Chapter 41
Cloud Storage Privacy in Health Care Systems Based on IP and Geo-Location Validation Using K-Mean Clustering Technique

Mamoon Rashid
Punjabi University, Patiala. Lovely Professional University, Jalandhar, India

Harjeet Singh
https://orcid.org/0000-0003-3575-4673
Department of Computer Science, Mata Gujri College, Fatehgarh Sahib, India

Vishal Goyal
Department of Computer Science, Punjabi University, Patiala, India

ABSTRACT

Cloud-based platforms are helping organizations like health care systems to improve conditions of patients and saving their lives. Medical professionals are making use of cloud technology to collect information regarding patients more than before and exchange it over different geographical regions. However, the exchange of patient data and information is taking place via complex systems with huge vulnerabilities and risks. In this article, the authors have outlined a model for preserving privacy in data storage used in health care systems by validating access to the data through IP based detection and geographical location-based security techniques. Later, the privacy is enabled by using k-mean clustering technique for validating the user access and avail subscriptions whenever consumer want to use the organization services. The authors also provide the concept of using constant key length encryption technique to secure data on cloud storage irrespective of the type of user.

DOI: 10.4018/978-1-7998-8954-0.ch041

1. INTRODUCTION

Proper utilization of Cloud Computing for storage of Electronic Health Records is significantly marking difference than relying on paper medical records which was hindering and limiting the coordination and communication between patients and doctors (Aziz & Guled, 2016). Cloud computing enables users to access information stored on shared pool of resources at remote places with different data transfer & delivery interfaces. Cloud computing definition in (Vouk, 2008) is "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet." A cloud storage provider provides support in terms of storage to the consumers to store their sensitive and non-sensitive data on the cloud (Dillon, Chen, & Chang, 2010). Cloud storage models can be implemented as public storage model, private storage model and hybrid storage model. A storage provider provides additional services to the consumers like file sharing, document compatibility, backup of data, big data storage, scale up and scale down, etc. (Naruchitparames & Gunes, 2011). Despite the enormous business and specialized favorable circumstances of the storage benefits of cloud computing, the confidentiality of data is one of the major flaws in the acceptance of cloud. Cloud is a multi-tenant environment in which consumers consume Cloud Service provider's infrastructure which is shared among other consumers (Grobauer, Walloschek, & Stocker, 2011). The question of privacy and confidentiality comes in mind immediately whenever a user shares information in cloud. Privacy and security become an obstacle in the adoption of the cloud on a massive level (Rong, Nguyen, & Jaatun, 2012). The major problem in cloud storage is that owner does not have full control over the data which is stored on the cloud. If any unauthentic user attempts to use the services of cloud of any user, then there need to have a full proof security mechanism to protect unauthorized access the data (Javaid & Ijaz, 2013). Therefore, consumer wants to have full proof security policies to apply before storing data on cloud.

The outline of the paper is structured as follows: Section 2 describes the related work on privacy and security of data storage on cloud. In Section 3, the problem is proposed and an approach for enhancing security on data storage is outlined. Section 4 discusses experimental setup and results are drawn in Section 5. Conclusion and future scope of the approach is given in section 6.

2. RELATED WORK

Several methods have been outlined to provide and preserve privacy to the shared data on cloud platforms and health care systems. Some privacy issues are highlighted in (Na & Xumin, 2010). In this paper, the authors analyse and survey security and privacy in cloud computing environments. Zissis & Lekkas, 2012) attempt to evaluate cloud computing security by introducing a trusted third party and eliminating unique threats.

(Dawoud & Turgay Altilar, 2017) defined and provided the possible scenarios for the integration of cloud systems with e-health care systems. The various requirements in terms of privacy and security for these scenarios are also defined. The authors have proposed the complete guidelines for the security and privacy challenges in e- health systems with cloud systems.

(Wang, Ma, Xhafa, Zhang, & Luo, 2016) described several identity-based cryptographic techniques including new identity based proxy re-encryption for securing e-health systems. They concluded that