Asian Journal of Research in Social Sciences and Humanities

Asian Research consortium

www.aijsh.com

ISSN: 2249-7315
Vol. 11, Issue 10, October 2021
SJIF –Impact Factor = 8.037 (2021)
DOI: 10.5958/2249-7315.2021.00092.7

A SURVEY OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATIONAL INSTITUTIONS

Dr. Kashif Qureshi*

*SOEIT, Sanskriti University,
Mathura, Uttar Pradesh, INDIA
Email id: kqureshi.cse@sanskriti.edu.in

ABSTRACT

Cloud computing provides a broad variety of advantages for higher education institutions, including new possibilities to integrate into the teaching process. Cloud services, on the other hand, are susceptible to a range of security threats. The supply of a safe cloud infrastructure is one of the major difficulties that educational institutions confront when embracing cloud computing technology. The authors of this article examine certain cloud advantages in the education sector, as well as the limits of common cloud services and the security issues that institutions confront when using cloud technology. The survey was performed at a range of educational institutions to learn about stakeholders' perspectives on cloud security vulnerabilities and solutions. Finally, this paper offers general guidelines for avoiding security concerns while using cloud computing in higher education organizations.

KEYWORDS: *Cloud Computing, Cloud Services, Deployment models, Higher Education, Security Issues.*

1. INTRODUCTION

Cloud computing plays a significant role in enhancing education quality and achieving needed performance by delivering numerous educational advantages such as low-cost infrastructure, flexibility, scalability, collaboration, and ease-of-use[1], [2]. Furthermore, it enables users to save and retrieve important information through the internet at any time and from any location. Users may use their personal computers or mobile devices to store and access their local data in a distant data center utilizing cloud services and apps.

Stakeholders at higher education institutions include students, lecturers, researchers, staff members, and anyone who have access to educational services. The major players in cloud computing in higher education institutions are shown in Fig. 1.

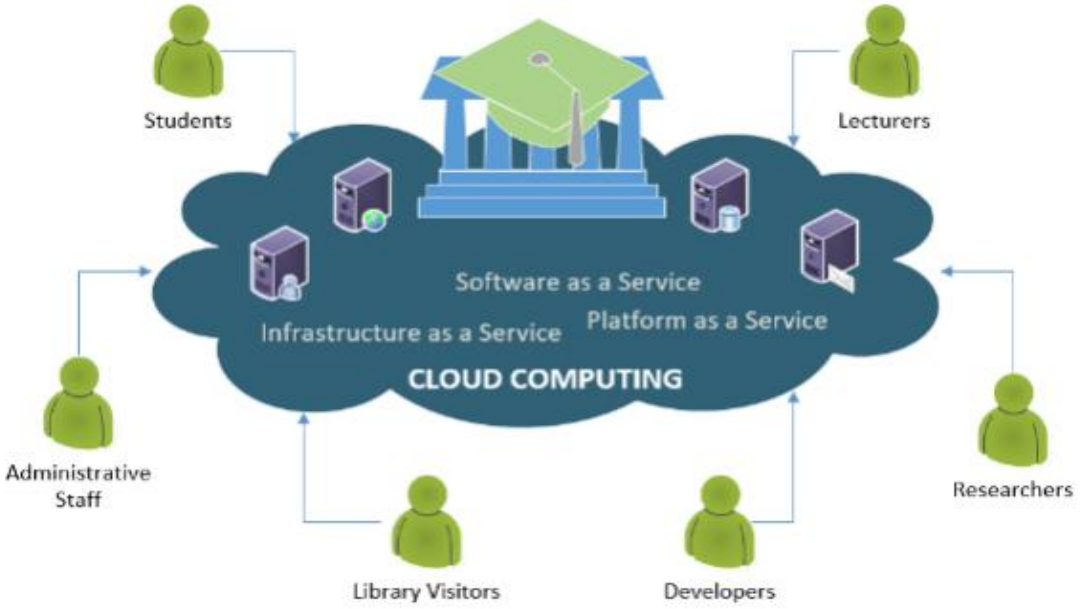

Fig. 1: Major players of cloud in an educational institution[3]**.**

1.1. Cloud Deployment Models:

The National Institute of Standards and Technology (NIST) categorized cloud computing deployment methods into four categories: private, public, hybrid, and community clouds[4]. Private clouds are installed inside an organization's perimeter and are provided for exclusive usage by particular customers; their data and services are not accessible from outside the company. A public cloud is one that is owned and maintained by a company, university, or government that offers cloud services to the general public. The hybrid cloud combines the benefits of both public and private clouds.

Infrastructure and services are provided for usage by a particular community of customers or by multiple companies with the same purpose or goal in the community cloud. It may be run and maintained by the community itself or by a third party.

1.2. Cloud Computing Characteristics:

Cloud computing services, according to the NIST definition, have five key characteristics: broad network access, on-demand self-service, rapid elasticity, resource pooling, and measured service. We'll go through the following basic education-related features of cloud computing:

1.2.1. On-demand self-service:

Because of the diversity of users at educational institutions, there is a wide range of functionality and operations that may be done. In this scenario, the stakeholder needs the ability to provide cloud services or resources as required without having to engage directly with the service provider. Typically, a web-based self-service interface allows users to setup and manage resources in an on-demand environment.

1.2.2. Broad network access:

Cloud services and resources must be readily available from a variety of devices, including computers, tablets, and mobile phones. Standard access methods and protocols are used to provide this ubiquitous access. To provide this degree of access in educational settings, services must be customized to the needs of various cloud users.

1.2.3. Resource Pooling:

Cloud providers pool large-scale computer resources and services to offer logically distinct services to many customers. This multi-tenant architecture is based on virtualization

technology, which dynamically assigns and reassigns resources based on cloud user demand. A multi-tenant system encourages location-independence, in which the user has no idea where data is kept or where it is being saved.

1.2.4. Rapid elasticity:

The user's cloud services or resources may be quickly scaled up and down depending on the user's policies and needs, without affecting the application or requiring any human involvement. In this scenario, various stakeholders in an institution, such as students, faculty, and administrative staff, may access and utilize resources as required, at any time, with precise capacity.

1.2.5. Measured services:

The use of cloud services or resources must be constantly monitored and metered using the pay-per-use function. Both the service provider and the customer benefit from the transparency offered by this report on resource use.

1.2.6. Resiliency:

Resilient computing refers to the capacity to recover from cloud resource failures and disasters by deploying numerous redundant cloud services across different physical locations. Multiple redundant locations provide continuity and enhance cloud computing processing dependability and performance. If any of the cloud resources become insufficient, additional redundant resources are automatically deployed.

1.2.7. Cost effectiveness:

When compared to local infrastructure, cloud services and resources are more cost efficient. Its expenses are split among many users in the same or other places.

2. LITRATURE REVIEW

One of the major problems that academics have lately focused on for implementing cloud computing in education is security difficulties and privacy issues.

In addition to addressing certain cloud-specific problems that have arisen with the introduction of cloud computing, Gowr et al. address broad security issues linked to the fundamental technologies utilized in cloud computing, such as APIs, virtualization, Internet protocols, and so on[5].

Srivastava et al. suggested a system to address security concerns by creating a connection between cloud service providers, allowing data about potential risks to be produced based on past assaults on other providers[6].

Pal et al. concentrate on the absence of security concerns in Service Level Agreements, as well as the most common security threats and vulnerabilities[7]. The framework was created using data gathered from security experts, practitioners, service providers, and their customers.

Karl et al. offer a methodological and theoretical research in which they seek the opinions of key stakeholders on the problem of cloud information security in South African higher educational institutions[8]. The authors show how trust is an important element in cloud computing adoption. For understanding and assessing cloud computing uptake in Higher Education settings, a trust-centric conceptual framework is suggested.

3. DISCUSSION

3.1. Cloud Service Models:

In general, three main types of services the user in the educational institution can gain when access cloud. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These services are built on the cloud upon each other as shown in Fig. 2.

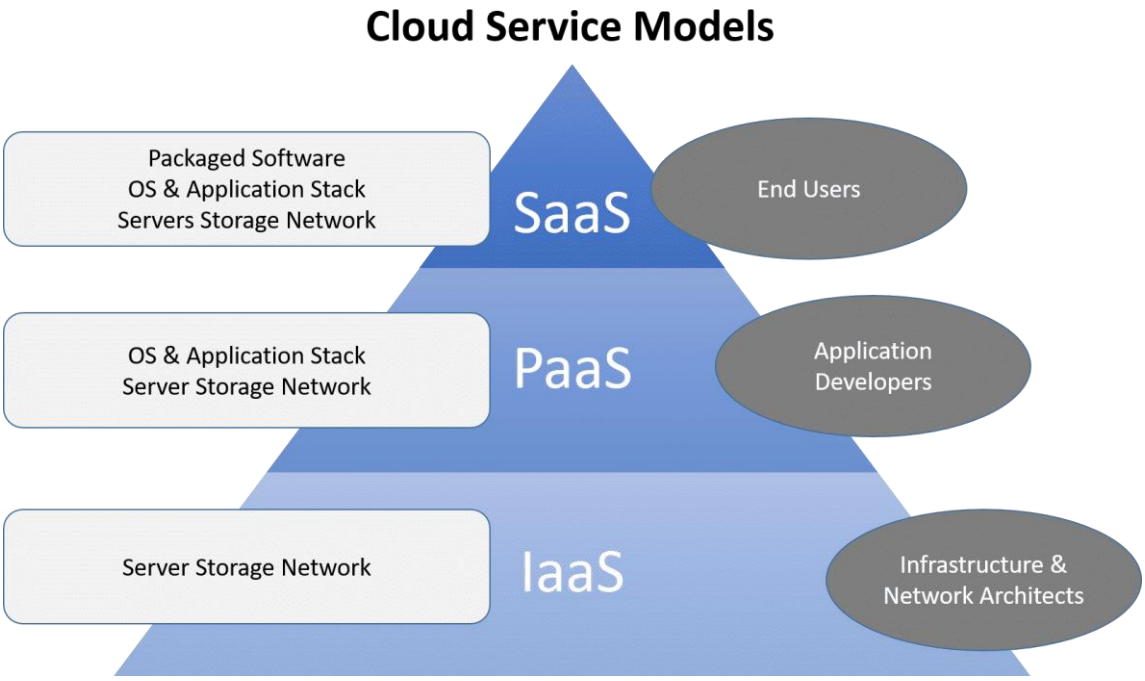

Fig. 2: Illustrates Cloud Service Models[9]**.**

3.1.1. Software as a Service (SaaS):

In the SaaS model, users gain access anytime and from anywhere to applications provided and managed by the service provider. Currently, SaaS is considered the most interested for stockholders in education. Google Drive, Twitter, Dropbox, YouTube, and OneDrive are general examples of cloud-based services. Both Microsoft and Google provide some services that are suited for education such as Google Apps andLive@edu.

3.1.2. Platform as a Service (PaaS):

In PaaS, the service provider offers for developers development tools to build or customize their applications or services in the cloud independent of the platform to run. The best-known example of PaaS is the Google App Engine where a developer can install and customize their applications using Python language.

3.1.3. Infrastructure as a Service (IaaS):

IaaS is a self-service model, the cloud vendor allows developers to access, monitor and manage computing resources (processors, storage, networks, etc.) in the data center remotely, and use them to run own operating systems and applications. The big advantage of using IaaS is that it offers an on-demand data center without requiring you to purchase or install new expensive equipment. Amazon's Elastic Compute Cloud is one common example of IaaS.

3.2. Cloud Benefits in Educational Institutions:

There are various advantages may be granted when adopting cloud computing technologies in higher education institutions. Some universities have adopted cloud computing in their programs for economic purposes, while other institutions use the cloud to provide scalable and flexible IT services. The key benefits of cloud computing in education can be categorized

according to stakeholders who use cloud resources and services in higher education institutions:

3.2.1. Benefits for Students:

The first beneficiary of the cloud technology in the educational institutions must be students. Some of the cloud benefits directed to students are reviewed:

- Cloud computing releases services for students with new capabilities that were not served well by traditional ways. Nowadays, the students can store anything electronically such as their schedule, class notes, reports and any other documents. Furthermore, they able to back up their files to the cloud and retrieve them when needed.
- The lab's applications and auxiliary resources that may be implemented on the Internet enable students to perform lab's tasks from anywhere and by low-cost personal devices. Therefore, the students do not need any more to buy expensive hardware or install special software.
- Students can earn e-copy of textbooks and have access to quality learning materials of their courses. This solves the problem of the student's reluctance to gain textbooks due to their high-cost prices. Furthermore, cloud-based textbooks solve the problem of using outdated materials in many of institutions and allow students to access the most updated learning resources.
- Real time collaboration between students themselves as a team or between students and their instructors on the other hand.
- Students have the opportunity to access the system easily at any time to get courses online, attend the online exam, and upload their assignments and projects through the cloud to the instructors.

3.2.2. Benefits for Faculty:

The faculty also can get various advantages over cloud-based applications:

- The faculty may be able to exchange experiences by establishing remote seminars to overcome the lack of skills among some faculty members.
- Cloud technology offers for instructors an easy and flexible platform to prepare their course tutorials, presentations, conferences, articles, etc.
- Collaboration with other instructors and sharing educational resources to avoid conflict and duplication of effort.
- Providing opportunities for instructors to work from home and use their own devices to finish assignments, prepare on-line tests, grading, and scheduling.
- Cloud provides for researchers a discussion area and accessibility to global computing resources and sufficient storage capacity.
- Getting feedback from students about the educational process.

Even though the great benefits of using cloud computing in educational institutions, there are some challenges that hinder the wide scale adoption of this technology in various sectors of the university. In the current circumstances, it is not easy to track the variety security issues in cloud computing environments.

3.3. Limitations in Cloud Service Models:

This section focuses on some limitations related to cloud service models that disserve adopting cloud computing in higher educational institutions.

3.3.1. Limitations in SaaS:

Two key limitations may effect on deploying applications under SaaS model: data locality, and integrity. Generally, the user does not know where the service provider stores data and how can be assured that no one can modify it. The lack of trust between cloud user and provider is a critical issue that should be addressed when using SaaS.

As a result, to avoid data leakage in the educational institutions the computer center in the university may host the SaaS application on its own private server or deploy it on infrastructure services provided by trusted third-party provider such as Amazon, Google, etc. For these reasons, most of higher educational institutions involved in this survey are using a private cloud, rather than public or hybrid cloud as shown in Fig. 3.

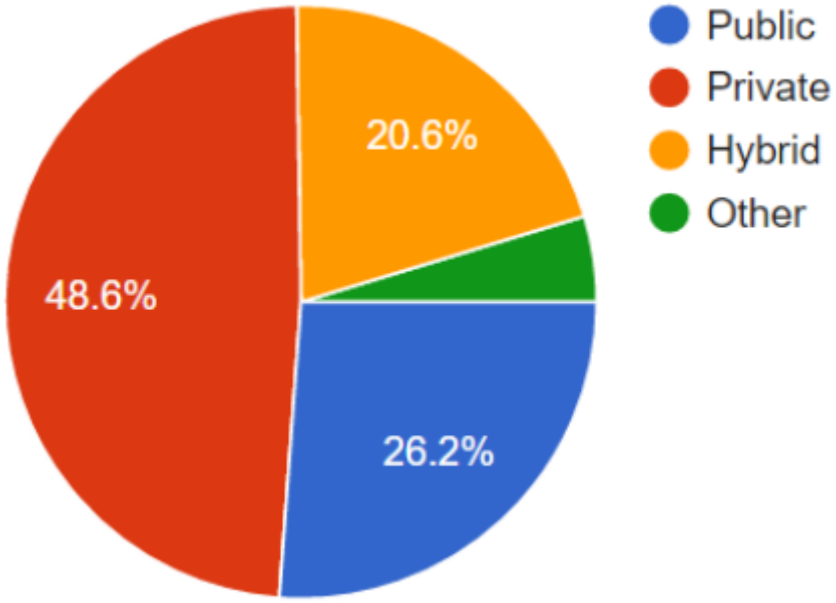

Fig. 3: Cloud models deployed in surveyed institutions

3.3.2. Limitations in PaaS:

Although PaaS platforms provide flexibility for developers in educational institutions to accelerate development of new SaaS applications and migrate them to the cloud. However, the developers might face some challenges when using PaaS platforms.

First, the cost is increased due to adding some new features enable developers to add and control own cloud-based applications. Another serious problem that faces PaaS users is lock-in programming models and high-level services with the vendor who provides service. These models and services are depending on particular environment and need to be completely rewritten when migrating to another PaaS environment. This less portability reduces user's freedom to migrate to another platform.

On the other hand, despite the fact that developers are able to build and control their applications on top of the platform, but they don't know any think about security below the platform which still is assigned by the service provider.

3.3.3. Limitations in IaaS:

Compared with first two service models, IaaS provides for user better control on security issues. The main factor should be considered the reliability of stored data in the provider's resources. The duty of IaaS model security is divided between service providers and their customers. The provider's responsibility involves main security controls such as physical and virtual environmental security. In turn, the cloud user is responsible for applying the suit security controls associated with software including operating system, developed applications

and data. Virtualization technology is a fundamental of IaaS model. In a virtualization environment, when users are utilizing the shared infrastructure resources, this may lead to a cross-tenant attack. In this case, the attacker gains root-level access and then penetrates most of the tenants' accounts in the cloud.

3.4. Security Challenges and Risks:

Organizers in education sector are wishing to use cloud services that are not radically different from those services that totally managed within their own centers[10]. However, they are in fact facing a range of substantial new challenges. This section addresses the critical security and privacy-related challenges and risks in cloud computing. To understand and successfully address the cloud security issues and its challenges in higher educational institutions, we need to investigate various aspects of cloud challenges such as threats, risks, and attack models. Challenges in cloud computing are categorized into four main aspects; Network, Access control, Cloud infrastructure, and Data Security. Table 1 below describes most of the possible attacks threaten cloud computing services.

TABLE 1: TRADITIONAL THREATS ON CLOUD COMPUTING[3]**.**

Threats	Risk Description
DoS	In Denial-of-Service attack, the attacker flooding the server with traffic in order to make services or resources unavailable to cloud users.
DDoS	A Distributed Denial of Service attack is an attempt to make services unavailable by overwhelming it with traffic from multiple machines that are distributed across the Internet.
MitM	A Man-in-the-Middle attack is a type of eavesdropping attack where an intruder inserts himself into a conversation between two parties, intercepts sensitive information from users, and then passes it to the third party.
IP Spoofing	IP Spoofing is a way to gain unauthorized access to the server, whereby an attacker illegally impersonates an IP address of trusted host to conceal his identity.
Packet Sniffing	Packet sniffer or analyzer is commonly used to diagnose network-related problems. However, an attacker to capture and analyze all transmitted sensitive information can also use it.
Port Scanning	Attacker sends queries to search for vulnerable ports on the server and attempts to identify kind of used service.
Session Hijacking	An attacker can hijack an active session and masquerade as one of the conversation parties.
Phishing	Phishing is the attempt to steal sensitive user data such as usernames, passwords, and credit card details. It occurs when an attacker, impersonate an identity of a trusted entity and fools a victim to open an email, or reading an instant message.

4. CONCLUSION

Cloud computing represents an opportunity for universities to take advantages of the enormous benefits of cloud services and resources in the educational process. However, the cloud users remain concerned about security issues that represent the major obstacle that may prohibit the adoption of cloud computing on a large scale. In this paper, the authors have provided an overview of cloud computing benefits for key stakeholders in the higher educational institution. The limitations of cloud service models were investigated in addition to challenges and risks threaten cloud computing. This study shows that the stakeholders are not familiar with possible security risks or procedures used to protect data or cloud application. Furthermore, it indicates that the most serious attacks might threaten cloud

networks are Denial of Service (DoS) and phishing attacks. A comprehensive list of recommendations has been provided to avoid security risks efficiently when adopting cloud computing in educational institutions.

In the future research, the security risks and challenges of virtualization technology will be covered in details to provide a secure infrastructure for IaaS service in the Educational cloud. In addition to focusing on improving QoS provided in cloud computing.

REFERENCES

1. A. Tarhini, K. Al-Gharbi, A. Al-Badi, and Y. S. AlHinai, "An Analysis of the Factors Affecting the Adoption of Cloud Computing in Higher Educational Institutions," *Int. J. Cloud Appl. Comput.*, 2018, doi: 10.4018/ijcac.2018100104.
2. A. Al-Badi, A. Tarhini, and W. Al-Kaaf, "Financial Incentives for Adopting Cloud Computing in Higher Educational Institutions," *Asian Soc. Sci.*, 2017, doi: 10.5539/ass.v13n4p162.
3. K. H., F. M., M. R., and H. Fajraoui, "Cloud Computing Security Challenges in Higher Educational Institutions - A Survey," *Int. J. Comput. Appl.*, 2017, doi: 10.5120/ijca2017913217.
4. NIST, "The NIST Definition of Cloud Computing," 2016.
5. P. Sheela Gowr and N. Kumar, "Cloud computing security: a survey," *Int. J. Eng. Technol.*, 2018, doi: 10.14419/ijet.v7i2.21.12439.
6. H. Srivastava and S. A. Kumar, "Control Framework for Secure Cloud Computing," *J. Inf. Secur.*, 2015, doi: 10.4236/jis.2015.61002.
7. D. G. Pal, "A Novel Open Security Framework for Cloud Computing," *Int. J. Cloud Comput. Serv. Sci.*, 2012, doi: 10.11591/closer.v1i2.371.
8. K. Van Der Schyff and K. Krauss, "Higher Education Cloud Computing in South Africa: Towards Understanding Trust and Adoption issues," *South African Comput. J.*, 2014, doi: 10.18489/sacj.v55i0.254.
9. F. Arron, "7 Different Types of Cloud Computing Structures," 2017. https://www.uniprint.net/en/7-types-cloud-computing-structures/ (accessed Sep. 08, 2018).
10. R. Parveen and E. Chikhaoui, "Legal issues and challenges in educational cloud computing in the kingdom of Saudi Arabia," *Int. J. Econ. Res.*, 2017.