IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 4 ISSUE : 07 Print / Issue Publication Date: 07-Jan-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2019.v04i07.001

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

A NOVEL MODEL FOR SECURING ACCESS OF CLOUD-BASED E-LEARNING SYSTEMS

Manahel Omar Hussen, Nirmla Sharma, Hosam F. El-Sofany
Department of Computer Science, Faculty of computer science,
King Khalid University, Abha, Saudi Arabia

Fakhry Abbas
Department of Computer Science,
Faculty of computer science,
Alneelain University, Khartoum Sudan

***Abstract*— Cloud computing is a recent computing model based on the grid computing, distributed computing, parallel computing and virtualization technologies define the shape of a new technology and information technology (IT). It is the core technology of the next generation of network computing platform, especially in the field of education, cloud computing is the basic environment and platform of the future E-learning. Educational services in the form of E-learning systems should be containing high quality of hardware and software infrastructure, which needs a substantial investment. Since the vast majority of educational organizations unable to invest in this area so the best way for them is to reduce the costs and provide the E-learning services by using cloud computing, which provides secure data storage, convenient internet services and strong computing power.**

Security of cloud-based E-learning products is critical and the security measures are essential to protect valuable data of users from security vulnerabilities and attacks. Therefore, the success of E-learning systems is happened if users meet security requirements than can overcome security attacks and threats. This research study tries to explore cloud computing and its positive effect on E-learning, presents recent security issues that is related to cloud-based E-learning systems which used to improve security, and provide solutions for E-learning Management systems. Our main goal is to introduce a novel secure model for Cloud-based E-learning systems that can help to improve the quality of E-learning in the universities.

Keywords— **cloud computing, e-learning, e-learning security, cloud-based e-learning system, cloud services, cloud security.**

I. INTRODUCTION

Cloud-based E-learning is a way to reduce and complexity of data access, which is controlled by third-party services. Traditional e-learning methods have been integrated with cloud computing to deliver tremendous benefits to academic users but are compromising security. The proposed methodology ensures the availability of data and provides a solution to protect the data indispensable from attackers. This study recognizes security problems in the cloud service delivery model with the aim of proposing a key in the form of security measures related to cloud-based e-learning. So many types of attacks have discussed in the e-learning delivery model proposed by the students. The threats, security requirements and challenges have involved also taken into consideration. This study calls for e-learning models to access their data in the cloud through a secure layer using the Internet.

The E-learning has one of the important technologies that help organizations create a good learning environment with the help of the Internet. The problems have related to security issues cause constraints on cloud vendors and users. Different combinations of signal transmission technologies, advanced web technologies, and other device developments have established secure e-learning [1, 2]. The introduction of cloud computing technology in the e-learning has displayed many advantages over existing e-learning methodologies in infrastructure and cost. This cloud e-learning technology is an alternative technology suitable for traditional e-learning. Security is the key issue in cloud computing or on cloud computing demand model. In an IDC survey of 224 IT managers, security was marked as 74.6% as shown in Figure 1 [3].

In this paper, we provide a short but good survey of cloud security trends. We know that there are three models for cloud services provision. SaaS has following examples: Google apps, salesforce.com, zoho.com and so on. PaaS has some examples Google App engine, force.com, Microsoft Azure and so on. IaaS has examples Amazon, IBM, and Rackspace

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

Cloud which includes cloud security. One of the great virtues of cloud computing is service abstraction and site transparency. However, from a security point of view, these two points in conjunction with external data control can lead to difficult security implications. The paper describes how to secure the cloud environment, the impact of security threats, and the comparative study of security threats.

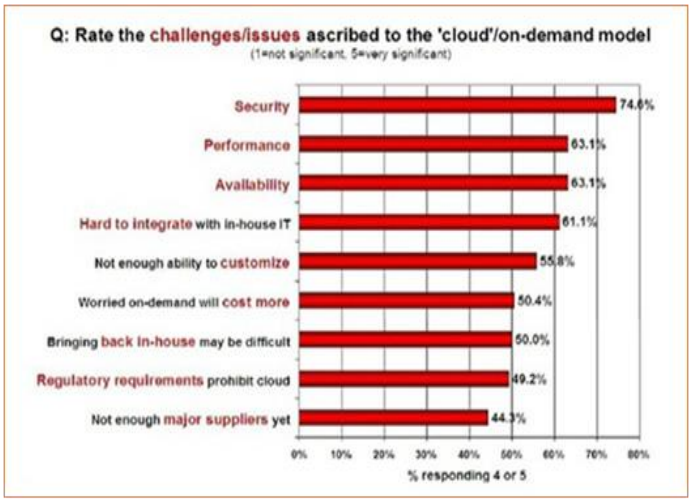

Fig1. IDC's survey report [4]

II. RELATED wORK

We reviewed some related work and found many research studies that dealt with the same area of our research study. These research papers explained about securing access of cloud-based E-learning systems.

In [5] the paper mainly focuses on the research of the application of cloud computing in e-learning environment. The research study has shown that the cloud platform has valued for both students and instructors to achieve the course objective. The authors present the nature, benefits and cloud computing services, a platform for e-learning environment.

In [6], writers tried to discover cloud computing and its positive influence on e-learning and put main focus to identify security issues that related to cloud-based e-learning efforts which have been improved security and offer keys in management challenges.

In [7] the use of web-based education through cloud computing is presented. The evaluation showed that it has strongly contributed to the effectiveness of E-learning by improving the quality of students' comprehension.

In [8] the researcher has presented a virtual and personal learning environment. It combines a wide range of technologies and tools for education. The author builds the proposed environment to support formal, informal learning to enable mashup of various learning services and the applications. The proposed cloud-based personalized e-learning system have three major functionalities: Web-based course management system (CMS), Personalized Learning Environment (PLE) and Smart Agents.

The authors in [9] discussed some of the theories in the learning field. The paper illustrates the building blocks of e-learning & traditional learning and the emergence of e-learning. It also describes about the emergence of cloud computing in e-learning and advantages of e-learning when implementing in cloud computing.

The researchers in [10] focused on rural schools in providing a quality education. It discusses about the problems faced by Indian Rural Education Environment. To solve this, the authors proposed advanced technologies and tools like Virtualization, cloud computing technology, Moodle which help in fixing the problems faced by them.

The authors in [11] discusses about the cloud computing definitions, types of cloud services and cloud service providers. Web Based Training (WBT) has one of the advancement of computer technologies which works with the help of preprogrammed software applications. Cloud based e-learning has five layers, namely hardware resource layer, software resource layer, resource management layer, service layer and business application layer. The expected benefits and issues are regarding the cloud based e-learning architecture has also discussed.

In [12] the researchers proposed architecture for e-learning based on cloud computing and presents a security issues in cloud computing, which we have to check before moving e-learning into the cloud.

III. CLOUD COMPUTING

Cloud computing uses three service models for improving organizations as presented in the following sections, through these models various types of services are delivered to the customers. Each service model has certain levels of security requirements in the cloud computing environment. These basic cloud service models include: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing models provide software, application, database, network platforms and infrastructure resources as a service. Figure 2 presents the different types of attacks that face these service models.

3.1 Security Issues in SaaS

The consumer is to depend on the supplier for security measures in SaaS. The supplier must prepare the work to keep various users from seeing each other's data. So it develops difficult for the user to ensure that right security measures and it is also complicated to get assurance. The request will be available when must avoid the risks of keeping high availability problems by having multiple copies of the data at several locations [13].

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

3.1.1 Data Security

The data play vital the role in cloud services because many of cloud service providers store customers' data on large data centers. There is no guarantee for customers' data during transition operations. Data corruption may synchronize to occur in multiple devices by one user. Data security can classify into two ways. First, data owner must fulfill that the cloud service provider will only process the data according to the customer instructions. Second, data owner must be satisfied that the cloud supplier has taken appropriate actions, when has unauthorized data access, data modification, destruction of data by intruders.

Cloud providers are initiated to give assurance for the following data security key issues.

- Take the preventive mechanism for unauthorized data access.
- Allow data owners to take back up frequently.
- Give legitimate authority to the data owners to data removal, data modification, and moving data to the other cloud provider

3.1.2 Network Security

Enterprises store sensitive data in the cloud server to manipulate by SaaS vendor. The data from leakage of sensitive information is protected to apply network traffic encryption techniques to manage data flow over the network.

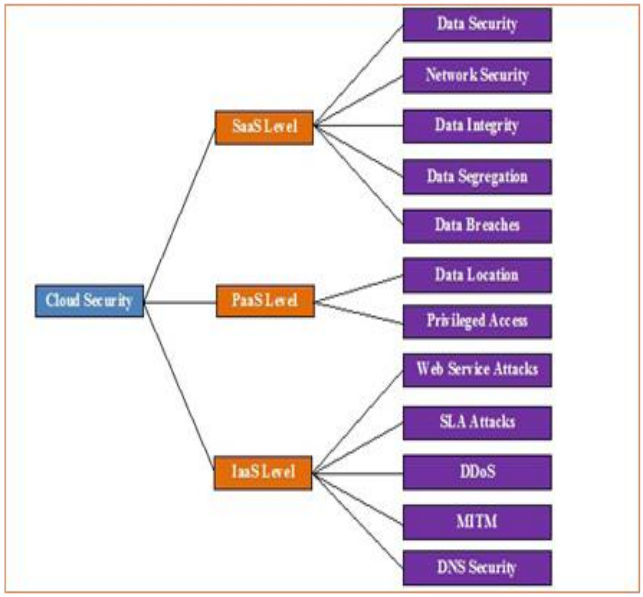

Fig2 Types of Security attacks in Cloud based E-Learning

Example Secure Socket Layer (SSL) and Transport Layer Security (TLS). Survey report says Amazon web services network layer provides significant security opposed to traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. Amazon yields maximum security using SSL. The following assessments inspect and validate the network security of the SaaS vendor:

- Network penetration and packet analysis
- Session management weakness.
- Insecure SSL trust configuration**.**

3.1.3 Data Integrity

Data integrity describes the correctness, accessibility, high quality, and reliability of kept data. Cloud provides integrity of data loadings for customer privacy. Third Party Auditor (TPA) get assistance to loss the risks of data integrity. The TPA has offered the capability of verifying any threats in online storage services by the cloud server. In a distributed environment, many data resources are concerned in database transactions to achieve data integrity. SaaS application needs multi-tenant situation for processing data and numbers of third parties are involved. According to survey [14], it discloses the information that encryption techniques are not sufficient to ensure the data integrity due to multiple sources. Hashing techniques, message authentication, and digital signatures are using to achieve the integrity of data.

3.1.4 Data Segregation

The data is presenting in the cloud in a shared situation; there multiple are sharing single location, so one customer's data is stored along with another client's information, which effects difficulty in data separation. The customer should observe the cloud provider's architecture to make sure correct a data separation. The customer should know protocols and implementation methods of the encryption system. Therefore, each user's the data limit should be considered by SaaS model.

3.1.5 Data Breaches

Ever since data from different users and business exist collectively in a cloud situation, break the data laws of cloud environment will certainly attack and damage the data of all the users. Therefore, the cloud has become important the worth target. In the Verizon Business, the report says that external criminals create the maximum threat (73%), but accomplish the very lowest impact, resultant value of Pseudo Risk Score of 67,500. Collaborators are middle in both (73.39% and 187,500) resultant value of Pseudo Risk Score of 73,125. However, SaaS supporters declare that SaaS providers can provide to improve security to customers' data than by conservative means still insiders have rights to use the data in a different way. The SaaS providers' employees have access to a lot more information, and a single event could represent information from many customers. SaaS application providers can submit their complaints with PCI DSS (Payment Card Industry—Data Security Standards) so that cloud users must meet the terms with PCI DSS.

3.2 Security Issues in PaaS

The cloud computing provides a computing platform and system software as a platform service. Cloud users have made a request by controlling software deployment and configuration settings from the providers. The major PaaS level security threats have in data site and privileged access.

3.2.1 Data Location

PaaS vendors offer services for application design, application development, deployment, team collaboration, web service integration, and testing. In this statement, the PaaS cloud users access the applications of SaaS providers to get service. So that, the customer does not know where the data is stored and processed, which makes vulner-ability to the system. According to the survey report, many countries have established universal security standards and data privacy laws for data location issues. For example South America and many EU countries, they never allow sensitive facts to move out of the kingdoms.

3.2.2 Privileged Access

The cloud provider has full rights to use data (including other users of the cloud and other third party suppliers). The data have stored in the cloud situation. There is no confidentiality of data in this cloud environment. The privileged user access has accomplished by at least any one or two approaches by the data owner. First one is to choose encryption method for store data and use another encryption method for data access; second one is to keep up high standard confidentiality of data, legally imposing the requirements of the cloud provider through contractual responsibilities and assur-ance mechanisms. The cloud provider must have security access control policies, technical solutions and frequent auditing of user movements to prevent unauthorized user access.

There are two challenges store encrypted data in the cloud storage. Challenge first is that the decryption keys must be disintegrated securely from the cloud environment to make sure that only an authorized party can decrypt data. Challenge second is that in the cloud situation, the more task about encryption is to prevent manipulations of encrypted data such that plain text, or any other meaningful data, has recovered and be used to break the cipher. If the cloud system user allows the cloud service provider to deal unencrypted data, then the cloud service provider must give guarantee that the data will protect to unauthorized access, both internally and externally.

3.3 Security Issues in IaaS

Infrastructure as a service model allows for the variety of resources such as servers, storage, networks, and other computing resources are as virtualized systems, which are getting access through the internet. Users can run any software with security on the allocated resources, so IaaS provides full control and management on the properties. Hence cloud providers are only responsible for configuring security policies. Some of the security issues have associated IaaS web service attack, SLA attack, DDoS attack, MITM attack and DNS attack [15].

3.3.1 Web Service Attack

Web service protocols have used by cloud users for getting service. SOAP is the most suspended protocol in web services; many SOAP-based security solutions have researched, developed, and implemented. A standard extension for security in SOAP is web service security, addresses the security for web services. It defines a SOAP header (Security) that transfers the Web Service Security extensions and determines how the existing XML security standards like XML Signature and XML Encryption have applied to SOAP messages. Well, known attacks on protocols using XML signature for authentication or integrity protection would be applied to web services consequently affecting the cloud services. Finally, an extreme scenario has presented the possibility of breaking the security between the browser and the clouds and has followed by the proposal to enhance the current browsers the security. These attacks belong more to the web services world, but as a technology used in Cloud Computing web services' security strongly influences the Cloud services' security [15].

3.3.2 SLA Attack

When customers have transferred their core business functions onto their committed cloud situation, they should be ensured the quality, availability, reliability, and performance of these resources, because cloud users do not have control over these computing resources. Cloud users are expected to get assurances from cloud providers on service delivery, which are rendered through Service Level Agreements (SLAs) to succeed among cloud providers and cloud users. The result is the explanation of SLA qualifications in such a way that it has an appropriate level of granularity, namely the transactions between expressiveness and complexity. IaaS, PaaS, and SaaS models have needed to determine different SLA Meta specifications. Finally, innovative SLA mechanisms need to ever mixed user feedback and customization features into the SLA assessment framework.

3.3.3 DDoS Attack

The attack has communicated with different dynamic networks to compromise as the DoS attack. The attackers only have the full control targeted system to access. Three functional units (a Master, a Slave, and a Victim) have used in the DDoS attack. Master is handling the work of launching the attack; Slave is acting as a launching platform in a network, where the master can launch the attack on the victim. Therefore, it is also called a synchronized attack The DDoS attack uses two different stages to operate functional units, the first is interference phase, where master check the possibilities

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

of loopholes and secondly, installing the DDoS attack tools attacking the victim server or machine. Purpose of DDoS attack has made the service unavailable to the authorized user for working procedure only the difference between the ways of launching.

3.3.4 MITM Attack

Man, In the Middle (MITM) attack is encountering when an attacker directs himself between two authentic users. This attack is also a class of eavesdropping. The attacker set up the connection between two users and tries to hear the communication or, it reveals false information between them. These kinds of attacks protect to develop following tools like Dsniff, Cain, Ettercap, Wsniff, Air jack and so on.

3.3.5 DNS Attack

IaaS cloud situation deals with the risky attack vector known DNS Attack, which translates the domain name to an IP address. The user using IP address is not realistic. It has routed to some other cloud virtual machine instead of original address. The cloud user and server get rerouted through some connection. Generally, applications depend for running Domain Name System according to achieve their functions as required. Websites use DNS in two ways, first handle own DNS and second authorize it to ISPs. The cloud service has difficult due to incorrect DNS. Domain Name Service security measures are taken still the route selected between the sender and receiver cause security problems.

3.4 Cloud Organization of Models

There are three types of cloud organization models as private, public, and hybrid which is frequently used. A further model is the community cloud, which is used occasionally. There are all facility models existing in cloud computing assumed under:

3.4.1. Private Cloud Model

A private cloud substructure is running for special practice through a distinct association including numerous clients (e.g., commercial components). It can be reserved, achieved, and functioned by the association, a third party, or roughly variation of them, and it can occur on or off properties [16].

3.4.2. Public Cloud Model

The Public cloud models have made available for the general request public through service provider storage, and other resources. These facilities have permitted to work on based on a pay-per-used model. Usually, public cloud facility as personal, major organizations Amazon, AWS, Microsoft and Google structure which has used through Internet.

3.4.3. Hybrid cloud Model

The Hybrid cloud has arranged two or more clouds (private, community or public) that continues exclusive objects but are certain composed, proposing the points of many assignment model [9,10], as shows in Figure 2.

3.4.4. Community Cloud Model

A Community cloud model segments organization between numerous groups from a complete community with problems (security, obedience, authority, etc.), whether attained to or through a third-party and presented inside or outside [16] Figure3.

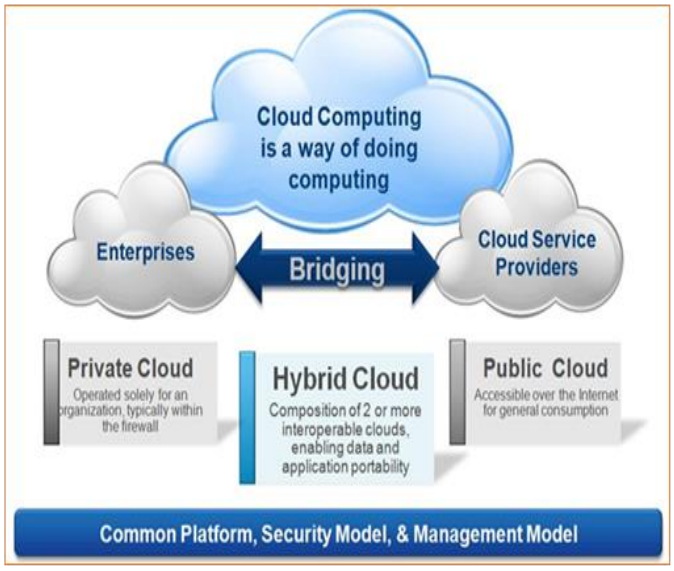

Fig3. Cloud Model [16]

IV. E- LEARNING SECURITY IN CLOUD COMPUTING

In the issue cloud computing security forecasts so numerous supports but immobile there are frequent concern and challenges reason for groups used the Cloud technology. Confidentiality of sensitive statistics is very important work, and devoted cloud servers are crucial if the cloud situation is to be recognized. When shifting e-learning in the cloud, main security concerns are about confidentiality, integrity and availability, as depicted in -Figure 4.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

Fig4.Cloud based e-learning system Apprehension region [17]

4.1. Paradigm of cloud computing in e-learning threats

There are numerous significant threats that should be considered before adopting the model of cloud computing in e-learning. These threats are described as follows:

4.1.1. Exploitation of Cloud

The exploitation of cloud services sources are frequently directed for weak organizations by partial scheme finding abilities. Exploitation consist of making junk, decoding and cracking of passwords, performing spiteful ciphers to access rich statistics like inquiry documents, culture resources, and assessments.

4.1.2. Software Access

In the software access, numerous software and APIs are used through the cloud consumers in e-learning to access and achieve the cloud services. These APIs offer an essential measure throughout provisioning, organization, arrangement and observing of the methods consecutively in a cloud environment.

4.1.3. Malicious Insider

Malicious insider occupied in the suppliers or consumer sites may competent to run inside attacks. This insider can hack the personal statistics of cloud consumers in e-learning.

4.1.4. Data Loss

In active failures, defective statistics and unreliable practice of encryption explanations may lead to a data loss. Active failure has scanning, change or removal without any backup of the source e-learning satisfied.

4.1.5. Unified Risk

Unified risk cloud service independently these futures and functionality by the essential particulars like interior security technique, formation increment, repairing, auditing and sorting. E-learning consumers can take conscious and guiding statistics and connected files have stored [17].

4.2. Security Measures Issues

Security continues held an integral part of information technology so that it was one of the 10 key issues related to the latest technology. While E-learning changes to the cloud, security apprehensions almost the consistency of the unique privacy, integrity and availability will occur in figure 4. There are varieties of security measures to overcome security threats in cloud computing, through sellers. These security measures recycled to overcome security difficulties and to respond, the threats that about of these activities are as following [18]:

4.2.1. Software as a Service (SaaS) security

In the field of (SaaS), numerous securities measures have performed in which facility presentation model is constructed in the cloud. Before the acceptance by users of the service model or companies, they should be aware of the security of data and sell policies.

4.2.2. Observation and security awareness

The committee of security may construct with providing rules and regulation about the security policies of the association. The commission will obviously describe the roles and responsibilities of security purposes.

4.2.3. Education and Training

This includes the introduction or definition of security and provides training, mentoring, education for team members; it serves as the basis of their education certificate; which is use the privacy of statistics and information management.

4.2.4. Methods and Standards

The primary and the furthermost significant object that security group has reflected in the major security of statistics with requirements of a commercial. These measures should be delivered with suitable certification and associate certification might also be the best approaches [18]. [14].

V. PROPOSED MODEL FOR SECURING CLOUD-BASED E-LEARNING SYSTEMSCONCLUSION

Cloud computing can connect different geographical distribution of resources including computers, databases, storage devices, into a relatively transparent to the user's high-performance virtual computing environment. User can access to resources through education interface. They can also access to an existing resource management system for all teaching resources database services, and can get new teaching resource information from the repository as shown in Figure 5.

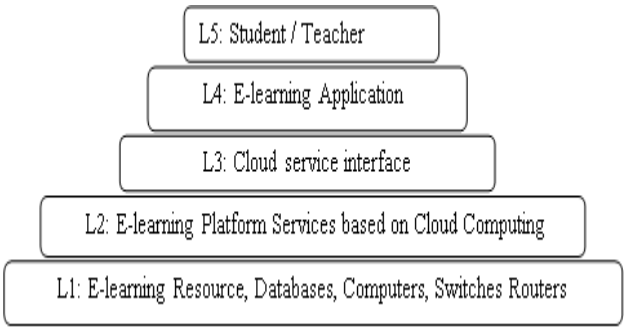

Fig5. E-Learning infrastructure based on cloud computing

The second layer (L2) has the E-learning cloud computing the platform service. It has attained services because this layer has transparent the students or the teachers. They do not need to know the facts of the layer. They do not need to know how the cloud services have implemented. For the layer which

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 1-9
Published Online November 2019 in IJEAST (http://www.ijeast.com)

services have implemented and how to provide services outside, these have released by the third layer (L3), i.e. called the cloud service interface. For students or teachers (L5), they need only enjoy the cloud services by the E-learning applications (L4).

A learning actor has involved entity in the learning process such as management, students, instructors and lab staff and so on. There have four types of resources that provisioned, and a learning actor can consume over the Internet [20].

1. Infrastructure resources: including computing power, storage, and machine provisioning.
2. Software resources: including middleware (cloud centric operating systems, application servers, databases) and development resources (development, testing tools, and deployment tools).
3. The application resources: the E-learning software applications have delivered by the SaaS model.
4. Learning processes: Applications have exposed to utilities or tasks. Learning process sharing is the learning driven application outsourcing, that supports provisioning reuse and composition.

5.1 The proposed E-learning model based on cloud computing

The proposed model contains physical hardware layer, virtualization layer, education middleware layer, application program interface layer, management system and security certification system as shown in Figure 6.

5.1.1. Physical hardware layer

It is a basic platform in the model, including servers, storage equipment's, and network equipment's.

5.1.2. Virtualization layer with the features

Dynamic configuration, distributed deployment, fee measurement realizes the five characteristics of cloud computing. The objective of virtualization layer has broken completely facts islands based on existing regional through the distributed technology and virtualization technology. This layer also consists of three parts: virtual servers, virtual storages, and virtual databases.

5.1.3. Education middleware layer- is the core layer, because it is the basic business platform. This layer is different from existing, and all information attached to it on different computing node counting ordinary file and database. So, all request systems on the middleware layer have

5.1.4. Application program interface layer- can promise model's scalability. Because of the variety of the current application system and an application system cannot content all the requirements of customers. In this layer also provide the necessary interface beside, and still need to be able to provide hosting service.

5.1.5. Management system- mainly watchers physical condition, virtualization software, hardware and software, open API. Management system can enhance the safety of the software platform.

5.1.6. Security system- includes identity authentication and authorization, single point login, virtualization soft- ware and hardware access control and audit, the education middleware and open API access control.

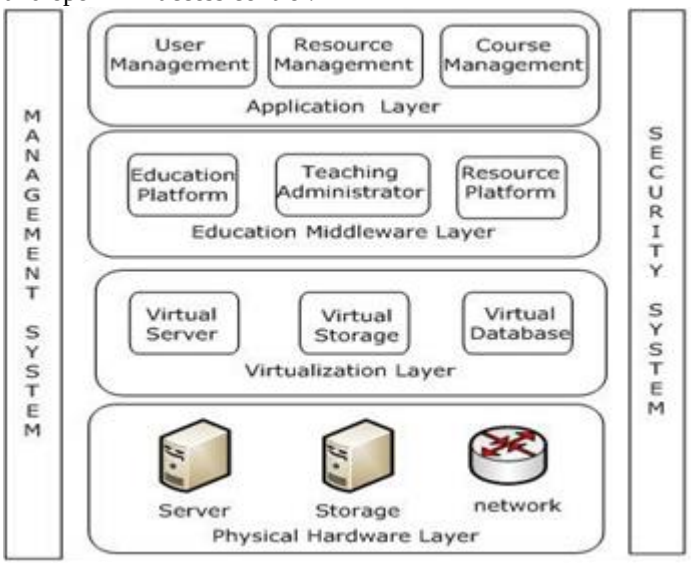

Fig6. The Proposed Secure Cloud E- learning Model

5.2. Security and privacy in the proposed model

Security and privacy problems have appeared in E-learning because of operation mechanism and policy mechanism. The failure of security technology creates personal privacy be spread, diffused, aggrieved and scouted without permission. Loopholes in the law have led the network manager's store, amend, exchange, and sell personal information without punishment. In this research study, we classify the privacy violation phenomenon of E-learning process during the information to be collected, used, saved, and deleted and so on. The primary concern in E-Learning is the security that can be summarized as following [18]:

5.2.1. User Authorization and Authentication

The elementary feature of E-Learning system is the reliable identification – recognition of the user as a genuine member of a user community because it is the basis for Access control to the E-learning system. Authentication verification of the user's has identity. Authorization permission has to access specific resources. The authorization has granted only to registered students and even their access has restricted to a certain subset of the E-learning material based on the billing if E-learning has offered on billing basis and on the level of learning of the registered student which will allow to him either to move to the next level or have a revision of the previous session.

5.2.2. Entry Points

There have many entry points in the E-learning system. A system has attacked only through its entry points. The designers can bound the security risks by decreasing the number of entry points, but the E-learning system cannot implement using this since there are a large number of multiple users from different geographic locations.

5.2.3. Dynamic Nature

The other challenge is the dynamic nature of these E-learning systems, where there are dynamic sessions where any process may join or leave the group sessions at any time. The security has concern with each particular member process, a strict session has to be maintained and the credentials are to be verified to control both at the session level and at the participant site.

5.2.4. Protection against Manipulation

One of the concerns of the E-learning has operation from the side of the students the system has protected beside manipulation. There have many possible solutions, where any manipulations can be protected by consuming the techniques of encryption, the digital signatures, the firewalls, etc.

5.2.5. Confidentiality

Confidentiality denotes to the assurance that facts and data are reserved secret and private and have not released to unauthorized persons, methods or devices. In an E-learning perspective, students want the assurance that their projects they submit online are reserved private and only released to the future examiner.

5.2.6. Integrity

Integrity is that authorized users have allowed modifying the contents which include creating, changing, appending and deleting data and metadata and the attacks on integrity have attempted to make actively adapt or finish data in the E-learning site without proper approval.

5.2.7. Availability

The E-learning material e-content data (or metadata) have made available to the learner at the specified session, when the user log on to the system for their session at the period of time, if the required material has not available the learner to lose interest and not grow the at most practice of the E-Learning system. There have two types of attacks via blocking attack and flooding attack, e.g.: Denial of Service, Node attacks, Line attacks, Network infrastructure attacks.

5.2.8. Non-Repudiation

Non-repudiation is the last step in proposed security model, where the learners have to be provided with E-learning services without any possible fraud such as when computer systems are broken in to or infected with Trojan horses or viruses, to deny the works or changes done by them in the system elimination of a refuted activity performed by a user.

VI. CONCLUSION AND FUTURE WORK

Security and privacy difficulties achieve in E-learning because of process device and policy mechanism. The failure of security technology makes personal privacy be spread, diffuse, and aggrieved. To overcome the security challenges in cloud-based E-learning, retailers and researchers have reserved possible alternatives in cloud services for all way of threats, to give more cloud-based customers who wish to use cloud-based E-learning. Security and confidentiality services in the cloud achieved and recognized through experienced collections that theoretically deliver capable security organization and threat assessment services. The main goal of this paper is to present a novel secure model for cloud-based E-learning systems that can help to improve quality of E-learning in the universities.

VII. REFERENCE

[1] Phankokkruad, M. " Implement of Cloud Computing For E-Learning System" , In: IEEE ICCIS (2012)

[2] Chandran, D., Kempegowda, S." Hybrid E-Learning Platform Based On Cloud Architecture Model: A Proposal", IEEE (2010)

[3] Dong, B., et al. "An E-learning Ecosystem Based on Cloud Computing Infrastructure", IEEE (2009)

[4] Carroll, M., Merwe, A., Kotzé, P. "Secure Cloud Computing Benefits, Risks and Controls", IEEE (2011)

[5] Hosam F. El-Sofany, Abdulelah Al Tayeb, Khalid Alghatani, and Samir A. El-Seoud, "The Impact of Cloud Computing Technologies in E-learning", International Journal of Emerging Technologies in Learning – iJET, Vol 8, Special Issue 1: ICL2012, Pages 37-43, http://dx.doi.org/:10.3991/ijet.v8iS1.2344, January 2013

[6] Sajjad Hashemi, Seyyed Yasser Hashemi. "Cloud Computing for E-Learning with More Emphasis on Security Issues". World Academy of Science, Engineering and Technology. International Journal of Computer and Systems Engineering, Vol:7, No:9, 2013

[7] Samir Abou El-Seoud, Hosam F. El-Sofany, Islam A. T. F. Taj-Eddin, Ann Nosseir, and & Mahmoud M.El-Khouly. "Implementation of Web-Based Education in Egypt through Cloud Computing Technologies and Its Effect on Higher Education". Higher Education Studies, ISSN 1925-4741; Vol. 3, doi:10.5539/hes.v3n3p62, No. 3; May 2013.

[8] Mohammed Al-Zoub "E-Learning on the Cloud", International Arab Journal of e-Technology, 2009.

[9] Faten Karim, Dr. Robert Goodwin. "Using Cloud Computing in E-Learning Systems", International Journal of Advanced Research in Computer Science & Technology, 2013

[10] Dinesha H A and Dr. V. k. Agrawal. "Advanced Technologies and Tools for Indian Rural School Education System", International Journal of Computer Applications, 2011.

[11] D.Kasi Viswanath, S. Kusuma & Saroj Kumar Gupta. "Cloud Computing Issues and Benefits Modern Education", Global Journal of Computer Science and Technology Cloud & distributed, 2012

[12] Divya. P, S. Prakasam. "Effectiveness of Cloud based E-Learning System (ECBELS)". International Journal of Computer Applications (0975 – 8887), Volume 119 – No.6, June 2015

[13] Masud, M.A.H., Huang, X.: An E-learning System Architecture based on Cloud Computing. IEEE (2012

[14] Jones, M.T.: Cloud computing and storage with OpenStack: Discover the benefits of using the open source OpenStack IaaS cloud platform. In: Developer Works (2012)

[15] G. Kumar, A. Chelikani, "Analysis of Security Issues in Cloud Based ELearning", Master's thesis, University of BORAS, Sweden, 2011

[16] Poonam R.Maskare et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 1281-1287

[17] Mell, P., Grance, T." The NIST Definition of Cloud Computing", NIST, Gaithersburg (2011)

[18] Gunasekar kumar and Anirudh chelikani,"Analysis of Security Issues in Cloud Based E-Learning", university of Boras 2011

[19] Divya. P, S. Prakasam," Effectiveness of Cloud based E-Learning System (ECBELS)" International Journal of Computer Applications (0975 – 8887) Volume 119 – No.6, June 2015.

[20] Hosam F. El-Sofany, Abdulelah Al Tayeb, Khalid Alghatani, and Samir A. El-Seoud, "The Impact of Cloud Computing Technologies in E-learning", International Journal of Emerging Technologies in Learning – iJET, Volume 8, Special Issue 1: ICL2012, Pages 37-43, http://dx.doi.org/:10.3991/ijet.v8iS1.2344, January 2013.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143