# Towards A Well-Secured Electronic Health Record in the Health Cloud

Babafemi O. Odusote and Nicholas A. Ikhu-Omoregbe

**Abstract**—The major concerns for most cloud implementers particularly in the health care industry have remained data security and privacy. A prominent and major threat that constitutes a hurdle for practitioners within the health industry from exploiting and benefiting from the gains of cloud computing is the fear of theft of patients health data in the cloud. Investigations and surveys have revealed that most practitioners in the health care industry are concerned about the risk of health data mix-up amongst the various cloud providers, hacking to comprise the cloud platform and theft of vital patients' health data. An overview of the diverse issues relating to health data privacy and overall security in the cloud are presented in this technical report. Based on identifed secure access requirements, an encryption-based eHR security model for securing and enforcing authorised access to electronic health data (records), eHR is also presented. It highlights three core functionalities for managing issues relating to health data privacy and security of eHR in health care cloud.

**Index Terms**—Cloud Computing, Data Privacy, Data Security, Electronic Health Records.

## 1 Introduction

Cloud computing has been defined by national institute of standards and technology (NIST) as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (software, hardware and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. It is an emerging and fast growing computing paradigm that uses internet technologies to enable and facilitate the provisioning of service-oriented, adaptable and scalable IT-based capabilities to external suscribers or clients [1], [3]. It has evolved primarily three widely referenced and adopted service models. [4], [5], [6], [7], [8].

### 1.1 Software-as-a-Service - SaaS (Application in the cloud)

Several applications and computing resources required to enable their execution can be provided to various suscribers on-demand as a service. SaaS model engenders the provision of computing capabilities resident in the cloud to suscribers or clients. In this service model, the management and control of the underlying cloud infrastructure is completely out of bounds to the clients. The provision of privacy protection and security for external clients is also integral to the SaaS service model.

The total cost of ownership (TCO) of IT facilities such as software, hardware, operations and maintenance is greatly reduced. Several examples include business applications such as Customer Relationship Management (CRM), On-line Payment Processing (OPP), Report Generation and Analysis (RGA), Order Management Systems (OMS), Inventory Management Systems (IMS), communications and collaboration tools (such as e-mail and Web conferencing), and a host of other computing capabilities.

### 1.2 Platform-as-a-Service - PaaS (Platform in the cloud)

Computing platforms upon which several computing applications can be developed and deployed can also be provided to various suscribers on-demand as a service. PaaS model is a deployment model that facilitates the deployment of computing applications either acquired or created and developed using programming languages and tools supported by the cloud infrastructure. In this model, the right of control and management of the deployed applications and possibly the application hosting environment configurations are granted to the client or suscriber.

PaaS implements two levels of privacy protection and security. They are application level and system level. The former requires the client to succintly define and specify the access control requirements and policies depending on the application provided, while at the latter level, essential security measures and mechanisms such as authentication, authorization and end-to-end encryption can be provided by the cloud host. The primary focus of the PaaS provider is to offer an effective platform for the deployment, management and control of the subscribers' applications.

### 1.3 Infrastructure-as-a-Service - IaaS (Infrastructure in the cloud)

With IaaS model, suscribers are provided with the fundamental computing capabilities – networks, storage, processing, etc in which they are enabled to arbitrarily deploy and run various classes of software applications and systems including operating systems. In this model,

- *B.O. Odusote is with the Department of Computer and Information Science, Covenant University, Ogun State, Nigeria.*
- *N.I.Omoregbe is with the Department of Computer and Information Sciences, Covenant University, Ogun State, Nigeria.*

the clients' right of control and management is strictly limited to the deployed applications and operating systems.

They do not have control over the underlying cloud infrastructure but the primarily responsibility for privacy protection and security rests with the application developer. However, the sole focus of the infrastructure provider is to keep the infrastructure up and running in consonance with the contract agreement while, the suscriber is left with the responsibility of application deployment, system management and control, monitoring, support, backup and failover. This would require higly skilled manpower within the clients' organization.

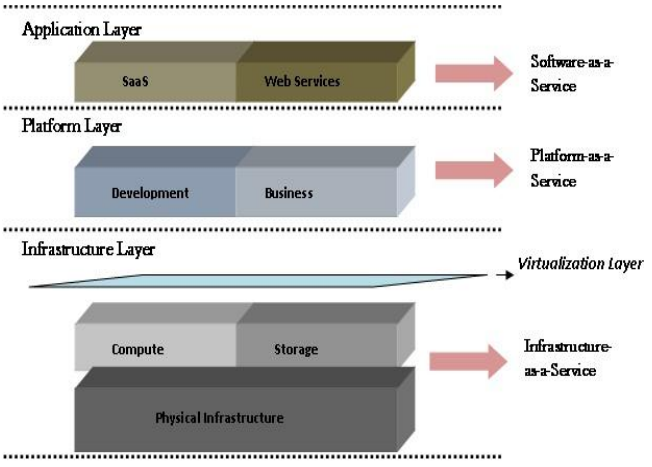


Fig. 1: A Typical Cloud Architecture [6]

The cloud has witness the emergence of a number of cloud computing platforms and technologies some of which are highlighted in [7]: Amazon Elastic Compute Cloud (Amazon EC2), Microsoft Azure, Google App Engine, Open Nebula, CloudSim, Sun Grid, Virtual Workspace etc.

Since the advent of Information Technology (IT), organizations and corporations globally have experienced enhancement and improvement in their various organizational processes and operations. The various health organizations are no exceptions [1]. Currently, the healthcare industry is faced with growing regulatory pressures coupled with high rising economic demands that pose a dire and urgent need for a change and improvement in its Information Technology (IT) infrastructure [9], [11]. This is potentially driving the imminent need for the adoption and acceptance of cloud computing, especially going by the various investments in the health industry by the governments in Sub-Saharan Africa (SSA) towards achieving the United Nations Millennium Development Goal (UN MDG) [10], [11]. It is a fast evolving computing paradigm that has the promising potential & inherent benefits to deliver this needed improvement [1].

Top on the priority list of the health care industry are: improved quality of health care, increasing access, reducing cost, and ensuring health data privacy and security [1]. However, a prominent and major threat that constitutes a hurdle for practitioners within the health industry from exploiting and benefiting from the gains of cloud computing is the fear of theft of patients health data in the cloud [1], [3]. Various investigations and surveys have revealed that most health practitioners are concerned about the risk of health data mix-up amongst the various cloud providers, hacking to comprise the cloud platform and theft of vital patients' health data [3].

The resultant effects of these which could range from time and cost of damage to lawsuit against the cloud provider or even the health organization would cause the organizations a lot of public disrepute and embarassment [3], [14].

This technical report, presents an overview of the diverse issues relating to health data privacy and overall security in the cloud. Based on identified secure access requirements, an integrated encryption-based security model for securing and enforcing authorised access to electronic health data (records), eHR is also presented. It highlights three core functionalities for managing issues relating to health data privacy and security of eHR in health care clouds.

The rest of the paper is organized as follows. Section 2 presents an overview of the diverse issues relating to health data privacy and overall security in the cloud. Section 3 illustrates an integrated encryption-based security model based on the identified secure access requirements for both patient and healthcare professional in the context of patient health care delivery. The presentation was summarized and conclusions were made in Section 4.

## 2 Related Works

Cloud computing paradigm leverages on the offerings of software-on-demand approach. It provides enterprises and organizations with several benefits such as reduction of IT-related operational costs. Health organizations no longer need to invest heavily in building, owning or maintaining applications for e-Health services such as Health Records Management (HRM), Electronic Health Records (eHR), Electronic Medical Records (eMR), etc, as they can access these services through a network and charged accordingly based on resource usage [13].

However, a clear undertanding of the various security implications is an essential step to successfully leverage health care on the cloud. Privacy and strict security enforcement are also crucial in attending to pertinent security concerns that exists, with data movement from the internal computing center of the organization to that of another organization.

Moreso, the quest for reduced IT-related operational that the adoption of the cloud offers should not comprise the responsibility for privacy and security. The organization is primarily held responsible for the state of the organization services – handling issues such as availability, performance, recovery and failover, monitoring and management still lie within the confines and control of the organization.

The issues sorrounding cloud security and data privacy in the cloud are well known and are not brand new in their entirety but are only casted in new computing perspectives, owing to the fact that cloud computing is an emerging paradigm from a combination of existing technologies such as service-oriented computing and architectecture (SOC/SOA), utility computing, virtualization, Web 2.0, etc. [15]. Consequently, cloud computing represents a non-conventional, thought-stimulating paradigm shift towards building a robust and wide-range healthcare industry.

W.A. Jansen [3] presented a significant detailed overview and classification of the diverse relevant issues relating to health data privacy and overall security in the cloud into several general categories. These categories are: trust, data protection, identity management, availability, architecture, software isolation.

Furthermore, R. Zhang and L. Liu [8] opined that risk management is in many ways usually involved in the exercise of migrating into the cloud computing environment from a dedicated internal computing environment. They suggested that, against the available safeguards and envisaged benefits, the associated risks however must be carefully balanced with the understanding that the organization will be primarily held responsible and accountable for the security. If the associated costs and risks are outweighed by the accrued benefits, it will be efficient and effective not to put too many controls [16]. One thing that must be ensured particularly, with computing programs and operations is right balance between the relative associated risks and the strength of controls. [3], [17].

## 3 THE INTEGRATED ENCRYPTION-BASED SECURITY MODEL

This security model is a component-based system of securely coupled core components that cater for the privacy and security requirements in the health cloud for patients through the adoption of a cryptography technique - encryption.

Considering the fact that within the healthcare organizations, health patients could have attending doctors and perhaps in some critical cases a number of other specialists or consultants from other health care delivery organizations attending to them, assuming an ideal health circumstance where an assigned doctor has to deal with a patient but the patient has some major health complications that resulted from acute disease like cancer such that the doctor would need to seek expert opinions and consultations from various practitioners who are specialists and consultants from the different health care delivery organizations particularly the patient's personal physician who is fully conversant with the patient's medical history. These practitioners can then form a consultative group for recommending the appropritate treatments for this patient.

A well-trusted independent third party medical agent can be norminated by the group to serve as the consultative group manager who would be responsible managing and monitoring the activities of the group in accordance with industry best practices. The manager will also dissolve the group after the completion of the patient's diagnosis and prescriptive treatement process. There is also a feedback means for the patient and the third party medical agent to liaise.

The group begins their consultation and diagnostic treatment with each consultant granted an authorized access to some of the patient's electronic medical records in the secured database of the patient's health organization in order to have a requisite knowledge of the medical history of the patient.

After every consultation, the practitioners who participated in the medical consultation would reach a medical conclusion regarding the next step treatment. The group's certified and endorsed outcomes such as diagnosis reports and treatment prescriptions recommended are transmitted to the patient to include to his personal medical records database. This sceanrio is depicted in fig. 2 below.

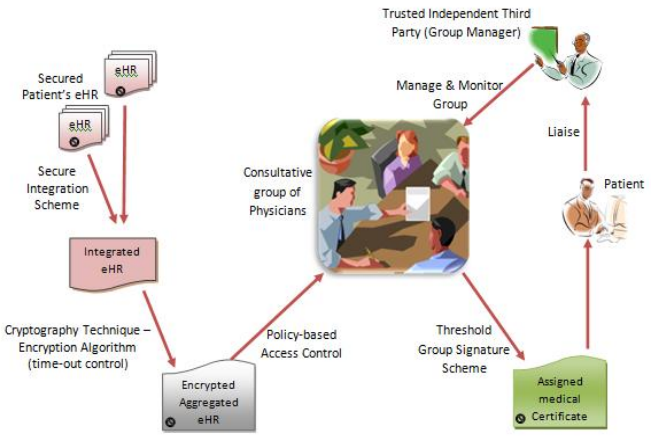


Fig. 2: A Typical Scenario of eHR Patient's Health Care Delivery

The consequence of the above described scenario raises and brings to the fore a number of privacy and security issues.

First, from the view point of the consultants and practitioners, two crucial concerns are, how to obtain the patient's medical records without breaching the patient's privacy and how to validate that the electronic health records from the various health organiztions where the patient has receive treatments or even the patient's personal health records are authentic. These two concerns are captured as Aggregation & Integration and Secure Storage & Acces Control Management of the patient's electronic health records.

Second, from the viewpoint of the patient is the patient's assurance and confidence in the trustworthiness of the certifed and endorsed consultation outcomes from the group of specialists. The patient would need to certify that the medical report/certificate forwarded by the group is authentic and genuine and has not been tampered with. This is captured as Secured Transmission of the medical report/certificate.

A proposed integrated encryption-based security model to cater for the implementation of the privacy and security requirements for the patient's health care delivery is highlighted as follows. This is depicted in the fig. 3 below.

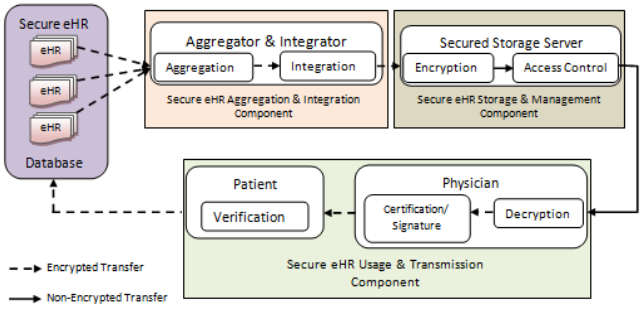


Fig. 3: An Integrated Encryption-based Security Model

### 3.1 Secure eHR Aggregation and Integration

This first component componet of the security model stems from the scenario described above as the first requirement to meet which is to securely aggregate and integrate the patient's various eHRs independently managed by different health care delivery organizations. The requirement is address by the eHR aggregator and integrator. It is designed to securely aggregate and integrate the various eHRs into a newly aggregated eHR with a signed security medical certificate attached. This is done only after it has successfully verified and certified the authenticity, confidentiality, integrity, non repudiation and minimum authorised disclosure compliance of the various eHRs from only the legitimate and trustworthy health care deliver organizations. In this kind of arrangement, a vital and critical concern that requires adequate consideration is semantic interoperability – the formats of storing the eHRs and the aggregated eHR must facilitate interoperability between the eHR systems in terms of effective data sharing and efficient combination of eHRs from multiple databases into an aggregated eHR.

### 3.2 Secure eHR Storage and Management

This is component is designed as a storage for the encypted integrated eHR and for enforcing authorised access. These are taken care of by the secured storage server which comprises of the encryption functionality and the access control unit. The access control unit is designed to prevent unauthorised access by enforcing stipulated access control policies. Authorized practitioners can only be permitted to access and obtain authorized parts of the encrypted integrated patient's eHR through authentication and authorization-based decryption mechanisms.

### 3.3 Secure eHR Usage and Transmission

This component is designed to provide the eHR users - both the patient and the health care practitioner authorised access to information that can be verified. This is captured by the certification/sigature and verification functionalities. After every consultation, the practitioners who participated in the medical consultation would reach a medical conclusion regarding the next step treatment. The group's certified and endorsed outcomes such as diagnosis reports and treatment prescriptions recommended are transmitted to the patient with the practitioners' digital signature. The patient can then verify the authenticity, confidentiality and integrity of the certificate eHR with his private key to include thereafter in his personal medical records database. The digital certificate is included for future reference in case of any disagreement in the future. It can easily be used to obtain the identities of the practitioners who participated in the consultative group and signed the medical result.

## 4 Conclusion

Improved quality of health care, increasing access, reducing cost, and ensuring health data privacy and security are issues top on the priority of the health care delivery organizations within the healthcare industry. However, the fear of theft of patients health data, hacking and data mix-up amongst various providers in the cloud have constituted major hurdles for practitioners within the health industry from exploiting and benefiting from the gains of cloud computing. In this technical report, an overview of the diverse issues relating to health data privacy and overall security in the cloud was presented. Based on identified secure access requirements, an encryption-driven eHR security model for securing and enforcing authorised access to electronic health data (records), eHR was also presented. It is strongly believed that the presentation in this report can be used as a background for cloud developers and particularly for health researchers and practitioners in Sub-Saharan Africa (SSA) towards achieving one of the United Nations Millennium Development Goal (UN MDG).

## References

[1] W. Dadong, A. Andrew, G. Jeanne, and E. Allan, "Six Questions Health Executives Should Ask About Cloud Computing," Accenture Institute of High Performance Press, 2010.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Version 15, National Institute of Standards and Technology, October 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing

[3] W.A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *Proc. of the 44th Hawaii International Conference on System Sciences*, 2011.

[4] G. Fowler and B. Worthen, "The Internet Industry is on a Cloud – Whatever That May Mean," *The Wall Street Journal*, March 26, 2009.

[5] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?," *IEEE Computer*, Jan. 2009.

[6] L.M. Vaquero1, L. Rodero-Merino1, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," *Computer Communication Review*, http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf, 2009.

[7] R. Buyya, C.S Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th Utility," *Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC '08)*, http://www.cloudbus.org/reports/CloudITPlatforms2008.pdf

[8] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," *Proc. of the 15th ACM symposium on Access Control Models and Technologies*, 2010, 125-134.

[9] Gartner, Factiva,(2010), "Cloud Computing in Healthcare," Accenture Institute of High Performance Press, 2010.

[10] The United Nations MDGs Report 2011, http://www.un.org/millenniumgoals/11_MDG%20Report_EN.pdf

[11] V.W.A. Mbarika, "Is Telemedicine a Panacea for Sub-Saharan Africa's Medical Nightmare?" *Comm. of the ACM, Vol. 47, No.7 (July 2004), 2 - 4.*

[12] CIO Cloud Computing Survey, CIO Magazine, June 2009.

[13] Arsanjani, A., "Service-Oriented Modeling and Architecture," IBM Developerworks, www.ibm.com, 2004.

[14] J. Brodkin, "Loss of Customer Data Spurs Closure of Online Storage Service" 'The Linkup,' Network World, August 11, 2008, http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1

[15] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," *ICSE Workshop on Software Engineering Challenges of Cloud Computing*, Vancouver, Canada, May 2009.

[16] R. Chow et al., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," *ACM Workshop on Cloud Computing Security*, Chicago, IL, Nov. 2009.

[17] B. R. Kandukuri, R. Paturi V, and A. Rakshit, "Cloud Security Issues," *IEEE International Conference on Services Computing*, Bangalore, India, September 21-25, 2009.

**Babafemi O. Odusote** is a Computer Science graduate of Covenant University, Nigeria in 2007. He holds a M.Sc. in Computer Science in 2011 from the same institution. He is currently on his Ph.D Program in the same Institution where he is a research fellow and lecturer in the Department of Computer and Information Science. His research interests include: Software Engineering, Mobile Computing, Grid Computing, Cloud Computing, Service-Oriented Computing, e-Learning, e-Commerce.

**N. A. Ikhu-Omoregbe** holds a B.Sc degree in Computer Science from the University of Benin, Benin City, a M.Sc. degree in Computer Science from the University of Lagos, and a PhD degree in Computer Science from Covenant University, Ota, Nigeria. His research interests include: Software Engineering, Mobile Computing, Multimedia technologies, Mobile Healthcare and Telemedicine Systems, and Soft Computing. He currently lectures in the Department of Computer and Information Systems, Covenant University, Ota, and has taught at Baden-Wurttemberg Cooperative State University, Heidenheim as a visiting lecturer in the area of e-Health Systems.