Towards HIPAA-Compliant Healthcare Systems in Cloud Computing

Ruoyu Wu, Arizona State University, USA
Gail-Joon Ahn, Arizona State University, USA
Hongxin Hu, Delaware State University, USA

ABSTRACT

In modern healthcare environments, there is a strong need to create an infrastructure that reduces time-consuming efforts and costly operations to obtain a patient’s complete medical record and uniformly integrates this heterogeneous collection of medical data to deliver it to the healthcare professionals. As a result, healthcare providers are more willing to shift their electronic medical record (EMR) systems to clouds that can remove the geographical distance barriers among providers and patients. Since a shared electronic health record (EHR) essentially represents a virtualized aggregation of distributed clinical records from multiple healthcare providers, sharing of such integrated EHRs should comply with various authorization policies from these data providers. In previous work, the authors present and implement a secure medical data sharing system to support selective sharing of composite EHRs aggregated from various healthcare providers in cloud computing environments. In this paper, the authors point out that when EMR systems are migrated to clouds, it is also critical to ensure that EMR systems are compliant with government regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Also, the authors propose a HIPAA compliance management approach by leveraging logic-based techniques and apply it to the cloud-based EHRs sharing system. The authors also describe evaluation results to demonstrate the feasibility and effectiveness of the approach.

Keywords: Cloud Computing, Compliance, Electronic Medical Record (EMR), Health Insurance Portability and Accountability Act (HIPAA) Regulations, Healthcare

INTRODUCTION

In modern healthcare domain, electronic health records (EHRs) (DesRoches et al., 2008; Eichelberg et al., 2005) have been widely adopted to enable healthcare providers, insurance companies and patients to create, manage and access patients’ healthcare information from anywhere, and at any time. Typically, a patient may have many different healthcare providers including primary care physicians, specialists, therapists, and miscellaneous medical practitioners. Besides, a patient may have different types of insurances, such as medical insurance, dental insurance and vision insurance, from different healthcare insurance companies. As a
result, a patient’s EHRs can be found scattered throughout the entire healthcare sector. From the clinical perspective, in order to deliver quality patient care, it is critical to access the integrated patient care information that is often collected at the point of care to ensure the freshness of time-sensitive data (Grimson et al., 2001). This further requires an efficient, secure and low-cost mechanism for sharing EHRs among multiple healthcare providers. Particularly, in some emergency healthcare situations, immediate exchange of patient’s EHRs is crucial to save lives. However, in current healthcare settings, healthcare providers mostly establish and maintain their own electronic medical record (EMR) systems for storing and managing EHRs. Such self-managed data centers are very expensive for healthcare providers. Besides, the sharing and integration of EHRs among EMR systems managed by different healthcare providers are extremely slow and costly. Thus, a common and open infrastructure platform can play a key role in changing such a situation and improve the healthcare quality.

Cloud computing has become a promising computing paradigm drawing extensive attention from both academia and industry (Mell & Grance, 2011). This paradigm shifts the location of computing infrastructure to the network as a service associated with the management of hardware and software resources. It has shown tremendous potential to enhance collaboration, scale, agility, cost efficiency, and availability of services. Hence, healthcare providers along with many other software vendors are more and more willing to shift their EMR systems into clouds instead of building and maintaining their own data centers. Cloud computing, as cornerstone, not only increases the efficiency of medical data management and sharing process, but also enables the access to healthcare ubiquitous since patients’ healthcare related data will be always accessible from anywhere at any time. Therefore, managing healthcare applications in clouds could make revolutionary changes in the way we are dealing with healthcare information today.

It is promising for both healthcare providers and patients to have EHR applications and services in clouds. However, this adoption may also lead to many security challenges associated with authentication, identity management, access control, policy integration, trust management, compliance management and so on (Takabi et al., 2010; Wu et al., 2010). If those challenges cannot be properly resolved, they may hinder the success of tapping healthcare into clouds. Our previous work (Jin et al., 2009; Wu, 2012) focuses on tackling access control issues when EHRs are shared with various healthcare providers in cloud computing environments. Sharing EHRs is one of the key requirements in healthcare domain for delivering high quality of healthcare services. However, the sharing process could be very complex and involved with various entities in such a dynamic environment. Each EMR system in clouds is associated with multiple healthcare practitioners with different duties and objectives. Also, a shared EHR instance may consist of several sensitive portions of patient’s healthcare information such as demographic details, allergy information, medical histories, laboratory test results, and radiology images (X-rays, CTs). Access control solutions must be in place to guarantee that access to sensitive information is limited only to those entities that have a legitimate need-to-know privilege allowed by patients. For example, a patient may not be willing to share his medical information regarding a HIV/AIDS diagnosis with a dentist unless a specific treatment is required.

Besides above access control issue, compliance management is also a very important problem when adopting cloud computing into healthcare domain. We have witnessed many healthcare providers have been suffering from sensitive information leakage and policy violations due to the lack of systematic compliance management mechanisms. For instance, recent data breach at ChoicePoint costs more than 27 million dollars (Otto et al., 2007). To protect patients’ privacies, Health Insurance Portability and Accountability Act (HIPAA) has been ap-
Mathematical Model for Information Technology Infusion for Healthcare Sector in Nigeria
www.igi-global.com/article/mathematical-model-for-information-technology-infusion-for-healthcare-sector-in-nigeria/202446?camid=4v1a