Journal of Information Sciences and Computing Technologies(JISCT)
ISSN: 2394-9066

SCITECH
RESEARCH ORGANISATION|

Volume 3, Issue 2
April 17, 2015|

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

Managing Access to Electronic Health Records in a Cloud Computing Environment

Emmanuel Kusi Achampong[1], Clement Dzidonu[2]
[1]Department of Medical Education and IT, University of Cape Coast, Cape Coast
[2]Accra Institute of Technology

Abstract

Access control methods are relevant in securing EHR from unauthorised users and access. It is therefore important that proper access control mechanisms are put in place in order to safeguard the privacy and confidentiality of health records.

This paper provides a review of the benefits and limitations of individual access control mechanisms.It also indicate thechallenges and advantages associated with the use of the individual access control methods vis-a-vis combined access control methods for accessing electronic health records (EHR) in a cloud computing environment.

This review concludesthat the use of one access control method is not sufficient to fully secure EHR in a cloud computing environment. A combined access control methods has the potential to offer strong security to EHR in the cloud setting. Maximising the benefits of the various access controls is essential for enhancing the security of EHR in a cloud computing environment.

Keywords: Access; Control; Electronic; Health; Records; Cloud; Computing.

1.0 Introduction

The increasing use of Electronic Health Record (EHR) systems for collection, manipulation, extraction, management, dissemination and searching of information, is also increasing the requirement for information security (i.e., confidentiality, integrity and availability) [1,2]. Even though EHR is a significant tool for health institutions and patients, there are certain barriers that makes it difficult for successful integration and implementation within the healthcare practice. Some of these barriers include not only security concerns [3] but costs,relational and educational issues [4,5].

Access control is an important aspect of information security that is linked to the main information security characteristics such as confidentiality, integrity and availability [6]. Cloud computing service providers (CSPs) and healthcare providers have certain responsibilities with respect to access control for EHR within the cloud environment. A collaboration of access control systems between healthcare providers and CSPs should have the potential to enhance the security of EHR within the cloud computing environment. CSPs should control access to service features based on specified policies and the type of service subscribed to by the customer[6]. CSPs must control access to client's data from other clients in multi-tenant cloud environments. CSPs in collaboration with customers should control access to regular user functions and other privileged administrative functions. CSPs in collaboration with clients should also maintain correct and up to date access control policy and user profile information. These responsibilities of CSPs and clients must reflect in the advancement of security for EHR [6].

Access control models are categorised under classical and current types. The classical access controls are thediscretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC).The following are classified under current access controls: Attribute-based Access Control (ABAC) and Policy-based Access Control. For DAC model, the object ownerdetermines access permissions for all other users. The UNIX operating system is a typical example for the DAC model. The object owner can separate permissions (read/write/execute) forusers in the same group and other users. DAC models are generallyemployedin legacy applications.DAC will therefore encountersignificant management overhead in cloud computing systems with modern multi-user and multi-application

systems[6].

Mandatory Access Control (MAC) models abstract the importance for resource-user mapping and thereforecan easily adapt to distributed systems[6]. The MAC model is normallyimplemented in multi-level security systems. For MAC models, access permissions are determined by the administrator of the information system, and not by the object owner. For multi-level MAC models, subjectsand objectsare identified with a particular security level of classification (e.g., Unclassified, Classified, Secret and Top Secret)[7]. The Bell LaPadula and Biba models recommend the "no- read-up", "no-read-down" rules and "no-write-down", "no-write-up" rules for maintaining confidentiality and integrityof information[6].

In RBAC, users have access to certain objects based on theirgiven role in the system. Roles normally are defined usingthe job functions. Permissions are also defined on the job authority and responsibilities. Operation on objects areactivated based on the permissions. Comparatively, RBAC models are more scalable than the DAC and MAC models.RBAC are more suitable for use in EHR systems and cloud computing environments, especially whereits difficult to track users of the services with fixed identity[6].

The relationship between resources and users is dynamic in the cloud andCSPs and users are not within the same security domain. DAC and MAC models cannot therefore be applied in a cloud computing environment, where resource nodesare not familiar, or may not know each other. Nevertheless, DAC and MAC models may play an important role in the hierarchy of managing EHR. It is impossible to identify users by fixed Internet Protocol (IP) addresses because users make use of different devices (mobile phone, tablet, notebook) to access the cloud network. In theseconditions, one cannot use the traditional firewalls to filter packets based on fixed IP addresses of users[6]. In a cloud, it is easy to identify users by their attributes or characteristics and not by any predefined identities. Thus, there is the need for a dynamic access control model in to order achieve cross-domain authentication[6].

In this paper, combined access control model (DAC, MAC, RBAC and ABAC) for EHR and cloud computing environment was the focus.There is a review of the current literature on each of the access control models and their variants (with respect to theircharacteristics and applicability).Combined access control model was discussed. The study identifies future research direction towards building effective access control models for EHR in a cloud computing environment.

2.0 Access Control Models

The advent of cloud computing and its associated challenges makes the classical access control models unsuitable for use within such an environment. Managing health records also require the use of these classical access control models in some form to ensure flexibility in the security of EHR within a cloud computing environment.

2.1 Discretionary Access Control (DAC)

Discretionary access control (DAC) is a type of access control where individual users set a mechanism for access control to deny or permit access to an object. DAC usually relies on the owner of the object to control access [8].

DAC is flexiblefor the object owner and this makes it the obvious choice for simple systems.DAC therefore grant users the exclusive right to control access to their data and to grant permission to other users. However, DAC is unable to ensure consistency with global policies and allow users to decide on the access control policies on the data.With respect to EHR, patients are not expected to be in full control of their health data. The health data is tool of communication between health professionals and should not be controlled only by patients. Patients can have access rights to read and write certain portions of their records (e.g. demography data) and should also be able to delegate access to others.

For DAC, copying of information can easily be done from one object to another.A delegated user can copy certain portions of health data of a patient.A "Trojan horse" program can easily change policiesand delete files on a users computer. These issues with DAC makes it unsuitable for single use for the management of EHR in a cloud computing environment. Thus, DAC cannot be fully implemented for EHR in a cloud computing. Some control may be granted to users to access their health information but other access control models have to be implemented to ensure secured, smooth and fine-grained access to the EHR in the cloud environment.

2.2 Mandatory Access Control (MAC)

In severalorganisations, users and clients do not own the information to which they are allowed access [8]. Normally, information is the sole property of organisations, and usersare not able to set-uptheir own permissions. In order to overcome the challenges associated with DAC in critical confidentialityenvironments, MAC was developed [7]. MAC was made to deal with confidential documents in computer systems (e.g., health records).

Mandatory access control (MAC) is a type of access policy controlled by a system which limits access to resource objects (devices, systems, data files, etc.) using the level of authorisation or permissionfrom the entity accessing the resource, be it process, person, or device [9].

Mandatory access control (MAC) restricts the ability of individual resource owners to deny or grant access to resource objects in a system. MAC criteria are normally defined by the system administrator, and are unable to be changed by end users. Mandatory access control (MAC)is implemented by allocating a classification label to every file system object. Each device and user on the system is allocated a similar classification and a clearance level. When a device or person attempts to access certain resource, the security kernel or system will check the credentials of the entity to ascertain whether access will be granted or not. MAC demands planning and continuous monitoring to maintain all users' and resource objects' classifications up to date[9].

A lot of restrictions are placed on user actions with respect to MAC which augur well for the security of the EHR. Nevertheless, this also prevents the flexibility needed to use the EHR to provide quality service to patients. MAC can needlessly overclassify data through its highwatermark principle.This would eventuallymake the sharing of EHR difficult by restricting the ability to transfer EHR between systems and users. MAC also is unable to address dynamic separation of duty, fine-grained least privilege, and validation or security of trusted components [10]. Although MAC may be applied in EHR, it is unsuitable for the cloud computing platform which demand unknown category of users.

2.3 Role-based Access Control (RBAC)

Access decisions for RBACare based on roles individual users have as part of an institution. Users normally take on assigned roles (pharmacist, doctor or nurse). Access rights are classified by role names, and resources are restricted to authorised individuals who assume the associated role. Users are admitted into roles based on their responsibilities and competencies within the institution [10].

Role-based access control (RBAC)[11] policies controlusers access to information basedon the activities the users do. "A role is a collection of permissions to use resources appropriate to a person's job function; it is thus defined as a set of actions and responsibilities associated with a particular working activity" [10].

Although RBAC is an improvement on flexibility as compared to MAC and DAC, it does not grantusers options with respect to the use of the access control [10]. Therefore, RBAC is difficult to use for supporting DAC policy. It is possible to implement DAC using RBAC by employingseveral roles related with each system object. This is the reason why it is important to implement EHR systems with combined access control methods [10]. Electronic health records implementation in a cloud computing environment would demandthat different access control systems are put together to strengthen the security architecture of the EHR application.

Another variant for RBAC is the task-role-based access control model (TRBAC) [12]which has the potential to be a very good model for EHR and cloud computing environments. TRBAC can dynamically authenticate access permissions for users depending on the given roles andtasks usersmust perform with given roles. A combination of TRBAC with other access controls has the potential to ensure a fine-grained access control system for EHR in a cloud computing environment [6].

2.4 Attribute-based Access Control (ABAC)

Attribute-based access control (ABAC)model's central idea states that access can be expressed based on several attributes presented by a user or subject [13]. Rules indicatethe conditions for which access is denied or granted.

The ABAC approach is more flexible compared to RBAC since it does not need separate roles for appropriate sets of subject attributes.For ABAC, rules can be quickly implemented to contain changing needs [14]. Using ABAC for managing access to EHR would enhance the access control model employed. Authentication of attributes might be distributed based on the power that releases a specific attribute, such as a hospital vouching for a user's or subject's professional status. Definition of attributes must be consistent and the same for all parties involved in the provision of health service [14].

Despite the benefits of ABAC, using it as a stand-alone access control method cannot satisfy all the access requirements of the EHR in a cloud computing environment. ABAC comes with complexities with the management of attributes which must be carefully distributed to guarantee uptimum usefulness of the system.Combining ABAC with other access control models would greatly enhance the security of EHR in a cloud computing environment.

3.0 Combined Access Control Model

The focus of research into access control models is aimed at delivering more expressive access control models that has the potential to consider emerging trends on temporal, context-aware, geographical, and pervasive computer systems. Mobile computing devices are forcing the inclusion of context awareness,geographical location and other important attributes into access control models.

Researchers are also focusing on access control policy administration [15,16]and shared security description in XML [17]. Combined access control models would also require joint policies to ensure secured EHR in a cloud computing environment.

Access control policies can be large in structures, and may involve many users and security administrators. Current research seeks to fill this combined access control policy gap bysuggesting methods for distributed policies, tools for facilitating design and maintaining access control policies. This is very important because most flaws in security are normally due to administrative mistakes or misconfigurations. AnyEHR in a cloud computing environment should define a security policy for the combined access control modeland ensure its enforcement.

Combined access control model has the potential to maximise the benefits of individual access control models whilst minimising their weaknesses. For the dynamic EHR in a dynamic cloud computing environment, combined access control model (MAC, DAC, ABAC and RBAC) and policy is most suitable. From the arguments so far, this paper postulates that individual use of any access control cannot grant maximum security to EHR in a cloud environment. The combination of all these access controls (MAC, DAC, ABAC and RBAC) would help strengthen security for the EHR in a cloud computing environment. This is crucial to support the security architecture for EHR in a cloud computing environment.

4.0 Conclusion and Future Research Directions

Access control is centralto security and paramount in protecting confidential information from unauthorised users and cyber attackers. Many models of access control have been built over decades to improve confidentiality, integrity, availability and administration flexibility. These access control models over the years have not been able to satisfy the privacy and security requirements of health and patient records. All access control models share a common criteria, i.e. they guarantee certain properties (confidentiality, integrity and availability of information, no conflicts of interest, etc.).

Combining these access control methods has the potential to extensively protect health records within a cloud computing environment. Their combination would minimise their weaknesses and enhance their strengths to protect the EHR from malicious health professionals and other cloud users.

The following future research directions for combined access control models for securing EHR in cloud computing environments have been identified.

- Further research to reduce insider threats to the EHR and cloud resources from a rogue CSP administrator and an employee in the healthcare organisation that seeks to exploit cloud weaknesses for unauthorised access.
- Further research to integrate the relationship between reputation and trust in combined access control models for secure and better quality of service within the cloud computing environment.

From the study, it is postulated that combined access control model has the potential to enhance security of EHR within a cloud computing environment. Their benefits are enhanced to mitigate their weaknesses when individual access control models are joined together.

References

[1] University, Carnegie Mellon;. (2003). *Overview Incident and Vulnerability Trends.* Carnegie Mellon University, CERT Coordination Center.

[2] Gollman, D. (1999). *Computer Security.* (1st, Ed.) John Wiley & Sons.

[3] Knitz, M. (2005). *HIPPA Compliance and Electronic Medical Records: are both possible?* Graduate Research, Bowie State University, Maryland.

[4] Sprague, L. (2004, September). Electronic Health Records: How close? How far to go? *NHPF Issue Brief* , 1-17.

[5] Miller, R., & Sim, I. (2004). Physicians use of Electronic Medical Records: Barriers and Solutions. *Health Aff (Millwood), 23* (2), 116-126.

[6] Maghanathan, N. (2013). Review of Access Control Models for Cloud Computing. *Computer Science & Information Science, 3* (1), 77-85.

[7] Bell, D., & Lapula, L. (1973). *Secure computer systems: Mathematical foundations and model.* The Mitre Corporation.

[8] Thion, R. (2008). *Access Control Models* . (F. University of Lyon, Ed.) IGI Global.

[9] Margaret, R. (2014, Jan). *Search Security*. Retrieved Jan 19, 2015, from Mandatory Access Control: http://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC

[10] Hu, V., Ferraiolo, D., & Kuhn, D. (2006). *Assessment of Access Control Systems.* Technical Report NISTIR-7316, National Institute of Standards and Technology.

[11] Ferraiolo, D., Kuhn, D., & Chandramouli, R. (2003). *Role-based Access Control.* Artech House, Computer Security Series.

[12] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. *Proceedings of the 13th ACM Conference on Computer and Communication Security*, (pp. 89-98).

[13] Karp, A., Haury, H., & Davis, M. (2009). *From ABAC to ZBAC: The Evolution of Access Control Models.* tech. reportHPL, HP Labs.

[14] Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding Attributes to Role-Based Access Control. *IEEE Computer*. vol. 43, no. 6 (June, 2010) , pp. 79-81.

[15] Sandhu, R., Bhamidipati, V., & Munawer, Q. (1999). The ARBAC97 Model for Role-based Administration of Roles . *ACM Trans. on Info. and Sys. Sec.*

[16] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, R., & Chandramouli, R. (2001). Proposed NIST Standard for Role-based Access Control . *ACM Trans. on Infor. and Sys. Sec.*

[17] Standards, O. f. (2005). Extensible access control markup language (XACML). *2*.