COPY RIGHT

IJIEMR Transactions, online available on 05th Jul 2023. Link

:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 06

10.48047/IJIEMR/V12/ISSUE 06/13

Title **Cloud Security for Education Sector**

Volume 12, ISSUE 06, Pages: 81-86

Paper Authors **Dr. Rinkey,Dr. Raino Bhatia**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

Cloud Security for Education Sector

Dr. Rinkey, Asst Prof,AIMT,Ambala City

Dr. Raino Bhatia, Principal,Akal College of Education,Eternal University,H.P.

Abstract: Implementing rules and solutions for cloud security is necessary to maintain regulatory compliance while safeguarding data, infrastructure, and assets from attack. Additionally, cloud security for the education sector becomes essential when any school system makes use of software-based cloud services that combine private and public delivery models. Without a doubt, cloud computing has altered the way that education is conducted worldwide. It improves instruction and learning while giving students and teachers alike access to a variety of learning resources.

Working together, communicating, and sharing technologically advanced information helps ensure that both students and teachers gain the same advantages from it. As more and more colleges avidly adopt cloud computing, it is crucial that security threats like data breaches and thefts be taken into account. It has extremely effective security systems integrated into university and institution operating models, such as installing CASB solutions offered by Cloud Access Security Brokers. To protect sensitive educational data and comply with security regulations, these services ought to be implemented.

Keywords: Cloud ,Security,Learning,CASB,Education etc.

1.Introduction

Most colleges and universities now use cloud computing, and many more will follow. Organisations can use resources that are far better than they could otherwise afford thanks to cloud computing. Additionally, it makes working remotely for instructors and students simpler.

While some educational institutions may find cloud computing intimidating, many have historically been hesitant to accept significant technological advances. If they want to stay competitive in the education sector and give their staff and students the improved experience that many now expect, they will need to change.

The majority of emerging technologies (ETs) still face significant security challenges. Emerging technologies may facilitate human activities and processes, but they also have some security flaws that frequently prevent their widespread use. Data storage has undergone several changes as a result of cloud technology, for both consumers and businesses. Although cloud storage, access, and recovery options are flexible, they are nevertheless subject to the same security risks as other ETs. Concerns have been raised regarding client privacy and data integrity in the cloud. When data is outsourced to the cloud, it is vulnerable to numerous types of assaults, including identity spoofing, data leakage, data tampering, repudiation, and denial of service (DOS) attacks. The security and integrity of cloud data may be jeopardised by these attacks, which are frequently organised by both insiders and outsiders. The majority of educational institutions have converted their data to digital form, which is then sent to the cloud and controlled by a third party. The study investigates the effects of cloud security issues on education while taking into account the sacred nature of educational data. The results demonstrate how important security is to the effective use of cloud computing in the educational sector. It also demonstrates how many educational institutions are reluctant to use cloud services due to the expanding security risks connected with cloud computing technologies. Therefore, in order to effectively combat both current and emerging cloud threats, all stakeholders, especially cloud vendors, must regularly enhance their cloud security systems. This would significantly improve customer trust and loyalty, protect their integrity and privacy, and make using the cloud safer.

2.Cloud Security:

Information technology security, or IT security, is the process of putting into place safeguards and systems to securely protect and preserve information (department and personal data, conversational information, still images, moving images, and multimedia presentations, including those yet to be conceived) using the various technologies created to create, store, use, and exchange such information against any unauthorised access, misuse, malfunction, or other irregularity. The management of people, processes, and technology with rigorous policies that protect data and applications running in the cloud is called cloud security. In order to fully protect the data, a department must first analyse how it processes and stores it before developing a tailored strategy. Employing the best cloud security practises is essential for any modern department because departments rarely have the budget to do significant harm to their reputation. Similar to how security has developed for all new technology and

breakthroughs, cloud security has changed. Having a cloud incident response plan in place is essential to lessen the effects of suspicious activity and minimise damage in the unfortunate event that a department experiences such a breach.

3.Cloud Security Challenges:

- Security: Data privacy is the main issue since users have no control over where their data is stored and are unaware of where it is.

- Interoperability: There is a high risk of vendor lock-in because there is no global consensus on cloud computing.

- Control: There are many different levels of control that a cloud user has over the cloud environment.

- Performance: All access to the cloud is done via the internet, introducing latency into each communication between the environment and the user.

- Reliability: Many of the current cloud infrastructures rely on commonly available hardware, which is known to fail suddenly.

- Performance of Language specific: Some cloud environments only support a limited number of systems and languages.

4.Cloud Security Issues in Education:

Cloud computing has security issues that may prevent consumers from enjoying the advantages of the technology. Cloud dangers do not exclude users in the educational sector. These dangers frequently originate from both the cloud architecture and the many network infrastructures that clients use to access cloud services. Customers of cloud services typically use the internet to connect to the cloud infrastructure, and some of these networks are susceptible to corruption and a variety of assaults, including malware injection, phishing, eavesdropping, and data leakage. When data is transported, stored, or processed and falls into the wrong hands, it is considered a security breach in cloud computing. As a result, if the network or server is not safeguarded, it may make the cloud service more vulnerable to assaults.

5.Cloud security benefits in Education:

- **24×7 Visibility:** The top cloud security solutions, like AppTrana, provide round-the-clock monitoring of cloud-based assets and applications. This enables organisations to continuously monitor their risk posture and the effects it has on users.

- **Effective protection against DDoS Attacks :** The most effective defence against DDoS attacks, which are growing in quantity, size, sophistication, and intensity, is offered by cloud security solutions. DDoS attacks are continuously monitored, recognised, analysed, and mitigated with the aid of cloud computing security. Such solutions can fend off volumetric, low-level, and sluggish attacks thanks to their built-in redundancies, customization options, flexibility, scalability, and intelligence.

- Data Security: Data security is built into the top cloud computing security solutions. To stop unauthorised parties from obtaining private data, they have security methods and policies in place, such as strict access controls and data encryption.
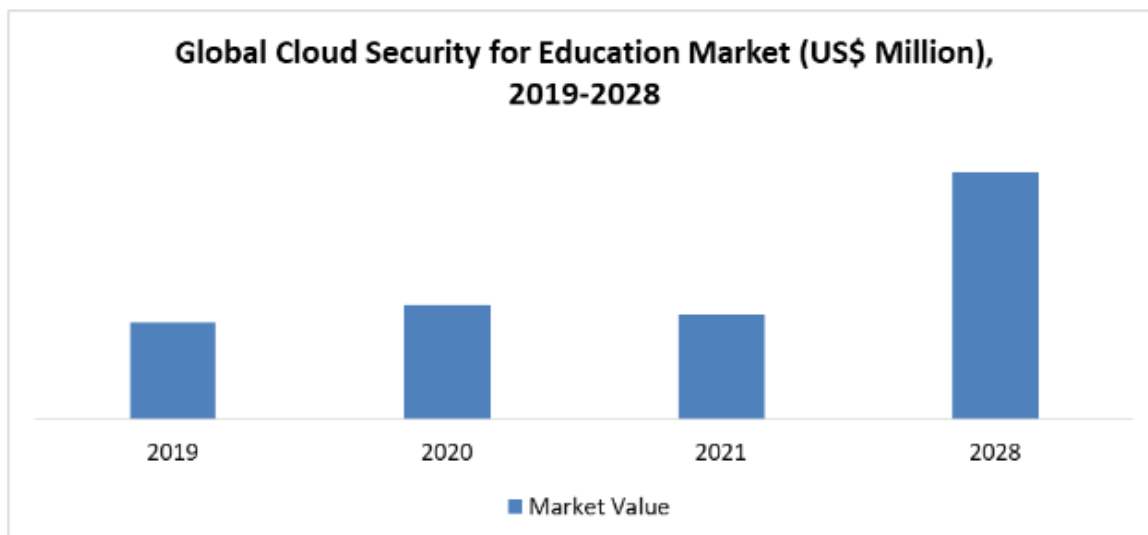

Fig1. *Source: DataM Intelligence Analysis (2021)*

Access to educational services can be made from anywhere at any time thanks to cloud security solutions that use the internet as a conduit. In a single, cohesive setting, all participants in the educational system are brought together. There is less need for onsite servers because schools can invest in multi-cloud solutions.

Instead, schools may allocate their resources more wisely with the help of secure cloud solutions. In fact, it is clear why cloud security products are the ideal option for advancing education when you consider the breadth and depth of the benefits.

Conclusion:

The study shows that cloud computing is a huge force in education, but consumers are still quite concerned about some of the security issues it presents. Cloud security concerns jeopardise cloud users' privacy and confidentiality and prevent the successful adoption of cloud technology in education. According to the report, the cloud provides students, teachers, and educational institutions with various chances for exploring and experiencing online learning, as well as potential for cost-effectiveness and reduction, communication, and cooperation. For the sake of efficiency, several academic institutions have moved their operations to the cloud. However, the growing security concerns with cloud computing may deter educational institutions from implementing the technology. In order to remove cloud threats, it is necessary to strengthen the cloud security system. Customers will be able to take advantage of cloud technology to its full potential in this way. It will also go a long way towards giving students the pertinent IT skills they need to improve their employability, productivity, and competitiveness in a world of work that is more digital. The use of cloud technology will be significant in the future of education, but in order to maximise its advantages, stakeholders must find a method to address the security concerns that come with it.

References

[1]. Aminur M.D. I; Faisal, B.A.K;, Shakib-Uz-Zaman. K; Md. Tarek H.; Farruk, A. (2017). Cloud Computing In Education: Potentials and Challenges for Bangladesh. International Journal of Computer Science, Engineering and Applications (IJCSEA), 7 (5), 11-17.

[2]. Anthony, B. and Syed, M. R. (2011). An overview of the security concerns in Enterprise Cloud Computing. Int. J. of Network Security & Its Applications (IJNSA), 3 (1), 30-45.

[3]. Arsalan, I. and Hina, S. (2014). Data Integrity Issues in Cloud Servers. Int. Journal of Computer Science Issues, 1 (3), 118-121.

[4]. Behrend, T., Wiebe, E.N., London, J., & Johnson, E. (2011). Cloud computing adoption and usage in community colleges. Behavior & Information Technology, 30 (2), 231-240.

[5]. Brandl, D. (2010, January). Don't cloud your compliance data. Control Engineering, 57(1), 23.

[6]. Chuleeporn, C. et al (2014). Students" Perceptions of Cloud Computing. Issues in Info. systems.15, 312-322.

[7]. Crucial Cloud Hosting (2014). Cloud Computing in Education: Introducing Classroom Innovation. Retrieved online via: http://www.crucial.com.au Accessed August, 2019.

[8]. CloudTweeks (2010, January). Plugging into the cloud. Retrieved from http://www.cloudtweaks.com/cloud-diagrams. Accessed August, 2019.

[9].Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance. Retrieved from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[10].Edeh, M.O. (2019a). Integration of Emerging Technologies in Teaching and Learning Process in Nigeria: The Challenges. Central Asian Journal of Mathematical Theory and Computer Sciences, 1 (1), 35-39.