to access EHR. Grunwell [27] used three scenarios, which are: a parent is given complete access to manage their child's EHR. 2. A healthcare worker is given access to manage the record of a patient with a mental disability under their care. 3. A doctor grants access to one of the nurses caring for one of his patients to add data to record. Nelson [33] proposed four different levels of consent. In general, there is full access to citizen's health data. General consent with specific conditions is a general agreement but some restrictions in terms of the person, data, and purpose are defined. General denial with specific conditions complements the consent type to give access to his/her data. General denial does not consent to give access to his/her health data.

In Lo [21] and Grunwell [27] models, the hospital has access to EHR of regular patient. But who is actually going to access the EHR is not clear. Sun [20] provides access control to doctor but patient's key is known by relative. There is no facility to track unauthorised access by patient's relative. [24] provides different levels but, these levels are statically defined. We can't predict in emergency which information doctor will require? Ming [23] also, focuses on static access control. [27] used three scenarios which use static access policy and which are prone to insider threat.

In the existing work, the data owner may be a patient, doctor, or hospital. When the data owner is a doctor or hospital, the patient has to request for data access and patient data is prone to insider threat. When data owner is patient information is collected by wearables or maybe by using sensor devices which is not possible every time for every patient. Also, remembering key or password depends on the patient's physical and mental health.

In this paper, we applied dynamic access control as well as information accountability to EHR. The focus of this work is on the patient's health status (unconsciousness) which is the motivation behind the use of dynamic access control.

3. PATIENT IDENTIFIERS:

Patient identifier is defined as information associated with patient that uniquely identifies individual as a patient to whom treatment is intended. From literature the patient identifiers used are fingerprint, DNA sequences, Iris scan, Facial recognition, Citizen ID, finger vein system.

TABLE 1: PATIENT IDENTIFIERS USED IN LITERATURE

SR.NO.	FINDINGS	REFERENCE
1	Patient identifiers-Patient's fingerprint	[10], [26], [11], [12], [13], [14]
2	Patient identifiers-Facial data	[16], [17]
3	Patient identifiers- encrypted mobile number, gender and name-value of patients	[18]
4	Patient identifiers-Iris identification	[15]
5	Patient identifiers-finger-vein system	[25]
6	Patient identifiers-DNA sequences	[19]
7	Patient identifiers-citizen ID	[10]

Facial recognition is not suitable as it is affected by different expressions, different physical and metal conditions, age. Remembering Citizen Id, mobile number is difficult for patient as physical condition may hamper his mental ability. Also, it is easy for intruder to get access to patient's EHR using his name, citizen id, mobile number. DNA sequences are highly intrusive and more expensive.

As our focus is to identify unconscious patient and access his health record, in this paper to capture patient identity we used fingerprint. For conscious patient we used his unique identification number.

ALGORITHM

1. THEORETICAL BASE FOR THE ALGORITHM

We used Northouse [6] and Northouse's health communication model as a base for the implementation of this algorithm. According to this model health communication refers to transactions between participants in healthcare and about health-related issues. [6][3] The model illustrates four relationships: professional-professional, professional-client, professional-client's significant others, client-significant others. Professional and client have unique characteristics, beliefs, values, and perceptions to the healthcare settings, which affects their interaction. Here, professional is doctor and client is patient under treatment. The client's significant other's include family, friends, work colleagues. This model considers the communication which is conducted among patient and doctor in doctor's cabin or hospital ward, which is face-to-face. In our work, we consider the changes in communication between patient-doctor, due to introduction of Electronic Health Record. In our model there are three role players: patient, doctor and relative. Most of the communication and information exchange is between doctor and patient. The role of relative is just to give consent to doctor to access most sensitive information of patient. This information exchange is designed for treatment setting, in which doctor requires information about patient's health history. Any role player can misuse information available to him, which is not considered by Northouse and Northouse's health communication model. We design our model by considering misuse of information and made the communication more secure. Our model also focus on availability of information when two (patient and relative) of the three role players can't provide information and still third role player (doctor) can access the records without disturbing security. In all this procedure information accountability is also prevented by taking credentials of each user.

2. MODEL FOR LEVEL-BASED ACCESS CONTROL:

This section explains about different level are maintained. These levels are based on doctor's specialization as well as patient's health status. As per doctor's specialization the model is classified into three main levels. General, Special, and complete, for which login gets changed as per patient's health status which may be conscious or unconscious. There are many definitions to define consciousness. In this model we used definition of consciousness given by [28] as condition of people or creature when they are awake and responsive to sensory stimulation. The three levels in this model are:

- General EHR: contains data about patient's visit to general physician.
- Special EHR: contains data about patient's visit to specialized physician and general visits. Ex. if Alice visits gynaecologist her doctor can view details filled by gynaecologist if any and her general EHR.
- Complete EHR: Contains data about patient's complete health.

We present here six scenarios that describes access control process in a hospital to enable medical staff members to gain access to patient's EHR even if patient is unconscious.

1) Conscious patient comes to general physician:
   When Alice comes to doctor bob, doctor used his login id and asks patient for her login id and can view the general EHR.
2) Unconscious patient comes to general physician:
   When unconscious Alice admitted to general physician Bob, doctor use his login id and uses Alice's fingerprint to view her general EHR.
3) Conscious patient comes to specialized physician:
   When Alice comes to gynaecologist, she wants to show her gynaecology records to doctor Bob, but she doesn't want to disclose about her psychiatry treatment. In this case doctor uses his login id, Alice uses her login id and fingerprint to access special EHR. This displays only gynaecology records and records filled by general physician.

4) Unconscious patient comes to specialized physician:
   When unconscious Alice admitted to gynaecologist, she wants to show her gynaecology records to doctor Bob, but she doesn't want to disclose about her psychiatry treatment. In this case doctor uses his login id and fingerprint, Alice's fingerprint is used to access special EHR. This displays only gynaecology records and records filled by general physician

5) Patient wants to view his records:
   When Alice wants to view her EHR by entering her login id she can view complete EHR.

6) Doctor (general or specialized) wants to view complete EHR of unconscious patient:
   When unconscious Alice admitted to any physician Bob who may be general or specialized and doctor wants to view complete EHR bob has enter his login credentials id and fingerprint, Alice's fingerprint and Alice's nominated relative's fingerprint.

4 PROTOCOL DEFINITION:

This section about how algorithm works with different access permissions.

Meaning of symbols:

D=Doctor,
Ds=Specialised doctor,
Dg=General doctor
P=Patient,
Pc=Conscious patient,
Pu=unconscious patient
T=Tuples of EHR,
Ts=Tuples of SEHR,
Tg=Tuples of GEHR
GEHR=general EHR,
SEHR=special EHR,
CEHR=complete EHR
d_{gid}, d_{sid} = id for a generalized and specialized doctor
p_{cid} = id for conscious patient
d_{sf}, p_{uf}, R_f =fingerprint for doctor, patient, relative

When doctor login in system as general physician d_g and patient is conscious p_c then login requires patient and doctor id (D_{gid}, P_{cid}) respectively. Then displayed records belongs to general EHR (gehr), which is intersection of all tuples T and tuples with general visits T_g. When doctor enters new record T_{new} one more tuple gets inserted in general tuples T_g and then updated T_g will be union of original T_g and T_{new}.

If {$D=d_g$ && $P=p_c$}

{

Login (d_{gid}, p_{cid})

Display (gehr where d_{sp}=general)

$T_g \leftarrow T_g \cap T$

Insert(gehr)

$T_g \leftarrow T_g \cup T_{gnew}$

}

When doctor is general physician d_g and patient p_u is unconscious, then login requires doctor id d_{gid}, doctor fingerprint df and patient fingerprint pf. Records displayed includes general EHR are intersection of general tuples and all tuples. New entry results in union function.

Elseif {$D=d_g$ && $P= p_u$}

{

Login (d_{gid},d_f ,p_f)

Display (gehr where d_{sp}=general)

$Tg \leftarrow Tg \cap T$

Insert(gehr)

$T_g \leftarrow T_g \cup T_{gnew}$

}

When doctor is specialized and patient is conscious, then records related r_{sp} to doctor's specialization d_{sp} get displayed. Login requires doctor's id, d_{sid} and patient's id p_{cid}.Ts includes tuples with doctor's specialization and tuples with general visits.

Elseif {$D=d_s$ && $P=p_c$}

{

Login (d_{sid}, p_{cid})

Display (Sehr where $d_{sp}=r_{sp}$)

$T_s \leftarrow T_s \cap T$

$Tg \leftarrow Tg \cap T$

$Ts \leftarrow Ts \cup Tg$

Insert(sehr)

$T_s \leftarrow T_s \cup T_{snew}$

}

When doctor is specialized and patient is unconscious, then login requirements are doctor's id d_{sid}, doctor's fingerprint d_{sf} and patient's fingerprint p_{uf}. Result displayed includes records matching to doctor's specialization and general records.

Elseif {$D=d_s$ && $P=p_u$}

{

Login (d_{sid}, d_{sf}, p_{uf})

Display (Sehr where $d_{sp}=r_{sp}$)

$T_s \leftarrow T_s \cap T$

$Tg \leftarrow Tg \cap T$

$Ts \leftarrow Ts \cup Tg$

Insert(sehr)

$T_s \leftarrow T_s \cup T_{snew}$

}

When patient wants to view his records, then login requires patient's id p_{cid} and complete EHR (cehr) get displayed.

Elseif {p= pc}

{

Then Login(p_{cid})

Display (cehr)

$T \leftarrow T \cup null$

Insert (cehr)

$T \cup T_{new}$

}

When doctor may be general or specialized and patient is unconscious and doctor wants to view complete EHR, login requires doctor's id d_{id}, doctor's fingerprint d_f, patient's fingerprint p_{uf} and patient's nominated relative's fingerprint R_f. Tuples displayed include all tuples.

Elseif {$D=d_s || d_g$ && $P=p_u$}

{

Login(d_{id}, d_f,p_{uf},R_f)

Display(Cehr)

$T \leftarrow T \cup null$

Insert(cehr)

$T \leftarrow T \cup T_{new}$

}

IMPLEMENTATION

[33] five methodologies namely: Formal, Experimental, Build, Process, and Model which are applicable to computing science research. Computing Science (CS) most of the time uses experimental methodology. Experimental methodology includes two steps. One is identification of a question and another is finding suitable solution. [37] define Experimental Computer Science (ECS)

as "the building of, or the experimentation with or on, nontrivial hardware or software systems." [31] discussed three methodologies in computing science: Theoretical, Experimental, and simulation. Theoretical methodology uses logic to prove relationships among different objects. Simulation enables scientists to examine their models virtually. Experimental methodology studies concepts which are related to human creation. Here, experiments are related to information. [31] conducted a survey to investigate methods applicable to research in computing. The results show strong support to experiments as the method of data collection. Experimental method is related to creation of new algorithms comparison of existing algorithms. So, considering all these points researcher has used experimental method to achieve research objective of this research. This model is implemented using WAMP server with PHP and MySQL. We have created databases in MySQL which described doctor, patient and relative information. Patient database includes fields which are, name of patient, his unique id, date of record insertion, Symptoms, doctor's specialization, medicines and medication_till_date. To complete this database, we took data from webMD and drug.com websites. This data includes names of medicines and symptoms to which medicines get applied. The focus is to implement access control scenarios and to view patient's records, so pseudo database is generated. The data is not related to any real patient, leads to no scope for ethical consent. Following are the steps user has to perform while searching health records:

1) Account creation and login
2) If user is doctor, he can access data based on his specialization
3) If doctor is general physician, then he can access GEHR
4) If doctor is specialist, then he/she can access SEHR matching to his/her specialization
5) If doctor (General Physician/ Specialist) wants to access CEHR he has to take permission from patient if he/she is conscious or from patient's relative if patient is unconscious.
6) When patient is unconscious patient identifier is fingerprint
7) For searching SEHR and CEHR identifier used for doctor and relative is also fingerprint.

DISCUSSION

The objective of this paper was to develop dynamic access control in EHR which will access even records of unconscious patients. To achieve this objective, researchers have used an experimental methodology. This paper discussed Northouse and Northouse's health communication model. The model described importance of players in the communication. According to this model, the setting in which communication is carried out also play important role. The settings which are mentioned in this model are doctor's cabin or hospital ward. The purpose of this communication is to capture more information about patient's problem, his health history, his symptoms and give his accurate treatment. We used this model, with players patient, doctor and relative. The prior model is best when doctor-patient or doctor-relative or patient-relative interact face-to-face. Whereas latter proves best when unconscious patient comes to doctor and doctor has no way other than patient's Electronic Health Record to access his health history. As introduction of EHR brings ease of access to information, security issues and information misuse together make up the other side of the coin. At that time our model with dynamic access control provides better solution. Researchers proposed this model which access system with fingerprints. When there is a scenario in which unconscious patient without hands comes to hospital there is need to use another patient identifier, which is future scope for this model. Dynamic access control will be applicable to other sensitive databases.

CONCLUSION

As EHRs are storing sensitive, as well as important information, we classified this information based on its sensitivity and importance. Sensitive information is classified as general EHR, Special EHR and complete EHR. To access details of unconscious patient we used fingerprints. Use of different access scenarios and different patient identifiers leads to future scope.

References:

1. Aviv Shachak, S. R. The impact of electronic medical records on patient–doctor communication during consultation: a narrative literature review. Journal of evolution in clinical practice, T 15, 641-649, (2009),

2. Bandar Alhaqbani, C. F. Access Control Requirements for Processing Electronic Health Records. QUT digital repository, 371-382, (2007),
3. Berry, D. Health communication theory and practice. Health psychology, (2007).
4. Jeffrey Hunker, C. W. Insiders and insider threat an overview of definitions and mitigation techniques. Journal of wireless mobile networks, 2(1), (2008)
5. Nedal H Arar, L. W. Refereed papers Communicating about medications during primary care outpatient visits: the role of electronic medical records. the journal of innovation in health informatics, 13(1), 13-22., (2005)
6. Northouse, L. Health communication: strategies of Health Professionals, Pearson Education. (1998).
7. Pradeep Ray, J. W. The need for technical solutions for maintaining the privacy of EHR. IEEE eng Med Bio Soc, (2006).
8. Ruben, B. D. Communication Theory and Health Communication Practice: The More Things Change, the More They Stay the Same. Health Communication, 31, 1-11. (2016)
9. Teutsch, C. Patient-Doctor Communication. Medical clinics of north america, 87(5), 1115-1145. (2003).
10. Tipporn Laohakangvalvit, M. O. Electronic patient referral system with data exchange and fingerprint patient identification. ResearchGate. (2015).
11. Names, T. Z. A New Cryptosystem based on Fingerprint Features. International Journal of Computer Applications. (2015)
12. Lyare, O. Development of a secured telemedical system using biometric feature. International journal of computer and information engineering. 10(1) (2016).
13. Shubham Nayak, M. D. fingerprint recognition approach for patient history extraction. International journal of computer engineering and applications. (2017).
14. TOKOSI. T, N. V. Electronic Patient Record System for Clinical Use: A Conceptual Framework. International Journal of Advances in Electronics and Computer Science. (2016).
15. Adebayo Omotosho, O. A. Exploiting Multimodal Biometrics in E-Privacy Scheme for Electronic Health Records. Journal of Biology, Agriculture and Healthcare. (2014).
16. Adebayo Omotosho, J. E. Private key management scheme using image features. journal of applied security research. (2015).
17. Guillen-GaMez, FD A proposal to improve the authentication process in m-health environments. IEEEAccess , 22530-22544. (2017).
18. Khan, S. I. , & Hoque, A. S. Development of national health data warehouse Bangladesh: Privacy issues and a practical solution. IEEEXplore, (2015).
19. Gritti, C. (2016). Contributions to Cryptographic Solutions towards Securing Medical Applications. University of Wollongong.
20. Jin Sun, X. W. A searchable personal health records framework with fine grained access control in cloud fog computing. PLOS, 13(11). (2018).
21. [Nai-Wei Lo, C.-Y. W. An authentication and authorization mechanism for long-term electronic health reocrds management. 8th international conference on advances in Information Technology. Procedia computer science.111, pp. 145-153. (2017).
22. Shaimaa Badr, I. G.-E. Multi-tier blockchain framework for IOT-EHRs systems. 159-166. (2018).
23. Yang Ming, T. Z. Efficient privacy-preserving access control scheme in electronic health record system. Sensors. (2018).
24. Yvonne O'Connor, W. R. Privacy by design: informed consent and internet of things for smart health. Procedia computer science, 111, 653-658. (2017).
25. Wencheng YangSong Wang, J. H. Securing Mobile Healthcare Data: A Smart Card based Cancelable Finger-vein Bio-Cryptosystem. IEEEAccess. (2018).
26. Barman, S. Approach to cryptographic key generation from fingerprint biometrics. International Journal of biometrics. (2015).
27. Daniel Grunwell, T. S. Delegation of access in an Information Accountability Framework for eHealth. ACM. (2016).
28. Rosenthal, David. Concepts and Definitions of Consciousness. 10.1016/B978-012373873-8.00018-9. (2015).
29. Darnasser, M. Toward privacy-preserving emergency access in EHR systems with data auditing. Thesis. Rochester Institute of Technology. (2013).
30. Abu-Bakar, N. Research methods in computer science. ResearchGate. (2018).
31. Gamukama, EA, Popov, O. The Level of Scientific Methods Use in Computing Research Programs. 31st International Convention on Information and Communication Technology (2008)
32. Hassani, H. Research Methods in computer science: the challenges and issues. ResearchGate. (2017).
33. Jose Nelson Amaral, M. B. About computing science research methodology. IEEE 27th International Conference on Software. Williamsburg. (2011).
34. Leigh, K. Communication with unconscious patients. Nursing times, 35. (2001).

35. Muhrer, J. C. The importance of history and physical diagnosis. Nurse Practitioner, 39(4), 30-35. (2014).
36. Sanders, L. Every patient tells a story-medical mysteries and the art of diagnosis (Vol. 8). springer. (2010).
37. Snyder, L.. Academic careers for experimental computer scientists and engineers. National Research Council (1994).
38. Zaith A. Bauer, O. D. Unconscious patient. stat pearls. (2021).