PriGen: A Generic Framework to Preserve Privacy of Healthcare Data in the Cloud

Farzana Rahman¹, Sheikh Iqbal Ahamed¹, Ji-Jiang Yang², and Qing Wang²

¹ Department of MSCS, Marquette University, Milwaukee, WI, USA
² Research Institute of Information Technology, Tsinghua University, China
{frahman,iq}@mscs.mu.edu, yangjijiang@tsinghua.edu.cn

Abstract. With the rise of Healthcare IT infrastructures, the need of healthcare data sharing and integration has become extremely important. Cloud computing paradigm is one of the most popular healthcare IT infrastructures for facilitating electronic health record sharing and integration. Many predict that managing healthcare applications with clouds will make revolutionary change in the way we do healthcare today. Enabling the access to ubiquitous healthcare not only will help us improve healthcare as our data will always be accessible from anywhere at any time, but also it helps cutting down the costs drastically. However, since healthcare data contains lots of sensitive private information, how to protect data privacy within the untrusted cloud is facing a huge challenge. Thus, a mechanism to protect the privacy of healthcare data is needed when these data are stored and processed within the cloud to provide various medical services. To address this issue, in this paper, we present a generic framework named PriGen that preserves the privacy of sensitive healthcare data in the cloud. PriGen allows the users to preserve privacy while accessing cloud based healthcare service without the help of a trusted third party. With making use of homomorphic encryption function on sensitive private information; our proposed framework maintains confidentiality of private information sent by the cloud users to untrusted cloud based healthcare service providers. In this paper, we also present a brief discussion of different components of PriGen framework.

Keywords: Healthcare data, Cloud computing, Privacy, Homomorphic Encryption, Framework.

1 Introduction

In recent years, the cloud computing technology has seen a revolutionary expansion, acceptance and support both by industry and governments. Computing infrastructure are now offered as a service, instead of being offered as a product. And this is possible due to the rise and acceptance of cloud computing technology. Instead of running on machines owned or controlled by the users or client these services are now run in the cloud. Now a day, platforms, storage, computational power, as well as software is designed, managed and delivered as cloud based services.
Cloud computing is also one of the popular IT infrastructures in the healthcare sector for facilitating electronic medical record sharing [1]. Cloud can provide an exchange platform that all hospitals and clinics can use, and can serve as an electronic medical record storage center. This can simplify the complex electronic medical record exchange procedure between different systems, and save the equipment setup expenses for smaller hospitals. In addition, through the use of cloud platform, patients only need one interface to find their complete medical history, instead of having to check through different hospitals and risk finding only partial medical history. Another benefit of using cloud computing in healthcare is that it allows users to have access to different types of healthcare services via internet. While cloud technology significantly changed how medical and healthcare services are offered, there is a major privacy violation issue that has been in the focus for quite some times. Cloud technology has been criticized in terms of the potential for cloud service providers to gain access over personal data. With detailed person specific data contained in healthcare data, sensitive information about individuals may be easily revealed by analyzing the shared data. An example in [2] shows that linking medication records with voter lists can uniquely identify a person's name and his/her medical information.

As a result of these privacy violation concerns, privacy protection laws are passed in many counties. Many approaches have been proposed over the years to ensure users privacy and help medical institutions or participants to comply with those privacy protection regulations. These approaches cover quite a lot of research areas. Privacy protection during data publishing phase is very famous area and these kinds of approaches try to protect patient privacy by transforming the healthcare data before they are shared. Privacy preserving data publishing models such as Kanonymity, l-diversity [4] and privacy preserving data mining models and methods like privacy preserving decision tree, privacy preserving associate rule mining [5] have been developed as a result of these research work. Allowing authorized access to sensitive private information is another famous research. Many access control models have been developed to increase the flexibility of private data management [3, 6, and 7]. Privacy preserving data storage in cloud platform has attracted quite a lot of attention in recent years. Approaches for privacy aware data storage and auditing in cloud environment are proposed to protect private data [8, 9]. However, there is still need of research in the area of privacy preserving health care data sharing framework that has practical view for real life application. One technique to ensure user privacy while using cloud computing in healthcare is to encrypt all the data that needs to be stored and processed in the cloud. But encrypting all data in the cloud very computation intensive and will reduce the data’s availability at the same time. To overcome the problems mentioned above, in this paper, we propose a framework named PriGen that preserves privacy of users while their healthcare related data are stored and processed in the untrusted cloud without the help of any trusted third party. Our major contributions in this paper are as follows:

- We present the architecture of a Privacy Preserving Framework, PriGen that protects privacy of healthcare data in the cloud without a trusted third party. By making use of homomorphic encryption function, PriGen is able to maintain confidentiality of sensitive private information sent by the cloud users.