International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 12
ISSN: 2454-4248
118 – 120

Security Issues in Cloud based e-Learning Part 4(Security Issues)

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

In the 4th part of this pure exploratory paper, security Issues and Measures are revealed.

*****

SECURITY ISSUES IN CLOUD BASED E-LEARNING

Security issues are more important in this kind of technologies as it ensures the reliability of technology in users' mind to handle it. Since the cloud based e-learning fundamentally depends the web based sources for its operational functionality, there are numerous threats waiting to attack the e-learners and the cloud based e-learning technology through the internet. Even though cloud provides plenty of advantages to e-learners, the cloud security is still in doubt for its security issues/challenges in a digital world. International data corporation (IDC) which conducted a survey with the 263 IT executives to estimate their mind-set on use of cloud services for their IT companies, they ranked the security as first for greatest challenges/issues of cloud computing. [1]

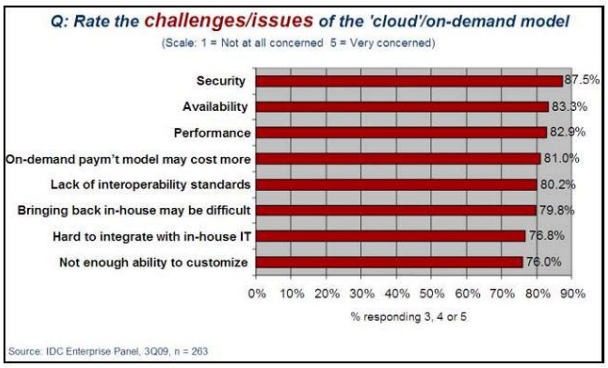

Figure 10: Results of IDC ranking security challenges [1]

IDC survey on cloud security challenges is one of the good examples to show the IT peoples and other stack holders concerns on security issues when implements the cloud services for their products. Nowadays, There are so many major IT companies like GOOGLE, MICROSOFT, AMAZON are become cloud vendors and provide their cloud services to various kind of users around IT world for various purposes. All these companies are already famous for their trustworthy applications and services to IT world, but still peoples are have doubts about cloud safety from those companies. So those companies are following many security standards and measures to ensure the security in their cloud products and services. In the same time, E-Learning solution vendors also have security standards and measures to overcome problems on e-learning applications and its security in e-learning materials and e-learners. Since cloud computing alone is not our track, we discuss the both cloud computing and e-learning technology's security issues and measures separately to find out the key security issues and measure for cloud based e-learning.

In these days huge investments are applied in the field of e-learning by several countries as there is a fact that the development of a country depends on the investment on the infrastructure in the field of education. From the past decade with the trend in the IT Industry and growing speed of the internet sources, there is a lot of scope to provide the education for the large number of people with ease. One can learn and gain the knowledge with less effort and with minimal requirements. Factors like expenditure, cost of the hardware in the case of e-learning was very effective and simple and one can easily acquire the required knowledge from many sources in that field. Along with the growing demand and popularity for the e-learning there are several security threats which grow along with the technology. There are several issues related to privacy are to be analyzed and also there is a need to implement several security functions and tools for the case of e-learning in order to solve all the issues related to the security. These functions are not only some specific software variances but also related to the hardware and also in some cases the combination of both of them like biometric etc. E-Learning is implemented when both information and communication systems have to work together and by using other kinds of electrically enabled technologies. E-learning includes several types of learning such as web based learning, computer based learning, virtual classroom etc. There are several logically located areas for e-learning at a similar time. Along with the other implications like technology, speed, reliability, flexibility of the e-learning systems security and privacy must also be considered as an integral part for those systems. [1]

So in this section of this paper, we discuss the cloud computing and e-learning technology security issues and also find out the measures and standards to overcome key security threats in cloud based e-learning.

SECURITY THREATS & CHALLENGES IN CLOUD BASED E-LEARNING

Since Cloud based e-learning is combination of cloud computing and e-learning technologies, in this section, we first discuss about key security concerns and threats involved in cloud computing technology and later about e-learning technology.

A) Cloud computing security threats:

Since the cloud computing offers numerous services provides to the various applications and technologies, some of key security concerns in cloud computing are mainly

 ISSN: 2454-4248
118 – 120

deals with server security and the information security stores in cloud sources from various technology and applications. Those key challenges and threats in cloud computing are as follows:

1) Basic Security concerns:

Some of the basic security concerns when using cloud sources to enhance the functionality of technology are listed here:

- Physical security is lost with the cloud model control, because companies don't have the knowledge or control of running resources when they share the computing resources with third party companies.
- In most cases, a company violates the law when they use cloud services. And also there is a chance of data seizure by foreign nations.
- Most of cloud vendor's services are not compatible with other cloud vendors. So it may be becomes a problem when the company tries to move their sources from one cloud vendor to another.
- When e-learning solution providers use the cloud source, a question arises on who should control the authentication procedures. Usually customers only have those encryption/decryption keys.
- Cloud providers need to ensure the data integrity by authorized transactions such as transfer, storage, and retrieval of data. For this problem, cloud providers need to follow same standards to ensure this problem on integrity issues.

Customers need to process against cloud vendors if customer's privacy rights are violated. Cloud providers should provide clear answers on how the customer's personal information is used or leaked to third parties.
Cloud vendors should provide the updates regularly to their customers to ensure up to date security.

2) Availability:

Availability of important applications and information on cloud servers for uninterrupted service to customers are the main concern cloud computing. A Denial-of-service attack (DoS Attack) or Distributed-Denial-of-service attack (DDoS Attack) are the popular online attacks which affect the availability of online servers, and thereby makes the servers and the data stored in it are unavailable for the users. Due to such attacks there were many incidents of cloud outage such as Gmail (one-day outage in mid-October 2008)(Chow et al., 2009), Amazon S3 (over seven-hour downtime on July 20, 2008)(Chow et al., 2009), FlexiScale (18-hour outage on October 31, 2008)(Chow et al., 2009), Google's blogger outage (over 48 hours downtime on May 12, 2011) (Bott, 2011), and Gmail reset problem (accidently resetting Gmail accounts on Feb 27, 2011) (Hollister, 2011).

3) Data Lock-in:

Nowadays cloud providers offer numerous tools, applications, standard data formats to their customers. But these services face problems when a customer tries to move to some other cloud provider, because mostly cloud providers are not compatible with one another. So customers are forced to stick with same cloud provider and cannot migrate to another cloud operator's services. This problem creates a dependency issue on those cloud operators to get continued service. [1]

) Insecure of Incomplete data deletion:

In most operating systems, data is not deleted completely even after the data erased from their physical machine. Customers are not able to know, whether their data is fully wiped out from all the virtual machines once after the delete command is applied. This problem leads to unsecured data on cloud. And also there may be a risk of this stolen data being used by unauthorized persons or hackers from the cloud. (ibid)

5) Increased Authentication demands:

Cloud providers offers various advantages to their customers, one of them is to provide software and its application access through online. So client machine need not be installed with any software applications to access for its functionality. Users need not bother about software piracy as these are run by centralised monitoring servers through cloud. But cloud providers should be careful to provide authentication to their customers for access by authorized persons. If cloud operators fail to provide these authentication procedures, it may lead to increase the threat of phishing or other vulnerabilities through unauthorised access of those applications on cloud. [1]

6) Browser security:

Cloud computing actually depends on remote servers for each and every computational tasks to be done. Client machine is only used with I/O devices to access any software applications. In this case, browser in client machine is the gateway to access the cloud servers. So browser security is crucial on total cloud security, because if the gateway is attacked by malware, then total cloud security becomes a problem. Modern web browsers here come up with the AJAX techniques like Java script, XML Http Request, Plugins which can operate I/O devices. Security policies and authentication certificates must be needed to ensure browser security. XML signature and XML encryption also help to ensure the browser security issues. [1]

B) E-Learning security Threats:

E-Learning security threats are nothing but the security problems which questions the safety of the users who work with e-learning environment. This section deals with the key security threats involved in the e-learning systems apart from cloud based security threats for cloud based e-learning.

1) Basic E-Learning security concerns:

Basic security concern of E-Learning technology usually arise when we use it enhance the functionality of traditional learning environment. They are listed here:

User authorization and authentication:

The user authorization is very essential and important when it comes to e-learning. In general the e-learners are from distant places, so provided with a user id and a password.

 ISSN: 2454-4248
118 – 120

With the use of these one can login into the e-learning server and can access the features.
The learner or the student can access the billing account according to the levels. Based on the billing method he may or may not be allowed to the next level of the learning provision.

Entry points:
Entry points are the number of terminals or passive ways where a possibility of security breach may occur in the case of E-learning. As there are number of clients in distant locations for each e-learning server there is lot of entry points for each of them and possibility of a security threat is more. In order to get rid of this threat the designers have to reduce the number of entry points. But it cannot be implemented as there are number of clients in different physical and geographical locations at the same time.

Dynamic nature:
One of the major concerns with the e-learning is more processes are available in the dynamic sessions where a process can join and end the session without the notice of the others. This is vulnerable for much security infracts where they can easily attack the server and the client locations. To get rid of this type of happenings one should have to maintain strict sessions and several security credentials have to be maintained at both the sites i.e., client and server. 31

Protection against manipulation:
Protection against manipulation is one of the key tasks to be implemented in an e-learning environment. It is specifically implemented in the case of students where manipulation is more possible. It can be prevented from the other users by using certain techniques like digital signatures, firewalls etc. similarly several other measures have to be taken in order to avoid manipulation from the registered users. Thus e-learning environment gets enhanced by following and using the security measures carefully which will create a smooth structure of data flow along the network.

Non-Repudiation:
In the step of information security, cases of data loss or infection with virus, Trojan horse and other malicious treats are common. The system must be provided with the capability that the data is not modified by these attacks.

2) Social aspects of security:
Online e-learning environment is different from tradition learning environment. The main change is submission of assignments by students to teachers. In the traditional learning environment, students submit their assignments in hard copy format to their teachers directly in class rooms. Whereas in online e-learning environment, students need to upload their soft copy of assignment. So, this kind of methods in e-learning technology brings the threats and vulnerabilities from internet to e-learning systems. To overcome these problems, basic security requirements such as the integrity, confidentiality and availability are to be observed. Those security concerns are explained in detail here:

Confidentiality: Confidentiality is an important aspect in security concerns, where the data or information sent through online is to be kept as secret and not to be disclosed to unauthorised 3rd party. Under e-learning perspective, students like to get the assurance that their submitted soft copies of assignments through online are kept secret and only revealed to their teachers on e-learning environment.

Integrity: Information or data is not accidentally or maliciously deleted or changed, and it should be kept accurate as in original form. Students feel assured if integrity standards are maintained. This can happen only when their assignments submitted to teachers are kept safe in original format without any further edition by others.

Availability: The reliable information should be present to access and modify it by authorised persons. Information present in e-learning servers must be present for students and teachers or other authorized persons on timely manner for their work. Students need assurance for uninterrupted reliable e-learning system to submit their assignments.

There are two main types of availability attacks which create problem on e-learning systems for the availability issues, they are (Ahmed et al., 2011):
i. **Blocking attack:** In this attack generally the e-learning content will be attacked by the external user and he obtains the permission to access the e-learning material. In this case one has to monitor the attackers IP address and block that address in order to get rid of this problem.
ii. **Flooding attack:** Flooding attack is the one where huge amount of requests to a specific service or large amount of data in the form of small messages are sent blocking the entire service or the session. This may also cause the loss of availability for more time due to processing delays. The counter measures for these types of attacks are to efficiently validate the incoming request or the message.

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