Chapter 14
Assessing Security With Regard to Cloud Applications in STEM Education

Ihssan Alkadi
Southeastern Louisiana University, USA

ABSTRACT

There are many steps involved with securing a cloud system and its applications (SaaS) and developed ones in (PaaS). Security and privacy issues represent the biggest concerns to moving services to external clouds (Public). With cloud computing, data are stored and delivered across the Internet. The owner of the data does not have control or even know where their data are being stored. Additionally, in a multi-tenant environment, it may be very difficult for a cloud service provider to provide the level of isolation and associated guarantees that are possible with an environment dedicated to a single customer. Unfortunately, to develop a security algorithm that outlines and maps out the enforcement of a security policy and procedure can be a daunting task. A good security algorithm presents a strategy to counter the vulnerabilities in a cloud system. This chapter covers the complete overview, comparative analysis of security methods in Cloud Applications in STEM Education and the introduction of a new methodology that will enforce cloud computing security against breaches and intrusions. Much light will be shed on existing methodologies of security on servers used for cloud applications in STEM education and storage of data, and several methods will be presented in addition to the newly developed method of security in cloud-based servers, such as the MIST (Alkadi). Not only can cloud networks be used to gather sensitive information on multiple platforms, also there are needs to prevent common attacks through weak password recovery, retrieval, authentication, and hardening systems; otherwise hackers will spread cyber mayhem. Discussion of current security issues and algorithms in a real world will be presented. Different technologies are being created and in constant competition to meet the demands of users who are generally "busy". The selling point of these technologies is the ability to address these demands

DOI: 10.4018/978-1-5225-5634-3.ch014

without adding more to any workloads. One of the demands often discussed is that users want to have their digital information accessible from anywhere at any time. This information includes documents, audio libraries, and more. Users also demand the ability to manage, edit and update this information regardless of physical location. Somewhat recently, mobile devices such as laptops, tablets, and smartphones have provided these abilities. This is no small feat as vendors and providers have reduced the size of these devices to increase mobility. However, as the amount of personal information that users are wanting to access has grown exponentially, manipulation and storage of it require more capable devices. To meet increased demands, increasing the capabilities of mobile devices may be impractical. Making mobile devices more powerful without technological advancement would require that the device be larger and use more resources such as battery life and processing power to function properly. Storing all of a user's information on a mobile device that travels everywhere also adds vulnerability risks. The best technical solution to having a user's information accessible is some sort of online storage where there is the convenience to store, manipulate and retrieve data. This is one of the most practical applications for the concept of cloud computing in STEM education. As storage capabilities and Internet bandwidth has increased, so has the amount of personal data that users store online. And today, the average user has billions of bytes of data online. Access is everywhere and whenever is needed. As everyone started doing so, people want their data safe and secure to maintain their privacy. As the user base grew in size, the number of security issues of the personal data started to become increasingly important. As soon as someone's data are in the remote server, unwanted users or "hackers" can have many opportunities to compromise the data. As the online server needs to be up and running all the time, the only way to secure the cloud server is by using better passwords by every user. By the same token, the flaws in the password authentication and protection system can also help unwanted users to get their way to other people's personal data. Thus, the password authentication system should also be free from any loopholes and vulnerabilities.

INTRODUCTION

Cloud computing has been the center of a lot of attention and implementation priority over the past ten years. Its immediate, important implementation and use has been very prominent. its eminence is due to its powerful infrastructure and feasible platform. However, its use and implementation has faced some notable complications; as a byproduct of popular use and demand, it brought on many questionable security challenges that need to be addressed and resolved, especially in STEM education. Universities and STEM divisions are trying to apply cloud computing to solve problems that relate to increasing computing complexities and storage. Cloud computing systems serving users within STEM's environment must at least involve the following factors and provide maximum security for the following capabilities as:

- Services and support to a wide range of students, teachers, and potential customers.
- A large number of course materials and academic support tools to instructors, teachers, professors, other educators, and university staff.
- A variety of diverse service environments.
- Operating cloud infrastructure as an economically viable model.