Engineering and Scientific International Journal (ESIJ)
Volume 13, Issue 2, April – June 2026
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Cloud Security in Educational Institutions: Threats, Countermeasures, Compliance and the Role of AI in Safeguarding Digital Learning Infrastructure in Zambia

Samani Fred Ikasaya[*1], Dr. J. Arockia Venice[2]
[1]*Student, DMI St. Eugene University, Zambia*
[2]*Professor, DMI St. Eugene University, Zambia*

Abstract —The rapid adoption of cloud computing in educational institutions has transformed the possibilities for scalable, cost-effective digital learning infrastructure enabling access to AI-powered learning platforms, collaborative digital tools, and large-scale data analytics that would be impossible in conventional on-premises computing environments. However, cloud adoption also introduces significant cybersecurity risks including data breaches, ransomware attacks, unauthorised access, and compliance failures that educational institutions are frequently ill-equipped to address with limited cybersecurity expertise and constrained IT security budgets. This article examines cloud security threats, countermeasures, and compliance frameworks relevant to educational institutions in Zambia, situating findings within global scholarship on cloud security architecture, AI-powered threat detection, blockchain-based data integrity assurance, and regulatory compliance in digital educational environments. Drawing on a descriptive survey of institutional IT practitioners, educators, and cybersecurity experts, findings identify inadequate access control, insufficient staff digital security training, absence of data encryption protocols, and limited regulatory compliance awareness as primary security vulnerabilities. AI-driven threat detection systems, zero-trust security architecture, and blockchain-enabled audit trails are identified as evidence-based countermeasures. Policy recommendations are presented.

Keywords *— Cloud Security; Cybersecurity; Educational Institutions; Zambia; AI Threat Detection; Blockchain; Data Protection; Compliance.*

1. Introduction

Cloud computing the delivery of computing services including servers, storage, databases, networking, software, and analytics through the internet has become the dominant infrastructure paradigm for educational technology deployment globally (Venice et al., 2025c; Vettriselvan et al., 2025c). Educational cloud platforms enable AI-powered adaptive learning, real-time collaboration, institutional data analytics, and remote learning at scales and costs that on-premises computing cannot achieve making cloud adoption an increasingly essential component of digital education strategy for institutions seeking to leverage AI and digital transformation benefits (Venice et al., 2025b; Arockia et al., 2025; K. G. Gurupriya et al., 2024). In Zambia, the progressive adoption of cloud-based educational platforms including learning management systems, administrative information systems, and digital assessment tools creates a new cybersecurity challenge for institutions whose IT security capacity has not kept pace with their digital infrastructure adoption (Vettriselvan et al., 2025c; Venice et al., 2025a).

AI-powered cybersecurity systems, zero-trust security architecture, and blockchain-enabled data integrity assurance offer technological pathways for addressing cloud security challenges in educational institutions whose limited cybersecurity expertise and budget constraints require automated, scalable security solutions (Venice et al., 2025f; Basha et al., 2025). This article examines cloud security in Zambian educational institutions and identifies evidence-based security improvement strategies.

2. Literature Review

2.1 Cloud Security Threats in Educational Environments

Educational institutions are high-value targets for cybercriminals due to their large repositories of sensitive personal data including learner records, health information, financial data, and research outputs combined with typically limited cybersecurity investment and heterogeneous user populations with variable security awareness (Venice et al., 2025f; Vettriselvan et al., 2025b). Data breaches unauthorised access to and exfiltration of sensitive institutional data through credential theft, phishing attacks, or system vulnerability exploitation represent the most consequential cloud security threat for educational institutions, with potential legal, reputational, and operational consequences (Venice et al., 2025a; Akila et al., 2025; Sreela Sreedhar et al., 2015). Ransomware attacks where malicious actors encrypt institutional systems and demand payment for decryption have caused operational paralysis at multiple educational institutions

DOI: 10.30726/esij/v13.i2.2026.1320020

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

globally, disrupting examination administration, payroll systems, and learning management platforms for extended periods (Venice et al., 2025f; Basha et al., 2025). Insider threats including accidental data exposure by poorly trained staff, intentional data theft by disgruntled employees, and negligent security behaviour generating exploitable vulnerabilities constitute a significant and frequently underestimated cloud security risk in educational institutions where security culture is underdeveloped (Vettriselvan et al., 2025d; Venice et al., 2025b). The shared responsibility model of cloud security where cloud service providers secure the underlying infrastructure while institutional customers are responsible for securing their own data, applications, and access controls is frequently misunderstood by educational IT administrators, creating accountability gaps that leave critical security functions unaddressed (Venice et al., 2025c; Vinodh et al., 2026a).

2.2 AI-Powered Threat Detection and Response

AI-powered cybersecurity systems represent a fundamental advancement in the capacity of resource-limited educational institutions to detect and respond to sophisticated cloud security threats (Venice et al., 2025f; Akila et al., 2025). Machine learning-based anomaly detection systems that continuously analyse network traffic, user authentication patterns, and data access behaviour can identify unusual activities indicative of credential theft, insider threat, or active intrusion generating security alerts in real-time rather than after damage has occurred (Venice et al., 2025b; Devi et al., 2025).

AI-powered threat intelligence platforms that aggregate vulnerability data, attack pattern information, and threat actor behaviour from global cybersecurity feeds provide educational institutions with actionable intelligence about emerging threats relevant to their specific cloud architecture (Venice et al., 2025a; Venice et al., 2025d). Zero-trust security architecture which eliminates the assumption that users within institutional network perimeters are inherently trustworthy, requiring continuous verification of all access requests regardless of origin represents the contemporary gold standard for cloud security design in educational institutions (Venice et al., 2025f; Vinodh et al., 2026a). AI-powered identity and access management systems that implement zero-trust principles through continuous authentication, behavioural biometrics, and risk-based access control substantially reduce the attack surface available to credential-based intrusion attempts (Venice et al., 2025b; Basha et al., 2025).

2.3 Blockchain for Data Integrity and Audit

Blockchain technology offers significant potential for enhancing data integrity assurance in educational cloud environments providing tamper-proof, immutable records of all data access, modification, and transmission events that support both security auditing and regulatory compliance demonstration (Rajeswari et al., 2026; Venice et al., 2025d). Blockchain-enabled audit trails that record all administrative actions on sensitive learner and institutional data including data access, export, modification, and deletion events provide forensic evidence for security incident investigation and regulatory compliance verification that conventional logging systems cannot reliably provide (Venice et al., 2025c; Akila et al., 2025).

Blockchain-based credential verification systems that enable instant, tamper-proof verification of educational qualifications without requiring institutional record requests address a significant vector for credential fraud in educational environments (Venice et al., 2025b; Rajeswari et al., 2026).

2.4 Regulatory Compliance and Governance

Data protection regulatory compliance encompassing national data protection legislation, sector-specific education data governance requirements, and international frameworks such as GDPR for institutions with international partnerships is a significant and frequently neglected dimension of educational cloud security (Vettriselvan et al., 2025d; Vinodh et al., 2026a).

In Zambia, the Electronic Communications and Transactions Act and the Data Protection Act create legal obligations for educational institutions handling personal data in cloud environments obligations that many institutions are currently unaware of or inadequately positioned to fulfil (Venice et al., 2025f; Vettriselvan et al., 2025c). AI-powered compliance management platforms that continuously monitor institutional cloud configurations for regulatory compliance violations and automatically generate remediation recommendations substantially reduce the expertise burden of regulatory compliance management for institutions without dedicated compliance specialists (Venice et al., 2025b; Venice et al., 2025d).

3. Methodology

A descriptive survey was employed to examine cloud security threats, countermeasures, and compliance in Zambian educational institutions. Mixed methods combined structured questionnaires administered to 30 institutional IT practitioners and security-responsible administrators, key informant interviews with 10 cybersecurity experts, and analysis of publicly available institutional data breach incident reports (Kombo & Tromp, 2014; Orodho & Kombo, 2012). Data collection instruments measured cloud security vulnerability awareness, implemented countermeasure assessment,

DOI: 10.30726/esij/v13.i2.2026.1320020

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

regulatory compliance knowledge, and technology adoption. Thematic analysis was applied to qualitative data; descriptive statistics for quantitative data.

4. Findings and Analysis

4.1 Cloud Security Vulnerability Profile

Security vulnerability assessment revealed significant weaknesses across all surveyed institutions: multi-factor authentication was implemented by only 35% of respondents; data encryption for data in transit and at rest was confirmed by 28%; formal cloud security policies were in place in 40% of institutions; and regular security awareness training for all staff was conducted by fewer than 20%. These vulnerability patterns are consistent with the attack surfaces exploited in documented educational institution data breaches globally (Venice et al., 2025f; Akila et al., 2025).

4.2 Threat Experience and Incident Response

Security incident experience was prevalent among respondents: 65% reported at least one phishing-related incident in the preceding 12 months; 30% reported unauthorised system access attempts; and 15% reported ransomware incidents of varying severity.

Incident response capacity was severely limited only 22% of institutions possessed a documented cybersecurity incident response plan, and fewer than 15% had conducted incident response simulations (Venice et al., 2025b; Basha et al., 2025).

4.3 AI and Blockchain Security Tool Awareness

Awareness of AI-powered threat detection systems was low (28% of respondents); blockchain security applications were essentially unknown (8%). However, interest in adopting AI security tools was high among respondents who were made aware of their capabilities (82%), indicating significant readiness to adopt AI security technologies if institutional procurement support and implementation guidance were available (Venice et al., 2025a; Venice et al., 2025f).

4.4 Regulatory Compliance Knowledge

Regulatory compliance knowledge was severely limited: only 35% of respondents demonstrated adequate awareness of Zambia's data protection legislation provisions relevant to educational cloud environments. GDPR awareness was minimal despite several institutions maintaining international student and research partnerships subject to European data protection requirements (Vettriselvan et al., 2025d; Vinodh et al., 2026a).

5. Discussion

The cloud security vulnerability profile documented across Zambian educational institutions reveals a systematic mismatch between cloud adoption pace and security investment institutions are progressively migrating sensitive learner and institutional data to cloud platforms while leaving foundational security controls inadequately implemented. AI-powered threat detection, zero-trust access management, and blockchain audit trail systems offer scalable, automated security capabilities that can substantially improve institutional security posture without requiring proportional increases in cybersecurity specialist staffing (Venice et al., 2025f; Akila et al., 2025; Rajeswari et al., 2026).

6. Conclusion and Recommendations

Recommendations: (1) mandate multi-factor authentication and data encryption for all educational cloud deployments (Venice et al., 2025f; Basha et al., 2025); (2) deploy AI-powered threat detection and behavioural analytics systems (Venice et al., 2025b; Akila et al., 2025); (3) implement zero-trust security architecture for institutional cloud environments (Venice et al., 2025f; Vinodh et al., 2026a); (4) establish blockchain-enabled audit trail and credential verification systems (Rajeswari et al., 2026; Venice et al., 2025d); and (5) develop mandatory cybersecurity awareness training and regulatory compliance education for all institutional cloud users (Vettriselvan et al., 2025d; Venice et al., 2025a).

References

[1] Akila, V., Prabhu, G., Akila, R., & Swadhi, R. (2025). Performance metrics in blockchain-enabled AIML for cognitive IoT in large-scale networks. In AI for large scale communication networks (pp. 265–288). IGI Global Scientific Publishing.

[2] Arockia, V. J., Vettriselvan, R., Rajesh, D., Velmurugan, P. R. R., & Cheelo, C. (2025). Leveraging AI and learning analytics for enhanced distance learning. In AI and learning analytics in distance learning (pp. 179–206). IGI Global Scientific Publishing.

[3] Ashifa, K. M. (2019). Developmental initiatives for persons with disabilities. Indian Journal of Public Health Research & Development, 10(12), 1257–1261.

[4] Ashifa, K. M. (2020a). Effect of substance abuse on physical health of adolescents. European Journal of Molecular & Clinical Medicine, 7(2), 3155–3160.

[5] Ashifa, K. M. (2020b). Physical health hazards of schizophrenia patients. Systematic Reviews in Pharmacy, 11(12), 1848–1850.

[6] Ashifa, K. M. (2021a). Analysis on the determinants of health status among tribal communities. Journal of Cardiovascular Disease Research, 12(3), 531–534.

[7] Ashifa, K. M. (2021b). Health status of primitive tribal women in India. Journal of Cardiovascular Disease Research, 12(5), 772.

[8] Ashifa, K. M. (2022). A situation analysis of the social well-being of elderly during the COVID-19 pandemic. International Journal of Health Sciences, 6(3), 10156–10163.

[9] Ashifa, K. M., & Ramya, P. (2019). Health afflictions and quality of work life among women working in fireworks industry.

DOI: 10.30726/esij/v13.i2.2026.1320020

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

International Journal of Engineering and Advanced Technology, 8(6S3), 1723–1725.
[10] Basha, R., Pathak, P., Sudha, M., Soumya, K. V., & Arockia Venice, J. (2025). Optimization of quantum dilated convolutional neural networks: Image recognition with quantum computing. Internet Technology Letters, 8(3), e70027.
[11] Devi, M., Manokaran, D., Sehgal, R. K., Shariff, S. A., & Vettriselvan, R. (2025). Precision medicine, personalized treatment, and network-driven innovations. In AI for large scale communication networks (pp. 303–322). IGI Global.
[12] Elkin, N., Mohammed, A. K., Kılınçel, Ş., Soydan, A. M., Tanrıver, S. Ç., Çelik, Ş., & Ranganathan, M. (2025). Mental health literacy and happiness among university students. Frontiers in Psychiatry, 16, 1541316.
[13] K. G. Gurupriya, Dr. A. S. Aneeshkumar, (2024). A Survey on Ciphertext Policy Attribute-Based Encryption Scheme based Cloud E- Healthcare Secure Framework, International Journal of Intelligent Systems and Applications in Engineering, 12(22), pp. 953–959.
[14] Gayathri, R. K., Vettriselvan, R., Rajesh, D., Balakrishnan, R., Kumar, R., & Kavitha, J. (2025a). Striking a balance: Mental health challenges and work-life integration among women faculty in Indian B-Schools. Texila International Journal of Public Health, 13(2).
[15] Gayathri, R. K., Vettriselvan, R., Rajesh, D., Balakrishnan, R., Kumar, R., & Kavitha, J. (2025b). Strategic role of human resource management in enhancing occupational health and safety practices. Texila International Journal of Public Health, 13(2).
[16] Jenifer, R. D., Vettriselvan, R., Saxena, D., Velmurugan, P. R., & Balakrishnan, A. (2025). Green marketing in healthcare advertising: A global perspective. In AI impacts on branded entertainment and advertising (pp. 303–326). IGI Global.
[17] Kariveliparambil, A., Rasi, R. A., Ahmad, M. S., Öztaş, N., & Ayan, F. S. (2026a). Evolving social capital in indigenous communities. Journal of Social Service Research, 52(1), 147–166.
[18] Kariveliparambil, A., R A, R., Ahmad, M. S., Ramesh, S., & Kuriakose, A. (2026b). Invisible burdens of platform work. International Journal of Qualitative Studies on Health and Well-Being, 21(1).
[19] Kombo, D. K., & Tromp, D. L. A. (2014). Proposal and thesis writing: An introduction. Paulines Publications Africa.
[20] Meena, G., Vettriselvan, R., Rajesh, D., & Velmurugan, P. R. (2025). Diversity and inclusion: Harnessing the power of inclusivity for business success. In Security and strategy models for key-solving institutional frameworks (pp. 203–234). IGI Global Scientific Publishing.
[21] Mohanbabu, S., & Vettriselvan, R. (2025a). Focusing supply chain and container terminal challenges. International Journal of Procurement Management, 24(1), 92–114.
[22] Mohanbabu, S., & Vettriselvan, R. (2025b). Will machine learning resolve the issues in container management. International Journal of Process Management and Benchmarking, 20(4), 559–575.
[23] Orodho, J. A., & Kombo, D. K. (2012). Research methods. Kenyatta University Press.
[24] Rajeswari, M., Rohini, V., Sathya Aarthi, R., Rameshkumaar, V. P., & Arul Krishnan, S. (2026). Blockchain 2.0 for secure, transparent, and autonomous logistics systems. In R. Vettriselvan & N. Suresh (Eds.), Intelligent motion control for human-centered systems (pp. 233–258). IGI Global Scientific Publishing.
[25] Ranganathan, M., Jacob, A., Ashifa, K. M., Kumar, G. J., Anthony, M., Vijay, M., & Kumari, R. B. (2024). An investigation of the effects of chronic stress on attention in parents of children with neurodevelopmental disorders. Universal Journal of Public Health, 12(1), 37–50.
[26] Rasi, R. A., & Ashifa, K. M. (2019). Role of community-based programmes for active ageing. Indian Journal of Public Health Research & Development, 10(12).
[27] Shanthi, H. J., Gokulakrishnan, A., Sharma, S., Deepika, R., & Swadhi, R. (2025). Leveraging artificial intelligence for enhancing urban health. In Nexus of AI, climatology, and urbanism for smart cities (pp. 275–306). IGI Global.
[28] Swadhi, R., Gayathri, K., Suresh, N. V., Catherine, S., & Velmurugan, P. R. (2025a). Leveraging machine learning for enhanced patient engagement and outcomes. In Impact of digital transformation on business growth and performance (pp. 313–340). IGI Global Scientific Publishing.
[29] Swadhi, R., Velmurugan, P. R., Gayathri, K., & Catherine, S. (2025b). Evolving critical themes in advanced human resource management. In Critical aspects in advanced human resource management (pp. 75–102). IGI Global Scientific Publishing.
[30] Vasantha, S., Swadhi, R., Gayathri, K., Selvalakshmi, V., & UmaDevi, A. (2025). Fostering personalized learning and achieving equity in education. In Transforming education with AI-powered personalized learning (pp. 201–236). IGI Global Scientific Publishing.
[31] Venice, J. A., Arivazhagan, D., Suman, N., Shanthi, H. J., & Swadhi, R. (2025a). Recommendation systems and content personalization. In AI for large scale communication networks (pp. 323–348). IGI Global Scientific Publishing.
[32] Sreela Sreedhar, Varghese Paul, AS Aneeshkumar, (2015). Solitude Conserve Attribute Cryptographic CP-ABFE Data Protocols in Fuzzy Cloud Service Provider, Indian Journal of Science and Technology, 8(25), pp. 1-5
[33] Venice, J. A., Vettriselvan, R., Jain, S., Madusudanan, K., & Aarthy, C. C. J. (2025b). Performance evaluation and metrics in blockchain powered AI/ML. In Transforming education with AI-powered personalized learning (pp. 143–178). IGI Global Scientific Publishing.
[34] Venice, J. A., Vettriselvan, R., Rajesh, D., Suresh, N. V., & Abirami, P. (2025c). Enabling personalized learning and adaptive systems through strategic management. In Bridging academia and industry through cloud integration in education (pp. 49–72). IGI Global Scientific Publishing.
[35] Venice, J. A., Vettriselvan, R., Rajesh, D., Xavier, P., & Shanthi, H. J. (2025d). Optimizing performance metrics in blockchain-enabled AI/ML data analytics. In Enhancing automated decision-making through AI (pp. 97–122). IGI Global.
[36] Venice, J. A., Sripathi, S. K., & Moonga, B. (2025e). Social deviance and the influence of internet exposure. ASET Journal of Management Science, 4(SI-1).
[37] Venice, J. A. A., Jio, W., Kant, S., Sharda, S., & Mittal, S. (2025f). Ethical leadership effect on the regulation of AI in cyber security. In Ethical challenges of AI and warfare (pp. 133–152). IGI Global Scientific Publishing.
[38] Venice, J. A. A., Muthuraman, M., Kant, S., & Mittal, S. (2026). Community engagement effect on school leadership through digital volunteerism. In Strengthening community engagement and school leadership through digital volunteerism (pp. 85–114). IGI Global Scientific Publishing.
[39] Vettriselvan, R. (2025). Harnessing innovation and digital marketing in the era of industry 5.0. In The future of small business in industry 5.0 (pp. 163–186). IGI Global.
[40] Vettriselvan, R., & Anto, M. R. (2018). Pathetic health status and working condition of Zambian women. Indian Journal of Public Health Research & Development, 9(9), 259–264.
[41] Vettriselvan, R., & Rajan FSA, A. J. (2019). Occupational health issues faced by women in spinners. Indian Journal of Public Health Research & Development, 10(1).
[42] Vettriselvan, R., Deepan, A., Jaiswani, G., Balakrishnan, A., & Sakthivel, R. (2025a). Health consequences of early marriage. In Social, political, and health implications of early marriage (pp. 189–212). IGI Global.
[43] Vettriselvan, R., Velmurugan, P. R., Varshney, K. R., EP, J., & Deepika, R. (2025b). Health impacts of smartphone and internet addictions across age groups. In Impacts of digital technologies across generations (pp. 187–210). IGI Global.
[44] Vettriselvan, R., Velmurugan, P. R., Suresh, N. V., & Catherine, S. (2025c). Strategies, best practices, and pitfalls in the era of digital transformation. In Impact of digital transformation on business

DOI: **10.30726/esij/v13.i2.2026.1320020**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

growth and performance (pp. 67–98). IGI Global Scientific Publishing.

[45] Vettriselvan, R., Selvi, K., Kumar, A. S., Ranjani, R. D., & Varshney, K. R. (2025d). Ranking methodologies: Criteria and controversies in global higher education. In Global university ranking systems (pp. 109–140). IGI Global Scientific Publishing.

[46] Vettriselvan, R., Gokuldas, P. G., & Sambamoorthy, N. (2025e). Designing language materials to motivate, engage, and empower learners. In Exploring the psychology of language materials development (pp. 279–302). IGI Global Scientific Publishing.

[47] Vettriselvan, R., Ramya, R., Selvalakshmi, V., Jyothi, P., & Velmurugan, P. R. (2026a). Empowering patients through knowledge: Educational strategies in rehabilitation. In Holistic approaches to health recovery (pp. 263–290). IGI Global Scientific Publishing.

[48] Vettriselvan, R., Velmurugan, P. R., Savariapitchai, M., & Swadhi, R. (2026b). AI and international volunteering. In Impacts of AI on international volunteering (pp. 1–24). IGI Global Scientific Publishing.

[49] Vijayalakshmi, M., Subramani, A. K., Vettriselvan, R., Catherin, T. C., & Deepika, R. (2025a). Sustainability and responsibility in the digital era. In Digital citizenship and building a responsible online presence (pp. 285–306). IGI Global.

[50] Vijayalakshmi, M., Subramani, A. K., Vettriselvan, R., Velmurugan, P. R., & Hasine, J. (2025b). Strategic collaborations in medical innovation and AI-driven globalization. In Navigating strategic partnerships for sustainable startup growth (pp. 85–110). IGI Global.

[51] Vinodh, N., Subramani, A. K., & Vettriselvan, R. (2026a). Navigating ethics, society, and governance in the digital age. In Ethics, justice, and governance in the age of AI and digital societies (pp. 1–26). IGI Global Scientific Publishing.

[52] Vinodh, N., Subramani, A. K., & Vettriselvan, R. (2026b). Transforming the future of management and medical education. In AI education strategies for future-proofing curriculum design (pp. 459–476). IGI Global Scientific Publishing.

[53] Zahoor, H., Mustafa, N., Ashifa, K. M., Safaei, M., & El Gamil, R. (2025). Unlocking resilience: Emotional intelligence and self-leadership shape stress perception among health students. International Journal of Innovation and Learning, 38(4), 395–419.

DOI: **10.30726/esij/v13.i2.2026.1320020**