International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 7
ISSN: 2454-4248
48 – 49

Security Issues in Cloud based e-Learning Part 1(Basic Introduction)

Dr Kamal K Vyas, Director SIET, Sikar (Raj), profkamalkvyas@gmail.com
Mr Dinesh, Assistant Professor, SIT Sikar,
Dr Sandhya Vyas, HOD (Deptt of Social Sc), BBV Pilani (Raj), profsandhyavyas@gmail.com

Key-words *: e-Learning, Cloud Architecture, Security Aspects, Security Standards, Mobile Learning.*

*****

Introduction

Cloud based E-Learning is one of the booming technologies in IT field which brings powerful e-learning products with the help of cloud power. Cloud technology has numerous advantages over the existing traditional E-Learning systems but at the same time, security is a major concern in cloud based e-learning. So security measures are unavoidable to prevent the loss of users' valuable data from the security vulnerabilities. Cloud based e-learning products also need to satisfy the security needs of customers and overcome various security threats which attack valuable data stored in cloud servers.

One famous study [1] investigates various security issues involved in cloud based e-learning technology with an aim to suggest solutions in the form of security measures and security management standards. These will help to overcome the security threats in cloud based e-learning technology. To achieve our thesis aim, we used theoretical and empirical studies. Empirical study is made through the information gathered through various cloud based e-learning solution vendors websites. And the theoretical study is made through the text analysis on various research articles related to our subject areas. And finally the constant comparative method is used to compare the empirical findings with the facts discovered from our theoretical findings. These analysis and research studies are leads to find various security issues [1] in cloud based e-learning technology.

Why Cloud enabled e-learning

E-Learning is one of the best and most important technologies which help them to create a good learning environment. Therefore, many countries including developing nations such as India are implementing the E-Learning software solutions to improve their educational standard. Although, they still have many problems regarding required facilities and infrastructure to implement the traditional E-Learning method to a wide range of educational institutes throughout the country. Thus, the cloud computing technology [1] is a proper superseding the traditional E-Learning method to overcome this problem.

There are numerous advantages [1] with substitutions of traditional E-Learning method by cloud computing technology. Cloud computing is portable and helps to make the e-learning solutions possible for mobile phones and other similar mobile devices such like as Tablet PCs, smart phones, PDAs. Cloud based e-learning solutions are very much helpful to reduce the cost in the traditional e - learning technology by its widespread cloud source. But still, there are some problems to be concerned when implementing cloud based E-Learning solutions to all educational institutes.

Why Cloud security is major concern

Now a days, people are concentrating more on the security features of those technologies irrespective of an electronic gadget or a web technology. People are very conscious on the security features of the technology when it comes to a web source, due to infinite vulnerabilities. Cloud based E-Learning technology is no way an exception from security vulnerabilities from the internet, when it deals with cloud power to enhance the features on an existing traditional e-learning technology. Since the E-Learning technology is not a new one to the technical field, it overcame already some problems to reach the current standard. So, it has many security standards to provide safety for the e-learning solutions and information of the end users on the server. Likewise cloud computing technology also has some security standards to maintain and provide security features for their end-users and investors from web vulnerabilities. But still the question is that whether cloud computing will fulfill and provide enhanced security to the e-learning technology, or create a security problem on the existing security features of traditional e-learning technology.

Security[5] is one of the people's peak concerns on all grounds. People are more concerned of the security especially when using the gadgets or technologies that involve internet. Because the internet has many loopholes that can crash the application or hack the application to gain access to the users or company details by hackers worldwide. E-learning technology is now incorporated with many latest technologies to provide more provision and reduce the complexity from traditional e-learning

 ISSN: 2454-4248
48 – 49

methodology to their users. So in this thesis, we are mainly focused on the security issues in e-learning technology when it is implemented with cloud computing technology. Because cloud computing is one of the fast developing technology which offer numerous benefits and provisions to users who used to enhance their existing technology with cloud power. But still cloud computing has not achieved the fulfillment on security issues. So there is a question raised on how the cloud provides security in e-learning technology and to the e-learners. As we explore, one research [1] throws light to identify the security issues with cloud based e-learning and the countermeasures took recently on those problems.

Perspective Thought

There are three different distinctions for research studies [1] that are widely used namely quantitative, qualitative and mixed study approaches. Quantitative studies which actually trust on quantitative data like numbers and figures, while Qualitative studies which actually trust on qualitative information like words, sentences and narratives whereas mixed approach is using both the statistical data in quantitative and the result orientation from qualitative view. So it is a mixture of both qualitative and the quantitative.

Security management

Security management [7] is the field which relates to asset management, physical security and human resource safety functions. The main aim of the security management is to protect the overall organisation from various kinds of security attacks. Security management varies for each and every field based on the core line which deals with the respective field. The main objective of the security management that deals with internet and network is to protect and ensure the user safety, information security, server security from various attacks, and protect the total system from various Virus attacks like Spam, WORM, Trojans, and Trapdoors. [1]

A) Management Standards

Management standards are used to ensure the quality of management and the services offered to their customers. Management standards are varied for each and every field based on the core line which deals with the respective field. Management standards are offered to the organisation for the quality of their services by many international organisations such as International Standard Organisation (ISO), World-Wide-Web Consortium (W3C), American national standard institute (ANSI). [1]

B) Information security

The security measures taken by the organisation or the individual user to protect the information on their system or products from the hackers are called information security. Information security methods are varied based upon the area of field where they are used like governments, military, corporate companies, hospitals, financial companies, and educational institutes. There are so many laws enacted by governments to make information security stronger against information stealing by hackers and unauthorised persons. [1]

C) Server Security

Servers are the storage units which store all the information for the web sites and web applications. The security of servers is important because servers deal with data of large number of individuals and organisations. So server security and server management is a big deal and numerous security measures are taken to save the data in server from hackers and natural disasters. Usually many websites like Google, yahoo have more number of backup servers to give safety to their user's data from server crash or overloading or other kind of security issues of server. [1]

D) Authentication

Authentication is a method followed to authenticate the valid user to use the product. This is a security measure which helps to avoid the intruders to hack the product or to access the products functionality to make malfunction. There are numerous authentication methods and techniques which are followed in the world of information technology. Based on the value of data on system, the Authentication methods vary. [1]

E) End User

User who uses the product and enjoys the full functionality of product's outcome is called an end user. End users are the customers of the companies for their products. Based on the expectation and demand of the end user, the companies modify their product till the user gets satisfied with products of the company. The product which satisfies the end user is called as a successful product in the market. [1]

Refereces:

[1]. Analysis of Security issues in cloud based e-leaning , G Kumar, Anirudh Chelikani
[2]. How to choose new LMS, Edu perspective, Feb 2013
[3]. Choosing an LMS – ADL
[4]. The Cloud changing the business Ecosystem
[5]. Cloud Security & Compliance – A Primer
[6]. Cloud Computing finding the Silver Lining, S Hanna
[7]. An Efficient Security Model in Cloud Computing based on Soft computing Techniques- Vijay & Raddy
[8]. Security in Hybrid Cloud, Bluelock