International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 2
ISSN: 2454-4248
511 – 517

# Security Issues in Cloud based e-Learning Part 5(Security Management Standards)

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 this part , Security standards are explored, hence all can be aware with available standards.

*****

**SECURITY MANAGEMENT STANDARDS IN CLOUD BASED E-LEARNING**

There are so many management standards used throughout the world for every technology or product to ensure its security. Since the cloud based e-learning is combination of two different technologies, we need to consider both technologies and its security standards to know the overall management standards to ensure the security of cloud based e-learning.

**1) Security management standards using in cloud computing sector:**

**A) Information technology infrastructure library (ITIL):**

ITIL is a set of rules that define an integrated and process-based operation to deal with the information technology services. It is utilized and implemented in almost all IT sectors including cloud computing. ITIL offers a systematic and professional access to the IT management and their services and helps to get good information security measures on all levels like strategic, tactical and operational levels. ITIL operations consist of many iterative processes like control, plan, implement, evaluate, and maintain. The main problem on ITIL is that only practioners can be certified as ―ITIL-compliant‖, so organisations and other management systems are not able to get certified as ―ITIL-compliant‖. IT sectors which implement and use ITIL guidelines get many benefits, some of them are:

o Cost efficiency.
o IT services are improved by ITIL's best policies and guidelines.
o Customers are more satisfied through a better service delivery with professional approach.
o Production becomes better and improved through ITIL's guidelines.
o ITIL helps to differentiate the administrative and technical tasks separately, so it brings more effective ways to assign the appropriate resources.
o ITIL helps to bring effective third party services delivery through its speciation or ISO 20000 as the standard on service procurements.
o ITIL helps to use the experiences in efficient way.

The ITIL-process Security management explains the overall planning for management organisation to fit the information security. This process is basically depends on the practice code used for the information security management which is now called as ISO/IEC 27002.

ITIL helps to crack the information security down into:

o Policies: This is the main goal of an organization which tries to achieve.
o Processes: These happen when the policy goals are achieved.
o Procedures: These procedures are to identify the persons and also to mention what and when he\she needs to perform the goals.
o Work instructions: These Instructions are helps to perform the specific tasks for perform the goal.

The main aim of security management is to control and ensure enough information security. The ultimate aim of information security is to save information/data from the security attacks. Usually these goals are explicated in terms of assuring the confidentiality, integrity and availability, which along with associated attributes or aims such as authenticity, accountability, non-reputation and reliability.

**B) International organization for standardization (ISO) 27001/27002:**

ISO/IEC 27001 basically determines the compulsory demands for an information security management system (ISMS). These standards also uses and certification standard for ISO/IEC 27002 to show the desirable information security controls among the ISMS.

Basically the ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 models help the IT sectors to respond and answer some fundamental questions like as:

o ―How do I ensure that the current security levels are appropriate for your needs?
o ―How do I apply a security baseline throughout your operation?‖
o ―How do I ensure that my services are secure?‖

 ISSN: 2454-4248
511 – 517

**C) Open Virtualization Format (OVF):**

OVF helps to provide the efficient, flexible, distribute secure software. It provides the mobility of virtual machines and the platform independence to customer's vendor. Customers are able to use OVF formatted virtual machine on their existing virtualization techniques. OVF offers numerous benefits to their customers to enjoy the enhanced virtualization with more flexible, portability, signing, versioning, verification, platform independence and licensing terms. OVF also help for customers like:

- user experience is improved with the help of streamlined installations
- customers get platform independence on using virtualization
- customers are easily able to create the difficult pre-configured multi-tiered services
- mobile virtual machines help to deliver the enterprise software with more efficiently
- extensibility helps customers to adopt their technology easily in virtualization and also helps by providing platform based enhancements
-

**2) Security management standards using in E-Learning technology sector:**

To develop an online e-learning solution there are number of factors and standards of distance learning in education to be considered, which will influence its survival and the growth in the future market. For different online learning vendors the main factors which are vital to sell the products in the markets are standardization and compatibility. There is also a factor to check whether different e-learning systems are compatible with one another or not. There are several working groups which are seeking to develop the standards for the e-learning sources. Those groups suggest the principles and standards concerned mostly on the sharable components and other resources. Principles involved in them also suggest the privacy and the security issues involved in the e-learning solutions. Some of the groups which work in the proposal and in development of these standards are [1]

- IEEE LTSC: IEEE Learning Technology Standards Committee
- IMS GLC: IMS Global Learning Consortium
- AICC: Aviation Industry Computer-Based Training Committee
- ARIADNE: Alliance of Remote Instructional Authoring and Distribution Networks for Europe and
- ADL-SCORM: Advanced Distributed Learning-Sharable Content Object Reference Model

In the Sections below we review the standards involved along with the privacy and security concerns involved in them.

**A) IEEE P1484:**

IEEE P1484 is the model which was proposed by IEEE LTSC. It involves the specification of Public and Private Information (PAPI) which effectively describes all the variances that deal with the privacy and the security features using the learner's information. They may create, store, retrieve the users information by using specific entities. It categorizes the views related to security from the different stakeholders involved in the system like developer, regulator etc. It also chooses the different entities involved in the customer management like their contact information, preferences, performance, personal information and portfolios.

As explained above it does not explain about a specific structure or a model or a technology but it explains all the security issues implemented in order to provide privacy factor. Also it does not provide any privacy or a security policy. It only explains that the administrators and the learners will act as the policy makers by applying the policy factor of privacy using certain security techniques and technologies. It uses a factor of logical division of learner information. Once if the learner information gets accredited in server it will become de-identified, partitioned and compartmentalized which will cover most of the privacy and security factors related to the user.

**B) IMS LIP:**

The IMS global learning consortium (IMS GLC) is an organization intended to develop open specifications for distributed learning. This is involved in addressing the key challenges and problems in distributed learning environments with a series of reference specifications which include Meta-data specifications, Enterprise specification, content & packaging specification, question and test specification, 35

Simple sequencing specification, and learner`s Information Package specification. Among all the specifications mentioned above IMS Learners Information package deals with the interoperability of the Learner`s Information systems with other systems which are supported by the internet learning environment.

It employs different ways to capture Learners' information which includes his education record, training log, professional development record, and life-long learning period, community service record (e.g. work and training experience). With the help of the learner's information the system can be made to respond to specific needs of the user or learner. By employing the learners' Information server the Learning system can be efficiently utilized by the user.

 ISSN: 2454-4248
511 – 517

For maintaining privacy and security for the learners, information for providing better support to the learner, enable certain mechanisms in the IMS LIP specification. A learner information server is responsible for sending and receiving learner's data to other information systems or other servers. The server is administered or monitored by a special authorized person. All the packages that are needed for importing or exporting the data from the Learner information server are provided below. Data Privacy and integrity are considered to be the most vital requirements for the IMS LIP specification. Nevertheless the IMS LIP specification does not avail the facility of having a look at the details of Implementation mechanisms or architectures that are employed for providing security and integrity to the Learners Information. The IMS LIP final specification V1.0 is not providing any following structures for enabling any suitable architecture for learner privacy protection.

i) **The privacy and data protection meta-structure:** If we consider a learner information tree structure, each tree node and leaf is associated with the set of privacy description which consists of privacy levels, access rights and data integrity. The granularity of information can be defined as the set of data which cannot be further breakdown the independent privacy data.

ii) **A "security key" data structure:** In general, password, public key and digital signatures can be considered as the security keys. Structure of the security key, the password and security codes are used for communication. Based on the structure we can allow the public key encryption, data authenticity, and password –based access control on learner information.

**C) Other E-learning Standards:**

For distance learning systems there are standards and some industrial organizations working on specifications. They are Aviation Industry CBT [Computer-Based Training] committee (AICC), the Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE), and the Advanced Distributed Learning-Sharable Content Object Reference Model (ADLSCORM). But most of them are providing very little reference to security and privacy but are concentrating more on content management, meta-data specification.

**For example:**

- The AICC focuses on practicality and provides recommendations on e-learning platforms, peripherals, digital audio, and other implementation aspects.
- The ARIADNE focuses mainly on meta-data specification of electronic learning materials with the goal of sharing and reusing these materials.[1]

**SECURITY MEASURES IN CLOUD BASED E-LEARNING**

From the previous research on cloud computing threats, we know the severity of problems involved in cloud based e-learning technology and for its vendors, as well as the e-learners. Cloud based e-learning technology also uses some sort of management standards and other security measures to overcome the security vulnerabilities and threats. Since cloud based e-learning is combination of two different technologies, we need to consider the both technologies on security measures and methods used to overcome security threats.

**A) Security measures taken in cloud computing:**

There are several security measures taken to overcome the security threats involved in cloud computing technology by cloud vendors as well as international committee for cloud computing organisation. These security measures answer how to overcome the security problems we discussed earlier. Those security measures are:

**1) Software-as-a-Service (SaaS) security:**

SaaS is a cloud service model in which most of the security practices and oversight will reside. Before adopting the service model by the corporations or end users they need to know the vendor policies on data security before using their services so that if they can block the unintended access of the data. The Gartner lists even security risks which one should discuss with a cloud-computing vendor before buying cloud-computing services.

**i) Privileged user access:** The users should gather information from the various management people who are accessing the data. They need to get useful information and oversight of all the privileged administrators, and the control over their access.

**ii) Regulatory compliance:** one should make sure that the vendor should be ready to undergo external audits and/or Security certifications.

**iii) Data location:** While using the cloud computing services we are not sure of where our data resides. It can store in various countries so that the cloud computing service vendors should be willing to accept the rules and regulations of the jurisdictions, and should undergo the contract with the local privacy requirements on behalf of their customers.

**iv) Data segregation:** The data should be able to encrypt at all the stages, and the encryption algorithms should be tested by experienced professionals.

**v) Recovery:** The cloud should provide the facility to recover the data and the infrastructure if the cloud has undergone some unintended attacks which can render the system complete destruction. So the vendor should provide facility to completely recover the data even after the destruction of the data.

 ISSN: 2454-4248
511 – 517

**vi) Investigative support:** If an unintended attack or illegal activity occurred on a cloud computing source one cannot easily investigate where it`s from. The users can login from multiple locations and from variety of host and data centers. The vendors should be able to provide privileges for the specific investigation along with the evidence that such activities are supported by the vendors. This investigation of the attacks can be done systematically.

**vii) Long-term viability:** In a business context it's quite common for the service provider to be acquired by a big company. Even then the customer or the user should be able to access the data and acquire all his data. In such a situation, the SaaS providers are expected to incorporate such security management practices to develop new ones for cloud computing environments.

**2) Security management (People):**

For organizations which provide technology based services it's obvious to have a security team. To make it possible for the employees or team members to reach their potential there should be a charter formulated clearly depicting the roles of the members of the security team. Lack of such proper plan that details the roles of the members of the security team renders the organization to be a failure.

**3) Security governance:**

A committee on security issues can be constituted in the organization. The main goal of this committee is to provide guidance and assistance regarding the security issues that align with the organizations strategies. The committee must clearly define the roles and responsibilities for the organization in providing information security functions.

**4) Risk management:**

Risk management involves a variety of tasks such as identification of technical assets and data and its direct indications to the business processes and applications, data stores, etc. The owners of the organizations have the authority and obligations along with accountability for the information assets that includes custodian's confidentiality, integrity, availability, and privacy controls.

**5) Risk assessment:**

Risk management is an important business process that keeps the organization informed while moving forward in taking a new step or a decision. The risk management helps the organization to decide on whether it could go for a new decision or not. The main challenge for risk management is to give equal priorities for the users or customers interest along with the security. Security assessments like threat modeling are recommended to be implemented with the applications and infrastructure.

**6) Security awareness:**

Creating security awareness is also one of the important actions that need to be done. Lack of proper security awareness can make them to reveal or expose vital data of the organization which in turn can cause the organization vulnerable to threats. Social engineering attacks, lowering reporting of and slower responses to potential security incidents can cost huge loss to the organization which is a result of poor security awareness.

**7) Education and training:**

This involves in providing proper training about the fundamental security issues and risk management skills for the security team and their internal partners. This involves in identifying the set of skills of the security team members and to provide them proper training and mentorship that can be as broad base of fundamental security, inclusive of data privacy, and risk management knowledge.

**8) Policies and standards:**

For developing policies or standards for the cloud computing systems it's always a good idea to take into consideration the already available templates and resources. The first and foremost important task of the security team is to consider data security along with the business requirements. These policies should strictly provide with proper documentation which supports the policies and standards. For maintaining relevancy these standards and policies should be revised from time to time with considering significant changes that occur in business or IT environment.

**9) Third party risk management:**

Lack of third party risk management can be of a huge loss for the organizations reputation, revenue losses due to the negligence on the part of the third party vendors.

**10) Vulnerability assessment:**

This is useful in classifying network assets to create enough significance and space for vulnerability-mitigation programs such as patching and system upgrading.

**11) Security image testing:**

Virtualization-based cloud computing is helpful in creating ―Test image‖ VM secure builds and to clone multiple copies. Gold image VMs provides the system to be up to date that reduces the exposure due to patching offline. Offline VMs can be patched off network which helps in providing better usage of resources with less cost and less production threatening way to test the security changes on the system.

 ISSN: 2454-4248
511 – 517

**12) Data governance:**
This framework mainly involves the roles by various stakeholders in data access and actions to be performed and the methods to be employed.

**13) Data security:**
Security to the data is demanded for the cloud based technologies that are present now in the market. The Organizations can provide encryption of certain types of data, which make it possible for the specified users to access the data. This also can provide compliance with the payment card Industry Data Security Standard (PCI DSS).

**14) Application security:**
Application security is all about the security features and requirements of application program and its interface. Application security is also used to review the security test results of application. Security team and development team work together to bring the efficient application security processes, guidelines for secure application coding, training, scripts using for testing and tools. Even though product development engineering teams concentrate on security design of application layer and its infrastructure layer, security team must supply the security requirements for the product development engineers to bring the best security measures and to implement their ideas.

**15) Virtual machine security:**
Cloud environment is usually grouped many physical servers into virtual servers to operate the virtual machines. In this cloud environment, not only the cloud vendors and their data security teams are secure the virtual machines to implement the important security controls for the data center. Those data security teams also give the guidelines to their customers to prepare their virtual machines and its security for cloud environment.

**16) Identity Access Management (IAM):**
IAM is one of the most important operations for any organization where the basic expectation from the SaaS customers on ―Principle of least privilege‖ is allowed for their information stored in cloud servers.

**17) Change management:**
Change management is the work taken by security teams under cloud vendors, in that they make some set of rules and guidelines for security management standards and the other small modifications in security measures. These guidelines are to give the self-service capability to the system to adopt those changes, which help to reduce the security team's time and resources to prioritize for those modifications on security measures and production.

**18) Physical security:**
Cloud computing does not allow their customers to have the access for the physical assets, so the security model should be reevaluated. Even though cloud computing customers valuable data is not stored in their own physical memory, but still their data is stored in somewhere on physical location of cloud vendor's. A huge financial budget needed to build high level security for physical data centers. That is the main reason behind the avoidance of companies to build their own data centers and for immigration to cloud services. So cloud vendors are needed to take many security measures for their physical data centers like:
1) 24*7*365(366) onsite security
2) Biometric security installation for access physical assets
3) Security cameras need to watch all the activities on physical properties throughout their service
4) Physical servers and other assets of cloud vendors should be maintained with right temperature, air flow, and humidity.

**19) Disaster recovery:**
When considering SAAS environment, the customers expect that the systems to respond and provide services 24/7/365 without any hassles. Using virtualization software virtual server can be copied, backed up, and can be easily relocated like a simple file.

**Benefits are:**
- No downtime are required to reallocate the computing resources in case of any natural or other kind of disaster affects the cloud servers.
- Able to provide and deliver the service level agreements (SLA) with high quality service.

**20) Data privacy:**
There is a need for constituting a committee for supporting in the decision making process that is related to data privacy. Another way of doing is to employ or hire a privacy expert, consultant in that area. This can create confidence for the customers that organization can meet data privacy needs.

**B) Security measures taken on e-learning:**
There are number of security measures taken up to overcome the security threats and vulnerabilities in cloud based e-learning by various vendors and organizations involved using this technology. Apart from all these security measures, e-learning technology already have some mechanisms to handle the vulnerabilities over internet and other incoming threats for its technology to protect e-learning materials and e-learners from those attacks. Those security mechanisms are discussed here:

 ISSN: 2454-4248
511 – 517

1) **SMS security mechanism:**
This process is used for the authentication of a legitimate user into the e-learning environment. The procedure is same like in the case of ―team viewer‖ where a user at first logged into the e-learning server with the help of a user name and a password which is provided during the registration period. After entering into the environment the user will get a pass code for that specific session in the form of an SMS (Short Message service) to his mobile phone which is registered in the server and thus security is maintained. As the logging phase of the user is specified from session to session with the different pass code it is mainly used to stop the provisions or illegal entry into the e-learning server from the outsiders or illegitimate users.

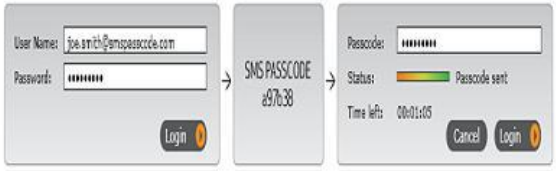


**Figure 11:** SMS passcode login scenario [1]

2) **Biometric Mechanisms:**
It is the mechanism in which the security is maintained. It gives allowance to the legitimate user by using one or more of their own physical or behavioral attributes. During the registration phase, one collects the physical traits of a user like finger prints, iris recognition or behavioral traits like voice recognition etc. and they will be stored in the database. During the login of the user the attributes of them will be compared to the one which is stored in the database by the use of some biometric scanning devices like finger print mouse etc. If both of them are same the content of e-learning is provided to the user. In this process it involves the physical presence of the user which is very keen, reliable and secure.

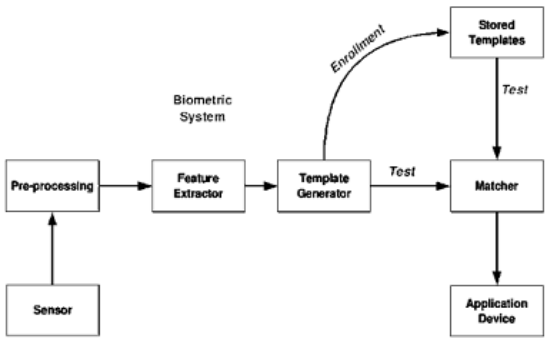


**Figure 12:** Biometric system diagram [1]

3) **Security Token:**
It is a common way of issuing authentication by many universities for their students where they provide a hardware security token. It is sometimes called as a cryptographic token and its acts like a key to gain access into the e-learning system. It is further provided with a password mechanism by showing the identity electronically and entering the password one can gain access to the system.

4) **ACL mechanism:**
ACL or Access Control List mechanism is the process to gain access to the server or the specific resources. In this the user can access their mechanism by using customization factor. The ACL factor will be attached or in built in the file. For example we want to add the user ―Shane‖ to gain access to the system then we have to specify user ―Shane‖ into the ACL file so that he can gain access to the system. We can also give several other functions to the user like ―read, write, delete‖: This option will give access to the user Shane to read, modify or to delete the specific file. These are all host based mechanisms and all the permissions are confirmed under the control of the service provider.

5) **Digital Signatures:**
Digital signatures are used to authenticate the identity of a sender. In this it is easy to find out whether the original content in the message has been modified or not. It consists of mainly three contents. At first an electronic signature has been generated from the sender while sending the message to the receiver from an insecure network. Along with the message and the signature, the sender will submit a certificate sort of thing which is produced from a hash algorithm and private key from the sender's computer. The main advantages with these digital signatures are to provide non-repudiation. Even though sender claims that he did not sign a message and kept his private key secret, we can claim that by using some non-repudiation algorithms which can produce a time stamp with that we can authorize and claim that the message has arrived from the sender. We can also check whether the data has been modified by the intended user.

6) **Security from passive attacks:**
In all the above methods we discussed about the active attacks from the outers. In case of passive attack one will not make any effect on source or the destination systems but the cipher text or in some case the plain text will be modified by the attacker. By using modern ciphering methods we can avoid these types of attacks. By using certain cryptographic methods like private key cryptography, public key cryptography and hash functions we can avoid passive attacks.
The key security threats in cloud based e-learning servers are analyzed and listed here:
1) Availability
2) Increased authentication demands
In order to overcome these security threats on servers, there are numerous security measures and security management

 ISSN: 2454-4248
511 – 517

standards which are being followed by cloud based e-learning solution vendors. They are:
1) Disaster recovery
2) Physical security
3) OVF security management standard

E-Learners are the main stakeholder of cloud based e-learning technology, so security concerns about e-learners are crucial. We also observed some of the key security threats faced by e-learners in this technology are:
1) Browser security
2) Social aspects of security
3) User authorization and authentication

Further, some counter measures and security management standards are in use by cloud based e-learning solution vendors. They are:
1) SMS security mechanism, biometric mechanism, ACL mechanism
2) Security token
3) Digital signatures
4) Security from passive attacks
5) XML signature and encryption methods
6) Security awareness
7) IEEE P1484 & IMS LIP Security management standards

**E-learning materials security in cloud based e-learning:**
E-Learning materials are nothing but the information/data which is used to teach the e-learners, and the data stored in server to run the cloud based e-learning solutions. These materials play a vital role on teaching e-learners through online by e-learning solutions. So if someone or some attack malfunctions or deletes these materials from cloud based e-learning solutions through server attacks or by any virus codes, it makes a huge security problem. So, the security concerns on e-learning materials used in cloud based e-learning are very important for the technology. We gather some key security threats over e-learning materials which are used in cloud based e-learning technology. They are:
1) Data lock-in
2) Insecure of incomplete data deletion

To overcome these security threats on e-learning materials in cloud based e-learning technology, some counter measures and security management standards are used by cloud based e-learning solution vendors. They are:
1) Data privacy
2) SaaS security
3) Security management standards:
a) ITIL
b) ISMS
c) ISO/IEC 27001
d) AICC
e) ARIADNE

**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