Managing Shared Technology Vulnerabilities: Effective Approach to Building Trust in Cloud-Based E-Learning System

Uchechukwu P. Emejeamara[1], Udochukwu J. Nwoduh[2], Catherine C. Asamonye PhD[3]
[1]IEEE Computer Society, Connecticut Section, USA
[2]Lecturer, Dept. Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria
[3]Lecturer, Dept. Educational Foundations/Administrations, Alvan Ikoku Federal College of Education, Nigeria

Abstract- **E-learning is a significant technological advancement that can help educational institutions foster a better learning environment for students as well as improved efficiency of education. For easier access in E-Learning, cloud computing is adopted which is comprised of a variety of computing resources from server and storage to other applications. However, the use of cloud computing is limited by security concerns brought by its multitenant nature, as well as the cloud service provider having remote control of its security and license issues. This research paper finds cloud encryption and key management crucial for addressing these shared technology vulnerabilities. The inherent trust issues associated with cloud-based e-learning system can be effectively resolved by choosing a reliable cloud service provider as well as adapting methods that can increase the security of the cloud such as providing Hardware Security Module service, external key generation for encryption use, and proper organization of files in the cloud.**

Index terms- **E-learning, cloud computing, cloud encryption, Cloud service provider, Hardware Security Module, key generation**

I. INTRODUCTION

E-Learning is a vital technological advancement that can help educational institutions foster a good learning environment and improve the efficiency of education through the help of the internet. E-Learning platforms can also be used to decongest student's population in a traditional school environment and minimize also the problems associated with an overpopulation of students while offering reduced cost since the physical environment is not required [10]. Besides, learning materials are easier to keep track and update and can be incorporated as well to various multimedia content to foster a friendly way of learning.

In the traditional E-Learning system which uses web-based learning mode, system construction, and maintenance are found inside the educational institution resulting in various problems including significant investment needed but without an increase in capital gains which leads to a lack of development potential [1]. Hence, cloud computing has been utilized in E-learning models considering its scale efficient mechanism. In cloud-based E-learning, the construction of an E-learning system is entrusted to cloud computing services or suppliers. The cloud-based system also creates a new generation of an E-learning system that can operate on a wide range of devices while keeping the data inside the cloud [1]. However, security is a major concern in cloud-based systems. Trust between provider and the users is vital in the cloud service and application.

In this paper, key security issues in cloud computing for E-Learning systems will be identified as well as solutions to these security issues to build trust in cloud computing for use in E-Learning systems.

II. E-LEARNING TECHNOLOGIES

A. Background

E-Learning has various technologies which include [10]:

1 Generic software application: This includes word-processing, databases, spreadsheets and tools for statistical and qualitative analysis used

by students to develop ideas and present their findings.

2 Presentation technologies: Example of which are Microsoft PowerPoint, digital projectors and interactive whiteboards used by students for data, report, and results presentation.

3 World Wide Web or Web: It provides access to various digital resources such as online libraries, journals, databases, and datasets. It can also be used for other types of learning such as resource, inquiry, and problem-based learning.

4 Computer Mediated Conferencing (CMC): It supports various types of discursive or collaborative activities. Examples of CMC applications include e-mail, discussion boards, bulletin boards, and chat tools.

5 Multimedia Materials: Supports the various learning styles of students and include graphics, pictures, animations, film, video, and audio.

6 Computer Assisted Assessment (CAA): It is an automated, online objective testing that can provide immediate and individual feedback to students.

7 Computer Assisted Learning (CAL) or Computer-Based Learning (CBL): Refers to any use of computers to foster learning and involves the use of online tutorials combining text, animations, sound, and video. and quizzes that are in a structured framework that can help students to develop their knowledge and topic understanding.

8 Audio/Videoconferencing: Includes the use of audio and/or visual communication through the web or mobile applications, or phone. Example of applications includes Microsoft Teams/Microsoft NetMeeting, Zoom, etc., which allow simultaneous conference, editing of documents and communication through chat or video/audio lines of the application.

III. CLOUD COMPUTING

A. Background

The Cloud computing term is derived from the way the internet is depicted in network diagrams. It is defined by a feature given by computation resources a computer network [8]. In traditional computing, the software and data needed to perform the computational operations are on the user's computer. On the other hand, in cloud computing, the needed software and data needed for computation operation are in the cloud system, and the user only needs a minimal operating system with a browser and stable internet connection to access the files and applications.

Cloud computing architecture consists of three layers namely; IAAS, PAAS, and SAAS which is significant to serve a variety of services to customers from the cloud suppliers [5].

1 IAAS (Infrastructure as a service): Offered by cloud suppliers which include hardware, storage, servers, and networking components. The cloud customers can extend this service from their cloud vendors to resize the services depending on the user's needs. The IAAS framework can also be offered through virtualization such as full and paravirtualization. Full virtualization pertains to one system or installed software from one machine which can operate another entire virtual system through its own emulation. Meanwhile, paravirtualization is a kind of extension from full virtualizations differing only from its ability to run various operating systems at the same time.

2 SAAS (Software as a service): Software is offered to customers through the cloud at a minimal cost. Hence, cloud users can save money from not getting licenses to use several software applications.

3 PAAS (Platform as a service): offers the environment for building, testing and delivering software applications or any other services through the cloud without the need to download and install applications in the machine of the cloud user.

Cloud computing offers a variety of computing resources from server and storage to other applications such as email, security, backup, and voice sent through the internet [1].

B. Types of Cloud

There are four different types of cloud in cloud computing depending on the modes of deployment of computing [8].

1 Public Cloud: In this type of cloud, third-party vendors provide the IAAS, SAAS and PAAS.

The users can have access to the services on an ad-hoc basis through the cloud.

2 Hybrid Cloud: It has in-house and third-party providers. Some portion of the cloud is private that can only be accessed internally while the remaining portion can be accessed externally.

3 Private Cloud: Pertains to an internal cloud that maintains and owns services such as PAAS, SAAS, and IAAS but can still be accessed by other cloud users through a private network.

4 Community Cloud: An external private cloud shared by various companies with the same requirements. Third-party cloud suppliers offer this cloud, but the cloud can also be accessed by the companies that operate in the community.

IV. APPLICATION OF CLOUD COMPUTING ON E-LEARNING

The cloud can be utilized by the E-learning system considering its ability to be utilized by many users, with many resources available and supported by the cloud [1]. The application of cloud in E-Learning can be seen through online classrooms and online training modules of companies where students/attendees can access the tools from any computer, regardless of platform, provided the computer can connect to the cloud. The educational materials are virtualized in the cloud servers that are made available to students in the form of a rent base from cloud vendors [8].

Cloud-based E-learning architecture can be visualized in Fig. 1.

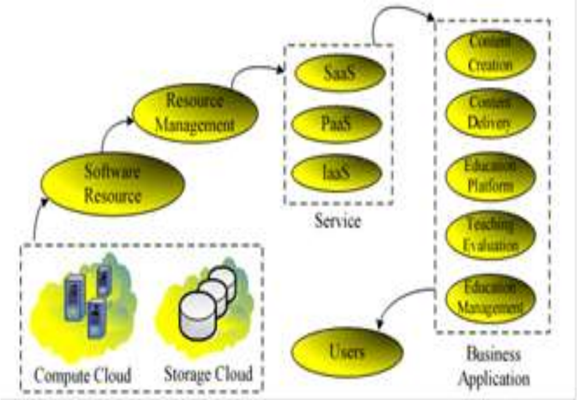

Fig.1.The Architecture of Cloud-based E-learning [8]

There are five layers in cloud-based e-learning which include the following [8]:

1 Hardware resource layer: It handles the important computing things such as physical memory and CPU which is the most vital for the total infrastructure of the system. Physical servers, network, and storage are grouped and called as upper software platform through the help of virtualization. Physical host pool is expanded dynamically as well as the memory is scalable at any time to ensure uninterruptible power to the cloud middleware services for the cloud-based E-Learning system.

2 Software resource layer: It is formed through the help of operating systems and middleware. Software solutions combine to form grouped interface for software developers through the help of middleware technology. Through this layer, software developers can create various applications for the e-learning system and embed them in the cloud. This enables cloud users to compute the applications through the cloud.

3 Resource management layer: It plays a significant role in coupling software and hardware resources. It brings uninterrupted on-demand software distribution for various hardware resources through the help of virtualization and cloud computing idea scheduling.

4 Service layer: Further divided into three levels that are previously discussed: IAAS, SAAS and PAAS. This enables cloud customers to use different forms of cloud resources for their products such as software resource, hardware resource and infrastructure resource.

5 Business application layer: This layer acts important business logic of E-leaning system and formulates the development of the cloud components for E-learning. It is comprised of content creation, content delivery, education platform, teaching evaluation and education management.

V. CLOUD SECURITY ISSUES

Despite various advantages of cloud computing utilization, challenges in security urgently calls for a solution to enable efficient and full-scale utilization [2]. Aside from security issues, other significant barriers to adoption of cloud-based E-learning are privacy, compliance and legal matters [6]. Security concerns on the utilization of cloud computing include the risks in the following areas: external data storage, lack of control, multiple users and integration with internal security, and dependency on the public internet.

The cloud contains various features such as its large scale and heterogeneous, distributed and totally virtualized resources owned by the cloud providers which may not be fully secured by traditional security mechanisms such as identity, authentication, and authorization. Security controls in cloud computing are almost the same as the security controls in any IT environment, however, the operational models and technologies used to enable cloud services poses various risks compared to traditional IT solutions [6]. Cloud computing requires the third party remote control and supports as well multi-tenant which may result in ambiguous situations by users that lower the trust level to the cloud and increases the risk of other parties to see or share the user's data [7]. Hence, choosing a reliable cloud service provider (CSP) is also a significant factor in convincing users to adopt cloud-based learning. The CSP should also ensure that users will continue to have the same level of security and privacy controls over their services and applications and provide proofs that their organization is secure can meet service level agreements and prove compliance to auditors.

Security issues and main vulnerabilities of cloud computing can be categorized into three as elaborated below:

A. SAAS security issues

This refers to reduced control of SAAS users over security among the three fundamental delivery models in the cloud.

1 Application security: Include flaws in the web applications that can create vulnerabilities to the SAAS applications. This also includes attacks on the web that compromises the security of user's computers as well as enabling the malicious activities of attackers such as stealing of sensitive/confidential data.

2 Multi-tenancy: Refers to the high risk of data leakage between multiple users considering data from multiple users is stored in the same database.

3 Data security: Depends on the service provider since they are the one responsible for data security while it is being processed and stored. Security risk may escalate when cloud providers subcontract other services such as backup from third party service providers. It also includes compliance issues considering data is located in the cloud provider's data centers and thus poses regulatory compliance issues such as data privacy, segregation, and security which should be enforced by the provider.

4 Accessibility: Ease of access through the web browser from any network device results in additional security risks considering various threats in the device and internet connection. These include information-stealing mobile malware, vulnerabilities in the device OS and official applications, insecure WiFi networks, insecure marketplaces, and proximity-based hacking.

B. PAAS security issues

PAAS depends on a secure and reliable network as well as on a secure web browser. The security of the PAAS application is comprised of two software layers: (1) security of the PAAS platform and (2) security of customer applications deployed on the PAAS platform. The following are the data security issues and challenges in the PAAS.

1 Third party relationships: PAAS offers third party web service components such as mashups that combine more than one source element into a single integrated unit. Hence, security issues related to mashups such as network and data security are also passed on to the PAAS models. Besides, PAAS users rely on both web-hosted development tools and third-party services.

2 Development life cycle: Security issues can arise from the compromise between the application development considering PAAS applications should be frequently updated. Developers should be informed of the data legal issues to ensure appropriate storage locations of data. Various storage locations with different legal considerations may compromise its security and privacy.

3 Infrastructure Security: Providers usually have control over the security of the infrastructure and its application services since developers usually

do not have access to the underlying layers. Hence, developers do not have the assurance that the development environment tools provided by the PAAS providers are secure.

C. IAAS security issues

IAAS offers different resources such as servers, storage, networks, and other computing resources in the form of virtualized systems that can be accessed through the internet. Through IAAS, cloud users have better security control that other model provided that there is no security lapse in the virtual machine monitor. However, security issues also arise from the fact that its underlying network, computational and storage infrastructure is controlled by cloud providers. The following are the security issues associated with IAAS.

1 Virtualization: This allows users to create, share, copy, move, and roll back virtual machines, enabling them to run various applications. Security concern arises from the extra layer that needed to be secured from attackers. A Virtualized environment is also vulnerable to types of attacks for normal infrastructures. Besides, virtualization adds more points of entry and interconnection complexity thereby posing security challenges.

2 Virtual Machine Monitor (VMM): It is a hypervisor responsible for virtual machines isolation thus if VMM will be compromised, the virtual machines might be compromised as well. The VMM entails security flaws considering it is only a low-level software that monitors and controls virtual machines.

3 Shared resource: Sharing of the same CPU, memory, I/O and other elements of VMs located on the same server decreases the security of each VM.

4 Public VM image storage: Offers vulnerable point to malicious users which can store images having malicious content or code to public repositories which may compromise the security of other users and even the cloud system.

5 Virtual Machine Rollback: Feature of VMs in case of an error, however, it can re-expose them to security vulnerabilities that were patched or re-enabled previously disabled passwords and/or accounts. To provide rollbacks, a copy of the VM is required to be provided which may lead to the propagation of configuration errors and vulnerabilities.

6 Virtual Machine Life Cycle: The different state of VMs (i.e. on, off, suspended) make it difficult for malware detection. VMs are also vulnerable even when they are offline and may be instantiated through an image containing malicious code that can start malware propagation by injection of malicious code within other VMs.

7 Virtual Networks: Sharing of network components by multiple tenants due to resource pooling also poses security risks since sharing resources allow attackers to launch cross-user attacks. Virtual networks increase the interconnectivity of VMs but also results in security vulnerabilities

VI. IMPROVING CLOUD-BASED E-LEARNING SYSTEM SECURITY

Fig. 2 below shows the proposed method to increase the security of cloud-based learning [4]

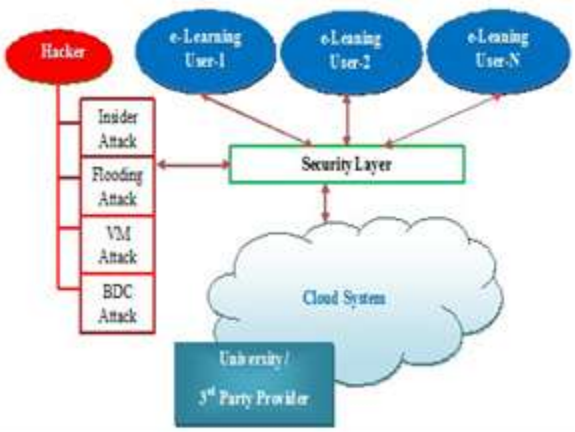

Fig.2. Cloud-based model to secure E-learning environment [4]

In a cloud-based system, if the server is overloaded or reaches the maximum load, it distributes some of its operational tasks to a nearby computational server, thereby increasing the efficiency of the cloud execution. When several unauthorized requests are received by the server, the service can be made unavailable to legitimate users. This type of attack is called Denial of Service (DOS) attack or flood request attack. To prevent this, all the servers must be organized in the cloud environment and distribute a particular job to each server. Another type of attack is

a backdoor attack wherein an intruder takes control of target systems resources. The backdoor channel attack affects the VM directly and makes it a zombie to start a DOS attack. To prevent this, anomaly-based intrusion detection techniques can be used [4].
Cloud encryption and key management can also be employed to increase the security of cloud-based e-learning by protecting the user's data [9]. Cloud-based key management can also provide audit information to software-based solutions while the service provider can provide Hardware Security Module service to protect its cloud users' keys. An option of external key generation for encryption use can also be utilized to strengthen cloud security.

VII. CONCLUSION

The use of Cloud-based E-learning system is an advanced technology that can help improve the learning environment of students and complement as well the traditional teaching methods. It offers a variety of benefits to users such as ease of access to the educational materials. However, it also raises some concerns in security that may slow down its use. Large data sets in e-learning platforms stored in the cloud increase vulnerability and as a result, raise a lot of trust issues. This research paper has successfully shown how these concerns can be addressed by choosing a reliable cloud service provider as well as adapting methods that can increase the security of the cloud such as cloud encryption and key management, as well as proper organization of files in the cloud.

REFERENCES

[1] R. Aruna, & S. Prakasam, - Enhancing Cloud based E- Learning using Knowledge Sharing System. International Journal Of Computer Applications, 84(9), 26-30, 2013.

[2] N. Azeez, & C. der Vyver, - Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108. doi: 10.1016/j.eij.2018.12.001, 2019.

[3] Cloud Security Alliance. (2017). - Top Threats to Cloud Computing + Industry Insights. Cloud Security Alliance. Available: https://cloudsecurityalliance.org/group/top-threats/

[4] M. Durairaj, & A. Manimaran, - A Study on Security Issues in Cloud Based E-Learning. Indian Journal of Science and Technology, 8(8), 757. doi: 10.17485/ijst/2015/v8i8/69307, 2015.

[5] Ernst and Young Global, Ltd. (2014). Building trust in the cloud: Creating confidence in your cloud ecosystem. EY. Available: https://www.ey.com/Publication/vwLUAssets/EY_-_Building_trust_in_the_cloud/$FILE/EY-grc-building-trust-in-the-cloud.pdf

[6] K. Hashizume, D. Rosado, E. Fernández-Medina,, & E. Fernandez, - An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. doi: 10.1186/1869-0238-4-5, 2013.

[7] S. Kassim, M. Salleh, A. Zainal, and A. Husin,- Risk tolerance and trust issues in cloud-based E-learning, linProc.2nd International Conference On Internet Of Things, Data And Cloud Computing - ICC '17. doi: 10.1145/3018896.3018973

[8] G. Kumar, and A. Chelikani, - Analysis of security issues in cloud based e-learning (Masters). University of Boras, Sweden, 2011.

[9] National Security Agency. (2020). Mitigating Cloud Vulnerabilities. National Security Agency. Available:https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

[10] O. Oludipe, O. Fatoki, N. Yekini,, and E. Aigbokhan, - Cloud-Based E-Learning Platform: From the Perspective of 'Structure' and 'Interaction'. International Journal Of Innovation And Research In Educational Sciences, 1(1), 1-6, 2014.