Privacy and Security Challenges in Cloud Based Electronic Health Record: Towards Access Control Model

Micheal Kubbo[1], Manoj Jayabalan[2], Muhammad Ehsan Rana[3]

School of Computing, Asia Pacific University of Technology and Innovation
Technology Park Malaysia, Bukit Jalil - 57000 Kuala Lumpur, Malaysia
kubbomicheal@gmail.com[1], manoj@apu.edu.my[2], muhd_ehsanrana@apu.edu.my[3]

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 patients' 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 patients' 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.

KEYWORDS

Access Control, Electronic Health Records, Privacy, Security, Cloud Platform.

1. INTRODUCTION

Traditional healthcare industry uses paper based health record to store the patients' medical history, medical multimedia data and etc. However there is a gradual shift towards Electronic Health Record (EHR) to provide quality service at faster pace [1]. According to the technology report, Malaysian healthcare sector uses the combination of paper and electronic format to store patients' information [2]. Paper based records cannot be completely eliminated in healthcare however it can be reduced to a certain magnitude [3]. EHR provides a platform to integrate several IT systems in an organization with the capabilities to share the information with other healthcare, insurance companies and etc. However, privacy still remains a very big concern for healthcare consumers [4].

EHR requires quite a huge investment on setting up an infrastructure with the overhead maintenance cost. Independent healthcare practitioners and small clinics gradually moving towards the cloud based EHR. Cloud computing has been recognized as a cost-effective technique for small healthcare providers due to the elimination of individually managed IT infrastructure [5].

Some of the other benefits which can be enjoyed using cloud solutions include affordability, no contracts, availability, and interoperability.

Privacy and security are the ultimate challenges for the healthcare organizations to devise their migration to cloud [6]. Cloud vendor stores the patients' data into different data centers which can lead to several vulnerabilities. Protecting patients' medical data is an utmost importance for any type of healthcare organization ensuring that the information is available only to authorized users. 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 [5]. This research provides an overview of the various access control mechanisms available for EHR, their strength, and weakness.

2. PRIVACY AND SECURITY CHALLENGES IN ELECTRONIC HEALTH RECORD

Technology advancement is rapid as never before and the aspect of privacy concerns in EHR remain unclear towards consumers as a result of prevailing breaches thus lowering the trust of the systems [4]. Healthcare should move towards the latest advent of technology to counter-measure the security incidents [12]. In this research, three categories of security challenges have been identified and included: - Human factors, Law and Ethics, CIA Protection.

2.1 *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 [13]. Therefore, EHR systems have a higher probability of being successfully implemented if the usability study is carried out beforehand adopting to the healthcare environment. Secondly, sufficient training of staff on the EHR usage and the need for patients' privacy requirements has to be addressed.

2.2 *Law and Ethics*

According to an exploratory study conducted in the US regarding third party access to medical records, it is argued that government should be able to override patients' privacy policies and rules regarding disclosure of their medical records to third-party companies. When there is a case of outbreak disease, the government is supposed to coordinate with these research agencies to make sure that these issues are dealt within the best possible way without affecting the privacy of patients, thus improving the quality of healthcare delivery [14].

Although a number of rules and regulations both at the state and federal level have been established to protect patient's privacy for instance: Health Insurance Portability Accountability Act (HIPAA), Health Information Technology for Economics and Clinical Health (HITECH) to leverage implementation of health IT infrastructure, privacy preservation of patients' data is still questionable [15].

2.3 *Confidentiality, Integrity and Availability (CIA) Protection*

As healthcare organization transform paper based health records into computerized records through the use of EHR system, security breaches will always be a concern to ensure only the authorized person should be able to modify the data and it is visible only to the respective person [16]. As a result, generic requirements for EHR systems have been provided by International directives such as HIPAA and European Data Protection which requires EHR to be implemented satisfying the CIA Traid [17]. Below is the definition of CIA security requirements [18].

2.3.1 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 [10]. 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 data centers which are usually distributed around several regions.

2.3.2 Integrity

Integrity can be understood as preserving the initial representation of data even in the case of any alterations [20]. Ensuring integrity is key in EHR systems since it guarantees the accuracy of data, thus minimizing errors and improving the safety of patients. Currently, authorized users can also participate greatly in creating inaccuracies if inadequately trained on the use of the system, for instance, the use of cut and paste feature. Drop down menus have been reported as one of the main cause of data inaccuracies in EHR. These operations are performed by physicians who are in a hurry, thus causing data integrity issues [10].

2.3.3 Availability

The system should be able to allow access anytime when required by authorized parties and entities. In case of an emergency situation, a specific physician should be able to access the patient's record to carry out diagnosis and approve medication. The systems should not be constrained to a specific time of the day, otherwise the physician's job will become even more difficult since decisions can't be made in real-time as required [15].

3. 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 [21]. Bill et.al [18] argues that for organizations to achieve these aspects, adoption of an appropriate access control mechanism is obligatory to enforce security and privacy protection.

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 methods.

3.1 *Discretionary Access Control (DAC)*

Trusted Computer System Evaluation Criteria (TCSEC) [21] 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 [2], [21]. This kind of access control design is implemented mostly in the commercial operating system currently in use for example Windows based OS and Unix [22].

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. Keeping in view that stated concerns, it is not a suitable model for a dynamic domain like healthcare [12].

3.2 *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) [2]. 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 [22].

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 [12]. 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.

3.3 *Role-Based Access Control (RBAC)*

RBAC came into existence in early 1970 when system administrators started experiencing data security issues and challenges as the information systems started to serve multiple users using heterogeneous applications [23]. RBAC provides a natural mechanism to control resources in an organization which has led to popularity gain and adoption by various organizations [21]. The system administrator will create roles that are linked by subjects' function, grant access rights to the roles, thereafter assigning the users to the roles with their responsibilities. [17] 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 might be objects that are stored in the operating system or a database management system [23]. Examples of objects include files, directories, rows, tables, columns to mention a few. In 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.

3.4 *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 [25].
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 [25]. 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 or she will be assigned a set of attributes, for example Jaya is a 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 for instance: medical records for heart patients can only be viewed and edited by nurse attached to the cardiology department. As a result, patients can define the consent on the data to allow access to these medical records.

ABAC provides flexibility and interoperability which assist subjects from other hospitals to access the specific object without the need of assigning them to particular role. 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.

4. 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 [21]. MAC is one of the model that is suitable for military and government organization which does not require granular level permission. Secondly, DAC is constrained with strict access to resources by authorized subjects, thus not a flexible model for healthcare organization where flexibility and scalability is a necessity [12].

RBAC deals with the complexity of roles and constraints using SOD principle which can also be expressed as "relationship based role" [23]. For flexibility in access control decisions based on user attributes and other environment constraints, ABAC might be the appropriate model [25].

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 [12] 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 [27] 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 [28] 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 [27], though this model utilizes XACML architecture and roles are based on OWL ontology. To leverage trust in cloud, a *trusted access control model* [29] that extends RBAC and task-based access control model, 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 [30], [31] 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, Nitin and Anupam [32] 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 [33] compared to ABAC policies. Although combining various access control seem inconvenient, Lawrence and Jim [34] argues that in order to keep security levels optimal, MAC can be integrated with ABAC to leverage flexibility in access control decisions vis-à-vis other security attributes that may include subject property, clearance or classification.

Study by [35] extends traditional ABAC to support attribute rules that are used for decisions and roles that are assigned depending on attributes linked to tasks which hold permissions. As cloud adoption dominates enterprises, various authors have proposed mechanism to protect cloud data [36] 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.

Cryptographic access control [37] mechanism facilitates authorization in a semi-trusted environment. The work is expanded based on [36], 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* [38] for cloud data with user revocation within a particular time frame in CBE, is not so different from other researches [36], [37], [39], [40] 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 [40] uses Cipher Text Policy Comparative Attribute-Based Encryption on top of ABAC thereby 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.

4.1 Limitations in Cloud Based Models

Various mechanisms to restrict access and protect resources in the cloud have been proposed in these articles [24], [27], [29], [37], [39] and [40]. 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 *patient's consent* [42]. A hybrid cloud-based EHR system design was proposed in [42] 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 patients' 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 exchange of medical records are also too complex [23], [25], [42]. 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.

5. 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 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 a nutshell, to better address the need of patients' privacy in the presence of security issues on cloud platform, a novel cloud privacy-centric access control model should be proposed and designed.

REFERENCES

[1] Hoerbst, A. & Ammenwerth, E., 2010."Electronic Health Records - A Systematic Review on Quality Requirements," Methods Inf Med, Schattauer, Volume 4, pp. 1-16.

[2] Tech Review, M., 2006."EMR-Health Technology assessment unit," Medical Development Division, Kuala Lumpur: Ministry of Health.

[3] Jurgen, S., Priv, D., Dietrich, K. J. I. & Dr Rer, N. M. B., 2003. "Comparing Paper based with Electronic patients Records: Lessons Learned during a Study on Diagnosis and Procedure Codes," Journal of the American Medical Informatics Association, 10(5), pp. 2-8.

[4] Jibin, J. & Vivek, A., 2010."Privacy in Electronic Helath Records Systems - Consumer's perspective, s.l.: Stockholm University.

[5] M. Lamar, "EHRS in the Cloud," Journal of AHIMA, vol. 82, no. 7, pp. 48-49, 2011.

[6] E. Brian, "HIT Think How to manage risk with cloud vendors," Health Data Management, 2016.

[7] M. Maslin and R. Ailar, "Cloud Computing Adoption in Healthcare Sector: A SWOT Analysis," Canadian Center of Science and Education, vol. 11, no. 10, pp. 12-18, 2015

[8] BitGlass, "Healthcare Breach Report 2016," BitGlass Inc., 2016.

[9] ClickCare, 2014."Healthcare BYOD and HIPAA Security," San Jose: ClickCare LLC.

[10] Edward, H. S., 1999. "The Evolution of Electronic Medical Records". Academic Medicine, 74(4), pp. 414-419.

[11] Ronald, B., John, S. & Robert, K., 2015. "New challenges for Electronic Health Records Confidentiality and Access to Sensitive Health Information About Parents and Adolescents," The Journal of the American Medical Association, 313(1), pp. 29-30.

[12] Ajit, A. & Eric, M. J., 2010." Information security and privacy in healthcare: Current state of Research," Int. J. Internet and Enterprise Management, 6(4), pp. 279-313.

[13] Experian,"Third Annual Data Breach Industry Forecast," Experian Inc., 2016.

[14] S. Chris and M. Christopher,"Healthcare's IoT Dilemma: Connected Medical Devices," Forrester Research Inc., 2016.

[15] Sicuranza, M. & Ciampi, M., 2014."A sematic Access Control for easy management of privacy for EHR Systems,"IEEE-Advancing Technology for Humanity, pp. 400-405.

[16] unim, B. & Rachid, O. A.-E. B., 2008."As a human factor, the attitude of healthcare practitioners is the primary step for the e-healthFirst outcome of an ongoing study in Morocco," Communications of the IBIMA, Volume 3.

[17] Patients' GP and hospital data to be linked to help plan services", Clinical Pharmacist, 2013.

[18] Ferreira, A., Cruz, C. R. & Antunes, L., 2011. "Usability of authentication and access control: a case study in healthcare," Journal of Informatics

[19] ISO/TR, 2005. "Health Informatics-Electronic Health Record, Definition, scope and context," s.l.: ISO/TR 20513Jose, L. F.-A., Inmaculada, C. S., Pedo, A. O. L. & Ambrosio, T., 2013. Security and Privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, Volume 46, pp. 541-562.

[20] Jose, L. F.-A., Inmaculada, C. S., Pedo, A. O. L. & Ambrosio, T., 2013."Security and Privacy in electronic health records: A systematic literature review," Journal of Biomedical Informatics, Volume 46, pp. 541-562.

[21] Bill, B., Tricia, B. & Erin, K. B., 2011."Information Systems Security & Assurance series. In: Access Control, Authentication, and Public Key Infrastructure,". Burlington: John & Barlett Learning, pp. 208-211.

[22] Nayer, J., Amit, S. & Praveen, A., 2015."Ethical issues in electronic heath records: A general overview," Perspectives in Clinical Research, 6(2), pp. 73-76

[23] Pierangela, S. & Sabrina De Capitani, d. V., 2000. "Access Control: Policies, Models, and Mechanisms," Brescia: Universita di Milano.

[24] Younis, A. Y., Kashif, K. & Madjid, M., 2014."An access control model for cloud computing,".Journal of Information Security and Applications, Volume 19, pp. 45-60.

[25] Ravi, S. S., Edward, J. ,. C., Hal, L. F. & Charles, E. Y., 1996."Role Based Access Control Models," s.l.: Seta Corporation.

[26] Vincent, C. H. et al., 2014."Guide to Attribute Based Access Control (ABAC) Definition and Considerations," McLean: NIST Special Publication .

[27] Mario, S., Angelo, E. & Mario, C., 2014."A patient privacy centric access control model for EHR systems," International Journal of Internet and Secured Transactions, 5(2), pp. 163-187

[28] L. Chen, Q. Zhou, G.-f. Haung and L.-q. Zhang, "A trust Role based context aware access control model," 2014.

[29] K. Aymen and T. Said, "A semantic role-based access control for intra and inter-organization collaboration," Toulouse, 2014..

[30] Y.-q. Fan and Y.-s. Zhang, "Trusted Access Control Model Based on Role and Task in Cloud Computing," Jinan, 2015.

[31] S. Mario, E. Angelo and C. Mario, "An access control model to minimize the data exchange in the information retrieval," Journal of Ambient Intelligence and Humanized Computing, 2015.

[32] C. H. Vincent, D. Richard and F. F. David,"Attribute-Based access Control," IEEE Computer Society, 2015.

[33] K. S. Nitin and J. Anupam, "Representing Attribute Based Access Control policies in OWL," Laguna Hills,, 2016.

[34] X. Zhongyuan and D. S. Scott, "Mining Attribute-Based Access Control Policies," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, vol. 12, no. 5, pp. 533-545, 2015.

[35] K. Lawrence and A.-F. Jim, "Combining Mandatory and Attribute-based Access Control," 2016.

[36] R. Khaled, Y. Zhu, H. Hongxin and A. Gail-Joon, "AR-ABAC: A new Attribute Based Access Control Model supporting Attribute Rules for Cloud Computing," in 2015 IEEE Conference on Collaboration and Internet Computing, Clemson, 2015.

[37] L. Zhiquan, C. Jialin, Z. Min and F. Dengguo, "Efficiently Attribute-Based Access Control for Mobile Cloud Storage System," in 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014.

[38] G. F. Kathleen and P.-F. Susan, "An Access Control Framework for Semi-trusted storage using Attribute-based Encryption with Short Ciphertext and Mediated Revocation," Quezon, 2014.

[39] B. Nihal and R. Sushmita, "Temporal Access Control with user Revocation for Cloud Data," 2014.

[40] F. Somchart and S. Hiroyuki, "An Extended CP-ABE based Access Control Model for Data Outsources in the cloud," in IEEE 39th Annual International Computers, Software & Applications Conference, 2015.

[41] W. Zhijie, H. Dijiang, Z. Yan, L. Bing and C.-J. Chung, "Efficient Attribute-Based Comparable Data

Access Control," IEEE Transactions on computers, vol. 64, no. 12, pp. 3430-3443, 2015.

[42] H. Vincent, F. F. David, D. K. Richard, N. K. Raghu and L. Yu, "Implementing and Managing Policy Rules in Attribute Based Access Control," Gaithersburg, 2015.

[43] Y. Chen, J. Lu and J. Jan."A secure EHR system based on hybrid clouds," J. Med. Syst. 36(5), pp. 3375-84. 2012.