Asian Journal of Information Technology 16 (2-5): 274-281, 2017
ISSN: 1682-3915

Privacy and Security Challenges Towards Cloud Based Access Control in Electronic Health Records

Muhammad Ehsan Rana, Micheal Kubbo and Manoj Jayabalan
School of Computing,
Asia Pacific University of Technology and Innovation Technology,
57000 Bukit Jalil, Kuala Lumpur, Malaysia

Abstract: Over the years, data theft has been rampant in financial institutions, however at present medical data is in the spotlight. Healthcare industry is considered as a potential target for hackers and cyber criminals for accessing patient's data. Electronic Health Record (EHR) provide flexibility, timely access and interoperability of patient information which is key in decision making by physicians and medical officers. With the advancement of technology, cloud has been spotted as a solution for healthcare practitioners to implement interconnected EHR as it reduces cost and hassle of infrastructure maintenance. Cloud platform allows data to be replicated in different geographical locations and retrieved and shared among various organizations in a timely manner. Healthcare sector is facing a dilemma on how patient's information can be protected while it is being managed by cloud vendors. Several cloud-based EHR apply cryptographic techniques to encrypt data at rest/data in motion and access control to eliminate unauthorized access. As a result, existing access control mechanisms in cloud mainly focuses on giving data access to physicians and other medical officers but overlooks privacy requirements of patients. This research discusses various access control models, their merits, limitations and roles to promote privacy in cloud based solutions.

Key words: Access control, electronic health records, privacy, security, cloud platform

INTRODUCTION

Electronic Health Records (EHR) assist healthcare organizations towards fast and better delivery of services and treatment to patients (Hoerbst and Ammenwerth, 2010). Several countries are gradually migrating to EHR to provide better decision making. However, the utilization of paper based health records are not completely eradicated (Stausberg *et al*., 2003). Due to the technology advancement, healthcare organizations have integrated distributed heterogeneous systems and share the patient information with participating healthcare, pharmaceutical companies, researchers, etc. which leads to privacy and security issues (Jacob and Agrawal, 2010).

Cloud computing has been recognized as a cost-effective technique for small healthcare providers which attracts EHR to be deployed in the cloud and harmoniously managed (Lamar, 2011). Recent study highlights that 60% of independent physicians have resorted the use of EHR due to costs incurred in the implementation of a cloud-based system is profoundly low as compared to a self-managed system.

Some of the benefits identified in using cloud-based solutions include affordability, no contracts, availability and interoperability among others. The healthcare organizations should devise a risk management program on the cloud vendors to illuminate and guarantee security and privacy of the information.

Data security and privacy has a higher risk associated with the cloud which leads to a dilemma for some healthcare organizations that wishes to transfer their services to the cloud. Protecting patient's medical data is an utmost priority for any type of healthcare organization ensuring the information available only to authorized users. As the cloud is exposed to vulnerabilities, the vendors should provide total visibility to EHR consumers through the applied security controls. One primary way to secure data and leverage privacy in the cloud is through the use of an access control mechanism since the highest percentage of security breaches are due to unauthorized access (Lamar, 2011).

Privacy and security challenges and threats have existed over years mostly in financial institutions and payment card industry. However, the focus has now

Corresponding Author: Muhammad Ehsan Rana, School of Computing,
Asia Pacific University of Technology and Innovation Technology, 57000 Bukit Jalil, Kuala Lumpur, Malaysia

shifted towards healthcare industry as a primary target due to the enormous amount of sensitive information. This study mainly focuses on providing awareness of privacy, security issues and access control in electronic health records as they migrate towards the cloud.

Privacy challenges in electronic health records: EHR holds patient's health data which is regarded as very sensitive and therefore such systems holding this information should be in position to follow the golden rule of Confidentiality Integrity and Availability (CIA) to lower chances of data compromise, inform of theft, data breaches, physical attacks and hacking among others (Maslin and Ailar, 2015).

Data breaches: According to a survey conducted in UK, it is identified that over 75% of patient's are inquisitive on how their health data is shared with third-party organizations and/or stored. The perception in patients may be due to the fact that health data has been reported as the most targeted data by hackers and cyber criminals (Papoutsi *et al*., 2015).

Healthcare industry and companies processing health related information still remain the most targeted sector as it holds highly valued data which is also exposed to vulnerabilities through mobile and IoT devices. Moreover, 89% of the data breach identified are fueled by a financial motive Papoutsi *et al*. (2015) says medical records are 10 times worth compared to credit cards numbers. Security breaches might be subjected to a jail term as per the HIPAA rules and regulations if the responsible party is identified.

Furthermore, a data breach report from office of civil Rights emphasized that healthcare sector was one of the highly affected domain. The report further stated that, a total of 155 million records of patient's were exposed to public as a result of inappropriate measure to implement security controls on the system holding the data.

EHR considered to deal with two identified aspects of privacy; 'contextual oriented privacy' and 'content oriented privacy'. The ability of malicious parties to identify what kind of sickness a patient has is referred to as 'contextual oriented privacy'. This is normally achieved through investigating the field of the patient's physician. On the other hand, 'content oriented privacy' specifies the likelihood of stakeholders in healthcare organizations to disclose patient's sensitive data to other parties for instances, insurance companies and marketing agencies without patient consent.

As shown in Fig. 1, medical data theft ranks the highest category of data breach incidents according to the report with almost 700 attempts throughout the

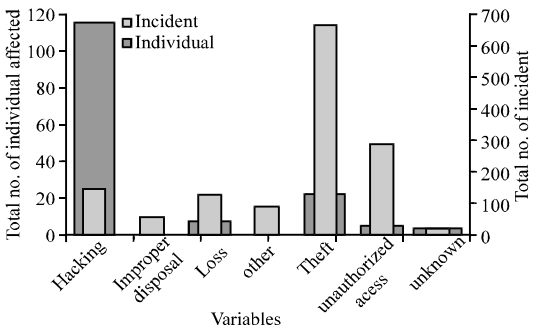

Fig. 1: Frequency of different data breach attack incidents with number of affected individuals from 2010-2016

course of 5 years. The hacking incidents also affected millions of individuals in the United States, although the frequency was moderately low compared to unauthorized access and data theft as shown in figure. These kinds of massive attacks in healthcare are a result of high monetary value attached to medical records making it the primary target for hackers.

Patient data visibility: As identified in the existing HIPAA privacy rule, patients should have full visibility of how their health records are used and for what purpose. However, this aspect has not been fully addressed by concerned parties and continues to be under violation. This is because, it is impossible for patients to oversee the usage of their health data unless they are included in the access control. Appari and Johnson (2010) argues that patient's involvement in management of their own health data in EHR would probably improve the privacy issues.

Security challenges in electronic health records: Security of healthcare information commences with the protection of patient medical records by guaranteeing that privacy, confidentiality and integrity of the EHR system is maintained at all times (Appari and Johnson, 2010). Technology advancement is rapid as never before, however the aspect of privacy concern in EHR still remain unclear towards consumers as a result of prevailing breach thus lowering the trust of the systems (Jacob and Agrawal, 2010). In this research, three categories of security challenges have been identified and included: human factors, law and Ethics, CIA protection.

Human factors: According to a study conducted by KTH university research students in Sweden over physicians, it was identified that around 76% of them considered human factor as the ultimate challenge in EHR implementation whereas 53% had little or no

interest in health IT. Therefore, EHR systems have a higher probability of being successfully implemented if the usability study is carried out beforehand adopting to the healthcare environment.

Robert further identifies human element as an important aspect in information security and privacy. The people interaction (usability) to medical data in the system should be considered during the design of EHR (Dlamini *et al*., 2009). Since, the current security threats are mostly assocaited with human aspects to the system. Thus, sufficient training to staff on the EHR usage and the need for patient's privacy requirements has to be addressed.

Law and ethics: According to an exploratory study conducted in the USA regarding third party access to medical records, it is argued that government should be able to override the disclosure of patient's privacy policies to third-party organizations. In the case of a disease outbreak, the government is supposed to coordinate with the research agencies to make sure that the consumption of medical data are dealt with in the best possible way without affecting the privacy of patients thus improving the quality of healthcare delivery.

Although, a number of rules and regulations both at the state and federal level have been established to protect patient privacy for instance: HIPAA, Health Information Technology for Economics and Clinical Health (HITECH) to leverage implementation of health IT infrastructure, privacy preservation of patient's data is still questionable (Sicuranza and Ciampi, 2014).

Confidentiality, Integrity and Availability (CIA) protection: As healthcare organization transform paper charts into computerized records through the use of EHR system, security breaches will always be a concern as this compromises the integrity and confidentiality of the health records (Bennani *et al*., 2008). As a result, generic requirements for EHR systems have been provided by International directives such as HIPAA, European Data Protection and requires EHR implementation to satisfy the CIA Traid. Below is the definition of CIA in EHR security requirements (Ferreira *et al*., 2011).

Confidentiality: This refers to the ability to safeguard information in the EHR system so that it can only be accessed by authorized subjects. Typically, authorized subjects will gain access based on the predefined role-based privileges. Therefore, no information about patients should be released without their consent unless otherwise as stated by privacy rule. Authorization is mainly carried out by a security mechanism called an "access control". It is a greater challenge for healthcare organizations since the medical data in the cloud based EHR is stored in cloud vendor centers which are usually distributed around several regions.

Integrity: Integrity can be understood as preserving the initial representation of data even in the case of any alterations (Fernandez-Aleman *et al*., 2013). Ensuring integrity is key in EHR systems since it guarantees the accuracy of data thus minimizing errors and improving the safety of patients (Appari and Johnson, 2010). Currently, authorized users can also participate greatly in creating inaccuracies if inadequately trained on the use of the for instance, the use of cut and paste feature. Drop down menus have also been reported as one of the main cause of data inaccuracies in EHR.

Availability: The system should be able to be accessed anytime when required by authorized parties and entities for example in the case of any emergency situation and a specific physician needs access to patient's record to carry out diagnosis and approve medication to a patient. The systems should not be constrained to a specific time of the day otherwise the physician's job will be made complex since decisions can't be made in real-time as required (Sicuranza and Ciampi, 2014).

Traditional access control in electronic health records: Information access control is considered as top most requirement for any healthcare organization implementing EHR in the cloud. Protecting patient's data and organizations resources from unauthorized disclosure while ensuring CIA triad is essential under any circumstances. Bill argues that for organizations to achieve these aspects, adoption of an appropriate access control mechanism is obligatory to enforce security and privacy protection over company's resources.

A wide variety of traditional access control methods have been implemented by various organizations depending on their structure. Below subsections discuss the different access control models.

Discretionary Access Control (DAC): Trusted Computer System Evaluation Criteria (TCSEC) defines this model as "a mechanism that restricts access to an object basing on identity attached to the subject or a group it belongs. In DAC, subjects can inherit and transfer access rights to each other unless otherwise if the restriction is enforced by mandatory access control."

One sole advantage of using DAC is that resource owners can specify and manage who can access particular resources, however, the access control design seems less

secure compared to MAC. Granting and revoking of permission is achieved through use of Access Control Lists (ACL) or identity-based access control. This kind of access control design is implemented mostly in the commercial operating system currently in use for example Windows based OS and Unix (Ozair *et al*., 2015).

EHR systems essentially hold data composed of thousands of clinical documents, these documents have various attributes like author, holder, patients and therefore identifying the owner of the document amidst these variables may be cumbersome. And not a suitable model for a dynamic domain like healthcare (Appari and Johnson, 2010).

Mandatory Access Control (MAC): Mandatory Access Control (MAC) is looked at as a solution for government systems that hold very sensitive information with label normally defined as top-secret (highest), secret, confidential and unclassified (lowest). The access control model is managed by a centralized authority that grants access decisions to the subjects requesting particular resources normally referred to as objects (Ozair *et al*., 2015).

MAC is generally more secure compared to the DAC and also follows the paradigm of using labels tagged with information to restrict object access by subjects. To illustrate the point, suppose a particular object is classified as confidential, only the subjects holding clearance level "confidential" can be able to access the specific object otherwise access is denied. To differentiate MAC from DAC, objects have to be identified and checked to ascertain whether they are associated with ACLs. MAC normally provides a high level of trustworthiness through the use security levels referred to as subject clearances. Therefore, an access class will be assigned to particular subjects and objects by the MAC that will secure how the information flows.

The model has been reported as "rigid" since it does not take into account dynamic and context-aware constraint for example; location, time, device among other constraints (Appari and Johnson, 2010). Secondly, MAC poses a greater challenge to implement in an environment with decentralized systems. In a nutshell, the model is expensive to implement and fails to support some important principles for instance; separation of duties, inheritance and least privilege.

Role-Based Access Control (RBAC): RBAC came into existence in early 1970 when system administrators started having data security issues and challenges as the information system started to serve multiple users along with heterogeneous applications (Samarat *et al*., 2001).

RBAC provides a natural mechanism to control resources in an organization which has led to popularity gain and adoption by various organizations (Bill *et al*., 2011). The system administrator will create roles that are linked by subject's function, grant access rights to the roles, thereafter assigning the users to the roles with their responsibilities. Unim and Rachid identifies three aspects that should be emphasized while dealing with this access control model.

Role assignment: A transaction can only be executed by a subject if and only if, a role has been assigned or selected, this aspect allows fine grain access to the specific resource by authorized subjects. Take an example if Mike has been assigned as role "Doctor" then, he is only allowed to access resources and act on them within that scope.

Role authorization: This simply allows users to only take up roles that they have been authorized, thus maintaining integrity however for DAC subjects can inherit privileges which can lead to privacy and confidentiality violation.

Transaction authorization: A transaction can only be carried out by an authorized subject with an active role. This aspect is considered as the basis on which an RBAC system operates.

Resources in an information system need to be protected, these system resources are in terms of objects that are stored in the operating system or a database management system (Samarat *et al*., 2001). Examples of objects include files, directories, rows, tables, columns to mention a few. RBAC objects do possess permissions which are assigned to roles. The model has a central component "role relations" which comprises of user assignment and permission assignment.

RBAC can be tailored to suit the changing needs of the organization, this is one key benefit of adopting this model. Secondly, it supports most fundamental security principle that include:

Data abstraction: Abstraction allows the establishment of abstract permissions for example from an account object like credit or debit. Therefore, the RBAC eliminates use of typical permission provided by the operating system that includes: read, write, execute.

Separation of duty: This principle is equally important in RBAC security, this allows mutually exclusive roles to be invoked to complete sensitive tasks. For example it will require the role of a doctor and laboratory technician to diagnose a patient and prescribe drugs.

Attribute-Based Access Control (ABAC): To fully understand how ABAC works, basic knowledge on how logical access control mechanism works is key. ABAC operates on logics to protect objects, data, applications and other forms of resources and services (Sandhu *et al*., 1996).

NIST provides an advanced definition of ABAC as an access control method where subjects requesting to carry out operations on the objects are evaluated basing on their own attributes, object attributes and policies that have been defined on the attributes and conditions. Therefore, the result of the evaluation is either a grant or deny access.

Next, ABAC utilizes a similar concept of policy management reflected in ACL or RBAC. However, in this case, policies can be evaluated based on more than one attribute (Sandhu *et al*., 1996). Implementations have been made to achieve ABAC with the use of RBAC, although compliance requirements have always been the case. This is because RBAC extends a high level of abstraction which makes a demonstration of requirements a costly and complex task.

In a healthcare setting, when a physician gets employed in the hospital, he will be assigned a set of attributes for example Jaya is nurse practitioner in the cardiology department. She will be assigned permission to the resources that can be invoked by her role. Authorized parties assigned to policies that have to be evaluated before access to any record is granted for instance: medical records for heart patients can only be viewed and edited by nurse attached to the cardiology department. As a result, object owners (patients) will create these policies once regarding who can have to access these medical records.

ABAC provides flexibility in such a way that suppose subjects from other hospitals need to access the specific object, they will be assigned attributes rather than roles thus making it easier for both objects owners and other authorities. ABAC provides total flexibility for EHR internal and external users, however since, external parties are assigned access to objects without prior knowledge of patients, this eventually raises accountability issues which are an important factor and requirement from international derivatives.

Table 1 summarizes a comparison of the supported components in traditional access control models. According to the table, all the access control models provide a certain level of security in restricting access to resources or objects however not all are suitable for EHR deployment for example: MAC, DAC and RBAC. ABAC Model is complex in nature in terms of deployment and would require great deal of managing the access policies if implemented in EHR system. In this regard, a hybrid tailored access control model that addresses all security requirements for cloud deployment and privacy needs to be investigated.

Table 1: Comparison between traditional access control models

	Supported components				
Access control	Flexibility	Privacy policy	EHR suitability	Suitability in cloud	Security
MAC	N/A	N/A	N/A	N/A	√
DAC	N/A	N/A	N/A	N/A	√
RBAC	√	N/A	N/A	N/A	√
ABAC	√	√	√	N/A	√

RESULTS AND DISCUSSION

To answer questions regarding how to eliminate unauthorized access in healthcare, different access control mechanisms have been developed and proposed to be applied depending on the organization and their privacy needs. MAC is one of the model that is suitable for military and government organizations. DAC is constrained with strict access to resources by authorized subjects thus not flexible and fit for healthcare organizations where flexibility and scalability is a necessity (Appari and Johnson, 2010).

RBAC deals with the complexity of roles and constraints using SOD principle which can also be expressed as "relationship based role" (Samarati *et al*., 2001). For flexibility in access control decisions based on user attributes and other environment constraints, ABAC might be the appropriate model (Sandhu *et al*., 1996).

Some of the previously proposed models on extending RBAC and ABAC are discussed in this section to find its applicability in cloud adopted EHR. Traditional access control models (Appari and Johnson, 2010) that mainly utilize access control lists and roles are not suitable for cloud deployment since they are rigid and cannot meet dynamic numbers of users involved in cloud deployments. Cloud require fine grained access control that can protect the confidentiality of outsourced data.

Trust context-aware access control model proposed (Sicuranza *et al*., 2014) to utilize trust level to acknowledge and verify the requestor of a particular resource. With trust computing employed, permissions are dynamically adjusted depending on the user behavior and the associated environment. Therefore, a predictive nature of authorization based on context information and trust level of the requesting subject will allow efficient resource sharing, however the model does not support privacy policy.

Similarly, semantic role-based access control model (Chen *et al*., 2014) allows collaboration among

heterogeneous platforms of an organization. The proposed model is generic and can be applied in any enterprise to allow run-time dynamic management and execution of access rights. Similarly, suppose the user roles change, this doesn't affect its operations, same as access model proposed by Sicuranza *et al.* (2014), though this model, utilizes XACML architecture and roles are based on OWL ontology.

To leverage trust in cloud, a Trusted Access Control Model (Kamoun and Tazi, 2014) that extends RBAC and task-based access control model this incorporates a reputation awarding mechanism that credits the user according to trust generated over time as per user behavior, the AC model seems to provide information security on the data however fails to address calculation of specific reputation value that reduces the accuracy level.

ABAC (Yue and Yong, 2015) defines a flexible access control model that allows attributes to be associated with users on the systems, this access control model defers a lot from RBAC in a way that attributed values are used as determinants for either denying or granting access to objects.

Additionally, (Hu *et al*., 2015) claims that ABAC Model was designed to overcome shortcomings addressed by classical access models like (DAC, MAC and RBAC) and also leverage security and information sharing. This includes the manual development of RBAC policies that are costly and difficult (Sharma and Joshi, 2016) compared to ABAC policies. Although, combining various access control seem inconvenient, Lawrence and Jim argues that in order to keep security levels optimal, MAC can be integrated with ABAC to leverage flexibility in access control decisions vis-a-vis other security attributes that may include subject property, clearance or classification.

Study by Kerr and Alves (2016) extends traditional ABAC to support attribute rules that are used for decisions and roles are assigned depending on attributes that are linked to tasks which hold permissions. As cloud adoption dominates enterprises, various authors have proposed mechanism to protect cloud data (Riad *et al*., 2015) that is based on encryption of attributes, this model employs a key policy attribute encryption scheme where key generation and decryption is outsourced to trusted authority. Moreover, with computational tasks being executed over mobile and sensors, the number of attributes will increase in the access policy as a result, a typical Attribute-Based Encryption (ABE) will not be in a position to retain its performance thus creating a computational overhead. Nevertheless, cryptographic access control (Lv *et al*., 2014) mechanism to facilitate authorization in the semi-trusted environment.

The work is expanded based on Riad *et al*. (2015), with an inclusion of a mediated revocation protocol component to address computation overheads identified in ABE. As the cloud is gaining massive attention by enterprise for adoption, Temporal Access Control Model (Figueroa and Pancho, 2014) for cloud data with user revocation, the solution is not so different from other researchers (Lv *et al*., 2014; Balani and Ruj, 2014; Fugkeaw and Sato, 2015), since all utilize the technique of CBE to protect the data outsourced. However, this proposed model provides an additional component that allows decryption of the data over a specified period of time by only the authorized subjects with user revocation capabilities.

Similarly, an extended access control model (Fugkeaw and Sato, 2015) uses cipher text policy comparative attribute-based encryption on top of abac there by supporting wildcards and negative attributes. This framework provides efficiency, since constant-size keys and ciphertexts are generated irrespective of the attributes involved thus providing a constant computational cost on lightweight mobile devices.

Limitations in cloud based access control models: Various mechanisms to restrict access and protect resources in the cloud have been proposed in these studies (Younis *et al*., 2014; Sicuranza *et al*., 2014). However, they fail to address security and privacy requirements for EHR conformance in the cloud, one of the most prevailing requirement as per HIPPA in access control is patients consent. A hybrid cloud-based EHR system design was proposed in which takes into account privacy and security requirement for example encryption of data at rest and in motion, notification of data owner on every access to patient's information, ultimate confidentiality, availability and access to records during an emergency situation. However, this design has not been implemented and its feasibility has not yet been established. Additionally, traditional models disregard patients from having access to their medical records as an exchange of medical records are also too complex. Some cloud EHR providers in the USA has demonstrated conformance to HIPAA requirements, patients have been granted a right to access a portion of their medical records as identified in privacy rule. However, the issues of total visibility and accountability on who and how medical records are accessed is generally still questionable.

CONCLUSION

Privacy and security are amongst the most challenging issues that are being faced by healthcare industry. These issues are mostly addressed by utilizing access control and cryptographic techniques. Patient's need for privacy is vital for EHR success. As a result, various authors have proposed access control models to deal with privacy related issues. A review of existing access control models reveals that most work presented in literature extend RBAC in order to provide flexibility and security however, do not address access control model requirements for instance a patient management service to allow 'patient consent'. As a result, trustworthiness between patients and EHR system can be improved by incorporating 'patient consent' as an integral EHR component.

In Nutshell, to better address the need of patients' privacy in the presence of security concerns in the cloud platform, a hybrid patient centered access control model should be proposed and designed to address patients' privacy requirements. Similarly, to further the research, the author seeks to implement and develop an access control model for cloud based EHR system that addresses security requirements as well as patient's privacy needs.

REFERENCES

Appari, A. and M.E. Johnson, 2010. Information security and privacy in healthcare: Current state of research. Int. J. Internet Enterp. Manage., 6: 279-314.

Balani, N. and S. Ruj, 2014. Temporal access control with user revocation for cloud data. Proceedings of the 2014 IEEE 13th International Conference on Trust Security and Privacy in Computing and Communications (TrustCom), September 24-26, 2014, IEEE, Atlanta, Georgia, ISBN:978-1-4799-6514-4, pp: 336-343.

Bennani, A., M. Belalia and R. Oumlil, 2008. As a human factor, the attitude of healthcare practitioners is the primary step for the E-health: First outcome of an ongoing study in Morocco. Commun. IBIMA., 3: 28-34.

Chen, Y.Y., J.C. Lu and J.K. Jan, 2012. A secure EHR system based on hybrid clouds. J. Med. Syst., 36: 3375-3384.

Dlamini, M.T., J.H. Eloff and M.M. Eloff, 2009. Information security: The moving target. Comput. Sec., 28: 189-198.

Fernandez-Aleman, J.L., I.C. Senor, P.A.O. Lozoya and A. Toval, 2013. Security and privacy in electronic health records: A systematic literature review. J. Biomed. Inf., 46: 541-562.

Ferreira, A., C.R. Cruz and L. Antunes, 2011. Usability of authentication and access control: A case study in healthcare. Proceedings of the 2011 IEEE International Conference on Carnahan Security Technology (ICCST), October 18-21, 2011, IEEE, Porto, Portugal, ISBN:978-1-4577-0902-9, pp: 1-7.

Figueroa, K.G. and F.S. Pancho, 2014. An access control framework for semi-trusted storage using attribute-based encryption with short ciphertext and mediated revocation. Proceedings of the 2nd International Symposium on Computing and Networking (CANDAR) 2014, December 10-12, 2014, IEEE, Quezon City, Philippines, ISBN:978-1-4799-4151-3, pp: 507-513.

Fugkeaw, S. and H. Sato, 2015. An extended CP-ABE based access control model for data outsourced in the cloud. Proceedings of the IEEE 39th Annual Conference on Computer Software and Applications (COMPSAC) 2015, July 1-5 2015, IEEE, Tokyo, Japan, ISBN:978-1-4673-6564-2, pp: 73-78.

Hoerbst, A. and E. Ammenwerth, 2010. Electronic health records: A systematic review on quality requirements. Methods Inf. Med., 4: 1-16.

Hu, V.C., D.R. Kuhn and D.F. Ferraiolo, 2015. Attribute-based access control. Comput., 48: 85-88.

Jacob, J. and V. Agrawal, 2010. Privacy in Electronic Health Record Systems Consumers Perspective. Stockholm University, Stockholm, Sweden,.

Kamoun, A. and S. Tazi, 2014. A semantic role-based access control for intra and inter-organization collaboration. Proceedings of the IEEE 23rd International Conference on WETICE 2014, June 23-25, 2014, IEEE, Toulouse, France, ISBN:978-1-4799-4248-0, pp: 86-91.

Kerr, L. and F.J. Alves, 2016. Combining mandatory and attribute-based access control. Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS) 2016, January 5-8, 2016, IEEE, Moscow, Idaho, ISBN:978-0-7695-5670-3, pp: 2616-2623.

Lamar, M., 2011. EHRS in the cloud. J. Ahima, 82: 48-49.

Lv, Z., J. Chi, M. Zhang and D. Feng, 2014. Efficiently attribute-based access control for mobile cloud storage system. Proceedings of the IEEE 13th International Conference on Trust Security and Privacy in Computing and Communications (TrustCom) 2014, September 24-26, 2014, IEEE, Beijing, China, ISBN:978-1-4799-6514-4, pp: 292-299.

Maslin, M. and R. Ailar, 2015. Cloud computing adoption in healthcare sector: A SWOT analysis. Can. Center Sci. Educ., 11: 12-18.

Ozair, F.F., N. Jamshed, A. Sharma and P. Aggarwal, 2015. Ethical issues in electronic health records: A general overview. Perspect. Clin. Res., 6: 73-76.

Papoutsi, C., J.E. Reed, C. Marston, R. Lewis and A. Majeed *et al.*, 2015. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed methods study. BMC. Med. Inf. Decis. Making, 15: 1-15.

Riad, K., Z. Yan, H. Hu and G.J. Ahn, 2015. AR-ABAC: A new attribute based access control model supporting attribute-rules for cloud computing. Proceedings of the IEEE Conference on Collaboration and Internet Computing (CIC) 2015, October 27-30, 2015, IEEE, Beijing, China, ISBN:978-1-5090-0090-6, pp: 28-35.

Samarati, P. and S. de Capitani di Vimercati, 2001. Access Control: Policies, Models and Mechanisms. Springer-Verlag, Berlin, Heidelberg, pp: 1-56.

Sandhu, R.S., E.J. Coyne, H.L. Feinstein and C.E. Youman, 1996. Role-based access control models. IEEE Comput., 29: 38-47.

Sharma, N.K. and A. Joshi, 2016. Representing attribute based access control policies in Owl. Proceedings of the IEEE 10th International Conference on Semantic Computing (ICSC) 2016, February 4-6, 2016, IEEE, Delhi, India, ISBN:978-1-5090-0662-5, pp: 333-336.

Sicuranza, M. and M. Ciampi, 2014. A semantic access control for easy management of the privacy for EHR systems. Proceedings of the 9th International Conference on P2P Parallel Grid Cloud and Internet Computing (3PGCIC) 2014, November 8-10, 2014, IEEE, Naples, Italy, ISBN:978-1-4799-7872-4, pp: 400-405.

Sicuranza, M., A. Esposito and M. Ciampi, 2014. A patient privacy centric access control model for EHR systems. Int. J. Internet Technol. Secured Trans., 5: 163-189.

Sicuranza, M., A. Esposito and M. Ciampi, 2015. An access control model to minimize the data exchange in the information retrieval. J. Ambient Intell. Hum. Comput., 6: 741-752.

Stausberg, J., D. Koch, J. Ingenerf and M. Betzler, 2003. Comparing paper-based with electronic patient records: Lessons learned during a study on diagnosis and procedure codes. J. Am. Med. Inf. Assoc., 10: 470-477.

Younis, Y.A., K. Kifayat and M. Merabti, 2014. An access control model for cloud computing. J. Inf. Secur. Appl., 19: 45-60.

Yue, Q.F. and S.Z. Yong, 2015. Trusted Access Control model based on role and task in cloud computing. Proceedings of the 7th International Conference on Information Technology in Medicine and Education (ITME) 2015, November 13-15, 2015, IEEE, Jinan, China, ISBN:978-1-4673-8302-8, pp: 710-713.