WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Evaluation of Security Challenges and Proposed Solution in a Cloud Based E-Learning

Sanusi Muhammad[1], Abubakar Sadik Mustapha[2]

[1]*Department of Computer Science University of Abuja, Nigeria*
[2]*Department of Computer Science University of Abuja, Nigeria*
DOI: https://doi.org/10.55248/gengpi.4.423.30598

A B S T R A C T

Cloud based E-Learning is one of the booming technologies in IT field which brings powerful e-learning products with the help of cloud power. Cloud technology has numerous advantages over the existing traditional E-Learning systems but at the same time, security is a major concern in cloud based e-learning. So security measures are unavoidable to prevent the loss of users' valuable data from the security vulnerabilities. Cloud based e-learning products also need to satisfy the security needs of customers and overcome various security threats which attack valuable data stored in cloud servers. This research study several number of Challenges as follows **(1) Cloud Computing Security Threats** which comprises i- Availability ii- Data Lock-in iii- Insecure of incomplete data deletion iv- Increase authentication demand v- Browser security **(2) E-learning Security Threats** which include i- User authorization and authentication ii. Protection against manipulation iii. Non-repudiation (**3) Social aspects of security** which include i-Confidentiality ii- integrity iii. Availability.

In view of these, number of solutions are proposed, these solutions include (1**) Security measures in cloud computing** including i. Software as a service (SAaS) Security ii. Security Management with users iii- Security governance iv-. Risk management v. Risk assessment vi. Security awareness vii. Education and training Viii. policies and standards ix. Third party risk management x. Vulnerability assessment Xii. Data Security Xii. Data governance Xiii. Application Security Xiv. Virtual machine security Xv. Identity access management Xvi. Physical security Xvii. Disaster Recovery Xviii. Data privacy (**2) Security measures taken on E-learning include** I. SMS Security Mechanism ii. Biometric Mechanism iii. Security Token IV. ACl Mechanism v. Digital Signatures VI Security from passive attacks

Keywords: Security, Challenges, Cloud, Evaluation

1. INTRODUCTION

Numerous new technologies are being released daily in this modern period, making life easier for people. Particularly web-based technologies have made significant contributions to the reduction of routine labour for humans. Many institutions and colleges are also introducing new courses to educate individuals about these technologies and prepare them for effective use. Institutions, however, are struggling to find qualified instructors to give those technical courses to their pupils. Many schools now offer online education services for the taught courses to address this issue. Therefore, one of the best and most crucial pieces of technology that helps them establish a positive learning environment is e-learning.

In order to raise their educational standards, several countries, particularly developing nations like India, are embracing E-Learning software solutions. However, there are still a number of issues with the infrastructure and facilities needed to apply the traditional E-Learning approach at a variety of educational institutions around the nation. As a result, the traditional E-Learning approach has been replaced by the cloud computing technology as the best way to address the issues.

In addition, regardless of whether a technology is an electronic device or a web technology, people are focusing more on its security aspects as it enters the market. Due to the numerous vulnerabilities in web sources, society is now aware of the security elements of technology. When using cloud power to expand the functionality of an existing traditional e-learning technology, cloud-based e-learning technology is in no way immune to security flaws on the internet. E-Learning technology has already overcome several issues to achieve the current standard because it is not a new innovation in the technical world. As a result, it adheres to a number of security standards to ensure the server's e-learning solutions and end users' data are secure. Similar to cloud computing technologies, security standards are in place to ensure that investors and end users are protected from web vulnerabilities. Still, it has to be seen whether cloud computing can complement and improve security for e-learning technology or if it would exacerbate security issues with the current security features of traditional e-learning technology. This thesis identifies the main security issues that stand in the way of using cloud-based E-Learning technology and describes their severity as well as potential solutions.

2. CLOUD BASED SECURITY E-LEARNING CHALLENGES

Cloud computing employs three service delivery models as listed below through which different types of services are delivered to the end user. Each service model has different levels of security requirement in the cloud environment, as described in 2.1-2.3.

2.1 Security Issues in SaaS (Software as a Service)

A- Data Security: Data plays vital role in the cloud services, because many of cloud service providers store customers' data on large data centres.

B- Network Security: Enterprises store sensitive data in the cloud server and SaaS vendor can manipulate it. To protect data from leakage of sensitive information, apply tough network traffic encryption techniques to manage data flow over the network.

C- Data Integrity: Data integrity defines the correctness, accessibility, high quality, and reliability of stored data. Cloud provides integrity of data storages for customer privacy. In order to defeat the risks of data integrity, get assistance of Third Party Auditor (TPA).

D- Data Segregation: Data is residing in the cloud in a shared environment; there multiple tenants are sharing single location, so one customer's data is stored along with another customer's data, which effects difficulty in data segregation.

E- Data Breaches: Ever since data from a different users and business concerns exist collectively in a cloud environment, break the data laws of cloud environment will certainly attack and damage the data of all the users.

2.2 Security Issues in PaaS (Platform as a Service)

A- **Data Location**: PaaS vendors provide 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.

B- **Privileged Access:** The cloud provider has full rights to access data (including other users of the cloud and other third party suppliers), once data is stored in the cloud environment. There is no confidentiality of data in this cloud environment**.**

2.3 Security Issues in IaaS (Infrastructure as Service)

A- **Web Service Attack**: Web service protocols are used by cloud users for getting service. SOAP is the most suspended protocol in web services; many SOAP-based security solutions are researched, developed, and implemented.

B- **SLA (Service Level Agreement) attack**: When customers have transferred their core business functions onto their committed cloud environment, they should be ensured the quality, availability, reliability, and performance of these resources, because cloud users do not have control over these computing resources

C- **Distributed Denial of Service (DDoS) attack**: is advanced version of denial of service in terms of denying the important services by giving large number of request, which is not handled by target server. In DDoS, the attack is communicated with different dynamic networks which have already been compromised unlike the DoS attack.

D- **MITM (**Man In The Middle) **Attack**: MITM attack is encountering when an attacker directs himself between two legitimate users. This attack is also a class of eavesdropping

E- **DNS (Domain Name Service)Attack**: IaaS Cloud environment deals with risky attack vector known as DNS Attack, which translates the domain name to an IP address.

Figure **1** shows the components affecting the relevant security issues in SaaS, PaaS and IaaS.

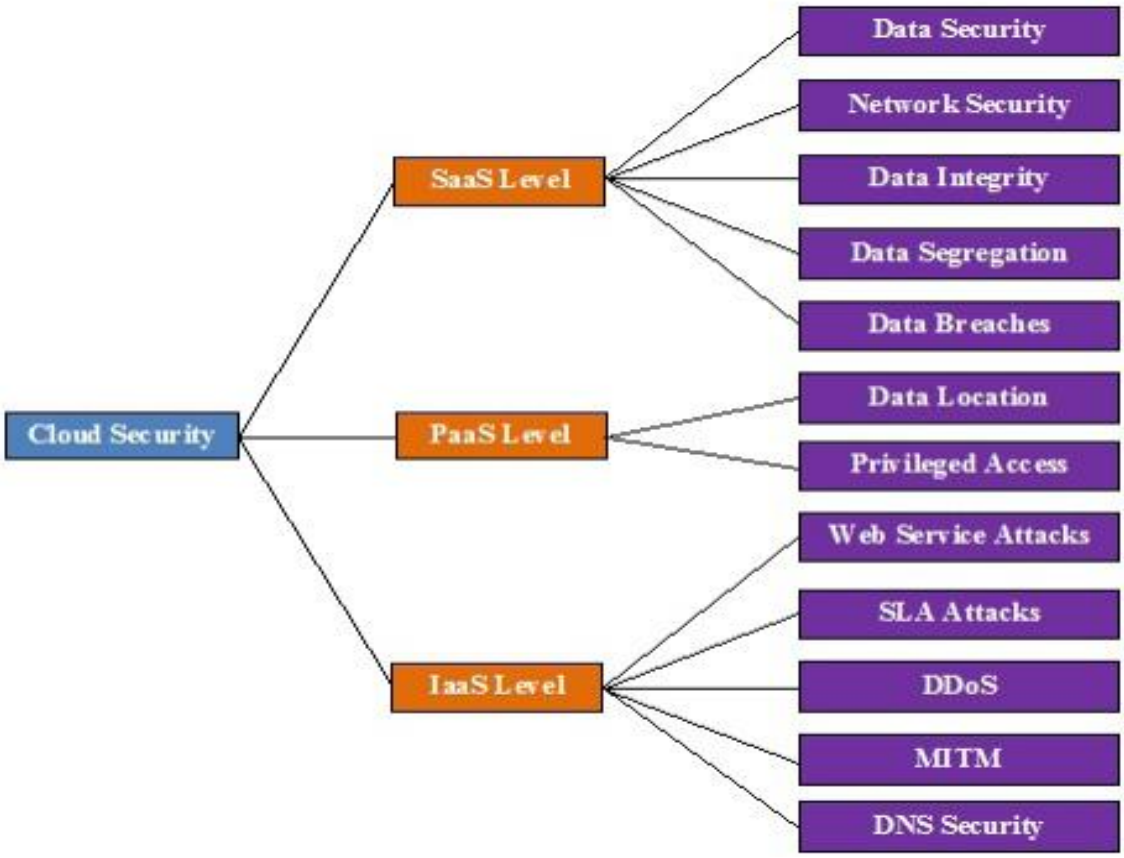

Figure 1: Security Challenges in Cloud based E-Learning

3. PROPOSED SOLUTIONS TO THE CHALLANGES

A- **Hacker:** Hacker denotes who observe defects in a computer or computer network to gain authorized/unauthorized access. There are some reasons to do hacking such as profit, protestation, or challenge. Different classifications of hackers are White Hat, Black Hat, Grey Hat, Elite Hacker, Script Kiddi, Neophyte, Blue Hat, etc

B- **E-Learning**: E-learning is electronic learning, and typically this means using a computer to deliver part, or all of a course whether it is in a school, part of your mandatory business training or a full distance learning course.

C- **Flooding Attack:** In a cloud system all the servers approach is service oriented. If server overloaded or reaches the maximum load, it shares some of its job to a nearby computational server. This distribution approach produces the cloud more proficient and quicker executing.

D- **Backdoor Channel**: Attack Backdoor channel attack is a passive attack, which avoids the traditional authentication methods to gain access in order to compromise legitimate users secrecy. An intruder takes control of target systems resources and possible to attempt DDoS attack, when backdoor channel attack is occurred. It can also be used to reveal confidential data of target user.

E- **VM Attack**: Virtualization is one of the key technologies for the infrastructure as a service cloud. It is very difficult task for the cloud service provider to secure their customer virtual machines. In a typical cloud services platform, the resources provided to the user are to virtual and rented.

F- **Insider Attacks**: Insiders' attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies / procedures.

G- **3rd Party Provider**: Cloud Third party service providers are responsible for secure service transaction, because cloud vendors outsource some of the services. Before adopting a cloud service, we should be aware of third party cloud provider's role and responsibilities that are clearly addressed in the contract.

H- **Security Layer:** Security layer is a standard security technology designed to establish an encrypted link between a server and a client. It allows confidential information like credit card numbers, social security numbers, and login passwords to be transferred securely.

Figure 2 shows the proposed architecture placement for users, hosts and the security layers.

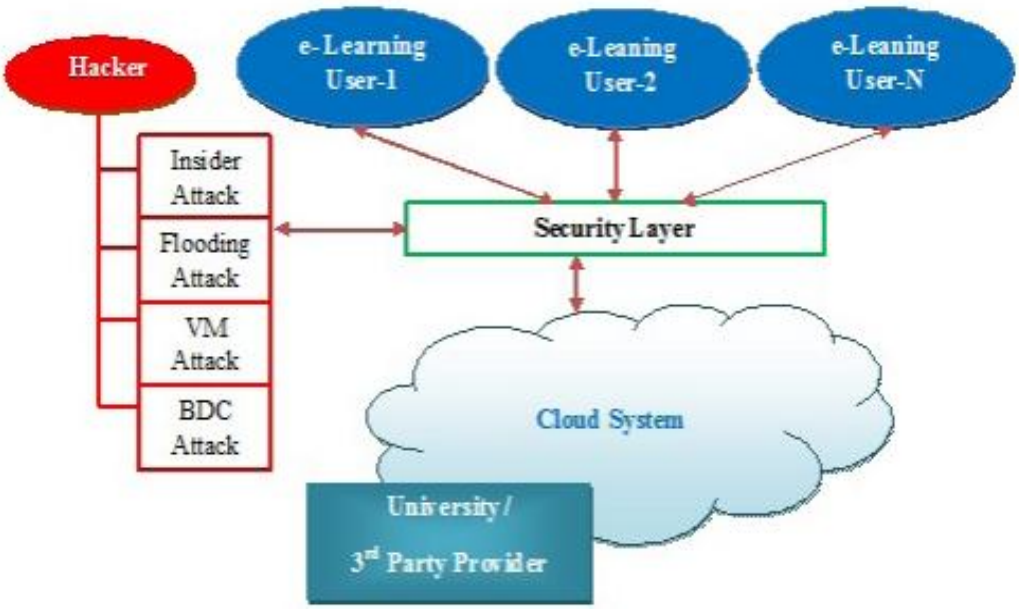

Figure 2 : CLOUD BASED MODEL TO SECURE CLOUD BASED ELEARNING ENVIRONMENT

4. CONCLUSION

Data availability issue is the major hindrance in accessing cloud data for E-Learners. Among all the distributed environmental attacks, Distributed Denial of service (DDoS) attack is the root attack for data unavailability. Literature study clearly reveals the risks in cloud based e-learning along its service delivery models and concluded solutions for each attack in an efficient manner. The proposed approach and considered architecture and layering structure including SaaS, PaaS and IaaS security solutions in this research are valuable to manage current and future cloud based E-learning platforms against attack.

References

Arunachalam AR. Bringing out the effective learning process by analysing of e-learning methodologies. Indian Journal of Science and Technology. 2014Jun; 7(S5):41–3.

Begum SH, Sheeba T, Rani SNN. Security in cloud based e-learning. Int J AdvRes Computer Science Software Eng. 2013; 3(1).

Chaudhary V. Software as a service: implications for investment in software development. International conference on system sciences; 2007.p. 209.

Cooper R. Verizon business data breach security blog. 2008. Available from: http://www.securityblog. Verizon business. com/2008/06/10/2008-data breach-investigations-report/s [accessed on: 11 February 2010].

Firdhous M, Ghazali O, Hassan S. Trust and trust management in cloud computing – a survey. Inter Networks Research Group. University Utara Malaysia; 2011. Technical Report UUM/ CAS/ Internetworks/TR2011-01.

Gharehchopogh FS, Hashemi S. Security challenges in cloud computing with more emphasis on trust and privacy. International Journal of Scientific and Technology Research. 2012; 1(6):49–54

Golden B. Defining private clouds. 2009. Available from: http://www.cio.com/article/492695/Defining private clouds part ones [accessed on:

Hurwitz J, Bloor R, Kaufman M, Halper F. Cloud computing for dummies. Wiley; 2012.

Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. IEEE; 2009.

Masud MAH, Huang X. An e-learning system architecture based on cloud computing. World Academy of Science, Engineering and Technology. 2012; Available from; http://www.waset.org/journals/waset/v62-15.pdf

PCI DSS.Requirements and security assessment procedures. 2009. Available from: https://www.pcisecuritystandards.

Piplode R, Singh UK. An overview and study of security issues and challenges in cloud computing. Int J Adv Res ComputSci Software Eng. 2012 Sep; 2(9).

Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–401.

Sugaraj Samuel R, Subhashini A. E-Learning, the next big name in education. Indian Journal of Science and Technology. 2011 Mar; 4(3):173–6.

Takabi H, Joshi JBD, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security Privacy Magazine.IEEE Computer Society.2010; 8:24–31.