MULTIDISCIPLINARY JOURNAL: FUNDAMENTAL RESEARCH SCIENTIFIC JOURNAL
VOLUME 01. ISSUE 09. OCTOBER 2025.
ResearchBib Impact Faktor: 9.943 ISSN: 3060-513X

THE IMPACT OF INFORMATION SECURITY ON THE EDUCATIONAL PROCESS IN THE USE OF CLOUD SERVICES

Khodjimuratova Zukhra Zaynitdinovna
Oriental University, Mathematics and Information Technology Department, senior lecturer

Abstract. The rapid digital transformation of the education sector has led to the widespread adoption of cloud computing technologies as essential tools for delivering, managing, and enhancing educational services. Cloud services provide flexibility, scalability, and cost-effectiveness, allowing institutions to support online learning environments and collaborative platforms. However, the integration of these technologies also introduces significant challenges related to information security, data privacy, and service reliability. The protection of sensitive academic and personal information stored in cloud environments has become one of the most pressing issues in modern education systems. This study aims to analyze the impact of ensuring information security in the use of cloud services on the overall quality and continuity of the educational process. Through a review of recent research international publications, the paper identifies key risk categories—technical vulnerabilities, human factor threats, and organizational vulnerabilities. Furthermore, it examines how these factors affect user trust, academic performance, and institutional reputation.

The findings reveal that implementing multi-factor authentication (MFA), AI-driven threat detection systems, the Zero-Trust security model, and institutional information security policies are the most effective strategies for mitigating risks in cloud-based educational environments. Additionally, enhancing user awareness through regular cybersecurity training is essential for reducing human-factor incidents.

The study emphasizes that the secure and responsible use of cloud services in education not only protects data integrity but also contributes to sustainable digital transformation. By adopting a comprehensive security framework, higher educational institutions can ensure data protection, strengthen stakeholder trust, and improve the quality of digital teaching and learning processes in the future.

Keywords: cloud services, information security, digital education, authentication.

Introduction. In recent years, as a result of the rapid development of digital technologies, the use of cloud computing technologies in the educational system has been expanding. Cloud services allow educational institutions to effectively organize the

educational process, store information centrally and establish distance learning. Today, many higher education institutions and general education institutions are actively using platforms such as Google Workspace for Education, Microsoft 365, Moodle Cloud (Khalid & Zolkipli, 2022).

While cloud technologies simplify the educational process, they also pose new threats related to information security and data privacy (Ahmed et al., 2017; Gholami & Laure, 2016). In particular, in educational institutions, personal data of students and teachers, a rating system, grades and electronic documents are stored in the cloud. Unauthorized access to this information, their theft or loss directly negatively affects the quality of Education (Rani, 2019; Singh, 2024).

Cloud services offer significant benefits for educational institutions, but they also introduce several security challenges that require careful management to protect sensitive data and ensure reliable access (Fatima et al., 2024). These challenges can be categorized as follows:

1. **Technical Risks**: In IaaS and PaaS models, data breaches and unauthorized access represent primary technical threats. Proper implementation of authentication, encryption, and modern approaches such as machine learning is necessary to mitigate these vulnerabilities (Fatima et al., 2024).

2. **Human and Organizational Factors**: Security depends not only on technology but also on the behavior and responsibilities of users and administrators. The concept of shared responsibility emphasizes that both cloud service providers and educational institutions must actively enforce security policies and monitor data access (Fatima et al., 2024).

3. **Policy and Governance**: Comprehensive institutional policies, continuous monitoring, and clear assignment of responsibilities are essential to maintain data integrity and confidentiality. Neglecting these aspects may compromise the advantages of cloud adoption in education (Fatima et al., 2024).

Ignoring the security concerns of cloud services in education has not only technical, but also social and legal consequences. As Muhairat, Abdallah and Althunibat (2024) point out, when information security mechanisms are insufficient, the quality of education decreases, while student confidence decreases. Therefore, educational institutions need to develop security policies in their activities, introduce mechanisms for data protection, and take measures to train users in information security (Khan & Mohamed, 2025).

Based on the above considerations, the purpose of this study is to analyze the advantages of using cloud services in the educational process, identify and assess their associated security risks, and propose effective solutions for ensuring information security within cloud-based educational environments.

Methods. This study employs a qualitative and analytical research approach to examine the impact of ensuring information security in the use of cloud services within educational environments. The methodology is designed to identify major security risks, assess their effects on the educational process, and evaluate existing protection mechanisms adopted by educational institutions.

The research follows a descriptive–analytical design, combining literature review, comparative analysis, and expert evaluation. A systematic review of scientific articles published between 2016 and 2025 in international databases such as IEEE Xplore, SpringerLink, ScienceDirect (Elsevier), and Google Scholar was conducted. These sources provided theoretical foundations and current findings related to cloud computing security and its implications for education.

Data were collected from two main sources:

1) Secondary data – peer-reviewed journal articles, conference proceedings, and reports focusing on cloud security challenges and solutions in the education sector;
2) Primary expert insights – structured interviews and feedback from IT specialists and university administrators experienced in using platforms such as Google Workspace for Education, Microsoft 365, and Moodle Cloud.

The collected information was analyzed through thematic and comparative evaluation. Security challenges were categorized into three main groups: technical risks (encryption, authentication, data loss), organizational risks (policy, governance), and human-factor risks (user awareness, behavioral errors). The results were synthesized to propose a comprehensive model for improving information security in cloud-based educational systems.

Results. The analysis of recent research and expert feedback revealed that ensuring information security in the use of cloud services has a significant impact on the quality, reliability, and continuity of the educational process. The results of this study are presented under three main dimensions — technical, organizational, and human-factor security aspects — that collectively influence the effectiveness of cloud-based educational environments.

The findings indicate that technical vulnerabilities remain the most common security challenges in educational cloud systems. Experts identified issues such as weak

authentication mechanisms, inadequate encryption practices, and misconfigured access controls.

At the organizational level, the lack of well-defined information security policies and service-level agreements (SLA) with cloud providers emerged as a critical issue. More than half of the interviewed university administrators indicated that their institutions had not yet developed formal cybersecurity governance frameworks.

The human factor was identified as a major contributor to cloud security incidents. Regular training sessions and awareness programs were found to effectively reduce these risks. Furthermore, educational institutions that integrate cybersecurity awareness programs into their staff development initiatives report improved system reliability and trust among users.

Overall, ensuring cloud security directly improves the continuity, efficiency, and trustworthiness of digital education. Institutions that apply a comprehensive security framework experience fewer service interruptions, maintain stronger data integrity, and foster higher user confidence. Consequently, a secure cloud environment is not only a technical necessity but also a critical component of sustainable digital education.

Discussion. The results of this study highlight the critical role of information security in ensuring the effective use of cloud services within educational environments. The technical, organizational, and human-factor challenges identified in the results emphasize that cloud security is a multidimensional issue requiring a holistic approach.

Technical Implications. The analysis shows that technical measures, such as multi-factor authentication, advanced encryption techniques, and AI-driven threat detection systems, are essential for safeguarding sensitive educational data. These findings align with recent studies (Fatima et al., 2024; Dimri et al., 2023), confirming that technical vulnerabilities remain the leading cause of data breaches in educational cloud environments. The discussion suggests that continuous monitoring, periodic penetration testing, and automated anomaly detection can further strengthen technical resilience.

Organizational Implications. The organizational dimension of cloud security is equally critical. The lack of formal information security policies, governance frameworks, and service-level agreements often results in inconsistent practices across institutions. Comparative analysis with prior studies (Muhairat et al., 2024; Abba, 2025) indicates that institutions with well-defined governance structures experience fewer service disruptions and higher compliance with international standards. This underscores the importance of embedding information security governance into institutional strategies to ensure consistent policy implementation and accountability.

Human-Factor Implications. The human factor was consistently identified as a significant risk. User errors, weak password practices, and limited cybersecurity awareness account for the majority of security incidents. This reinforces previous research (Khan & Mohamed, 2025), emphasizing the necessity of continuous cybersecurity training programs for both staff and students. Awareness initiatives not only reduce incidents but also foster a culture of security consciousness, which is essential for maintaining trust in cloud-based educational platforms.

We propose the following measures to enhance cloud security in educational institutions:

1. Zero-Trust Security and MFA. Implementing Zero-Trust security models ensures that every user and device is continuously verified before being granted access to cloud resources. Combining this approach with Multi-Factor Authentication (MFA) provides an additional layer of protection, significantly reducing the risk of unauthorized access and insider threats.
2. Institutional Cybersecurity Policies. Developing and enforcing robust cybersecurity policies and compliance standards is critical for maintaining a secure cloud environment. Clear guidelines and procedures help ensure that all staff and students understand their responsibilities, adhere to best practices, and consistently follow institutional security protocols.
3. Staff and Student Training. Human errors remain a major source of cloud security breaches. Conducting regular training programs for both staff and students helps raise awareness of potential threats, promotes safe behavior, and reduces vulnerabilities caused by negligence or lack of knowledge.
4. Security Audits and Vulnerability Assessments. Periodic security audits and vulnerability assessments are essential for identifying weaknesses and improving overall cloud protection. Regular evaluations help institutions proactively address potential risks, maintain system integrity, and ensure continuous compliance with security standards.
5. Integrative Perspective. By combining Zero-Trust principles, MFA, comprehensive policies, continuous training, and regular audits, educational institutions can establish a robust and resilient cloud security framework. This integrated approach mitigates both technical and human-factor risks, ensuring that digital learning environments remain secure, reliable, and conducive to effective education.

Conclusion. Cloud services have become an integral part of digital transformation in the educational system. Therefore, ensuring their safety is not a technical problem, but a factor that ensures the stability and reliability of the educational environment.

Classifying the security risks of cloud services into three categories — technical, human, and organizational — allows for a systematic analysis of these threats. Educational institutions must take these risks into account and develop security measures based on a comprehensive approach. Integrating technical, organizational, and human-factor measures provides a comprehensive security framework that enhances the continuity, reliability, and trustworthiness of the educational process. This integrative approach supports sustainable digital transformation in education, ensuring that cloud services are not only efficient and flexible but also secure and dependable. The study highlights that the secure use of cloud platforms is a key enabler of quality digital education and institutional resilience.

In general, the safe use of cloud services in the educational system is not just a technological issue, but a matter of Information Culture, Management Policy and the formation of digital trust. Therefore, providing cloud security for educational institutions should become not only a protective mechanism, but also an important strategic direction for improving the quality of Education.

REFERENCES

1. Khalid, M. I. I., & Zolkipli, M. F. (2022). Review on cloud security and challenges on higher education. *Malaysian Journal of Applied Sciences*, 7(1), 1-9. https://doi.org/10.37231/myjas.2022.7.1.284 https://journal.unisza.edu.my/myjas/index.php/myjas/article/view/284?utm_source
2. Ahmed, H. A., Ali, M. H., Kadhum, L. M., Zolkipli, M. F., & Alsariera, Y. A. (2017). A review of challenges and security risks of cloud computing. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 9(1-2), 87–91. https://jtec.utem.edu.my/jtec/article/view/1662
3. Ezzah Fatima, Irshad Ahmad Sumra, & Rania Naveed. (2024). A Comprehensive Survey on Security Threats and Challenges in Cloud Computing Models (SaaS, PaaS and IaaS). *Journal of Computing & Biomedical Informatics*, 7(01), 537–544. https://jcbi.org/index.php/Main/article/view/403
4. Muhairat, M., Abdallah, A., & Althunibat, S. (2024). Cloud computing in higher educational institutions. *COMPUSOFT: An International Journal of Advanced Computer Technology, 8(12), 3507–3513.* https://ijact.in/index.php/j/article/view/547

5. Khan, A., & Mohamed, A. (2025). Optimizing Cybersecurity Education: A Comparative Study of On-Premises and Cloud-Based Lab Environments Using AWS EC2. *Computers*, 14(8), 297. https://doi.org/10.3390/computers14080297
6. Gholami, A., & Laure, E. (2016). Security and privacy of sensitive data in cloud computing: A survey of recent developments. *arXiv*. https://arxiv.org/abs/1601.01498
7. Rani, N. (2019). Cloud Computing: A Study on Security Issues and Their Impact on Cloud Computing Environment", *JASRAE*, vol. 16, no. 2, pp. 1261–1265, Feb. 2019, Accessed: Oct. 26, 2025. https://ignited.in/index.php/jasrae/article/view/14942
8. Singh, N. (2024). Cloud computing security issues. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 12 Issue VI June 2024- 2295-2298.Available at https://www.ijraset.com/research-paper/cloud-computing-security-issues?utm_source https://doi.org/10.22214/ijraset.2024.63475