Chapter 60
Security Issues Related to Cloud Applications in STEM Education

Yong Chen
Old Dominion University, USA

ABSTRACT

Learning based on cloud computing, denoted as cloud learning (CL) in short, is a disruptive innovation and a current buzzword in education. It provides a learner-centered platform that benefits learners, instructors, and education providers. However, because it requires the Internet and is built on cloud computing, CL has inherent security issues. By analyzing the benefits and the security threats inherent in CL, this chapter aims to help CL stakeholders in STEM Education (namely cloud service providers, cloud content providers, and cloud users) to better understand the security issues inherent in CL from the perspectives of confidentiality, integrity, and availability. The discussions about the risks that CL stakeholders in STEM education incur as a result of prevailing security threats and system vulnerabilities will help those stakeholders to assess the cost effectiveness of security countermeasures.

INTRODUCTION

STEM is an acronym that stands for Science, Technology, Engineering, and Mathematics. This conglomerate started as an educational focus to improve U.S. teenagers' interests and accomplishments in math and science (Kim & Park, 2012). According to Terkowsky, Haertel, Bielski, and May (2013), three learning technologies are recognized clearly as supporting tools for STEM education: remote labs, personal learning environments, and portable devices. For example, scientific computational/visualization tools such as Matlab and Octave have been adopted widely in STEM education (Judd & Graves, 2012). However, limitations in educational institutions' information and communication technology infrastructures, security concerns, and web technology issues have prevented online labs from being utilized by STEM teachers (Gillet, De Jong, Sotirou, & Salzmann, 2013). Furthermore, the computing capabilities of portable devices hinder the further development of STEM education.

Cloud computing is "a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)

DOI: 10.4018/978-1-5225-5634-3.ch060

that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011:p2). It uses machines in large data centers to deliver services in a scalable manner (Wyld, 2009; Paquette, Jaeger, & Wilson, 2010). It is a disruptive convergence of the development of computing power and data transmission and the use of the Internet and mobile communication (Castells, 2001). As a new supplement, consumption, and delivery model for information technology, cloud computing involves the provision of dynamically scalable and often virtualized resources over the Internet (Knorr & Gruman, 2009). It aims to provide flexible services, scalable computing applications, storage, and platforms in a transparent manner (Sun, Chang, Sun, & Wang, 2011). Recently, because of advances in virtualization (Staff, 2012), distributed computing with server clusters (Barroso, Dean, & Holzle, 2003), and the availability of broadband Internet access (Atayero & Feyisetan, 2011), cloud computing has been developing at an amazing pace (Zhou, Zhang, Xie, Qian, & Zhou, 2010) and has attracted significant attention in diverse realms, such as academia, industry, the government, and the military. Specifically, this new computing model provides potential benefits for online learning because cloud computing can reduce the costs of setting up and maintaining servers and networks for online learning providers, can improve their infrastructures' flexibility and scalability, can provide instructors and students flexible and on-demand services (He, Cernusca, & Abdous, 2011), and can provide dependable data storage and data sharing (Chandran & Kempegowda, 2010). Furthermore, Bai, Shen, Chen, and Zhuo (2011) point out that cloud computing can help instructors pay more attention to improving their teaching and can help learners to concentrate on building and enhancing their intelligence.

Learning based on cloud computing, denoted as cloud learning (CL) in short, is "a shared pool of learning courses, digital assets, and resources, which instructors and learners can access via computers, all types of mobile devices, satellite, and even IP-TV" (Bai, Shen, Chen, & Zhuo, 2011, p3460). Based on cloud computing, CL provides a platform that benefits learners, instructors, and education providers. On the one hand, it enables teachers to take advantage of cloud services to support student learning and innovation. Instructors can easily create teaching environments, can design teaching resources, and can organize teaching activities in collaboration via CL. On the other hand, CL allows learners to build personal learning environments for effective learning (Bai, Shen, Chen, & Zhuo, 2011). CL is a learner-centered platform that facilitates resource sharing and collaboration among learners anytime and anywhere (Bai, Shen, Chen, & Zhuo, 2011; Masud, Huang, & Yong, 2011). Furthermore, education providers are beginning to realize the benefits of CL as well because they have recently been plagued by low budget and high costs (Bhatia, 2013).

Due to its architectural design and characteristics, cloud computing possesses a number of security benefits, namely centralization of security, data and process segmentation, redundancy, and high availability (Zissis & Lekkas, 2012). However, each component of cloud computing, including operating systems, storage, networking, and virtualization, has its own inherent security issues (Atayero & Feyisetan, 2011). Especially because CL is built on cloud computing, which requires the Internet to achieve resource sharing and collaboration, security concerns about CL are rising (Bai, Shen, Chen, & Zhuo, 2011).

For the public cloud, the most cost-effective deployment model of cloud computing, security is a big issue because the physical location of cloud providers' infrastructures usually traverses many national boundaries (Atayero & Feyisetan, 2011). Since learners' individual private data are stored on the other side of the Internet and since services are offered by other parties (e.g., cloud providers and cloud content providers) in CL, security breaches, such as data leakage and unauthorized access (Bai, Shen, Chen, & Zhuo, 2011), are very likely to happen. In response to increasing security threats, researchers have developed a number of countermeasures and solutions to improve security in CL. To date, the discus-