International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.2, No.6, December 2013, pp. 417~420
ISSN: 2089-3337

Electronic Health Record (EHR) and Cloud Security: The Current Issues

Emmanuel Kusi Achampong
Department of Medical Education and Information Technology, University of Cape Coast, Ghana

Article Info

Article history:

Received Aug 15th, 2013
Revised Oct 20th, 2013
Accepted Nov 30th, 2013

Keyword:

Cloud Computing,
Electronic Health Record,
Security

ABSTRACT

With the advent of the cloud computing and its associated challenges, building a secured electronic health record (EHR) in a cloud computing environment has attracted a lot of attention in both healthcare industry and academic community. Cloud computing concept is becoming a popular information technology (IT) infrastructure for facilitating EHR sharing and integration. In this study we discuss security concepts related to EHR sharing and integration in healthcare clouds and analyse the arising security and privacy issues in access and management of EHRs. This paper focus on the current challenges that comes with the use of the cloud computing for EHR purposes.

Corresponding Author:

Author,
Department of Medical Education and Information Technology,
School of Medical Sciences,
University of Cape Coast, Cape Coast,
Ghana
Email: eachampong@ucc.edu.gh

1. INTRODUCTION

Electronic Health Record (EHR) has a lot of definitions, such as the electronic record that keeps patient's medical information in a health record system managed by healthcare providers [1]. Despite EHR positive impact on healthcare services; its adoption progress is slow in most healthcare institutions worldwide; especially in developing countries due to several common challenges. Security of patient data has been a concern from the beginning of medical history and is still a key issue in contemporary age. The Oath of Hippocrates was instituted on the principle of confidentiality, and has thus turned out to be an honoured action in clinical and medical ethics. Protecting the privacy and confidentiality of patient information is of utmost importance; security gives rise to trust. Security of medical records mainly covers confidentiality and privacy [2]. Cloud computing introduces the possibility to access large volumes of patient information in a short period. This increases the chance of an unauthorised person accessing patient records easily. Silverman, (1998) [3] repeats this feeling when he states that "Unlawful access to traditional medical records (paper-based) was always possible, but the introduction of computer magnifies a small problem into a very big issue" (p29).

Cloud computing is a model for enabling convenient, on-demand network access, to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [4]. Cloud computing technology is considered to be the new, most interesting and comprehensive solution in the IT world. Its main objective is to leverage internet or intranet for users to share resources [5]. Cloud computing is a cost effective, automatically scalable, multitenant and securable platform that is managed by the Cloud Service Provider (CSP).

The upsurge of cloud computing opens a new chapter for healthcare delivery. The cloud computing model of network is based on the idea of subcontracting corporate information technology (IT) setup to other service providers, a distributed group of computer storage and computing network resources and facilities which becomes available quickly and on request. Benefits of cloud computing include easy and active resource provisioning, simple and automatic management of IT setups and the distribution of almost limitless CPU, storage space and bandwidth due to resource virtualisation, with upward enhancements and great cost discounts with respect to setup administration. The core security challenge of cloud computing is that the information owner does not control the hardware that is operating on his data. Cloud computing therefore needs a new security model for EHR that distributes the security responsibility between cloud service providers (CSPs), clients and users.

Recently, researchers have started using cloud computing services to solve many problems in healthcare information technology (IT) adoption [6]. But, not many researches entered the field of integrating EHR with the cloud services yet [6]. Integrating EHR with cloud service is a daunting task and must be done in a holistic manner. Information security becomes an important issue when moving EHR to the cloud environment. The use of cloud may accelerate externalisation of system user identities, security, infrastructure and services, especially in the context of public clouds. This externalisation could mean the loss of direct control of this dynamic security perimeter. This also includes the overall governance of privacy and IT security within the cloud.

2. CLOUD SECURITY

Cloud consumers face security challenges from both external and internal attacks [7]. Many of the security matters involved in protecting the cloud from external threats are related to those already facing large data centres. However, in the cloud, this information security responsibility is shared among many parties. These parties include the cloud user, the CSP, and any other service provider that consumers depend on for sensitive security software and configurations. The cloud consumer is in charge of application-level security. The CSP is in charge of physical security and applying external firewall policies. Security for the middle level of software load is distributed between the consumer and the CSP; the lower the levels of abstraction open to the consumer, the more the responsibilities that accompany it.

The consumer responsibility, in turn, can be subcontracted to other service providers who trade in special security services. The uniformity and standardised interfaces of system's platforms, example EC2, increases the possibility for an institution to provide services in configuration management and firewall-rule analysis. CSPs must guard against theft and denial-of-service attacks by consumers. Consumers must be protected from each other. There are some organisations and international bodies drafting cloud standards and application programming interfaces (APIs) [8]. Some of the risks that are seen by most consumers are that the CSP have to manage possibly millions of clients and this may present a challenge [9]. This shows that many people are concerned that the CSPs will not be competent enough to manage the enormous scale of or that the infrastructure may not be able to balance correctly with enormous amounts of usage.

Confidentiality and privacy is essential for institutions, especially when personal information or sensitive information is being kept. It is not yet entirely understood whether the cloud computing infrastructure will be capable to support the storage of sensitive information without making institutions responsible for breaking privacy regulations [8]. It is believed that cloud authorisation systems are not tough enough. With a username and password, one is given access to the system. In many private clouds, users can have similar usernames, debasing the authorisation measures further. When sensitive information is stored on a private cloud, there is a high probability that somebody can view the information easier than many might believe. The client is counselled to only give their data or use the CSP system if they trust them. Encryption can help secure health data but what come along with the benefits of encryption are the drawbacks as encryption can be processor exhaustive. Encrypting is not always the best for protecting data. Thus, combining different security measures to protect health data is the best way to guard sensitive data against unauthorised access and use. There can be times when little hitches occur and the data cannot be decrypted leaving the data corrupt and useless for customers and the CSP.

The resources of the cloud can also be misused as CSPs reassign IP addresses when a client no more needs the IP address. Once an IP address is no more needed by one client after a period of time, it then becomes accessible to another client to use. CSPs save money by reusing IP addresses. Many of these idle or used IP addresses can make the CSP open to misuse of its resources. Another client of the same CSP can possibly get access to another client's resources by routing through the CSP's networks, if no or little security measures are put in place. Data or information is like money for cyber criminals. Clouds can hold vast amounts of data and this is making clouds an attractive target for these cyber criminals. Therefore, cloud security must have a high standard and should not be ignored [10].

Clouds API's and SaaS are still developing which means updates can be regular. But some CSPs do not notify their clients about these changes when they are made. Modifying the API also means modifying the cloud configuration which eventually affects all instances within the cloud. The modifications can affect the security of the system as one modification could fix one problem (bug) but create another. It is therefore the responsibility of clients of the CSP to always ask if any updates are made and should inquire about what security applications have been put into place to secure their data.

Another major security mechanism in today's cloud is virtualisation. It is a potent defence, and guards against most efforts by consumers to fight one another and the primary cloud setup. It must be understood that not all resources are virtualised and not all virtualisation environments are free from bugs. Virtualisation software is known to have bugs that allow virtualised code to explode to certain extent. Inappropriate network virtualisation may permit consumer code access to critical portions of the CSP's setup, and/or to other consumer resources. These challenges are related to those involved in handling enormous non-cloud data centres, where different applications need to be secured from one another. Any large Internet service must ensure that one security hole does not compromise other things.

One final security issue is guarding the cloud consumer against the CSP. The CSP by definition will be in charge of the administration of the software load, which efficiently circumvents most known security procedures. Absent fundamental improvements in security technology, it is expected that consumers will employ agreements and law, as a substitute to smart security methods, to protect against CSP malfeasance. The one significant exception is the risk of unintentional data loss. It's challenging to envisage Amazon snooping on what is contained in VM memory; it's simple to envisage a hard disk which is being destroyed without totally deleting the data/information on it, or an authorisations bug making data visible inappropriately. This is an issue in non-cloud settings. The standard defence, i.e., consumer encryption, is also reliable in the cloud. This is normal for very important data in non-cloud environment, and all the tools and skills are easily accessible.

3. HER AND CLOUD SECURITY

Accessibility and use of health information has been a challenge in the 21st century. Various technologies have been employed in their quest to make communication of EHR among different healthcare providers easy. Health Information Exchange (HIE) has been deployed in various institutions to facilitate communication between healthcare providers. With the use of different proprietary and open software by these institutions, interoperability issues have become a challenge for these institutions. Thus, making it difficult if not impossible to have smooth communication between different healthcare providers on patients.

Cloud computing on the other hand can make it possible for different healthcare providers to have access to one big EHR that can be shared among these various institutions. Therefore cloud EHRs enable efficient communication of medical information, and thus reduce costs and administrative overheads [11]. Furthermore, EHRs help to reduce incidents of medication error. Moreover, a patient's health records are currently often distributed over multiple sites with no single healthcare professional having access to all of this data. EHR systems in a cloud computing environment aim to solve these challenges.

In a medical setting, cloud computing offers the potential for easy access to EHRs both for healthcare providers and patients. Quick access to a person's medical history could speed up treatment, help to avoid complications, and even saves lives [12]. In addition, the cloud could make it easier for patients to locate and keep track of their own medical history.

However, to achieve these potential benefits, the healthcare industry must overcome several significant obstacles. Presently, health information is stored in a variety of proprietary formats using numerous off-the-shelf and custom-built hospital information systems. This result in a severe interoperability challenges in the healthcare sector [13].

Also, the security of patient's medical data is a major issue [14] which, if not addressed in both a technologically-efficient and transparent way, will lose the patient's and healthcare provider's confidence in and trust of the EHR system. Chhanabhai and Holt (2007) [15] showed in their EHR usability survey that 73.3% of participants were highly concerned about the security and privacy of their health records.

Several solutions are available to overcome the security concerns associated with EHR and cloud computing systems. However, progress to date has not been sufficient to meet the security requirements of a federated healthcare environment (cloud computing) [16]. Most of the information security models developed so far have been designed to satisfy healthcare security requirements in a controlled environment, such as the EHR database maintained within a hospital [17]. Current studies [17] focussed on encrypting and decrypting health records in a controlled environment without considering how encryption and decryption keys can be distributed in the cloud. Traditional access control mechanisms (DAC, MAC, and RBAC) have not been able to significantly secure health records in the cloud since they normally employ only username

and password. Cloud computing environment presents a more complex challenges compared to a controlled environment (one institution). Security of cloud EHR takes a different approach since users in the cloud are unknown. These relatively unknown users must have access to patient records for quality service to be provided to the client. Thus, the application of straight-forward encryption and access control methods cannot be used in the type cloud EHR environment.

4. CONCLUSION

Keeping EHR in a cloud computing environment will open up accessibility to patient records. It will be easy to have access to health information anywhere in the world and thus help improve health outcomes of patients and other clients of healthcare providers. This easy accessibility requires robust security infrastructure for the EHR in the cloud settings. The issue of protecting privacy and confidentiality of patient records is very important for the uptake of cloud services. Simple access control and encryption methods cannot be used to properly secure EHRs. Secured access control methods and encryption key management methods must be in place to safeguard the security of EHR in the cloud.

REFERENCES

[1] T. Spil, "Value, Participation and Quality of Electronic Health Records in the Netherlands". *43rd Hawaii International Conference on System Sciences*, (pp. 1-10). 2010.
[2] M. Amatayakul, "EHRs and the Consumer: A New Opportunity". *In Murphy GF, Hanken MA, Waters KA eds*, 26-68. 1999
[3] D. Silverman, "The Electronic Medical Record System: Healthcare Marvel or Morass". *Physician Executive, 24*(3), 26-36. 1998.
[4] P. Mell and T. Grance, "*NIST Definition of Cloud Computing"*. USA: National Institute of Standards and Technology. 2011
[5] L. Zhang and Q. Zhou, "Cloud Computing Open Architecture". *IEEE International Conference on Web Services*, (pp. 607-617). Los Angeles, CA. 2009.
[6] H. Mirza and S. El-Masri, "Cloud Computing System for Integrated Electronic". *Stud Health Technol Inform*. 2013.
[7] P. H. Disha and R. Sridaran, "An Analysis of Security Challenges in Cloud". *International Journal of Advanced Computer Science and Applications, 4*(1). 2013.
[8] ENISA. (2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security*
[9] B. Ohlman, A. Eriksson and R. Rembarz, "What Networking of Information can do for Cloud Computing". *18th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises.* Groningen. 2009.
[10] P. Wayne, "Cloud versus Cloud-A Guided Tour of Amazon, Google, AppNexus and GoGrid". *InfoWorld*. 2008
[11] HealthConnect Business Architecture. *HealthConnect Business Architecture.* 2003
[12] L. Gottlieb, E. Stone, D. Stone, L. Dunbrack and J. Calladine, "Regulatory and Policy Barries to Effective Clinical Data Exchange". 2005.
[13] M. Eichelberg, "A Survey and Analysis of Electronic Heaelthcare Record Standards". *ACM Computing Surveys, 37*(4), 277-315. 2005.
[14] P. Ray and J. Wimalasiri, "The Need for Technical Solutions for Maintaining the Privacy of EHR". *28th Annual International Conference of the IEEE, Engineering in Medicine and Biology Society*, (pp. 4686-4689). 2006
[15] P. Chhanabhai and A. Holt, "Consumers are ready to accept the Transition to Online and Electronic Records if they can be assured of the Security Measures". *Medscape General, 9*(1). 2007.
[16] B. Finance, S. Medjdoub and P. Pucheral, P. "Privacy of Medical Records: From Law Principles to Practice". *18th IEEE Symposium on Computer-based Medical Systems*, (pp. 220-225). 2005.
[17] E. AbuKhousa, N. Mohamed, & J. Al-Jaroodi, "e-Health Cloud: Opportunities and Threats." *J. Network and Computer Applications 35 (1)*, 211-220. 2012.