Al-Badarneh et al.

Regular Issue Vol. 2 Issue 3, pp. 26-37

Date of Publication: 04th January, 2017

DOI-https://dx.doi.org/10.20319/lijhls.2016.23.2637

This paper can be cited as: Al-Badarneh, A., Najadat, H., & 'Hassan Abu Yabes', E. (2017). Cross-Cultural Factors That Influence Adjustments Of Foreign Care Workers In Japan: Towards A Three-Layered Structural Model. LIFE: International Journal of Health and Life-Sciences, 2(3), 26-37.

AN ADAPTIVE ROLE-BASED ACCESS CONTROL APPROACH FOR CLOUD E-HEALTH SYSTEMS

Amer Al-Badarneh
Jordan University of Science and Technology, Irbid 22110, Jordan
amer.b@just.edu.jo

Hassan Najadat
Jordan University of Science and Technology, Irbid 22110, Jordan
najadat@just.edu.jo

Enas 'Hassan Abu Yabes'
Jordan University of Science and Technology, Irbid 22110, Jordan
enas.issa10@yahoo.com

Abstract

Securing and protecting electronic medical records (EMR) stored in a cloud is one of the most critical issues in e-health systems. Many approaches with different security objectives have been developed to adapt this important issue.This paper proposes a new approach for securing and protecting electronic health records against unauthenticated access with allowing different hospitals, health centres and pharmacies access the system, by implementing role-based access control approach that could be applied smoothly in cloud e-health systems.

Keywords

EMR, Security, Privacy, Role-Based Access Control, Cloud Computing.

1. Introduction

Many healthcare providers recently have assumed some design of electronic health record systems, in spite of the fact that most of them keep medical records in concentrated databases in the framework of electronic records, As a rule, a patient may have numerous health care providers, including medical attendants, doctors, experts, dental specialists, and others.. Likewise a patient may utilize a few medicinal services insurance agencies for various types of protections.

Currently, every provider has its own database for electronic health records. Exchanging data between medicinal services institutions is limited and managed by administrative tasks, sharing information between electronic health systems through various health centers is slow. Costly and inefficient usability are the biggest difficulties to adopt health systems (Carlos Roli et al., 2010).

Cloud computing supplies an efficient information technology design to reduce the cost of e-health systems related to both ownership and repair efforts for various medical operations. It is generally realized that cloud computing and open standards are imperative techniques to arrange and manage healthcare whether it is for saving health records, supervision of patients, administrating diseases or analysis of data. Managing health care systems with clouds will make revolutionary change in the way of health care operations (Carlos Roli et al., 2010).

In traditional health systems, protecting the privacy of patients' information is the responsibility of the independent Institutions like hospitals, clinics and medical centers. By using highly information technologies like cloud computing where the system data is distributed in different storage areas. Patient information can be accessed with patients, physicians and any other related institutions.

This will force health care industry towards a more open medical information infrastructure and to upgrade the quality of health systems. In addition, health care industry also gives a number of new issues in insuring patient medical information to keep it in confidentiality and availability. An open health care requires complementary security management approaches

and policies to prevent the existence of serious potential violations of security and privacy (Rui Zhang, and Ling Liu ,2010).

The main requirements for securing electronic health records are first, effective access control model that satisfies expressiveness and flexibility needed by privacy policies, second, the system should be operated smoothly in various environments and the system should contain and manage rich meta information (Ming Li, et al 2010).

Operative administration of electronic health records is a very complicated and critical problem. Patient protection issues, at the same time with dangers that could uncover medical data insures the importance for privacy and security mechanisms combined with medical systems and could be implemented toward a different collection of dissimilar systems and networks, a shared electronic health record simply a complicated combination of critical information, containing patient particulars, medical histories, checking results, etc. There is also an important necessity for protection models that respond to legitimate and administrative approaches, while at the same time guaranteeing that entrance to delicate data is restricted and committed just to those beings that have a permissible need to know approvals allowed by patients. For example, a patient may choose to obviously conceal his medical information from general medical information sharing session unless a certain treatment choice is implied. It's important to look for safe and sharable policy that permits patients to rapidly and smoothly grant a collection of medical sub organizations to access their critical information partially or in whole.

Role-Based Access Control (RBAC) is one of the access control mechanisms to classify and determine many of the requirements of security administration in distributed information systems. So this paper concentrates on how to implement role based access control in cloud electronic health systems. There are some essential benefits in electing RBAC for ensuring patient privacy and security. First, roles, those are an important indirection between users and authorizations, immediately arranges healthcare institutional positions, like doctors, physicians, and nurses.

The access rules should support important procedures to achieve distinct jobs' tasks. For example, the system should confine read, duplicate, and print work on basic data to just the imperative stuff for a specific period.

Access control need to recognize who has entry to the information, which type of access is permitted, what works that are provided, under what circumstances, and for what period This paper presents a role based access control approach, that takes into account the function in hand and the turn of the user and writing analysis on the patient's record on the other hand.

The paper is organized as follows. Section 2 illustrates the motivation of the research .Section 3 reviews related work. Section 4 introduces the proposed approach. Section 5 gives more discussions about the proposed approach. Section 6 concludes the paper.

2. Motivation

In spite of the fact that forcing privacy by RBAC could be easily deployed in systems already adapting RBAC. The embracing of role based access control in cloud e-Health systems requires some essential additional requirements. Healthcare is a complicated environment which naturally includes multiple domains. Also, not only the content of electronic medical records needed to be protected and secured but also some meta information about electronic medical records, such as owners of records, integrity constraints, privileges granted to users, default column values. So role based access control mechanism should be customized in an efficient manner to guarantee a burst secure and protected environment.

3. Related Work

A number of solutions have been proposed to address security and access control issues associated with e-health systems. (Löhr, Sadeghi & Winandy, 2010) proposed a model where electronic medical records are managed by health specialists only. In most countries this needs various allowable prerequisites and an obvious differentiation between personal health records and electronic health records, so infrastructures that contain electronic health records are more complicated than simple e-health cloud model which clarified previously. The common needs that proposed are still the functional and meaningful of the information saved in the electronic health records. The electronic health records are designed, directed, and administrated by health care providers, and can be shared across the central server in the cloud with other health specialists. Also the health care providers have the ability to access billing services that manage their accounting with the health insurances of the patients.

According to the proposed approach by (Josh Benaloh et al. 2009) the patient may determine to give his dental specialist access to both the dental records feature and the fundamental medical information feature. This will permit to the dentist to read all data related to the dental clinic visits, dental x-rays, surgeries and medications. The dentist will not be able to decrypt any of the health records of the patient, or his personal data, for instance, the server that saves the health information will not be able to get the secret key, or any of the sub keys given to the doctor, so he will not have the ability to decrypt the data.

The hierarchical model that is proposed by (Josh Benaloh et al. 2009) is easily expandable; the patient and possibly other clients to whom the patients give the appropriate authentications can append additional sub features during any existing group. So within the medications group, the patient's dentist might append a new feature for doping or visiting on a certain date. Once the patient gives the specialist authorizations to his drugs, if his dentist adds a new feature, all records in that subcategory will be spontaneously accessible to the doctor. According to this, the patient can easily give access to a group, without the need to know all the types of files that might be involved in it.

The same thing is for doctors; they can add sub features with random names, without support from the patient. This will be certainly valuable if we can't foretell the names of all probable sub features, for example if a specialist needs to append a feature for a new kind of test, or if features are assorted by visit dates. The drawback of this model is that there is only one method in which can split the records, and if we need to grant access privileges according to something else, for example, record sort or receptiveness of information, we should take a gander at all the low-level characteristics included, and give a different decryption key for each. A specific supposition is taken about the configuration of the patients' record; the patient's record is stored as an accumulation of passage, where every passageway contains the name of the document, additionally the name of the minimal feature including that record which the patient can use to get to the record, and the encrypted copy of the file (Josh Benaloh et al. 2009).

(Jacques Wainer et al., 2006) addressed the Integrity confidentiality and control issues with the following key features:

- Availability: the electronic health records should be available when the health specialists require it, so all attention in making the system firm and reliable is important.

- Up-to-datedness: the electronic health records should include all of the recent related information with taking into account the patient's health; so there should be no crucial postponement from when data is entered into the record and when it becomes obtainable to different specialists. If the health specialist decides some medication to the patient, that information should be contained in the electronic health record directly, so if the patient asks another health specialist for another treatment, then the information must be obtainable.
- Usability: In spite of the fact that usability is not considered as an integrity issue, it is also important to perfect utilization of the electronic health records, the health specialist should not have to read through all of the patient's records to determine the usability conditions.

- No access rights to the patient: the patient has no privileges to access or modify the electronic health record, and the patient can only depute access privileges to his own records to health specialists.
- Emergency Access: There are believable cases in where health specialists can access a patient's record without his predetermined delegation can happen obviously in emergency cases, if the patient comes to an emergency clinic then the health specialist must be able to access to his electronic health records.
- Implicit acceptance of health organization structure: by granting the patient's electronic health record to the health specialist, the patient according to this may accept any deputy needed for health specialist.
- Limited read access for public health: legitimate and professional humans may have a restricted and unknown read access to the electronic health records without taking into account the patient's agreement.

The authors (Ammar Alkassar et al., 2011) improved a usable and secure end-client sample that can save basic medicinal information from being gotten to or adjusted by illegal clients, they called it MediTrust. The following objectives are defined to be achieved:

- Preserving medical data that are manipulated on the same developed model with other functions.

- Building security architecture that securely divides the data of different operations.
- Supplying an efficient and smooth model that does not require any load in the normal process of health specialists.

The scenario that is applied here is that the doctor utilizes a computer system to prepare electronic health records of patients that are registered on a centric server. A similar PC framework is utilized to send information to a human services accounting and billing server, the PC is likewise used to connection to alternate services , for example web sites on the internet. Privacy domains are built for medical data as a technical magnitude to help in the execution of privacy and data protection mechanisms.

The client model, like desktop or notebook computers, should divide execution situations for applications into discrete scopes that are distinguished from each other. The information inside a security space and the area foundation ensures that only the legitimate customers can join this area. In addition, data infiltration from the domain is prohibited by the security model and the domain infrastructure. A similar framework ought to be able to be used for different operations that are completely isolated. So, the importance of MediTrust is on the execution of secure customer structures that can be used not just to access basic health records and joined accounting data securely, but also working frameworks and programming that are completely isolated from the basic information and the medicinal services customer application (Ammar Alkassar et al., 2011).

A set of roles are proposed (Hema Narayanan& Mehmet HadiGüneş , 2011) starting by implicit access control and tasks to stand by explicit access control. A lessee in the cloud system has various users. Every user is given a role; roles are given to a workflow or non-workflow functions, and functions are given to permissions. Users with an assigned role are able to run different tasks through workflow and non-workflow functions given to their role. Authorizations are given to roles according to their functions and assigned authorizations and changes dynamically according to the current function.

Authorization specifies who can do which functions with what role under what circumstance. It is determined by the states or rows (U, R, T, P, and C) where U is the set of users'u_i, R is the set of roles r_i, T is the set of tasks t_i, P is the set of permissions p_i, and C is the set of constraints c_i. For instance, the tuple (Jack, doctor, read patient information, read, daytime

and office location) determines the way that Jack as a doctor reads patient information from office during office hours.

The factors important to healthcare cloud systems are tenant: is customer like clinic hospital or pharmacy in a health care system, user, task, information resource, business rule, permission, session: is a map of different rules for certain user.

The factors that are important to healthcare cloud systems are (Hema Narayanan & Mehmet Hadi Güneş, 2011): Work Flow, Business Rules: is a set of regular activities of users that the organization follows, Least Privilege: the essential privileges assigned to each user, Least Separation of Duty separating the obligations regarding assignments in a work process between various members and ensure against trick activities ,Tenant_User Assignment : A cloud system has many tenants each with different users, User-Role Assignment: A user can be assigned one or more roles, And the same role can be given to different users.

Task-Role Assignment: A role can have multiple tasks and a task can have multiple roles. Permission-Task Assignment: Tasks are given permission to be executed, Task-Workflow Assignment: the duties that belong to approval classes are assigned to a particular workflow, Least Privilege: the essential privileges that is assigned to the user.

The significant imperatives in getting to control are Least Privilege: the most essential privileges that every user have in the cloud to see a certain information, Dynamic and Static Separation of Duty: dynamic separation of duty prevent Simultaneous execution of at least two sole assignments by a similar role, Delegation: delegation means assigning a role by another user, Spatiotemporal Constraints; User's location and time is considered for giving access to a task. When a tenant registers in the system, its office and clinic locations are registered for more temporal checking (Hema Narayanan& Mehmet HadiGüneş , 2011).

4. Proposed Approach

The proposed approach supplies access control decisions based on tasks associated with authorized evaluators. For instance, a doctor at a certain hospital has features including his title, appointments, specialty; every preserved record contains implicitly a complicated access control approach to specify which users can access the record. This approach helps clients who do not

have recognized functions, like medical scientists. For instance an individual may be given access only to records created within certain time period, with a particular record kind.

The proposed approach includes the following entities: Users, Roles, Permissions, Preconditions, Data, and Metadata.

- The User: is the human being like doctor, physician, nurse and more.
- The Role: is a specific job or a specific task in a job.
- Users are granted roles based on their credentials and responsibilities in the organization.
- Roles are granted to users by many to many relationships: The role structure is hierarchal where every role has 0 to 1 parent role and 0 to N leaf roles; whenever the user granted certain role, the parent role will be implicitly granted to the user but not the leaf roles.
- Permissions are the types of privileges granted to Role: query, modification, insert, administrative roles, executing functions, permissions are granted to roles; a many to many relationships applied between the permission and roles. An implicit grant of permission is executed whenever a certain function that is granted to certain role contains query of modification permissions.
- Preconditions are predetermined validations that are used to decide if a certain user can access a role or not; this property can be used in an efficient way if for example a certain user have the authorization to grant particular roles to another users, according to the preconditions the system will determine if the user needs the roles he granted or not according to the user features and tasks.
- Data are the objects that are stored as resources in the cloud such as tables, images, columns, rows, raw files and X-ray photographs.
- Meta Data are the information about the data such as definition, allocated and utilized capacity estimate for information objects, default column values, integrity constraints, names of and privileges granted to users, auditing information and more.

In the proposed approach the meta data can be combined with roles to make assigning roles more efficient and secure by assigning roles to users according to the data description of objects, for example, the pediatrician can have access to information related to patients with ages less than 12 years old, and gynecologist can access records related to female patients only.

5. Further Discussion

So far this paper addressed a role based access approach that can be implemented easily by relying on the structure of the health system as various roles will interact with the information. Access roles to resources must be given to users according to their tasks. For instance, a specialist ought to be allowed access to restorative history of a patient.

Cloud e-Health systems should allow access to resources only when it is required and protect users from unintended problems. Furthermore, access policies should support core operations to achieve job tasks; the system should manage read, copy, and print operation on critical information to only the specialized users according to their tasks. Access control should determine who has access to information, which type of accesses are permitted, what duties are given and under what circumstances.

6. Conclusion and Future Work

Patient privacy and data security can be achieved using role based access control techniques by determining the main entities for the model, and assigning each user one or more tasks after explicit and implicit grants of the predetermined roles for the legal users, the advantage of applying implicit grant is to simplify the complicated structure of the role based access control hierarchy.

The future work is to improve the role based model for adapting access to electronic health records in the situations of emergency where access typically occurs in an ad-hoc and spontaneous way**.**

REFERENCES

Rui Zhang, and Ling Liu. (2010). Security Models and Requirements for Healthcare Application Clouds, IEEE, and 3rd International Conference on Cloud Computing, 268-275. doi: 10.1109/CLOUD.2010.62.

Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter (2009). Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, in the ACM workshop on Cloud computing security, 103–114. doi: 10.1145/1655008.1655024.

Hans Löhr, Ahmad-Reza Sadeghi, Marcel Winandy (2010). Securing the E-Health Cloud, in the ACM International Health Informatics Symposium, 220-229. doi. 10.1145/1882992.1883024.

Ammar Alkassar, Biljana Cubaleska, Hans Löhr, Ahmad-Reza Sadeghi, Christian Stüble, Marce Winandy. Medi Trust (2011). Secure Client Systems for Healthcare IT to Protect Sensitive Data of Patients, The International eHealth, Telemedicine and Health ICT Forum, Luxemburg, 4, 385-389.

Jing Jin, Gail-Joon Ahn, Hongxin Hu, Michael J. Covington, Xinwen Zhang (2010). Patient-Centric Authorization Framework for Electronic Healthcare Services, 30,116-127. doi:10.1016/j.cose.2010.09.001.

Hema And Al Jayaprakash Narayanan, Mehmet Hadi Güneş (2011).Ensuring Access Control in Cloud Provisioned Healthcare Systems ,In the Consumer Communications and Networking Conference (CCNC), IEEE.doi:10.1109/CCNC.2011.5766466.

Ming Li, Shucheng Yu, KuiRen, and Wenjing Lou (2010). Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. doi:10.1007/978-3-642-16161-2_6

Jacques Wainer, Carlos Jos´e Reis de Campos, Daniel Sigulem (2006).Security requirements for a lifelong electronic health record system based on non-standard ethical principles, Department of Health Informatics. 2, 160-165. doi: 10.2174/1874431100802010160.

Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker West Phall, Jorge Werner, Armando Fracalossi, Giovanni Schmitt Salvador (2010). A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. 95-99. doi: 10.1109/eTELEMED.2010.19.