INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN: 2455-0620 [ Impact Factor: 6.719 ]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 8, Issue - 9, September - 2022 Publication Date: 30/09/2022

DOIs:10.2015/IJIRMF/202209033 --:-- Research Article

# An Efficient Architectural Framework for Autonomous Cloud Computing Under Deployment: An User Prospective For Cloud Based E-Learning

**[1]Tanmaya Kumar Das, [2]Sasmita Mishra, [3] Hari Narayan Pratihari**
[1]Ph.D Scholar, Dept. of Computer Science& Engineering, Indira Gandhi Institute of Technology, India.
[2]Professor, Dept. of CSE & Application, Indira Gandhi Institute of Technology, Odisha, India.
[3] Professor, Dept. of Electronics & Communication Engineering, St. Martin's Engineering College, Dhulapally, Secunderabad, Telangana, India.
Email - research.tanmaya@gmail.com

***Abstract:*** *Learning resources that are managed and controlled by third-party service providers can be more easily accessed through cloud-based E-learning. The management of appliances and services has become more difficult as IOT devices are increasingly used in education. Network systems of today's complexity and dynamicity require an interacting architecture capable of autonomously changing the system's structure and functionality with the minimum human intervention. In addition, the cloud platform's elasticity necessitates a constant need for service reconfiguration in the event of unexpected failures, such as system crashes, network problems, or natural disasters, which typically cause service unavailability. E-learning also necessitates a cloud platform that protects vital information from hackers and ensures data is always available. As well as an efficient framework for a self-sufficient cloud computing platform, this paper suggests some security measures for online learners.*

***Keywords:*** *Cloud Architecture, e-learning Security, Autonomous System, Third Party Provider, Cloud Interface Manager.*

## 1. INTRODUCTION:

The use of cloud technologies in the academic setting has the potential to open up new avenues for improving and innovating the learning process [1].It became necessary to update teaching methods in response to the rapid development of new technologies. In order for them to achieve success, they needed to be able to learn whenever and wherever they desired [11].The Cloud Computing (CC) paradigm is a cost-effective solution for providing computational resources as a service. CC is an on-demand computational model that provides end-users with the services they require [03]. The services available are delivered over the Internet and are characterized by their flexibility and scalability. As a result, innovative solutions must be created that can dynamically adapt to cloud elasticity. However, ongoing service must be ensured, as well as a high degree of performance. Furthermore, the quality of the cloud environment affects various network services. As a result, any network failure, such as traffic delays or connections breakdown, has a significant impact on the cloud's quality of service (QoS) [11].

The application of IoT in the field of E-learning improves the efficiency of the learning process for both students and teachers. During the COVID-19 Pandemic, all E-learners used smart phones, desktops, laptops, and tablets etc. as IoT devices [01]. Learners in rural areas, on the other hand, found it difficult to benefit from the E-Learning process due to geographic differences and socio-economic barriers to using appropriate IoT devices with Internet facilities, as well as some security-related issues such as data availability on demand and in real time mode, which severely limits the learners' ability to stay up-to-date with their curriculum. This study presents an effective architectural framework for autonomous cloud computing deployment, as well as addressing some of the E-learning difficulties that arise in this situation [01].

## 2. BACKGROUND:

Industries are opting for cloud computing services for the following reasons:
***Low Cost:*** One of the most compelling reasons to migrate to the cloud is the cost savings potential. With the cloud, the user can only pay for the programmes that they need, and a large number of applications are included for free [03].

***Scalability***: One of the primary reasons for utilizing cloud computing is that it is measurable. Cloud computing enables universities, schools, and IT industries to simply scale up or scale down their IT needs as needed [03].
***Ease of access:*** Simply put, cloud computing is simple to set up and use. Rather than having to transfer and/or install software systems by the user, everything is available in the cloud. Cloud computing performance should be increased for exploitation [03].

**Cloud-Based Learning Architecture:**

The Cloud computing design in distant learning is a technique that may be used to improve performance and flexibility, but this model can also be used to transform the traditional classroom into something much more dynamic and operational. Cloud services serve as a middleware, physical memory, and CPU in this paradigm. These units must be combined with a variety of versatile tools that have been developed for academic institutes, field network architectures, and internet-based technologies at a very low cost in order to improve information and qualifications. The planned model can cover a variety of advantages such as powerful computing methods and large storage capacity, high security and visualization, and the planned design uses extremely limited resources. Learners and practitioners will proceed by sending an initial request to the server, which will then manifest the user request and provide the service once it is acknowledged [08].

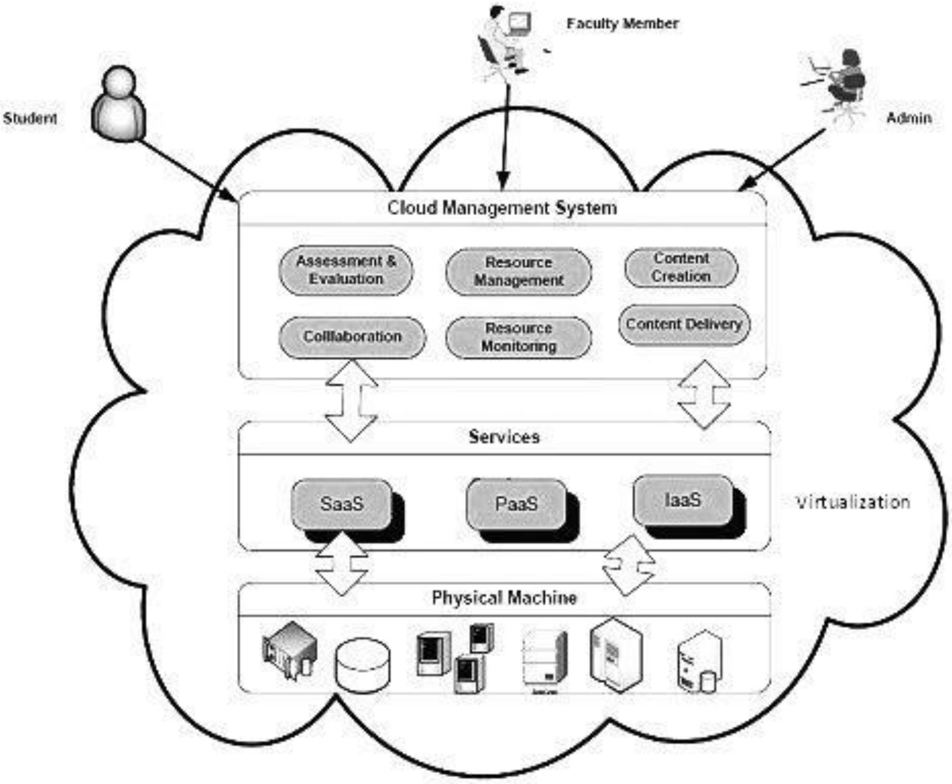

Fig. 1. Cloud Based Learning Architecture

**Virtualization:**

The term "virtualization" refers to the process of using any computer's resources to simulate the use of another computer's resources or even an entire computer[13].A virtualization environment that enables the design of systems (that is, compute power, bandwidth, and storage), as well as the development of individual virtual machines, has emerged as a crucial component of cloud computing environments in recent years. Because it offers a platform for maximizing complex information technology resources in a scaling (efficiently increasing) manner, virtualization is ideally suited for the delivery of services[13].At its most fundamental level, the technology behind virtualization makes it possible to abstract or otherwise decouple the application payload from the underlying physical resources[13]. On-demand provisioning is a phenomena for changing or transforming physical resources into virtual or logical resources on user's demand15].The traditional ways involve using a mixed environment of hardware, a multitude of administration tools, consistent application patching and updating, complicated workloads, and multiple software architectures[15].On the other hand, cloud data centers use significantly improved strategies, such as a consistent environment, standardized management tools, minimum application patching and upgrading, straightforward workloads, and a single standard for their software architecture[15].

**Challenges of Cloud Computing:**

Cloud computing appears to be a wonderful support to the end user, but it is not without its hurdles and issues. The most important aspects of cloud computing are security concerns. It is extremely risky to entrust all of an organization's data and information to a cloud provider, as well as to execute an application at another's location. Data loss, phishing, and threats are all typical problems [04].During data transfer and storage, privacy and trustworthiness must be protected. User data including identity, operation history, and perceptive data must be obtained from the cloud provider because of the nature of this shared infrastructure [13]. In the absence of user administration and third-party access, cloud is not responsible for illegal use and retrieval. A large number of software, programs, and services are offered to the general public for free. This means that stealing and using floating data without identifying or authenticating the user is a simple and direct and quick process [13].

A Cloud Service Provider (CSP) promises to supply a service but is unable to meet the customer's expectations due to over-utilization of capacity. Cloud computing is further hampered by Internet latency, which makes it difficult for Cloud Service Providers to deliver services on time. Both the cloud service provider (CSP) and the end user are in charge of auditing the data in a given service or application [13].The data can be replicated, shifted, and altered by the Cloud Service Provider [11]. As a result, clients must keep a close eye on all of these operations to ensure that the Cloud Service Provider does not engage in these activities outside of their jurisdiction. As a result, auditing every single bit of data is impractical, and deciding which data should be audited is difficult. Furthermore, the issue of co-habitation is a major concern [13].As the number of apps running on a node increases, the bandwidth allotted to each app decreases, suggesting that the average number of apps and the allocated bandwidth are inversely related. This results in the system's performance at risk [13].

## 3. MOTIVATION:

Because e-learners are still unsure about cloud computing validity, its current acceptability is fraught with difficulties. The single most significant factor impeding cloud computing adoption is security concerns. The idea of utilizing their own CPU to run software that is stored on the hard drive of another person makes a great deal of people uncomfortable[16].Data loss, phishing assaults, and bonnets (which run remotely on multiple workstations) are all examples of well-known security weaknesses that pose significant risks to the data and software of a company. In addition, the multi-tenancy model of cloud computing and the use of shared computing resources have given rise to new security challenges, which necessitate the development of new approaches to resolve them[16]. Hackers, for instance, are able to design cloud environments in which they can employ bonnets to launch attacks against other computer systems [16].

## 4. OBJECTIVE:

The purpose of this study is to investigate the hazards that are associated with cloud-based e-learning, as well as the service delivery techniques that are used and the definitive solutions for each attack [12]. It will be beneficial in the future to manage and build new techniques for safe cloud-based electronic learning. This work makes a contribution to the creation of an e-learning technique for the benefit of e-learners and to the achievement of 24/7 data availability in the cloud computing environment [12].

## 5. CONTRIBUTION AND PROPOSED FRAMEWORK:

The proposed framework offers a cloud-based, self-contained architecture for securing E-Learning environments. This concept is designed with E-Learning consumers, Secured Layer, and third-party supplier in mind. To reinforce this paradigm, the hacker's techniques are also explored. The following diagram depicts a cloud-based model for securing an E-Learning environment [01].

**E-learning environment:**

There are a variety of ways to use e-learning, whether it's in a classroom, as part of your company's mandatory training, or as a full distance learning course [12]: It is now possible to employ mobile devices like smart phones and tablets, as well as various interactive designs, in the classroom or at work, making distance learning both exciting for students and practical as a delivery method for lessons. Cloud data can be accessed through the Secured layer [12].

**Hacker:**

A hacker is someone who notices flaws in a computer or computer network and exploits them to gain permitted or unauthorized access. Hacking can be done for a variety of motives, including profit, protest, or challenge. The hacker's attacks include the followings:

**Flooding attack:** All servers in a cloud system are service-oriented. One or more servers can be used to distribute some of the workload if one server gets overburdened [12].Using this distribution technique, the cloud is more efficient and faster to implement. Service is inaccessible to legitimate users when the server receives a huge volume of illegitimate requests [12]. A denial of service (DoS) attack occurs when a large number of requests are sent to a server at the same time. Monitoring CPU, memory, and hardware utilization can reveal suspicious activity [12]. To prevent flooding assaults on servers, group all the servers together in a cloud environment and assign each server a specialized job, such as managing the file system or managing memory[12].

**Backdoor channel attack:** The backdoor channel attack is a type of passive attack that sidesteps the conventional authentication procedures in order to compromise the users' privacy who are using the system legitimately [12].An intruder gets control of the resources of the target system when a backdoor channel attack happens, and they might try to launch a distributed denial of service attack [12]. It is also possible to utilize it to divulge private information about the user you are targeting. This type of back-door channel attack directly impacts the Virtual Machine (VM) that is housed in a cloud computing environment, transforming it into a zombie that may then be used to conduct a DoS or DDoS attack[12].Anomaly-based intrusion detection strategies should be utilized in order to safeguard the system against assaults directed at the Hypervisor or the VM. Techniques that are based on signatures or anomalies are utilized in the commission of flooding and backdoor channel attacks [12].

**VM attack:** Virtualization is an important component of the cloud computing platform known as infrastructure as a service [12].Cloud service companies face a challenging task related to securing the virtual computers of their customers [12].In a platform that provides cloud services, the user is often provided with virtual resources that are paid for on a monthly basis. These actual needs put a limit on both the virtual and physical resources that are available[12].Because multiple tenants share the same resources, it is possible that multiple virtual resources will be connected to the same physical resources in cloud computing[12].If there is a vulnerability in the cloud platform's virtualization software's security protocols, then other users may be able to access the user's data [12].

**Insider attacks:** In contrast to external attackers, insiders have access to the system and may be knowledgeable with network architecture and system policies / procedures [12]. This gives them an advantage. It's possible that internal attacks aren't as well protected as they could be because so many companies are focused on defending against exterior threats. Cloud data has been exposed by malicious insiders working for cloud service providers [12].In addition, cloud computing is vulnerable to other insider risks. Rogue administrators are individuals working for cloud service providers who have ulterior motives [12].

**3rd party provider:**

In the cloud, it is the responsibility of third-party service providers to guarantee the safety of all service transactions [12].Before we start using a cloud service, we need to make sure that we are familiar with the role and obligations of the third-party cloud provider, which are spelled out in the contract. Learners need to investigate whether one cloud vendor outsources work to another cloud vendor. Data from services such as Drop Box (SaaS), for instance, is kept in a data centre run by Amazon Web Services (IaaS). In the presented situation, a customer's privacy in the cloud may be compromised due to the existence of a confidential contract [12]. This danger can be avoided if the cloud provider takes into consideration the proposal, which includes disclosing the name of the third party and identifying the service it provides[12].The cloud provider's security standards and procedures should be followed by any third-party suppliers who access their cloud. If there is an issue, the cloud provider will only bear direct responsibility for the customer's data in every way possible [12].

**Autonomous system:**

A concept which derives its inspiration from biological processes is known as autonomous computing [11].The goal of these types of systems is to simplify the complicated task of regulating nature's broad diversity. This is performed by automating the capacities for self-management. As a result, there is as little involvement from humans as possible in the management of large systems [11].

It's necessary for a system to have one or more self-properties, which in turn provide autonomic capabilities. Listed below are [14]:

Self-configuration refers to the capacity of a system to autonomously conduct configurations in accordance with certain pre-defined high-level policies. This should be done in a manner that is as smooth as feasible [14].

Self-optimization refers to the capacity of a system to continuously monitor and control the use of the resources it has access to in order to achieve the goal of increasing the system's performance as a whole[14].

Self-healing refers to the capacity of a system to autonomously recognize, diagnose, and fix any errors that might occur inside it[14].

Self-protection refers to the capacity of the system to actively recognize and defend itself against any type of malicious assault or cascade failure. Self-healing mechanisms don't fix these types of issues [14].

**Local cloud interface manager (LCIM):**

This module is linked to local data centers to deliver services by improving data processing in cloud-based computing systems by performing it closer to the source of the data, i.e. the E-learning site, so that in the event of a transmission delay or network failure to the cloud, the request can be stored and processed at the edge and services delivered to the learners [17].

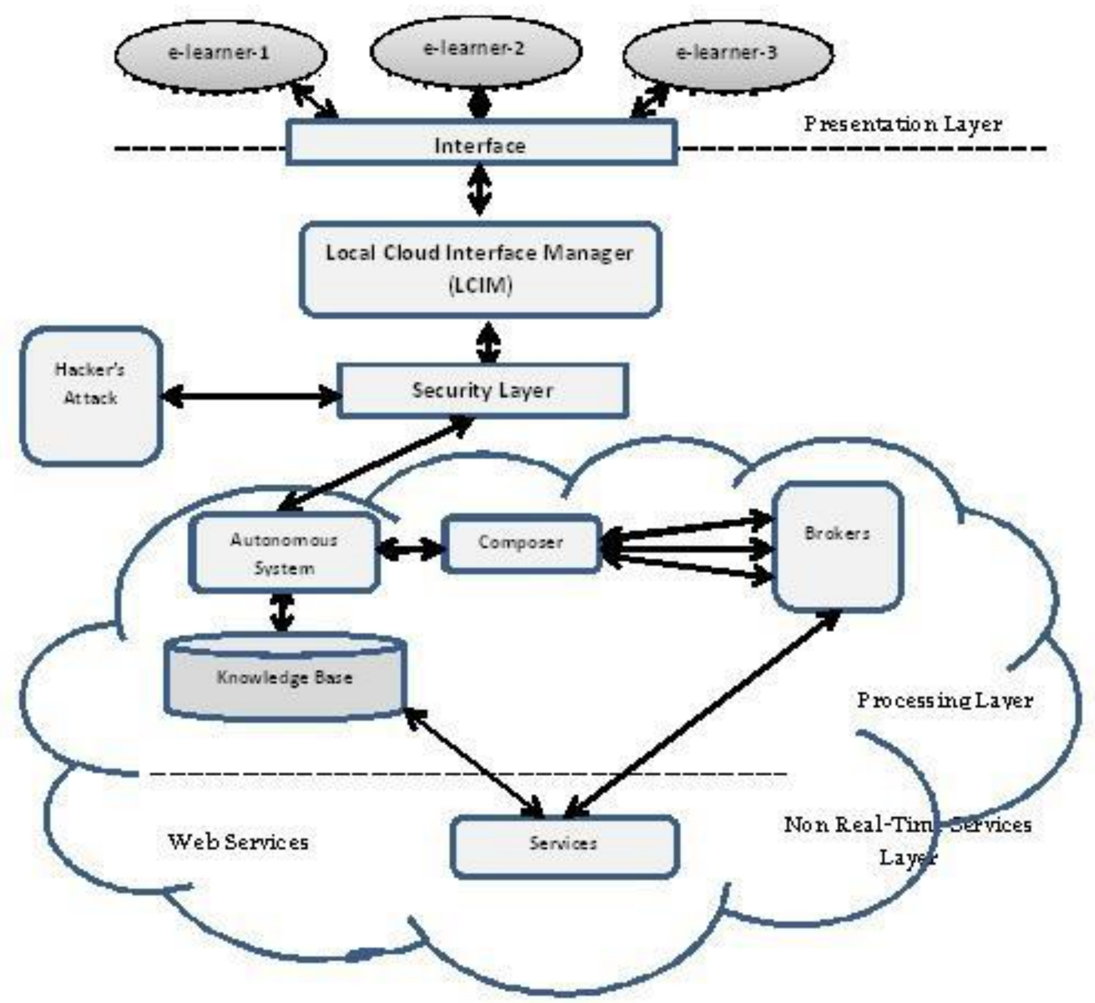

Fig. 2. Framework for an autonomous cloud computing platform for E-learners

## 6. LIMITATIONS AND FUTURE WORK:

The proposed framework will allow e-learners to dynamically access services in their field of study and will be useful in the event of system crashes, network problems, or natural disasters among other things [03].However, it has limitations such as machine constraints, bandwidth, cost effectiveness, and scalability because the learners are spread across different geographical areas with varying socio-cultural and socio-economic diversity. Future work may be expanded to operate and provide services in real time using current IoT technology trends [03].

## 7. CONCLUSION:

This research proposes a new framework for cloud computing environments. The suggested architecture includes SOA, autonomous computing with knowledge-based reasoning, and a cloud interface manager for the local cloud. Non-real-time services and crucial real-time services are the two types of services available. On the other side, the architecture is divided into four levels. The presentation layer provides end-users with an Internet-based interface to the cloud. The processing layer is made up of the autonomous manager, knowledge-based, and brokers. A network outage has no effect on the services that are running since the core services are run via the non-real-time services layer. Finally, the real-time services layer, often known as the home network (LAN), manages critical services using distributed autonomous control. The failure of the cloud has no impact on the rest of the system.

## REFERENCES:

1. Kumar SC. Awareness, benefits and challenges of e-learning among the students of Kurukshetra University Kurukshetra: A study. Int J Inf Dissemination Tech. 2019;8(4):227-230.doi: 10.5958/2249-5576.2018.00048
2. Keis O, Grab C, Schneider A, Ochsner W. Online or face-to-face instruction? A qualitative study on the electrocardiogram course at the University of Ulm to examine why students choose a particular format. BMC Med Educ. 2017;17(1):194. Doi: 10.1186/s12909-017-1053-6.
3. Thanji M, Vasantha S. ICT factors influencing consumer adoption of ecommerce offerings for education. Indian J SciTech. 2016;9(32):1-6.
4. Barbera E, Clara M. Time in e-Learning Research: A Qualitative Review of the Empirical Consideration of Time in Research into e-learning. ISRN Educ. 2012;2012.doi: 10.5402/2012/640802.
5. Jawaid M, Ashraf J. Initial experience of eLearning research module in undergraduate medical curriculum of Dow University of Health Sciences: Development and students perceptions. Pak J Med Sci. 2012; 28(4):591-596.
6. Iqbal S, Shafiq A, Iqbal N. Perceptions of undergraduate dental students towards e-Learning in Lahore Medical and Dental College. Pak J Med Heal Sci. 2016; 10(4):1191-1193.
7. Sethi A, Wajid A, Khan A. E-Learning: Are we there yet?. Prof Med J. 2019; 26(04):632-638.doi: 10.29309/TPMJ/2019.26.04.3367.
8. Schwartz AM Wilson JM, Boden SD, Moore Jr TJ, Bradbury Jr TL, Fletcher ND. Managing Resident Workforce and Education During the COVID-19 Pandemic: Evolving Strategies and Lessons Learned. JBJS Open Access.2020;5(2):e0045. Doi: 10.2106/JBJS.OA.20.00045.
9. Wang SL, Wu PY. The role of feedback and self-efficacy on web-based learning: The social cognitive perspective. Comp Educ. 2008; 51(4):1589-1598. Doi : 10.1016/j.compedu.2008.03.004.
10. Kruger J, Dunning D. Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. J Pers Soc Psychol. 1999;77(6):1121.

1. 11.Bhaktiand, M., Nugroho, H., Firmansyah, Paputungan, I., Oktiawati, U.: Taking up Autonomous SOA framework into Cloud Computing. IEEE Trans. Cloud Computing and Social Networking (ICCCSN) (2012).

11. www.slideshare.net
12. www.iaesjournal.com
13. www.mdpi.com
14. www.ijsrcseit.com
15. www.sdiwc.net
16. www.lanner-america.com
17. www.jcreview.com