Analysis of (IaaS) Cloud Computing Security Issues Concerning Websites, Moodle eLMS as an Example

Dr.Azza Yousif Elmaghrabi
Capital Equipment-Virtual Training Center

Dr.Maria Altaib Badawi
Majmaah University

Summary

The aim of this study is to analyze (IaaS) cloud computing websites security, this was handled by providing a detailed analysis of websites security, focusing on the problems associated with the users loggings for Moodle eLMS as an example. In order to maintain a reasonable security level of Moodle website We designed and implement a suitable model containing procedural steps which should be followed when installing and using Moodle, and also selecting some security supporting plugin tools that should be integrated to it and moreover specifying the important instructions which should be followed by Moodle admins. The proposed model was implemented and examined in a real environment.

Key words:
IaaS Cloud computing (Infrastructure as a service), Moodle (Modular Object Oriented Dynamic Learning Environment), eLMS (Electronic Learning Management Systems), SEB (Safe exam browser).

1. Introduction

Getting use of cloud computing is growing rapidly in many sectors. Both public and private organizations use the cloud computing to provide better services, in educational institutions using Internet is associated with most of the academic and administrative activities .so cloud computing is the most suitable economic IT solution, especially in supporting e-learning systems (eLMS) websites. The security issues and problems facing the cloud computing service in educational institutions also increase In parallel with usage increment **[1].**

2. Theoretical Consideration

Cloud computing takes place in developing web-based technology, which provides various services for Information technology infrastructure and availability, flexibility, availability, scalability, efficiency, and reliability and also It reduces IT costs and increases capacity and service development potential.

Interacting with IT services by offering a strong base of virtualized services in both hardware and software platforms when delivering different on demand business models.

A. Cloud computing

Has been identified as a new paradigm in the field of computer networks services and has changed many sectors and it is defined [1] as a set of information technology services that are provided to a customer over a network on the leasing basis and with the ability to expand or reduce service requirements and usually a cloud computing services are provided by a third-party provider that owns the infrastructure. If the service providers did not do a good job of securing their own environments could be a problem. Measuring the quality of a cloud provider's security approach is difficult because many cloud service providers will not describe their infrastructure to customers.

Cloud computing is based on a technology called virtualization. Virtualization allows the creation of only a digital, simulated "virtual" computer that behaves as if it were a physical computer with its own devices. The technical term for such a computer is a virtual machine. Virtual machines are protected on the same host machine from one another, so they don't interact with each other at all. Files and applications from one virtual machine are not visible to other virtual machines even if they are on the same physical device. Virtual machines also make it more efficient to use the devices they host. By running many virtual machines simultaneously, one server becomes many servers, and a data center becomes a complete group of data centers, capable of serving many organizations. Thus, cloud computing service providers can offer to use their servers for a much larger number of clients simultaneously

If individual servers go down, then cloud computing servers should be online and should be always available. Cloud computing service providers maintain back up in multiple devices. Users access cloud services either through a browser or through an application, over the Internet through many interconnected networks.

B. Importance of cloud computing in Educational Institutions

Manuscript received November 5, 2020.
Manuscript revised November 20, 2020.
https://doi.org/10.22937/IJCSNS.2020.20.11.1

The most common uses of cloud computing in education are e-learning systems and various training program platforms on the internet. Cloud computing facilitates access to educational materials and educational activities accompanying the process and confidentiality in the use of assessments and surveys. It is also used in the management of student records, which facilitates access and handling of student data in particular institutions with different buildings and universities, which makes the academic process more efficient and reduces the cost of material expenses

Cloud computing stores information on a large group of servers around the world. This helps ensure quick access at any minute, and backup data. Large amounts of information could be send and saved to the system in order to assists in creation of reports and statistics for quality assurance regarding academic accreditation including presenting quality evidence.

C. Cloud computing services models

All cloud computing models allow users to run applications and store data over the Internet, and each model provides a different level of control and flexibility.

There are three main cloud service delivery models as shown in figure (1):

Infrastructure as a service (IaaS), Platform-as a service (PaaS) and Software as a service (SaaS).

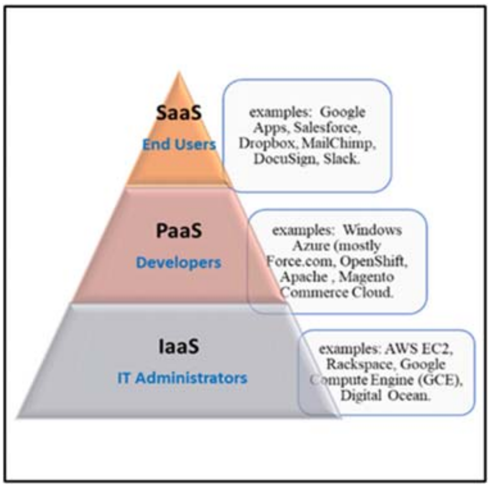

SaaS
End Users
examples: Google Apps, Salesforce, Dropbox, MailChimp, DocuSign, Slack.
PaaS
Developers
examples: Windows Azure (mostly Force.com, OpenShift, Apache , Magento Commerce Cloud.
IaaS
IT Administrators
examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean.

Fig.no(1) Saas vs Paas vs IaaS

SaaS (Software as a Service) allows users to run examples of online applications: Microsoft 365 Docs, Flickr, and Salesforce.

PaaS (Platform as a Service) allows users to create their own cloud application using resource-specific language tools and examples Windows Azure, Force.com, Google **App** Engine, and OpenShift.

IaaS (Infrastructure as a Service) allows users to use whatever applications they want on their cloud devices D.

Safety Considerations for IaaS

The security of any service running in the cloud depends on the security of the cloud infrastructure. Generally, devices cannot be protected against a compromised hypervisor. Hence, infrastructure Security vulnerabilities are an additional security concern that goes beyond those facing traditional servers. In general, the cloud service provider is supposed to maintain its infrastructure well and properly configured, thus reducing the risk of some exploitable vulnerabilities.

Insider threats: cloud service provider has access to hypervisors, provisioning systems, and authentication infrastructure. The risks of such threats can be reduced by reducing the number of virtualization drivers and other features that the hypervisor supports (reduce the attack surface), robust use of SE Linux in enforcement mode, and intrusion detection tools.

Broken authentication: cloud user interface, for example, installing an administrator keylogger on the desktop could represent part of a wider penetration of the internal network. It can save access to any API data, database credentials, or private keys used by the cloud service

Breaking the cipher :one way to access the cloud is to crack the encryption. Most of the cloud services and APIs are protected with the TLS protocol, which in turn relies on PKI for authentication. A typical way to crack a cipher is to crack the PKI.

IaaS cloud computing uses a set of resources such as servers and storage networks and other computer resources in the form of virtual systems, accessed through the Internet and users have the right to run any program with full control and management of the data and files of this program . As the control of computing, network and storage infrastructure are IaaS cloud providers' responsibility. They strive for securing their systems

Here are some of the security issues associated with IaaS.

Virtual simulation, Virtualization allows users to create, copy, share, and migrate, Virtual machine retrieval,

Offers new opportunities for attackers due to securing the additional layer, Virtual environments are vulnerable to all kinds, Normal infrastructural attacks, however security is the biggest challenge as virtual simulation adds more access points, Virtual Machine Monitor. Therefore, like any conventional program, it has security flaws.

Keeping the VMM simple and small as possible reduces
VM Public Image Repository

E. e-Learning

E-learning is one of the most advanced models that appeared in educational institutions, and it is one of the most important products that generated from the The integration of e-learning with information and communication technology in education.

E-learning is defined as a learning method that uses on multimedia and information and communication technologies to present educational content to learners in a way that allows them to interact with the content and with their participants.

F. Moodle eLMS

Moodle (Modular Object Oriented Dynamic Learning Environment), is an open source software under general Public License(GNU), everyone is allowed to download, install, use, modify and distribute Moodle packages for free, developed by Martin Dogiamas (2002).

Moodle offer online courses and also could support traditional education, thousands of educational institutions around the world uses Moodle. It supports dozens of languages.

Technically Moodle can easily work on any PHP computer for Unix, Linux and Windows operating systems. It can support many types of databases, specially Mysql, [2] Moodle. The system takes into account educational rules in its structure. It is based on an educational theory described in Moodle documents, it is constantly being updated by hundreds of developers around the world. The system can serve a university of more than 40,000 students.

Related studies: Related studies in (IaaS) Cloud Computing precisely considering eLMS are not widely available , here are some studies related to the current study:

Migration of Virtual Machine to improve the Security in Cloud Computing

This paper [2] contains, migrating a Virtual Machine to Improve security in cloud computing. Based on the survival analysis of VMs Discrete Time Chain Markov (DTMC) analysis, the algorithm was designed in order to generate a secure positioning arrangement that the guest VM can move Before the attack succeeds,

The researchers found that virtualization Device Migration is a useful tool for migrating OS instances, reduce power consumption, and facilitate system maintenance activities.

(VM) migration is a powerful management technology

It gives data center operators the ability to adapt the placement of virtual machines in order

To meet better performance targets, and to improve resource utilization, achieve fault tolerance, and finally VMs could make a big difference to conditions for security levels.

An analysis of security issues for cloud computing

This paper [3] analyzes the problems of cloud computing models .The security levels for IaaS, PaaS, and IaaS differences giving more concerns in cloud computing, storage, networking and virtualization which allow Multiple users share a single physical server from Big concerns for cloud users .The paper also discussed some of the surveys about security issues without making any difference between the weaknesses and threats in order and to be able to identify what the gaps and how to implement these threats and make more strong system design some solutions

Technical security and also redesigning traditional solutions that can work with cloud architectures.

Cloud computing and E-learning: Potential pitfalls and benefit Cloud computing

This paper [4] presents a new model of Cloud computing combined with E-Learning in schools and universities aiming to understand the model and its potential benefits and pitfalls. The proposed model is able to offer e-learning environment for schools and universities to share their computing resources with minimum cost.

Investigating Security Issues in Cloud Computing

This paper [5] discusses the different types of cloud computing technology. The researchers design a survey in order to examine the obstacles preventing organizations from adopting cloud computing focusing on security issues. They suggested a future work which should include development and testing of an e-learning tool using virtualization, web services and open source platforms to assess the feasibility of adopting cloud computing technology with minimal security fears. The proposed work should produce recommendations to organizations wishing to adopt cloud technology, and the effectiveness of the cloud computing in learning environment.

should be evaluated.

Critical Security Issues in Cloud Computing: A Survey

The paper in [11] focuses on a variety of security issues in cloud computing and accomplishes a survey that addresses three major security dimensions of cloud security, including computer security, network security, and information security. The researcher described the research results as a theoretical support, that can provide future work with evidences in the field of cloud security

Improved Cloud Computing Security

this paper [14] Algorithm has been designed and implemented to improve cloud security The by generating dynamic keys in cloud computing based on multiple techniques. These techniques have used the coding, permutations and reorder bit by the search method using artificial intelligence. depending on polynomial equations to expand the original key. The algorithm has the ability to manage clients, generating secret keys of varying length and damage the key after the using period and also a block cipher algorithm has been designed and implemented to protect the data that sent between clients.

3. Experimental Consideration

Since fast and reliable access to Moodle eLMS website is required from large number of users and this access could create potential security problems which would face the system managers related to the different user's roles Loggins. So the proposed work of this paper is to analyze and study the factors that could increase the level of data security in Moodle website as one of IaaS cloud computing applications. And then designing and implementing a practicing model as a proposed solution of theses security issues

Analysis

Like any web application Moodle has its own security requirements according to its structure and functionality. to analyze Moodle, we had to recognize its components, the environment and constituent elements which the system deals with are shown in figure (2) which represents the context diagram.

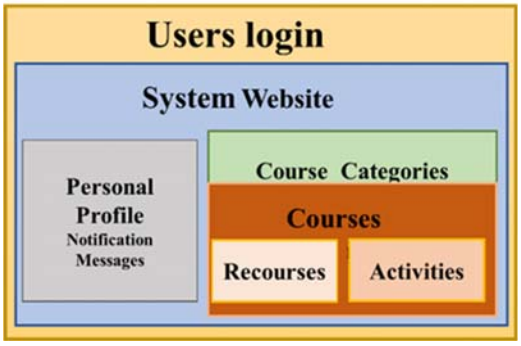


Fig.no (2) Moodle context diagram

Describing Moodle in terms of the relationships and the set of scenarios actions between the different users of the system (administrator, course Instructor and students) is shown in Figure (3), the system administrator creates the categories and courses, enroll course instructor and students in their required courses, the course instructor creates the course contents from sources and activities and the student reviews the course contents and study according to what is required of him.

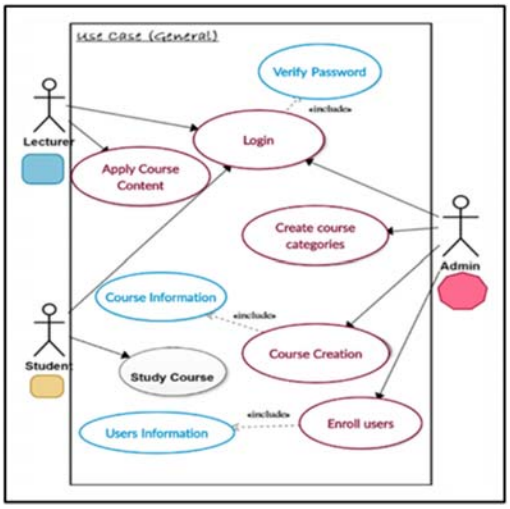


Fig.no (3) Moodle users relation ship

Moodle basic security dimensions

Because Moodle is an application that works on any type of network (local, intranet, or Internet). It is essential to provide security conditions and this is done by securing the basic elements that making up the system like any other web application systems :(the database, database server, operating system(OS) and Moodle system itself (Php)) each of these elements or components is supposed be checked, On the other hand, common types of Moodle eLMS security vulnerabilities could be summarized in the following points

-Unauthenticated access -Cross-site order fraud (XSRF)-Brute-forcing login -Cross-site scripting (XSS)-SQL Injection-Command line injection -Data loss -Configuration information leaked

-Insecure configuration management -Session fixation -Denial of service.

Framework Design

The proposed frame work for this research paper was designing, implementing and practicing a model consisting of three procedural steps, including different tools in order to maintain a suitable security level with retention ability of fast and reliable access to Moodle platform website. The model focuses on the security problems could face system managers which is associated with different user loggings.

We have created an experimental Moodle site in order examine the proposed model, the procedure and steps we followed to implement our frame work is shown in figure (4).

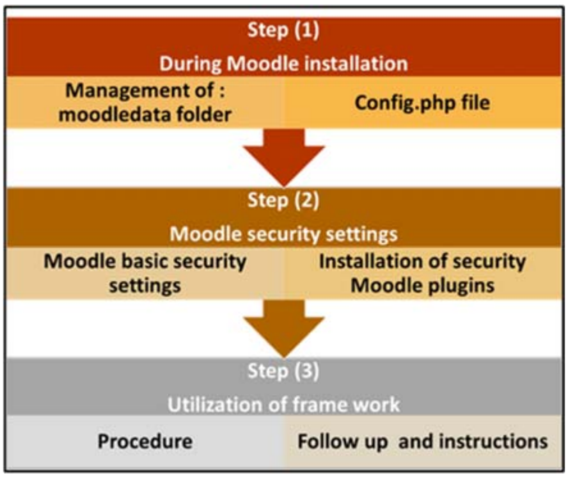

Step (1)
During Moodle installation
Management of : moodledata folder
Config.php file
Step (2)
Moodle security settings
Moodle basic security settings
Installation of security Moodle plugins
Step (3)
Utilization of frame work
Procedure
Follow up and instructions

Fig.no (4) Frame work design steps

Step (1): During Moodle installation

To examine the proposed model and procedures performance, we started our work by installing a copy of Moodle Software version 3.9 from Moodle website.

In order to prevent the access to the system settings in the config.php file (which is created during Moodle installation process). We made it read-only after the installation was completed, then all the basic settings for the site were done, then, an experimental course was added and modules were created inside the course . Users registered as instructor and student's roles

Step (2): Moodle security settings

(A) Basic security setting in Moodle

The settings for Moodle system security available against common types of vulnerabilities which is a responsibility of the system administrator only were done at the following manner, getting to it through the Site administration link, the security items to be set is shown in figure 5:

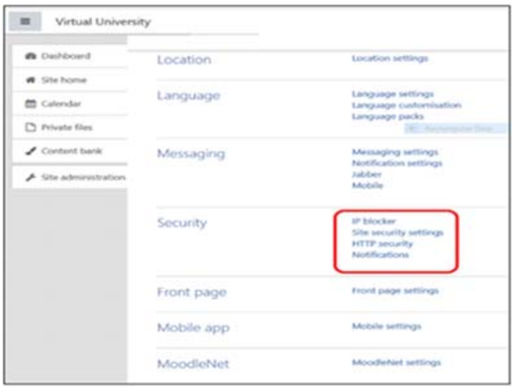


Fig. 5 Moodle security settings

1-The IP blocker shown in Fig (6)
Home ► Site administration ► Security ► IP blocker.

Fig. 6 IP blocker settings

2-Site Polices shown in Fig.7 is very important it allows control to essential security setting like passwords policy settings

Home ► Site administration ► Security ► Site polices

Fig. 7 Site Polices

3-HTPP Security as shown in Fig. (8)
Home ► Site administration ► Security ► HTTP Security

Fig. 8 HTTP Security

4-Notifications as shown in Fig.(9)
Home ► Site administration ► Security ► Notification

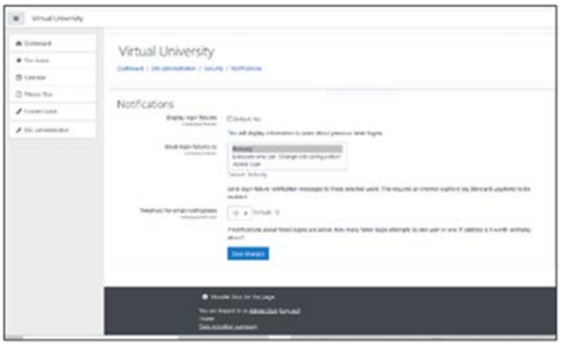


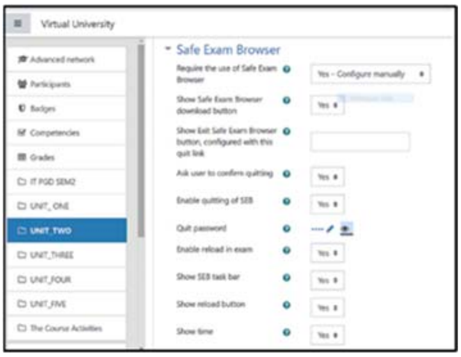
Fig. 9 Notification settings

(B) Integration of security tools and plugins

1-Safe exam browser SEB

SEB is a software that creates a web browser environment in order to carry out online exams safely it is specialized web browser that allow teachers to restrict students access to tools and resources while they are taking exam it changes any computer into a secure workstation.

Fortunately, the SEB could be activated in Moodle 3.9 quiz setting as shown in Fig. (10)



Safe Exam Browser

Require the use of Safe Exam Browser: Yes – Configure manually

Show Safe Exam Browser download button: Yes

Show Exit Safe Exam Browser button, configured with this quit link:

Ask user to confirm quitting: Yes

Enable quitting of SEB: Yes

Quit password: ••••

Enable reload in exam: Yes

Show SEB task bar: Yes

Show reload button: Yes

Show time: Yes

Fig.no 10Enabling SEB in quiz setting

but before activating SEB in Moodle, EBS Software should be downloaded installed in the computer lab used to for the exam. We have to follow the process of configuring the EBS as shown in figures (11)

Fig.no 11 SEB configuration page

Figure (12) shows the screen that will appear to the student when opening the quiz link

Fig. (12) Logging quiz

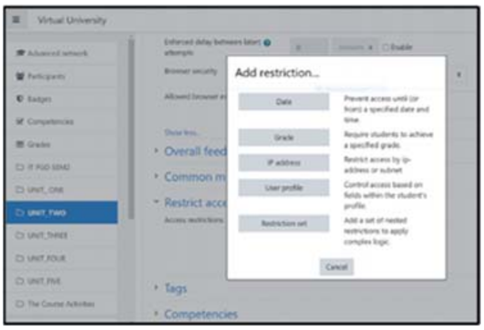
The quiz will appear in full screen nothing else could be displayed by the student during taking the exam

As shown in figure (13) ,the student could exit the ESB screen after submitting the quiz with password or as the configuration SEB settings done by the administrator

Fig.(13) Quiz page as it appears in the screen

2-Availability IP address plugin

Restrict access to any activity by IP-address. This plugin can be used to make any chosen activity unavailable based on the user's IP. The plugin when installed gives addition restriction in the restriction settings for assignment as shown in figure 14.



Add restriction...

Date	Prevent access until (or from) a specified date and time.
Grade	Require students to achieve a specified grade.
IP address	Restrict access by ip-address or subnet
User profile	Control access based on fields within the student's profile.
Restriction set	Add a set of nested restrictions to apply complex logic.

Fig.(14) Assignment restriction settings

3-Anti-hammering - Login blocker plugin

When installing this Anti Hammering plugin, smart detection program works to prevent the possibility of penetrating your system administrator registration system login. The program tracks IP address and the entered username and. It stores its information to block the users and / or their IP address. The program creates breakthrough report and login report

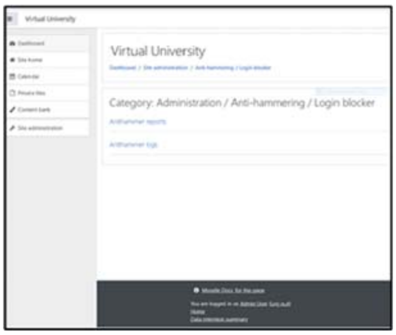

Virtual University
Dashboard
Site home
Calendar
Private files
Content bank
Site administration
Virtual University
Dashboard / Site administration / Anti-hammering / Login blocker
Category: Administration / Anti-hammering / Login blocker
Antihammer reports
Antihammer logs
Moodle Docs for this page

Fig.(15) Login blocker plugin setting

Step (3) Utilization of the framework

1-Procedure

We have created an experimental course in Moodle, and then enrolling sample of users (Instructor & students), for the purpose of testing the security settings and plugins created we had done in the system. we registered Moodle site in moodle.org to be aware about information concerning the Moodle site vulnerable, and also in order to keep tracking of the latest developments news and getting security alerts and new releases notifications received by your registered email. In general, when setting up Moodle system we should find a reasonable balance between users supposed allowed features needs and the system security.

2-Follow up and instructions

Since smart handling and good management of passwords necessary for all system users, (system administrators, course instructors, and students) we specified some guiding instructions and remarks and we provided this to the system administrator including the important points that should be taken into account, to enhance the security level.

In the aspect of passwords handling, we have announced the following points:

- It is important to make sure to change your password from a computer you wouldn't normally use like a work computer
-When changing the account password, reuse of the password should be avoided
-Avoiding the using the same password for multiple accounts
-Do not save password in devices
-The admin is requested to change passwords periodically
-Users should be Requested to change initial passwords or "default initial" passwords
-Force strong passwords and also continue changing their passwords periodically avoiding sharing passwords with others

4.Conclusion

As the advantages of using IaaS cloud computing is accompanied with its security challenges In this study the main security considerations and challenges that currently facing websites cloud computing were highlighted and discussed. The researches have been trying to conduct a suitable model which could become a manual guide for system admins when installing and using Moodle eLMS in order to enhance security level regarding users loggings.

Security threats in IaaS cloud computing generally could be divided into to the following categories (threats based on the Internet, application-based threats and threats from users).

The work done throughout this study was analyzing the factors that could enhance the security level of Moodle website as one of IaaS cloud computing applications, and that was done by designing and implementing a practicing proposed model consisting of three procedural steps, including different tools in order to maintain a suitable security level.

References

[1] S.O. Kuyoro & Others , " Evaluating Moodle As An Open Source Cloud Computing Security Issues and Challenges" . International Journal of Computer Networks, Volume (3) : Issue (5). India, 2011.

[2] N.Chandrakala , & T.Rao, " Migration of Virtual Machine to improve the Security in Cloud Computing" . International Journal of Electrical and Computer Engineering, Vol. 8, ISSN: 2088-8708, 2018, India.

[3] K. Hashizume & others ," An analysis of security issues for cloud computing " . Journal of Internet Services and Applications, ISSN No. 4-5, 2013, U.S.A.

[4] M.Watfa ," Cloud computing and E-learning: Potential pitfalls and benefits "Sixth International Conference on Innovative Computing Technology, DOI: 140-144,(2016) ,Ireland.

[5] T.Moyo & J. B. Bhogal ," Investigating Security Issues in Cloud Computing "International Conference on Complex, Intelligent and Software Intensive Systems, DOI: 141-146 / CISIS,2014 U.K.

[6] D.G.Chandra & D.B.Malaya, "Role of Cloud Computing in Education", International Conference on Computing, Electronics and Electrical Technologies, DOI: 10.1109/ICCEET, 2012 U.S.A.

[7] H.M. Juan , " Moodle Security Vulnerabilities "2008 5th International Conference on Electrical Engineering, Computing Science and Automatic Control, 2008.

[8] C.Schultz ," Information Security Trends and Issues in the Moodle E-Learning Platform: An Ethnographic Content Analysis" Journal of Information Systems Education, Vol. 23(4) Winter, 2012.

[9] R.Gil& others , " Biometric Verification System in Moodle & their Analysis in Lab Exams " IEEE International Conference on Computer as a Tool, vol. 9, pp. 133-145, New Jersey, United States, 2011.

[10] R.A.Azaiza , " Detection and Prevention of XSS Vulnerabilities in Moodle" International Journal of Computing and Digital Systems ISSN (2210-142X) Int. J. Com. Dig. Sys. 5, No.5,2016.

[11] X.Sun , " Critical Security Issues in Cloud Computing: A Survey IEEE International Conference on High Performance and Smart Computing,, BDS-HPSC-IDS/ 216-221, United States,2018.

[12] G.Kumar & A.Chelikani, "Analysis of security issues in cloud based elearning" Master’s (one year) thesis in Informatics, No 2011MAGI23 University of Boras, Inc, Sweden.2019.

[13] IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011 ISSN (Online): www.IJCSI.org http://ijcsi.org/papers/IJCSI-8-4-2-509-516.pdf [Accessed on: 02-01-2018].

[14] R.T.Hameed & others," Improved Cloud Computing Security "1st Annual International Conference on Information and Sciences, AICIS /170-175. Iraq,2018.

[15] Z. Muhsen & others, “Moodle and e-learning Tools“. Modern Education and Computer Science, Vol. 5, No. 6. Hong Kong,2013.