International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

An Analysis of Security and Privacy in Cloud Based Electronic Health Record Systems

Ms. Farog Fatema Khan[1], Dr. G.R. Bamnote[2]

[1]Department of Computer Science and Engineering, PRMITR, Badnera, Maharshtra, India
[2]HOD of Computer Science and Engineering, PRMITR, Badnera, Maharashtra, India

---

Abstract: *Many recent advancements in Information and Communication Technology has undoubtedly improved services in all sectors in the world. Specifically, Information Technology has led to a very vital innovation in health sector called electronic health. In order to optimize full and excellent benefits of this innovation, its implementation in a cloud-based environment is important. However, with noticeable and numerous benefits inherent from e-Health in a cloud computing, its full utilization is still being hampered by challenges of security and privacy. Medical organizations find it challenging to adopt cloud-based Electronic Health Records (EHR) services due to the risk of data breaches and the resulting compromise of patient data. The privacy of the patient and the security of their information is the most imperative barrier to entry when considering the adoption of electronic health records in healthcare industry. This paper focuses on review of existing literatures of various approaches and mechanisms being used to handle security and privacy related matters in Electronic Health Records (EHR) services.*

Keywords: EHR, e-health, security, privacy.

1. INTRODUCTION

In this current world of digitalization, the cloud computing technology is adapted by many institutes and individuals due to its nature of easy sharing and easy distribution of assets. Cloud computing is a type of model or service that aids omnipresent, suitable, on-demand access to the network to a common pool of computing resources such as networks, servers, storage, applications, and services and requires least management work or service provider collaboration [1]. Applications, servers, networks, and storage with a user-oriented platform are the resource sharing services provided by cloud computing. Two of the basic characteristics of the cloud are; storage, a system used to keep data, and the other one is data sharing, the process of transferring data from one person to another.

So basically, the cloud is a type of virtual storage system used on-demand in which its users can store their personal, financial, business data as well as share them with others. The cloud system can be classified into two types; the first one is public cloud system providing offsite solutions with various models like software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). Windows Azure services platform and Google AppEngine are examples of the public cloud [2].

The e-health (electronic health) system as the name suggests is a kind of health system which uses computer or electronic systems and cloud technology as its main source of operations for storing and sharing patient's medical data between healthcare service providers and patients [3]. It is different from the pen-paper based traditional health system. International Organization for Standardization (ISO) describe that Electronic Health Record (EHR) is a storage, secure exchange and access to patient information in digital format by several authorized users. This information includes the patient's past, present, and future information. Objective of EHR is to support the maintenance of integrated, efficient and quality health. Electronic Health Record (EHR) can be defined as an electronic version of a patient's health history that documents all the relevant clinical details over a period of time and is maintained by healthcare providers. These EHRs help organizations provide improved healthcare services by automating patient information access and management [3].

An EHR can contain important personal information such as name, address, phone number, birth date and Social Security Number. It also holds vital medical information about a person like diagnosis, treatment history, lab results, and prescriptions. There are great advantages to using electronic records more extensively, within both the offices of individual providers, where they are known as electronic medical records (EMRs), and when such records are linked across multiple providers, in which case they are known as electronic health records (EHRs). [4] Another benefit of the EHR is that vital medical information and patient history could be accessed at any location with ease of use and with immediate results. It also reduces the amount of time, money, and resources spent on copying multiple versions of a patient's history.

In developing of EHR, some of the barriers are encountered, which can be categorized as technical, organizational, personal, financial, and moral-legal barriers [5]. Hence in regard to this, the use of new technologies such as cloud computing is effective in its successful implementation.

There are many security and privacy issues that have raised difficulties for the adoption of cloud-based EHR

systems. In the United States, compliance to HIPAA (Health Insurance Portability and Accountability Act) [6] is often cited as the requirement to preserve the confidentiality of medical records including EHRs. In accordance with HIPAA guidelines, a set of valuable security and privacy requirements must be put in place for effective utilization of e-Health. These are presented in Table 1 [7].

Requirement	Description
Patient's understanding	This implies that patients have an exclusive right to know and understand how their sensitive and private health information are kept and utilized by any healthcare provider.
Patient's control	This allows patients to be given permission to determine who can access his/her health data.
Confidentiality	Health information should be kept away from people who should not access it. The sanctity of the information should be maintained.
Data integrity	This ensures that manipulation and omission of health information is totally prohibited. Hence, health information being shared should be a true representation of original information without any form of amendment or alteration.
Non-repudiation	Healthcare practitioner should deny the fact that it has performed a certain activity on the sensitive data of patient. Such activity should be supported with evidence to avoid dispute or suspicion.

Table 1: Security and privacy requirements as recommended by HIPAA

As cloud service providers are not trusted to store EHRs unencrypted, even when access controls are in place [8], EHR encryption must be required in cloud-based EHR systems. Also, security and privacy in EHRs can be seriously threatened by hackers, viruses, and worms. Many reports of accidental loss or the theft of sensitive clinical data have appeared in recent years. Knowing the security and privacy features that EHR systems have could be critical if these risks are to be confronted and measures to increase the data protection of EHRs are to be adopted [9].

Providing access to EHRs is a vital next step in activating patients in their care and improving the health system. However, this opens new security threats. There is a real concern about both people's and entities' access levels to patients' EHRs. A patient's EHR might be fragmented and accessible from several sites. Security defects in some of these systems could cause the disclosure of information to unauthorized persons or companies, and health data therefore need protection against manipulations, unauthorized accesses and abuses, which includes taking into account privacy, trustworthiness, authentication, responsibility and availability issues. EHRs also have difficulties in maintaining data privacy, to the extent that administrative staff could for example access information without the patient's explicit consent [9].

2. LITERATURE REVIEW

There has been an increased adoption of cloud-based EHR services for efficient health data management and control. This can be attributed to the elasticity, high level of availability, and reduced cost of cloud services. Various research efforts have been proposed with major focus on secure, cloud-based EHR systems. This section presents review of several articles in journals, conference proceedings on various security approaches and mechanisms being used in e-Health.

Automating medical health record management systems has been the focus of much past research. Edward H. Shortliffe, in his article he describes the problems associated with paper-based record keeping and the promise of the electronic medical record, emphasizing the areas of clinical trials and decision support. He then discusses the issues that must be addressed and the requirements that must be met if electronic medical record systems are to move beyond intranet environments within single health systems or practices and to integrate instead with regional, national, and international resources via the Internet [9].

The traditional way of obtaining and gathering patient information is paper based. Csiszar submitted that medical institutions would still rather use paper to gather information from their patients and also to record surgical procedures, observations and prescriptions. Some practitioners and physicians find accessing digital records somewhat complicated than obtaining a notepad and a pen. The thing that makes manual keeping of records very exhausting may be the mere undeniable fact that every day, a large number of new records are being stored in hospitals. It will be very complicated to sort medical records of all patients that keep increasing every minute [10]. This complexity often arises to errors that will greatly get new daily happenings in hospitals, clinics and all sorts of other healthcare institutions. Aside from being time-consuming, collating records can be hard if you have no main paperback that may contain all information.

Joshi et.al. developed an access control model based on Attribute Based Access Control (ABAC). This model evaluated an access decision based on the attributes of the user requesting a document and those of the requested document. Access control decisions were evaluated against an organizational confidentiality policy. This work demonstrated the use of policy-based, semantic web approach of implementing ABAC at a document level. The system has been improved to evaluate an access decision on the fields of a document rather than the entire document [11].

The previously developed system by Shi et. al. demonstrated the concept of edge computing, where the organizational boundary was considered to be the edge of the system. The cloud service provider was considered as an untrusted entity and thus laid beneath the organizational edge. All data transactions between the organizational edge and the cloud were encrypted, obscuring the access patterns between the organization and the cloud service provider [12].

Shin et al. (2014) examined various security models for healthcare applications and attempted to see how information leakage could be protected. They evaluated various security requirements to ensure security and privacy in electronic health. To find solution to identified security challenges in electronic health, they employed extended Role Based Access Control (RBAC) security model. They came up with u-healthcare service integration platform where extended RBAC model was deployed. The architecture was designed to carry out four main functions: exchanging health information, meal recommendation, transaction of health information and management of health information on any smart devices [13]. It is however worthy of note that security issue was not properly resolved. The model is not suitable for any distributed environment. As a result, the solution provided has limited applications. The application does not also consider expansion in the number of users. It is however worthy of note that security issue was not properly resolved. The model is not suitable for any distributed environment. As a result, the solution provided has limited applications. The application does not also consider expansion in the number of users.

To protect data privacy and threats, various encryption models have been proposed. Attribute Based Encryption (ABE) is one approach where a user's ciphertext, secret key and private key are associated with her attributes. Goyal et. al. proposed an attribute-based system called the Key-Policy Attribute Based Encryption (KPABE) in which ciphertexts are tagged with attributes corresponding to access control structures [14].

Bethencourt et al. have developed a system called the Ciphertext-Policy Attribute Based Encryption (CPABE) for implementing ABE using the attributes of the user encrypting the document. The EHR Manager uses the CPABE toolkit to prototype the research effort. ABE has been one of chosen technologies for electronic health record management systems too [15].

Akinyele et. al. has presented a design and implementation of Electronic Medical Records (EMRs) using attribute-based encryption on mobile devices. In their system, they provide off-line support for updating the medical records with support for eventual consistency. However, their model does not support a field-level encryption of the EHR. Researchers at Microsoft developed a patient controlled electronic medical record system with attribute-based encryption [16]. As the name suggests, this system put all the access control in the patient's hands. The control and distribution of access keys was the patient's responsibility. However, this approach requires a high level of control overhead on the patients end. The EHR Manager however, does not impose any overhead on the patient. The central system handles all the secure access and distribution of the EHR [17].

A secured patient-centric electronic health information schema was proposed by Barua et al. for providing reliable access privilege in a cloud-based environment by using a protocol called Proxy Re-encryption. The schema which has five main stages makes use of Attribute Based Encryption to permit patient-centric access control. The performance analysis reveals that the schema has a good and excellent performance. The weakness is that it is not flexible enough for other form of distributed systems. What is more, the schema doesn't give room for scalability and flexibility [18]. Only limited number of users was considered during evaluation. Also, priority needs to be set when there is a simultaneous request by users.

Kumar et al. (2013) proposed a new framework for electronic health on encryption technique; Attribute Based Encryption (ABE). In this case, users are divided into two principal domains: personal and public domains. The essence of this is to handle key management complexity [19]. In the personal domain, every owner is allowed to encrypt/access only data under his attributes while public domain allows users to adopt and make use of multi-authority ABE to enhance the security countermeasures. The great challenge with this approach is the issue of scalability and flexibility because integrating Attribute Based Encryption into large scale Electronic Health Record system poses serious and great key management challenge.

Zhu et al. (2014) proposed a secure and reliable framework that makes use of re-encryption and Attribute Based Encryption (ABE) with proxy encryption that is Rivest Shamir and Adleman (RSA) enabled. The objective of using proxy was to introduce separation mechanism to guarantee the validity of patient's data. In this case, only the professionals are given the write privilege keys while

the read privilege keys are given to patients [20]. The essence of this is to prevent full authorization by the patients. Through this framework, the computation overhead has been drastically reduced. With this approach, the healthcare practitioner can easily be prevented from getting the read keys without approval from both ends. However, the scheme gives room for limited number of users.

Table 2 provides the summary of reviewed papers.

3. CONCLUSION

Health care practice involves collecting, synthesizing, and acting on information and therefore poses a great challenge to ongoing research and development for general frameworks and standards. EHR is one of the most valuable assets for a healthcare organization. Even though they are doing everything they can within their budget to protect EHRs from any sorts of damage, there are some issues to be take into account as they have been discussed in the previous sections.

EHR services are required to ensure secure and authorized access of patient data. At the same time, they must be able to automatically delegate access of patient data to various caregivers to deliver timely treatment to patients. Security of cloud based EHR services is especially challenging since they are often accessed remotely by the end users.

Author	Title	Source	Model Used	Finding
Joshi et.al	Semantically rich, oblivious access control using abac for secure cloud storage	Edge Computing (EDGE), 2017 IEEE International Conference on. IEEE, 2017, pp. 142–149	Attribute Based Access Control	This model evaluated an access decision based on the attributes of the user requesting a document and those of the requested document. It has scalability bottleneck.
Shin et al.	Constructing RBAC based security model in u-healthcare service platform	Sci World J 2014;1–13	Role Based Access Control security model	They examined various security models for healthcare applications and attempted to see how information leakage could be protected.
Zhu et al.	SPEMR: A new secure personal electronic medical record scheme with privilege separation	IEEE International Conference on Communications Workshops (ICC) 2014, pp. 700–705.	Attribute Based Encryption	They developed a secure and reliable framework that makes use of re-encryption and ABE with proxy encryption that is RSA enabled.
Adebayo et. al.	An Enterprise Cloud-Based Electronic Health Records System	Journal of Computer Science and Information Technology June 2014, Vol. 2, No. 2, pp. 21-36	Anlysis	They discussed the primary reasons for going to a "paperless" environment and the complexity often arises due to errors that will occur in daily happenings in hospitals, clinics and all sorts of other healthcare institutions.
Kumar et al.	Personal health data storage protection on cloud using MA-ABE	Int J Computer Application 2013;75(8):11–6.	Multi Authority Attribute Based Encryption	It is new framework for electronic health on encryption technique, where users are divided into two principal domains: personal and public domains. The essence of this is to handle key management complexity.
Barua et al.	PEACE: An Efficient and Secure Patient centric Access Control Scheme for eHealth Care System	International Workshop on Security in Computers, Networking and Communications 2011, pp. 970–975	Attribute Based Encryption	They developed a secured patient-centric schema for providing reliable access privilege in a cloud-based environment by using a protocol called Proxy Re-encryption.

J. Benaloh et. al.	Patient controlled encryption: ensuring privacy of electronic medical records	Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.	Hierarchical Identity Based Encryption Scheme	They developed system that puts all the access control in the patient's hands. The control and distribution of access keys was the patient's responsibility.
E. H. Shortliffe et al.	The evolution of electronic medical records	ACADEMIC MEDICINE-PHILADELPHIA-, vol. 74, pp. 414–419, 1999	Analysis	They describe the problems associated with paper-based record keeping and the promise of the EHR.
Goyal et. al.	Attribute-based encryption for fine-grained access control of encrypted data	Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98	Key-Policy Attribute Based Encryption	They proposed an attribute-based system called the Key-Policy Attribute Based Encryption in which ciphertexts are tagged with attributes corresponding to access control structures.
Bethencourt et al	Ciphertext-policy attribute-based encryption	Security and Privacy, 2007. SP'07. IEEE pp. 321–334.	Ciphertext-Policy Attribute Based Encryption	They developed a system called the CPABE for implementing ABE using the attributes of the user encrypting the document.

Table 2: Summary of Reviewed Papers

It is very vital to implement e-Health solution in any country of the world to enhance excellent healthcare delivery system. To maximally enjoy the services of e-Health, it is very important and fundamental to put in place the required security and privacy mechanisms to prevent any form of security breach and vulnerability. Many papers have been reviewed on security and privacy in e-Health and also identified lapses in the existing solutions.

REFERENCES:

[1] Paul, P. K., & Ghose, M. K. (2012). Cloud Computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science. Procedia engineering, 38, 2222-2227.

[2] Dilip Kumar Yadav, Sephali Behera, "A Survey on Secure Cloud-Based E-Health Systems", EAI Endorsed Transactions on Pervasive Health and Technology 08 2019 - 11 2019 | Volume 5 | Issue 20 | e2.

[3] Kamoona, M. A., & Altamimi, A. M. "Cloud E-health Systems: A Survay on Security Challenges and Solutions" In proceedings of 2018 8th International Conference on Computer Science and Information Technology (CSIT), (IEEE) :pp.189-194.

[4] Terry, N. P., & Francis, L. P. (2007). Ensuring the privacy and confidentiality of electronic health records. U. Ill. L. Rev., 683.

[5] Sittig DF, Singh H. Defining health information technology - related errors: New developments since To Err Is Human. Arch Intern Med. 2011; 171(14): 1281-4.

[6] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems. 2009; 25(6): 599-616.

[7] Pussewalage H, Oleshchuk V. Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions. Int J Inf Manage 2016;1161–1173.

[8] Kanagaraj G, Sumathi AC. Proposal of an open-source Cloud computing system for exchanging medical images of a Hospital Information System. In Trends in Information Sciences and Computing (TISC), IEEE 3rd International Conference, 2011 144-9.

[9] E. H. Shortliffe et al., "The evolution of electronic medical records," ACADEMIC MEDICINE-PHILADELPHIA-, vol. 74, pp. 414–419, 1999.

[10] Abayomi-Alli, Aderonke J. Ikuomola, Ifeoluwa S. Robert and Olusola O. Abayomi-Alli Journal of Computer Science and Information Technology June 2014, Vol. 2, No. 2, pp. 21-36 "An Enterprise Cloud-Based Electronic Health Records System".

[11] M. Joshi, S. Mittal, K. P. Joshi, and T. Finin, "Semantically rich, oblivious access control using abac for secure cloud storage," in Edge Computing (EDGE), 2017 IEEE International Conference on. IEEE, 2017, pp. 142–149.

[12] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

[13] Shin M, Jeon H, Ju Y, Lee B, Jeong S. Constructing RBAC based security model in u-healthcare service platform. Sci World J 2014;1–13.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.

[16] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.

[17] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 75–86.

[18] Barua, M, Lu, R, Liang, X, Shen, X, PEACE: An Efficient and Secure Patientcentric Access Control Scheme for eHealth Care System. In: The First International Workshop on Security in Computers, Networking and Communications, Shanghai, China, 2011, pp. 970–975.

[19] Kumar M, Fathima M, Mahendran M. Personal health data storage protection on cloud using MA-ABE. Int J Comput Appl 2013;75(8):11–6.

[20] Zhu, H, Huang, R, Liu, X, Li, H, SPEMR: A new secure personal electronic medical record scheme with privilege separation. In: 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, NSW, Australia, 2014, pp. 700–705.