

Analysis of Security in Cloud-Learning Systems

Sangeetha Rajesh

K.J. Somaiya Institute of Management Studies and Research,

Available online at: www.isroset.org

Received 26th Dec 2016, Revised 12th Jan 2017, Accepted 30th Jan 2017, Online 28th Feb 2017

Abstract- Developments in computing are influencing many aspects of education. ELearning introduced a new learning environment. The e-learning systems need to cope its processes with the progressive technologies like cloud computing. Cloud computing is highly scalable virtualized resources that users can access. Cloud computing made a significant influence in the educational environment. Throughout paper elearning system using cloud technology is referred as cloud-learning systems. This paper mainly emphasizes on the impact of cloud computing in e-learning system with respect to security. In this paper architecture for cloud learning system is proposed which has security as a service model. The responsibilities of each participant in the system and the services provided by security as a service model are also studied.

Key Terms: Cloud Computing, cloud-learning, eLearning, IaaS, PaaS, SaaS, SCaaS

I. INTRODUCTION

Elearning is the use of network technology to design, deliver, select, administer and extend learning [1]. Elearning software focus on providing educational services based on internet services and virtual websites. It is the convergence of learning and the internet. Elearning is a widely accepted learning model. It provides new advances in learning system. Cloud computing introduced a new computing platform where services can be achieved as a purchase in demand or pay per use [2]. Elearning services based on cloud computing can significantly reduce costs and improve efficiency. Security is an issue in cloud computing related to information security and privacy protection. Since cloud computing depends on the web based sources, various threats attack the e-learners and the cloud based e-learning technology through the internet.

The objective of this paper is to study the cloud based elearning system, security issues related with this system and to propose cloud learning system model with security as a service.

Rest of the paper is organized as follows: Section I discusses the relevance, motivation and objective of selecting this topic. Section II covers the summary of literature review on cloud computing and its features. Section III reveals the concepts of elearning system. Section IV depicts the architecture of cloud based elearning systems. Section V illustrates the security issues related with the cloud learning systems. Section VI presents the proposed architecture of cloud learning system with security as a service model. Finally, section VII concludes the paper with future scope.

II. CLOUD COMPUTING

Cloud computing is a model for providing scalable access to networks and applications. Common set of configurable computing resources that can be provided and released immediately with minimal effort or involvement [3-7]. Users can use the computing resources on demand and pay according to the usage. It is a model where the services it provides are the computing resources [8]. It shifts the responsibility of configuring, deploying and maintaining computing infrastructure from clients to cloud providers [9]. They provide an interface for clients to interact with their resources as if they are their own standalone resources. The user doesn't necessarily know the details of location or configuration of their resources. They are provided with virtualized computer resources hosted in the cloud [10]. Figure 1 depicts the different services and deployment models of cloud architecture. Various cloud services are presented into three models.

- Infrastructure as a Service(IaaS)
- Platform as a Service(PaaS)
- Software as a Service(SaaS)

A. IaaS

IaaS providers supply a virtual server instance and storage as well as application program interfaces(API) the let users migrate workloads to a virtual machine(VM). Infrastructure is not managed or controlled by the client in this model. The client has control over the operating system and storage.

B. PaaS

PaaS providers host development tools on their infrastructures. Users access those tools over the internet

using APIs. It enables the OS and middleware services to be delivered from a managed source over a network.

C. SaaS

It enables software to be delivered from a host source over a network as opposed to installations or implementations. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access.

Different cloud deployment models are follows:

- Private cloud
- Public cloud
- Community cloud
- Hybrid cloud

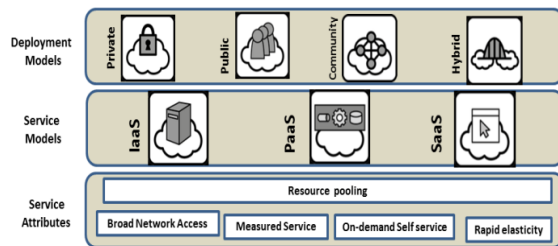


FIGURE 1: CLOUD SERVICE MODEL

Key features of Cloud computing are :

- Resource Pooling
- Broad network access
- Rapid elasticity
- On demand self service
- Measured service
- Quality of service

III. E-LEARNING SYSTEM

E-Learning is one of the most famous technologies discovered to make the traditional way of education, learning easier with the help of software applications and virtual learning environment. The word —E means the electronic way of learning in the E-Learning. There are various names that are used to express the term E-Learning in a technological world such as Computer based training (CBT), Internet based training (IBT), and Web based training (WBT) [11]. These terms, express the way of E-Learning teaches the lesson to the e-learner. E-learning comes through a network enabled computer and transfers the knowledge from the internet sources to end user's machine [12]. Through E-Learning environment the students get access to the materials and tools relating their studies. Two important E-learning environments are:

- Virtual learning environment: The students are able to get face to face classroom environment through computer applications with the help of web sources.
- Personal learning environment: The E-Learners to manage and modify their own learning.

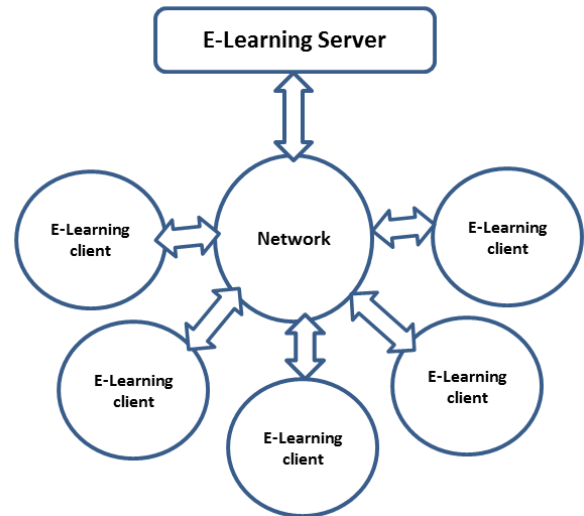


FIGURE 2: E-LEARNING SYSTEM

The architecture of a distributed e-learning system includes software components, like the client application, an application server and a database server and the necessary hardware components. Traditional learning in the remote and rural areas has many difficulties like shortage of teachers and problems in quality of teaching. Such problems can be overcome by eLearning. Educated academicians can give their input for educating rural students also.

IV. CLOUD-LEARNING SYSTEMS

Cloud-learning is using cloud computing technology for e-learning systems. Cloud based e-learning provides hardware and software resources to enhance the traditional e-learning infrastructure. Once the educational materials for e-learning systems are virtualized in cloud servers these materials are available for use to students and other educational businesses in the form of rent base from cloud vendors [11]. Benefits of cloud learning systems are listed below.

1. Virtualization
2. Centralized data storage
3. Lower costs
4. Improved performance
5. Instant software updates
6. Easy monitoring
7. Improved document format compatibility

Cloud-learning systems is divided into five layers [12]

- Hardware resource layer
- Software resource layer
- Resource management layer
- Service layer
- Business application layer

Figure 2 represents the cloud architecture of cloud learning system without security as a service.

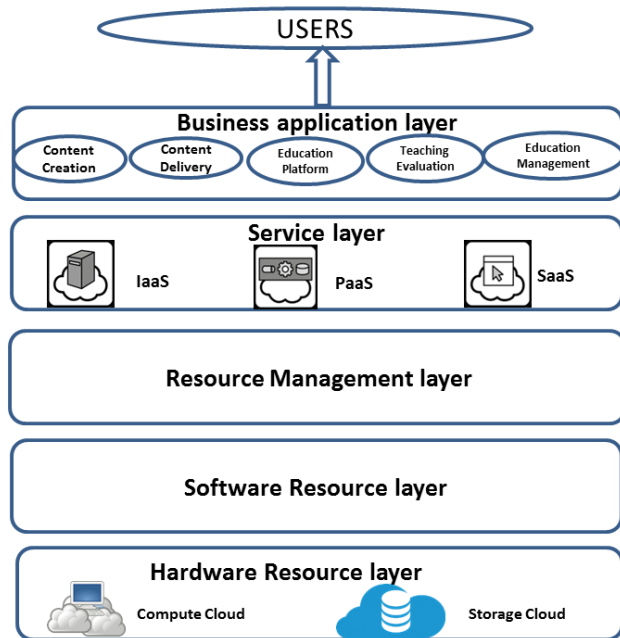


FIGURE 3: ARCHITECTURE FOR CLOUD-LEARNING SYSTEMS

V. SECURITY ISSUES IN CLOUD LEARNING SYSTEM

Security issues have significant importance in this technology as it ensures the reliability of technology in users mind to handle it. Since the cloud learning depends on the web based sources numerous threats are waiting to attack the e-learners and the cloud based elearning technology through the internet [11]. Cloud technology provides plenty of advantages to elearning systems; security is still in doubt for its security issues and challenges in digital world. Issues related to cloud learning systems are follows.

1. Confidentiality violation: An unauthorized party gaining access of the assets present in the cloud learning system.
2. Integrity violation: An unauthorized party accessing and tampering with an asset used in cloud learning system.
3. Denial of service: Prevention of legitimate access rights by disrupting traffic during the transaction among the users of elearning system.
4. Repudiation: Learner’s denial of participation in any transaction of documents

VI. PROPOSED ARCHITECTURE

In the proposed architecture, security is provided to the user as a service - Security as a Service (SCaaS) is shown in Figure 4.

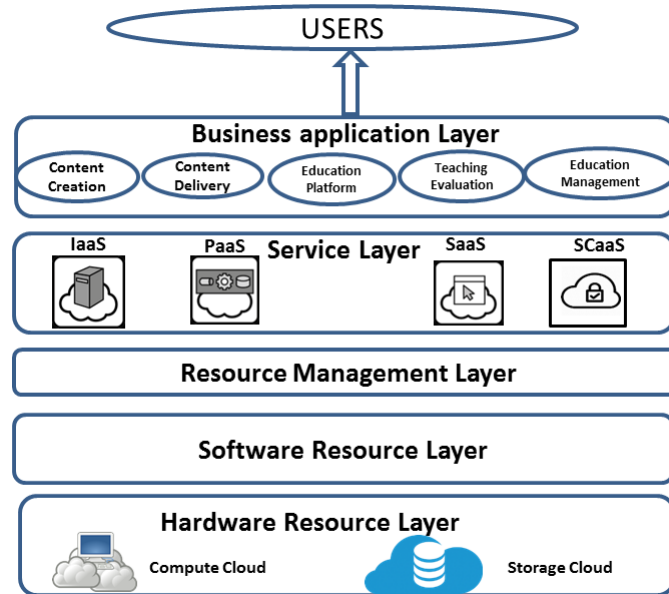


FIGURE 4: ARCHITECTURE FOR CLOUD-LEARNING SYSTEMS WITH SCAAS

The cloud learning system participants are:

1. End user –students
2. Cloud Service Provider(CSP): An organization that makes the service available.
3. Cloud service requester(CSR):Educational institute staff
4. Cloud Security Provider(CSP): Provides the security services
5. Auditor: Independent IT security assessor

The security related responsibilities of each of these users are as follows:

- End user or CSR
 - Security awareness to everyone involved in the system.
 - Access agreements
 - Malicious code protection
- CSP
 - Regular audit and monitoring to analyze, repair, verify, track and capture malicious activity
 - Monitoring for unauthorized configuration changes
 - Utilizing monitoring tools to maintain a secure information system environment.
 - Backup and recovery
 - Environmental controls for the customer and provider
 - Physical access for customer and provider.
- End user or CSP
 - Account management

- Account enforcement
- User identification and authorization
- Device identification and authorization
- Authentication management
- Cryptographic key establishment and management
- Auditor
 - Security assessment
 - Security certification
 - Security accreditation

Security enhancing services which can be used to provide security for cloud learning systems by the SCaaS are described below.

A. Email Security

CSP will provide email security as a service securing inbound and outbound emails. This service can be used to protect against malicious attachments which may affect security of the cloud learning systems by email or email attachments through enforcing of corporate policies on spam mails and acceptable use of email is made more secure.

B. Web gateway security

It is real time service; secure gateways operating via the cloud to redirect web traffic to the cloud provider. It is accomplished by policy management, web access control, control web traffic and back up of data.

C. Identity and access management

Identity management includes the identity provisioning as well as de-provisioning. When access of resources in the cloud learning needs to be managed to allow responsible access and also deny access when no longer sees necessary for a user to have access to cloud resources.

Access management comprises the authentication and access control services. The learners should be authenticated and access managed through developing trusted user profiles and policies to control cloud service access in a responsible and traceable manner.

- Access and password management
- Administration provisioning
- Automated provisioning and de-provisioning
- Multifactor authentication and governance
- Reporting
- Alerting and analytics

D. Security Information and Event Management(SIEM)

It aims to collect log and event data from both virtual and real network, applications and systems. This information is them compared and analyzed in the cloud for real time reporting and alerting on potential threats and compliances.

E. Remote vulnerability and security assessment(RVSA)

RVSA service has the challenges of inventory assurance, architecture and configuration security logging and monitoring covered.

F. Intrusion management

The strategies and systems for prevention and detection of intrusion are implemented on cloud servers at entry points to the cloud for broad coverage. The enterprise environment is monitored at key vantage points to locate potential threats. Unauthorized access and traffic is effectively made impossible either through event based detection or traffic network based detection.

G. Encryption

Data can be secured at rest, in transit and in use with encryption. This should be prerequisite when computing in the cloud to ensure all valued information is secure and upholds its integrity.

H. Disaster recovery and business continuity

It includes the procedure deployed to assure resiliency in the event of a disaster any disruption in service both minor or major. Back up can be made at multiple locations allowing for reliable failover and recovery.

I. Network security

It is accomplished through a combination of the services already mentioned as part of the SaaS offering, identity and access management, web security and intrusion management.

The mentioned security services can be categorized into different categories as given in table 1.

TABLE 1.SCaaS SECURITY POSTURE

Category	Domain	Protective	Preventive	Detective	Reactive
1	Identity and access management	✓	✓		
2	Data loss prevention		✓		
3	Web security	✓		✓	✓
4	Email security	✓		✓	✓
5	Security assessment			✓	
6	Intrusion management	✓		✓	✓
7	Security information and event management			✓	
8	Encryption	✓			
9	Business continuity and disaster recovery planning	✓		✓	
10	Network security	✓		✓	✓

VII. CONCLUSION

Cloud computing is a recently developed advanced Internet-based computing model. By combination of cloud computing and e-learning, building cloud-learning system opens up new ideas for the further development of e-learning.

The use of new technologies instead of the traditional method always lessens the manpower, but results in many security issues. In this paper, we discuss security concerns of cloud based eLearning. I propose architecture to overcome the threats in the cloud-learning systems by including security as a service model to the cloud-learning system. The responsibilities of each role in the system and the service model are specified. Security related to the cloud computing technology can be considered as a major research area and future work can be done on the same.

REFERENCES

- [1] SOM NAIDU," E-Learning A Guidebook of Principles, Procedures and Practices" 2 Revised Edition, CEMCA, 2006.
- [2] Xiang Tana, Bo Aib, "The Issues of Cloud Computing Security in High-speed Railway", International Conference on Electronic & Mechanical Engineering and Information Technology 2011.
- [3] H. Takabi, J. B. D. Joshi, G.Ahn., "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security Privacy Magazine, Vol. 8, IEEE Computer Society, 2010, pp.24-31.
- [4] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol-01, Issue-01, Page No (31-37), Feb 2013.
- [5] Surabhi Shukla and Dharamjeet kumar, "Cloud's Software-Security as a Service(S-SaaS) via Biometrics", International Journal of Computer Sciences and Engineering, Vol-02, Issue-03, Page No (119-124), Mar -2014.
- [6] Shaheen Ayyub and Devshree Roy, "Cloud Computing Characteristics and Security Issues", International Journal of Computer Sciences and Engineering, Vol-01, Issue-04, Page No (18-22), Dec -2013.
- [7] Sajjad Hashemi, Sayyed Yasser Hashemi, " Cloud Computing for Elearning with more emphasis on security issues" International Journal of Computer, Control and Quantum and information engineering, Vol 7, No. 9, pp.607-612, 2013
- [8] Rajesh Piplode, Pradeep Sharma and Umesh Kumar Singh, "Study of Threats, Risk and Challenges in Cloud Computing", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol-01, Issue-01, Page No (26-30), Feb 2013.
- [9] A.A. Elusoji, L.N. Onyejegbu & O.S. Ayodele (2013). "An Effective Measurement of Data Security in a Cloud Computing Environment". Afr J. Of Comp & ICTs. Vol 6, No. 2. pp 67-76
- [10] cloud-basedlms-etec522. Weebly (2015, September 16). (Online). Available.<http://cloud-basedlms-tec522.weebly.com/security.html>.
- [11] Vishal Kadam, Makhan Kumbhkar , "Security in Cloud Environment", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Volume-02, Issue-03, Page No (6-10), Jun 2014.
- [12] D. Kasi Viswanath, S. Kusuma & Saroj Kumar Gupta "Cloud Computing Issues and Benefits Modern Education" Vol XII, Issue X Version I, pp. 15-19, July 2012.
- [12] Vishnu Patidar, Makhan Kumbhkar, "Analysis of Cloud Computing Security Issues in Software as a Service", International Journal of Scientific Research in Computer Science and Engineering, Vol-02, Issue -03, PP (1-5) Jun 2014.
- [13] Cloudcomputingadmin.com, 2016, May 26, (online). Available: <http://www.cloudcomputingadmin.com/articles-tutorials/security/security-service-cloud-based-rise-part1.html>