E-Learning Based On Cloud Computing for Educational Institution: Security Issues and Solutions

Muhammad Saqib Malhi[1], Usman Iqbal[1], Muhammad Mustafa Nabi[2], Muhammad Aaqib-Ishtiaq Malhi[3]

(Corresponding author: Muhammad Saqib Malhi)

School of IT & Engineering, Melbourne Institute of Technology[1]
The Argus, 288 La Trobe St, Melbourne VIC 3000, Australia
Department of Computer Science, Preston University[2]
Shahrah-e-faisal Karachi, Pakistan
Department of Management Sciences, Ripah International University[3]
Adjacent Fish Farm Satyana Road, Faisalabad Punjab, Pakistan
(Email: saqibmalhi1@live.com)

(Received Aug. 25, 2020; revised and accepted Nov. 15, 2020)

Abstract

In shaping successful individuals, education plays an important part. It gives us the opportunity to develop all the skills necessary for becoming a productive part of a civilized society. However, the modes of Education changes from time to time. And if talked about new morden era delivery of education is more focused online. With time this system of online process changed with Cloud storage and students can access anytime and at anywhere. So, the concept of E-learning based on cloud computing comes in. In this paper we will be discussing about the cloud, Cloud models and how the concept of cloud computing helps in delivering more efficient E-learning which is centralized networks. We will also discuss the major security concerns and the possible solutions to them.

Keywords: Cloud Computing; E-Learning; Security

1 Introduction

These days E-learning is broadly use by educational institutes fo supporting their learning procedures and give whenever students need to get to learning materials and data. E-learning gives numerous advantages, for example, flexibility, decent variety, measurement, and other, even though its numerous troubles in its implementation.

The primary issue experienced when to begin applying E-learning is the high beginning expense or at the end of the day is the financial factor [7]. It is turning into a significant concentration for the foundations that will executing E-learning. Establishments are sorted as low spending plan positively be hard to actualize e-learning, regardles of whether the organisation has a satisfactory financial plan additionally experts an insignificant spending that can be spent to execute e-learning [6]. E-learning

is one of the broad advancements of technology, which assistes with sharing the information among students, teachers, and colleges. So, the concept of cloud computing is been used to deliver E-learning.

Next generation of the Internet is the distributed Cloud Computing. Cloud Computing systems that are highly scalable and as a function resources are provided. In this paper we will be discussing how E-learning is based on cloud computing is more efficient. Which model of cloud computing delivers E-learning and their architecture and most important the security concers [7].

2 Litrature Review

2.1 Cloud Computing

Cloud computing is essentially the distribution of computation resources over Internet ("cloud," for instance) to provide quicker innovation, versatile sources and economies of scale, including servers, storage , data bases, networking, applications, analytics and intelligency re-sources.According to NIST(National Institute of Standards and Technology) cloud comouting is defined as a "model for on-demand network access to a shared pool of configurable resources" [10]. Most commonly used services of cloud computing are Amazon,google cloud,apple cloud system that is being used the clients and manufacturer and every individual looking for storage, data management and relevant essential services for their organisation even [14].

In general, you pay exclusively for cloud services, which help you reduce your operational costs, operate your infrastructure more efficiently and increase as your business needs change [11]. One of the latest developments is cloud computing. It is found on the internet 48 million times. It all started in 2006 When Companies like Google and Amazon started using Clouds to store their Files and more people access software to safe their file in cloud instead of Desktop and laptops. Latest product in cloud computing is Microsoft Azure [11]. Some of the main charasticts of cloud computing are mentioned below:

1) Self Service on Request: When needed without the intervention from the service provider, users can access computer resources through the cloud. In order to ensure users are controlled and agile for meeting their evolved needs, computing services should be available on demand [9].

2) Wide access to the network: The network are freely available from cloud computing services through the chosen devices of users (e.g. laptops, Mobiles, etc.) [9].

3) Pooling of resources: Cloud computing is the pooling of computer services on a wide scale. Multiple consumers are assigned resources such as storage, memory, processing and bandwidth on demand [9].

4) Flexibility: To access the resources, Flexibility is very important. Resources need to be correctly and rapidly distributed to accommodate large rises and decreases in demand without disruption of the service or deterioration of quality [9].

2.2 Cloud Computing Model

Cloud is divided on two models:

1) Delpoyment Model: Deployment Models offers the type of cloud like Public, Private or Hybrid [12]. Hybrid cloud computing is the combination of private cloud with public cloud services depending on their usage and requirements and the goal is to create a unified and an automated environment for cloud computing [5].

2) Service Model:Three primary service models included cloud solutions and they are

- Software as a Service (SaaS) cloud provider make sure that on demand software reuquirements of the user should be fulfilled and the platform is available for the use to access on internet with subscription where needed for example ERP (enterprise resources planning)softwares,accounting softwares and other applications such as Customer relationship manage-ment (CRM) [13].
- Infrastructure as a Service (IaaS) basically a computer infrastructure pro-vided by the provider in a virtuallised environment according to the de-mands of the user it can be optimized and performance efficient doesn't require regular maintenance as compare to hardware devices maintenance [13].
- Platform as a Service (PaaS) a platform for running web-based applications [13].

2.3 E-Learning

E-learning is simple to understand. ELearning is learning to navigate educational curricula out-side of a conventional classroom using online technologies [3]. It refers in most cases to a fully online course, programme, or degree. Many terms are used to describe online learning, via the internet, from distance learning to electronic learning, online learning, Internet learning and many more. We describe eLearning as courses which are distributed to someone else other than the classroom in which the teacher teaches through the Internet. The course is not distributed via a DVD, CD, video or TV channel [4]. E-learning can be in two forms.

One is virtualized form and other one is personal form. In virtual learning environment students and teachers can get access to wide variety of topics and students can easily understand the topics because of the virualisation of the topic [9]. It says that if students see things from eyes they can understand more easily as when compare with teaching them theoretically. While, it is easy for teachers as well as they can have variety related to one topic to make things easily understandable for students. Some of the features of virtual learning are:

- Update information announcements page on course topics.
- Schools which canot support large variety of courses due to infrasturacture can use Virtual learning to introduce more variety of courses and student can access them online [7].
- Students can get their study material at anytime and anywhere.
- Virtual Learning can provide flexibility and cost effectiveness to the syudents thus more students can get education.

Talking about Personal learning environment, it is a single use of E-learning where student in its personal space can use materials to improve their skills. Following are the features of the personal learning environment that users can use them:

- Users can interact with other users in their e-learning process.
- Students can improve and set their learning goals in the e-learning system.
- In learning systems, users can manage teaching and learning materials [3].

3 Advantages of Cloud Based E-Learning

E-learning in the cloud is an important part of cloud computing that is related to education and e-learning systems. Traditionally, cloud-based e-learning tools provide both the hardware and software required for enhancing education. Educational problems for e-learning systems are virtual in cloud servers and the subjects used by students and business are available from cloud vendors. Following are some of the benefits of the Cloud based E-learning are as follows [3]:

- Access Remotely: Students can remotely access the study materials from anywhere. This promotes independent learning and encourages the complete participation of distance learners [6].
- Efficiency In Cost: Educators can usually adopt a flexible system, which is payable when using a cloud based LMS system. Many fundamental cloud-based learning platforms are completely free to use. Cloud-based e-learning offers great value for money, compared to the costs for both traditional and non-digital teaching methods [6].
- Keep Up To Date: The cloud centralises remote systems, speeds up market time and eliminates the manual implementation required of a decentralised system. Instead of the gruelling processes of individual system updates, administrators run updates through the nube. Saving and implementing third-party server software enables administrators to implement updates and then go back and watch students access their content everywhere [12].
- Environmental Open Research: Cloud-based eLearning architecture enables you to experience a rich and immersive learning experience with interactive features such as quizzes and voice overview, challenges user understanding profundity and retention level by reflecting the traditional back and forth that comes in person [7].
- Collection of Data: With a centralised, cloud-based network, eLearning suppliers gain insight into the behaviours and success of their customers. eLearning service providers are using this data to supply relevant study material on problem areas or to monitor programme efficiency to encourage a unique eLearning ecosystem for all users [3].
- Global Education: For eLearning, it is flexibility that eliminates geographical barriers and time constraints that is the most compelling argument. Far away conferences could be revolutionary for a growing population, empowering students to manipulate their pace and enabling teachers to build up their field of influence [3].

4 Security Concers in Cloud Based E-Learning

Although cloud-based e-learning has many advantages, there are still some disadvantages to e-learning technology in cloud computing. These limitations are discussed in this section.

In this type of technology, security issues are more important, because Technology reliability in the mind of users. Since web-based e-learning depends fundamentally on web-based sources for its functions, e-learner, and cloud-based e-learning technology is under numerous threats through the Internet [7].

4.1 Cloud Computing Security Threats

Cloud comouting is an emerging component in the industry of information technology and it provides facilities to the user by increasing their efficiency and performance with the help of clud based service which is more reliable,faster and economical.While on the other hand there are some major security

concerns to cloud computing, *i.e.* data breaches,credentials of individuals at stake and is due to lack of managaement of cloud computing and their defence mechanism [1]. Given that cloud computing provides multiple services for different applications and technologies, several key security concerns in cloud computing and cloud security storages in various technology and applications [8]. Cloud computing's key challenges and threats are:

1) Concerns on basic security: Data integrity by approved transactions such as data transfer, storage, and recovery must be maintained by cloud providers. Cloud providers must meet the same standards to ensure that integrity issues are resolved [7].

2) Availablity: The main concern of cloud computing is the availability of major applications and cloud server information for continuous customer service. The most popular online attacks affecting online server availability are a denial of-service (DoS Attack) or a distributed denial of services (DDoS Attack) attack, which makes servers and stored data unavailable to users [6].

3) Increased demands for authentication: If cloud providers do not provide authentication, the possibility of phishing or other vulnerabilities can be increased by unauthorised access to these applications on the cloud [8].

4) Browser Security: The key to access cloud storage is the client-powered browser. Thus, browser safety is essential in total cloud security because the entire cloud security be-comes a problem when the gateway is malware attacked [12].

4.2 E-Learning Security Threats

Safety threats to e-learning are nothing but security problems that challenge the safety of e-learning users. This section covers key security threats to e-learning systems in addition to cloud-based e-learning security threats [9].

1) User Authorisation and Authentication: When it comes to e-learning, the authorisation of users is quite important. E-learners are generally located from far away, so they have a user identification and a password. By using them you can connect to and access the e-learning server. The student or the parent can access the account by point. Based on the accounting method, the next level of the learning provision may or may not be allowed [8].

2) Confidentiality: The confidentiality of data or information sent via the Internet should be kept as secret and not be disclosed to unauthorised third parties. This is an important aspect for safety concerns. From an e-learning point of view, students want to make sure that their soft copies of tasks submitted on the Internet are kept secret and revealed only to their e-learning teachers [7].

3) Blocking Attack: In the event of this attack, the external user generally attacks the e-learning content and gets authorisation to access the e-learning material. In this case, the IP address and block that address of the attackers must be monitored to resolve this problem [3, 7].

4) Flooding Attack: Flood attacks are the one that blocks the whole service or session with large numbers of requests for a specific service or large amount of data in small mes-sages. Due to delays in delivery, this can also cause a loss of accessible time. The counter measures for 32 such attacks would validate the incoming request or message effectively [8].

5 Security Measures in Cloud Based E-Learning

We are aware that cloud-based e-learning technologies, their suppliers, and their elearners, have serious security problems. E-learning technologies based on the Cloud also use some form of management standards and other protections to resolve vulnerabilities and threats to security. As cloud-based e-learning combines two different technologies, we must look at both security measures and security threat management technologies [7]. According to some researcher some of the security precaution should be taken into consideration while working with cloud comouting i.e. using multifactor authentications for secure access,strong passwords containg complicated and string values, backing up the data regular basis, anti-software in check all the time *etc.* [2]. Whereas, following security measures are the detail about how to secure cloud comouting and what factors should be considered while dealing with a cloud environment.

5.1 Security Measures in Cloud Computing

Various steps have been taken for tackling cloud technology security threats by cloud vendors and the international cloud-based organisation group [8]. These security measures respond to the safety issues that we discussed earlier. Such safety measures are as follows:

1) SaaS (Software-as-a-Service): SaaS is a cloud software model that incorporates much of the protection and monitoring activities. Before the business or final users adopts the service model, they must know the data protection policy of vendors before using their services so that unauthorised data access can be blocked [4].

2) Governance of security: In the company, a safety committee can be set up. The main aim of the Committee is to provide advice and support on security issues in line with the strategies of the organisation. While providing information security services, the committee must clearly identify its positions and responsibilities [7].

3) Management of risks: Risk management involves a variety of functions, including the detection and direct indication of technological assets and data for business processes and applications, data storage etc [7]. The owners of these organisations have respon-sibility for the confidentiality, completeness, availability, and privacy checks of infor-mation properties [8].

4) Security Awareness: Creating awareness of security is also an important step. It is im-portant. A lack of adequate safety awareness can enable them to disclose or expose the organisation's vital data that may in turn threaten the organisation. The organisation's losses can be enormous because of a poor security awareness, as well as the reduced reporting and slow response to potential safety incidents [7].

5) Methods and Standards: It is a good way to always check the sources and patterns to develop cloud system methods and standards. The first thing that should be considered by the security team is the security of data with business needs. These procedures should provide adequate documentation and supporting documentation should also be defined in relation to standard methods (these procedures must be followed as a framework) [7].

5.2 Security Measures in E-Learning

Several security actions are taken by various suppliers and organisations using this tech-nology to address security threats and vulnerabilities in cloud-based e-learning. Besides all these security measures, e-learning technology already has some mechanisms for addressing Internet vulnerabilities and other

threats to e-learning materials and e-learner technology to protect it against these attacks. Here we are discussing the security mechanisms:

1) Mechanism of SMS safety: This method is used to authentically access the elearning environment of a legal person. The process is similar to the one for the — team app, if a person signed into the e-learning portal first with a username and a registration password. After you enter the environment, you will get an SMS pass code to a mobile phone that is registered on the server and therefore safeguarded for that specific session [7]. Since the user logging process is defined by means of the specific pass code from session to session it is mainly used for stopping requirements or unauthorised access from the external or unauthorised users on the e-learning site [7].

2) Biometric: This mechanism is the best for maintenance of security. This requires the right user to use one or more of his / her own physical or behavioural assets. During registration, the physical characteristics of a user such as fingerprints, iris reconnaissance or behavioural features such as voiced recognition etc [7] are collected and saved in the database. When logging into the user, the attributes of the scan devices like finger printing mouse, etc are compared with the attributes which are stored in the database [7]. If they are the same, the user will receive the content of e-learning. It involves a highly active, reliable, and secure user's physical presence [7].

3) Digital Signatures: To authenticate the identity of a sender, digital signatures are used. This makes it easy to determine whether the original meaning of the message was al-tered. Mainly three items are included [7,8]. At first the sender generated an electronic signature while sending the message from an unsafe network to the receiver. The sender must also submit a certified form of item created from an algorithm hash and a private key from the sender's machine with the message and the signature. Non-repudiation is the key benefit of these digital signatures. Since the sender states that he has not signed the message and kept his private key secret, we can say that we can approve it and say to have reached the message by using certain non-repudiation algo-rithms that can generate a time stamp [7]. We can also check whether the intended user has changed the data.

4) Security for Passive Attacks: We discussed active attacks from the outside in all the above methods. If passive attack occurs, the source or the destination systems are not affected, but the cypher text or the plain text in some cases is altered to the attacker. We can avoid these types of attacks by using modern chip methods [7]. We can avoid passive assaults by using certain cryptographic methods such as private key encryption, public key encryption and hash functions.

6 Conclusion

E-learning system faces challenges with a huge demand and growth of users about programmes, media contents and educational tools. Cloud computing has evolved as a suitable forum for e-learning framework migration. Some challenges and issues are facing cloud-based eLearning, such as security, data lockout, and bandwidth. But customers / customers / users are still appealing to move to cloud computing [3, 8].

References

[1] A. Aljumah, T. A. Ahanger, "Cyber secuirty threats, challenges and defence mechanism in cloud computing," *IET Communication*, vol. 14, no. 7, pp. 1185-1191, 2020.

[2] M. Bain, *Stormid*, Aug. 23, 2018. (https://blog.stormid.com/7-cloud-computing-security-measures-to-take-now/)
[3] G. C. Bhure and S. M. Bansod, "E-learning using cloud computing," *International Journal of Information and Computation Technology*, vol. 4, pp. 41-46, 2014.
[4] A. Fernández, D. Peralta, F. Herrera, J. M. Benítez, "An overview of e-learning in cloud computing," in *Workshop on Learning Technology for Education in Cloud (LTEC'12)*, pp. 35–46, 2012.
[5] J. S. Hurwitz, R. Bloor, M. Kaufman, F. Halper, *Cloud Computing For Dummies*, Johny Willey & Sons, 2020.
[6] K. Kanagasabapathi, S. Deepak, P. Prakash, "A study on security issues in cloud," *Indian Journal of Science and Technology*, vol. 8, no. 8, pp. 757-767, April 2015.
[7] G. Kumar, A. Chelikani, "Analysis of security issues in cloud based e-learning," *Master's Thesis in Informatics, University of BOras*, 2011.
[8] M. Lynch, *7 Benefits Of Cloud Based E Learning*, The Tech Advocate, 11 March 2018. (https://www.thetechedvocate.org/7-benefits-cloud-based-elearning/)
[9] A. H. Masud, R. Islam, J. Abawajy, "Security concerns and remedy in a cloud based E-learning system," in *International Conference on Security and Privacy in Communication Systems*, pp. 356-366, 2013.
[10] T. P. Mell, "The NIST definition of cloud computing," *NIST Special Publication* 800-145, USA, 2011.
[11] Microsoft, *What is Cloud Computing?*, 2020. (https://azure.microsoft.com/en-au/overview/what-is-cloud-computing/)
[12] P. C. Patnaik, S. Putta, Md. Ismail, "Role of cloud computing to overcome the issues and challenges in e-learning," *Journal of Basic and Applied Engineering Research*, vol. 1, no. 7, pp. 66-70 , Oct. 2014.
[13] A. Sivakumar, "A survey on cloud computing model and its appliation," *International research journal of Engineering and Technology*, vol. 6, no. 12, pp. 1928, 2019.
[14] K. Yin, "Cloud computing: Concepts, models and key technologies," *ZTE Communications*, vol. 8, no. 4, pp. 21-26, 2010.

Biography

Muhammad Saqib Malhi is studying Master of Networking (Cybersecurity) in School of IT & Engineering at Melbourne Institute of Technology, The Argus, 288 La Trobe St, Melbourne VIC 3000, Australia. Interest: Cybersecurity & Networking.

Usman Iqbal is studying Master of Networking (Cybersecurity) at Melbourne Institute of Technology, The Argus, 288 La Trobe St, Melbourne VIC 3000 Australia. Interest: Network and Information security.

Muhammad Mustafa Nabi is studying at Preston University, Shara-e-faisal Karachi, Pakistan. Interest: E-commerce Security.

Muhammad Aaqib Ishtiaq Malhi is studying at Ripah International University, Adjacent Fish Farm, Satayana Rd, Faisalabad, Punjab 44000, Pakistan. Interest: Information systems and security.