



REVIEW ARTICLE

Review on Cloud Security and Challenges on Higher Education

**Khalid, Muhamad Irwan Ihfan¹ and Zolkipli, Mohamad Fadli¹*

¹School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

*Corresponding author: muhamad_irwan_ihf@soc.uum.edu.my

Received: 15/05/2021, Accepted:24/04/2022, Published: 30/04/2022

Abstract

Many new developments are often plagued with security concerns. Although emerging innovations have all the potential to change systems and people's lives, security issues hinder their adoption and usage. The transformations of data management brought by cloud technologies have helped both individuals and companies. While the cloud allows data storage, connectivity, and recovery stability, it is not immune to the security threats that other new technologies pose. Concerns have been presented over the protection and privacy of cloud users' data. Data leakage, data manipulation, condemnation, a Lack of Services assault, impersonating personalities, also unauthorised access to data are all examples of activities which can appear while data is outsourced to a cloud. Individuals and organisations will orchestrate these attacks, which will jeopardise the reliability and security of cloud networks. The vast majority of colleges and universities are digitising their records, which are then stored in the cloud and handled by a third party. Despite the sacred importance of educational information, the study explores the impact of cloud security problems on schooling. According to the findings, security is crucial for the secure migration and application of cloud technology in the educational sector. It also shows that the growing security threats associated with cloud technology can prevent many education institutions from using cloud services.

Keywords: Cloud technology, Cloud Security, Educational, Information leakage, Privacy

Introduction

The use of emerging technologies in education is becoming increasingly common around the world. The evolution of new technology is transforming all aspects of the instructional process, including classroom design, curriculum quality, methodologies, student participation, and assessment (Edeh,2019a). Cloud networking, mobile computing, distributed computing, artificial intelligence, the internet of things, big data, block chain, and wearable devices have all had a huge impact on education around the world. These technologies have a variety of appealing

characteristics that make them appealing and powerful teaching and learning tools. Cloud Computing evolution has led the model away from conventional IT procurement and toward a more flexible, agile, and open method in the cloud. The cloud is now being used by most modern organisations and agencies, including educational institutions, to outsource their records.

Data recovery and cost savings was made easier in the cloud, reducing the burden of data processing. Education is one of the industries that cloud computing has had a major impact on. To automate operations, connectivity, and storage, many educational organisations have turned to cloud platforms. Today, millions of people use cloud technologies for educational purposes all over the world. In an educational environment, cloud computing will have a greater range of advantages (Al-Issa, Ottom, Tamrawi 2019). Cloud computing is becoming more common with businesses as a way to reduce costs and boost profits (Mohanta, Jena, Panda, Sobhanayak 2019). Also Cloud computing, according to Kumar and Goyal (2019), is Internet-based computing in which applications, shared services, and knowledge are made accessible to devices on demand. However, using the cloud computing model may have both positive and negative implications on user data protection.

The current state of cloud computing is discussed in this article, with an emphasis on security problems and concerns in higher education, as well as current activities. In this paper is organised: Section 2 delves into the literature review; Section 3 delves into the benefits, security concerns, and problems of current cloud technologies in higher education; Section 4 delves into the solutions and practises used to address the issues; and finally, Section 5 delves into the study's thesis and possible work.

Materials and Methods

Cloud computing infrastructure provides a variety of tools that aid in the accomplishment of educational goals. It is widely available, which makes it much more useful for integrating technology into every educational environment. Several reports on cloud deployment to education have been conducted, and all tend to believe that cloud is an important educational tool, but protection remains a problem that must be addressed in order to maximise its benefits. According to Tabrizchi and Rafsanjani (2020), Cloud - based apps are mainly used for teamwork, content distribution, networking, and accessing educational activities, and higher education is rapidly embracing Cloud services because of the economic benefits, speed, agility, accessibility, and elasticity. Nassif et al., (2021) gave an outline of current learning architectures and addressed concerns regarding how higher education institutions manage cloud computing services. He also provided rationales for the difficulty of indexing online tools for maximum search ability by learners and lecturers. Nassif, Talib et al., (2021) offer a thorough overview of cloud computing in higher education. Tabrizchi and Rafsanjani (2020) investigates how cloud computing can be used effectively in higher education institutions. He concentrated on the educational technologies of cloud computing and how they would be supported in a sensible state.

A study of cloud infrastructure security issues in higher education institutions was conducted by Bharati et al., (2021). He discovered that computer protection threats are the most significant barrier to cloud computing adoption in higher education, and cloud users are worried about security concerns, which he believes is the most significant barrier to cloud computing adoption on a wide scale. Chitturi & Swarnalatha (2020), for example, conducted research on "data confidentiality problems in cloud servers." They discovered that one of the most pressing issues for developers today is the privacy of user data on cloud servers. Sun (2020) looked at how cloud technology should be used in education. Cloud computing, according to the report, provides an interface, forum, and educational resources that provide an accessible and creative learning atmosphere; an environment that enables cooperation between all participation of learners as well as between various educational institutions, which improves educational efficiency.

Sun (2020) conducted a report on Cloud Computing Adoption with in higher Education Sector. "Cloud storage is taking centre stage in academia because of its many benefits," he concluded, adding that "many learning institutions use multiple cloud-based technologies to help their students and employees accomplish both instructional and business-related activities, as well as to increase their productivity." Shabbir et al., (2021) also looked at the use of cloud computing in higher education. His results demonstrate that the cloud will allow students, professors, faculty, parents, and employees gain on-demand access to critical information from any laptop, at any time. According to the preceding, the documentation on cloud technology is increasing, but it seems there is a gap in the literature on the impact of cloud protection issues on higher education. The aim of this research is to close the void.

Results and Discussion

Advantages of Cloud Technology

That cloud computing appeals to a wide range of individuals and organisations, from start-ups, telecommunications providers, educational schools, corporations, government agencies, and even begin. It provides consumers with many benefits and expense savings, allowing them to save vast sums of money that should have been spending on data storage facilities and infrastructure. The cloud-enabled operations depicted in Figure 1 are just a few sources of cloud technology's vast functionality in the education system, as well as other human endeavours. The benefits of cloud in education, according to Sun (2020), are as follows:



Figure 1. Cloud Computing Resources (Sun, 2020)

Data sharing is also a distinct aspect of cloud computing. The opportunity to exchange files lays the groundwork for creating instructional resources archives that are accessible to all students. Sharing resources among teacher aids in the dissemination and reuse of educational materials (Shabbir et al.,2021). For today's higher educational setting, cloud computing is critical. It would improve the use and application of technologies in the teaching and learning process, as well as ensuring that education is connected and collaborative. The cloud makes schooling more

interactive and flexible. It extends the boundaries of education and training far beyond confines of schools and classrooms. As a result, cloud technology is unquestionably one of the innovations that would have a major impact on higher education.

Cloud Computing and Higher Education

The educational ecosystem from around global is constantly changing and evolving, owing to major challenges posed by attempts to incorporate modern and innovative technology and learning environments into their teaching and learning processes (Balani et al., 2020). Admittance, enrollment, instruction, and record keeping are only a few of the many aspects of education that have become technological. Cloud computing services can be used to boost competitiveness in almost all areas of education. According to Balani et al., (2020), the cloud computing paradigm supports both faculty and learners as well as academic institutions. Students, faculty, administrative assistants, assessment division, and entry branch are among the clients of an educational cloud system, according to Sun (2020), shown in Figure 2.

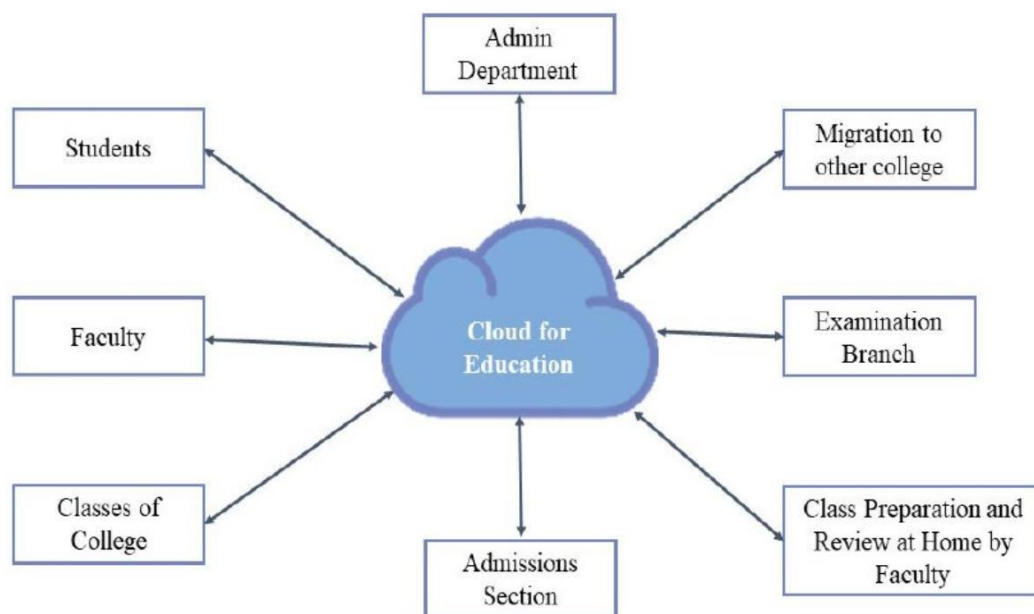


Figure 2. Cloud System in educational Setting (Sun, 2020)

According to Ari et al., (2019), cloud technology enables teachers with a simple and scalable interface to plan course lectures, workshops, conferences, and papers, and also the ability to work at anywhere and do their own computers to complete tasks, prepare on-line exams, grade, and schedule classes. Cloud learning also has potential to play a significant role in the digital educational future. To satisfy the need for using new technology in education, higher education institutions will also have to adopt the cloud. According to Alsaadi et al., (2020), schooling is a guiding factor for cloud computing improvement. Cloud computing provides a variety of services to customers, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), many of which are useful in the educational field. Today's "cloud" systems, such as "Microsoft" and "Google," provide free resources to students and faculty at educational institutions, such as email, contact lists, schedules, database collection, document formation and distribution, and the ability to build websites (Sheik and Maple 2019). The proper use of cloud technologies makes it easier to integrate technology into curriculum. Cloud computing infrastructures, according to Balani et al., (2020), facilitated the introduction of various technical

technologies in education, and its facilities and services could be accessed by colleges on request. Teachers may use cloud tools to help them plan a teaching portfolio, a lecture on teaching to a local audience, a conference presentation, or a draught for publishing (Sun, 2020).

Students and employees can conveniently access educational tools from the cloud using cloud software such as Microsoft Office 365. Cloud computing infrastructure is assisting the idea of Massive Open Online Courses (MOOCs). The usability of teaching resources contained in the cloud allows teachers to quickly enhance their content areas. The widespread use of mobile devices in recent years is a development that is often paired with cloud technology (Balani et al., 2020). Computer computing, smartphone learning, immersive learning, and remote schooling are all aided by cloud technologies. Mobile technologies, such as smartphones and laptops, are widely used by students (Edeh, 2019a), and they can conveniently access valuable cloud-based content. Increased access to educational opportunities has the potential to improve students' academic success. Cloud storage also helps to modernise learning by easing the transition from conventional to revival pedagogical, which accommodates diversity in education and learning.

Cloud Security Challenges

Cloud computing's acceptance and spread are being hampered by security problems. It's because several people have become more weary of the cloud as a result of privacy concerns. Despite the numerous advantages of cloud technology, there appear to become some significant concerns about cloud information security all over the board. Many of the main features to make cloud storage so appealing have not only put the current security infrastructure to the test, but also have revealed security challenges (Tabrizchi and Rafsanjani, 2020).

According to Chitturi and Swarnalatha (2020), cloud computing it would skyrocket in the not-too-distant future, increasing cloud services exposure to viruses, worms, hackers, and cyberattacks because organised crime, terrorists, and foreign groups would see that as a new concept to try and steal private information, disrupt services, and cause damage to an organization. Many security issues exist in cloud computing, most of them are still present in all the other new technologies. Dependent on the network service model in operation, these threats and vulnerabilities take different types. Several analysts already documented a variety of cloud protection problems. Alsaadi et al., (2020), for example, outlined cloud problems in a Table 1.

Table 1. Cloud Security Challenges (Alsaadi et al., 2020).

Security	The main issue is security and privacy: people just have no idea where your data is kept and also have no control of it.
Interoperability	Since no uniform cloud standard has been developed, there is a major risk to vendor support.
Control	The amount of influence a cloud customer has over their world varies significantly.
performance	Any cloud connectivity is achieved across the internet, which introduces latency into every connection between infrastructure and the customer.
Reliability	Many current cloud infrastructures depend on commodity hardware that has a history of failing at inopportune times..
Performance of Language specific	A few cloud systems only accept a limited number of platforms and language.

Cloud Security Issues in Education

Customers rely heavily on technology to link to cloud computing, and most of these services are vulnerable to data theft, Denial of Service, collecting information, spoofing, malware injection, and phishing. Information leakage is a common security problem in cloud storage, and it occurs when

sensitive information gets into the wrong hands while being transmitted, recorded, or analysed (Sasubilli et al., 2021). As a result, whether the network or server is not secure, it will make cloud services more vulnerable to attacks. According to Jonathan (2018), the following are the most important security issues faced by higher education institutions that use various clouds in Table 2.

Table 2. Cloud Security Issues in Education (Jonathan, 2018).

Poor visibility	Each cloud provider takes a different approach to protection, making uniform policies and realistic visibility extremely difficult.
No integration or coordination	Piecemeal and isolated security precautions are common..
Reactive security	Schools can't afford to be reactive in their defence policy in this age of zero-day attacks and shrinking intrusion-to-breach windows.

Solving Cloud Security Challenges

Individuals and organisations must assess the risks associated with cloud platforms before adopting them. This is because, as analysts try to address emerging cloud security concerns, new threats arise, making it even more difficult to address cloud security issues. This suggests that cloud providers must devote more resources to data protection in order to maintain their customers' confidence and loyalty. Institutions who wish to outsource your information to the cloud can take the following measures to check and appreciate cloud protection offered by a cloud service provider, according to Sun (2020), as quoted Kumar and Goyal (2019) like Understanding the cloud begins with an understanding of how the cloud's peculiar loose arrangement impacts the confidentiality of data submitted there. This requires a thorough understanding of how cloud computing transmits and manages data, Demand Transparency by confirming that now the cloud service provider is able to accept routine security audits and will offer specific details on its security architecture. An autonomous entity or federal government should conduct the daily security audit, Strengthen internal protection by ensuring that the service provider's internal security technology and policies, such as firewalls and access control lists, are robust and compatible with cloud security protocols, and Consider the Legal Consequences by understanding how rules and legislation can impact whatever you upload to the cloud. Also Keep an eye on any developments or improvements in cloud technology and procedures that could have an effect on the protection of your files (Kumar and Goyal, 2019).

To prevent data loss in higher education institutions, Balani et al., (2020) proposed that the university's I.T. centre host the SaaS programme on its own personal server or instal it on infrastructure servers offered by trusted third-party providers including Amazon, Google, and others. The following steps are recommended by the current report to better mitigate cloud protection risks Access Control, the use of digital signatures and hashes, and the use of intrusion prevention systems are only a few examples. Encryption that is solid A strong regulatory mechanism to punish hackers is in place. Authentication and Authorization are two terms that are used interchangeably. Users' awareness of cloud protection issues should be raised. In the event of a catastrophe, you should have a backup of your data. To prevent insider attacks, proper screening of employees and users is needed. Network and server policing on a physical level.

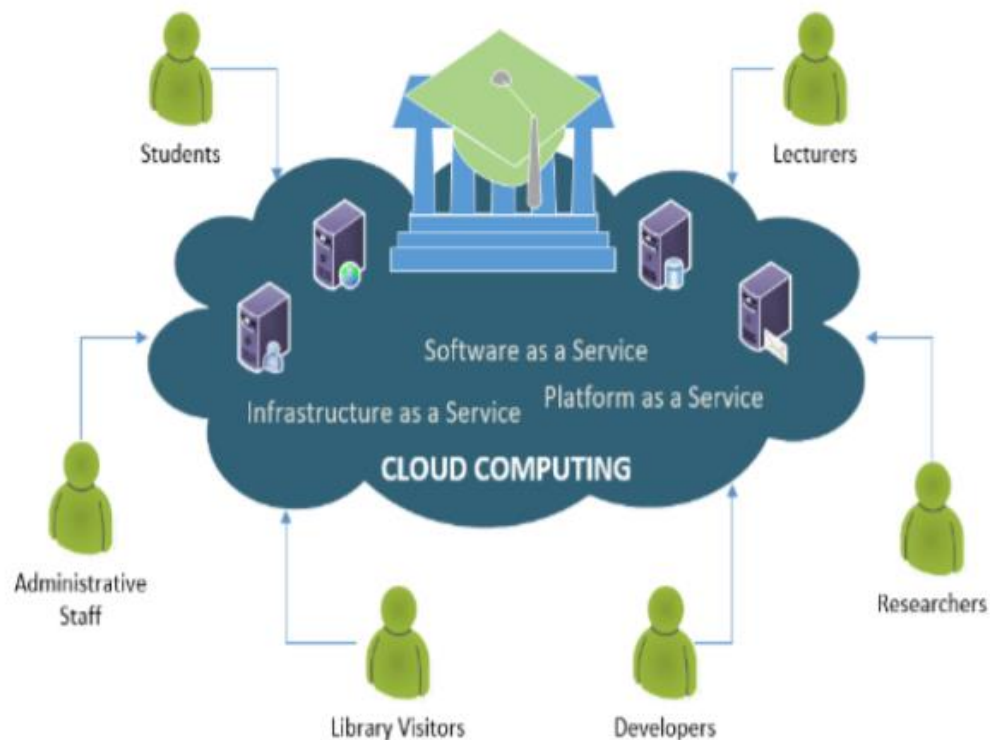


Figure 3. Stakeholders of Cloud in an Educational Institution (Balani et al., 2020).

To ensure a better cloud for present and future generations, the stakeholders displayed in Figure 3 must work diligently and collaboratively. Educational agencies are also responsible for funding studies into future cloud-related technologies. To encourage partnerships, there needs to be a greater partnership among universities, research organizations, and cloud service providers, especially in the area of defence.

Conclusion

Cloud computing is becoming a power in education, consumers are still concerned about security issues. Cloud protection challenges inhibit its use of cloud technologies in education and jeopardise cloud users' privacy and confidentiality. The study concludes that cloud computing provides several educational advantages to students, educators, and academic institutions, include resources for educational technology discovery and experience, cost savings and elimination, networking, and cooperation. Several educational establishments already moved to the cloud to make their operations more effective.

However, the growing security problems in the cloud have the potential to deter educational institutions from implementing the technology. As a result, in order to remove cloud attacks, it is necessary to improve the cloud protection infrastructure. People will be able to reap the full benefits of cloud computing as a result of this. It will also go a long way toward equipping students with requisite I.T skills to improve student employment prospects, success, and competition in today's digital workplace.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and University Utara Malaysia.

References

- Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. *Journal of healthcare engineering*, 2019.
- Alsaadi, Elham Mohammed Thabit A, Fayadh, Sabah Mohammed, & Alabaichi, Ashwak. (2020). A review on security challenges and approaches in the cloud computing. *AIP Conference Proceedings*, 2290(1). <https://doi.org/10.1063/5.0027460>
- Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Mohamadou, A., & Gueroui, A. M. (2019). Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges. *Applied Computing and Informatics*.
- Balani, Zina, & Varol, Hacer. (2020). Cloud Computing Security Challenges and Threats. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–4.
- Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and Challenges of Cloud Integrated IoMT. In *Cognitive Internet of Medical Things for Smart Healthcare* (pp. 67-85). *Springer, Cham*.
- Chitturi, A. K., & Swarnalatha, P. (2020). Exploration of various cloud security challenges and threats. In *Soft Computing for Problem Solving* (pp. 891-899). *Springer, Singapore*.
- 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.
- Elzamly, A., Messabia, N., Doheir, M., Abu Naser, S., & Elbaz, H. A. (2019). Critical Cloud Computing Risks for Banking Organizations: Issues and Challenges. *Religación. Revista de Ciencias Sociales y Humanidades*, 4(18), 673-682.
- Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, 8, 100107.
- Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33, 1-48.
- Jonathan, N. (2018). Overcoming multi-cloud Security Challenges in Education. Published by FORTINET. Retrieved from online via www.fortinet.com/blog/industry-trends/overcoming-multi-cloud-security. Accessed August, 2019.
- Nassif, A. B., Talib, M. A., Nassir, Q., Albadani, H., & Albab, F. D. (2021). Machine Learning for Cloud Security: A Systematic Review. *IEEE Access*.
- Rizwan, Syed, & Zubair, Muhammad. (2019). Basic Security Challenges in Cloud Computing. 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), 1–4. <https://doi.org/10.1109/ICEEST48626.2019.8981695>

- Sasubilli, Manoj Kumar, & R, Venkateswarlu. (2021). Cloud Computing Security Challenges, Threats and Vulnerabilities. 2021 6th International Conference on Inventive Computation Technologies (ICICT), 476–480. <https://doi.org/10.1109/ICICT50816.2021.9358709>
- Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access*, 9, 8820-8834.
- Sheik, A.T, & Maple, C. (2019). Key Security Challenges for Cloud-assisted Connected and Autonomous Vehicles. *Living in the Internet of Things (IoT 2019)*, 17. <https://doi.org/10.1049/cp.2019.0142>
- Stergiou, C., & Psannis, K. E. (2020). Recent advances delivered in mobile cloud computing's security and management challenges. In *Modern principles, practices, and algorithms for cloud security* (pp. 21-43). IGI Global.
- Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 160, 102642.
- Suthar, F., Khanna, S., & Patel, J. (2019). A Survey on Cloud Security Issues. *International Journal of Computer Science Engineering*, 7, 120-123.
- Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, 76(12), 9493-9532.
- Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2020). Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure. *IEEE Access*, 8, 123044-123060.

How to cite this paper: Khalid, Muhamad Irwan Ihfan & Zolkipli, Mohamad Fadli (2022). Review on Cloud Security and Challenges on Higher Education. *Malaysian Journal of Applied Sciences*, 7(1), 1-9.