World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Towards a secure infrastructure-as-a-service adoption in emerging economies: evidence from Kenyan organizations

Moses Oduor Ojwang *, Joshua Agola and Castro Yoga

Department of Computer Science and Software Engineering Jaramogi Oginga Odinga University of Science and Technology, KENYA.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(01), 329–336

Publication history: Received on 20 M 2026; revised on 26 April 2026; accepted on 29 April 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.1.0239

Abstract

The adoption of Infrastructure as a Service (IaaS) is accelerating across organizations in emerging economies, driven by the need for scalable, cost-efficient, and flexible IT infrastructure. However, persistent security concerns including data breaches, regulatory non-compliance, vendor lock-in, and limited organizational readiness continues to hinder secure adoption, particularly in contexts characterized by evolving regulatory frameworks and constrained cybersecurity capacity. Existing cloud security frameworks such as NIST, ISO/IEC 27001, and the Cloud Security Alliance (CSA) Cloud Controls Matrix provide valuable guidance but remain largely generic and insufficiently adapted to the socio-technical realities of developing environments.

This study addresses this gap by proposing a context-aware security model for IaaS adoption in Kenyan organizations. Drawing on a quantitative research design, data were collected from 150 IT and security professionals across 30 organizations. The study integrates key dimensions like security risk management, governance and compliance, organizational readiness, trust, and user awareness into a unified conceptual framework.

The proposed model extends existing literature by bridging the disconnect between technical security controls and organizational adoption factors, offering a holistic and empirically grounded approach to secure cloud adoption. By contextualizing global security standards to local regulatory and institutional conditions, the study provides actionable insights for policymakers and practitioners seeking to enhance cloud security in resource-constrained environments. The findings contribute to advancing cloud security research in emerging economies and support the development of more resilient and adaptive IaaS adoption strategies.

Keywords: Infrastructure as a Service (IaaS); Cloud Computing Security; Trust; Cybersecurity Awareness; Emerging Economies

1. Introduction

The rapid digitization of organizational processes has intensified reliance on cloud computing infrastructures, yet this transition has simultaneously heightened exposure to cybersecurity risks. In Kenya, organizations are increasingly adopting Infrastructure as a Service (IaaS) to enhance scalability, flexibility, and cost efficiency; however, persistent concerns regarding data breaches, regulatory non-compliance, and loss of control over outsourced infrastructure continue to impede secure adoption (Singh, 2020; Alghofaili et al., 2021). These risks are particularly critical given that IaaS forms the foundational layer upon which other cloud service models depend, thereby amplifying the potential impact of security vulnerabilities (Sharma et al., 2019).

* Corresponding author: Moses Oduor Ojwang

Recent studies consistently identify security and privacy concerns as the primary barriers to cloud adoption, including unauthorized access, data leakage, multi-tenancy vulnerabilities, and vendor lock-in (Zhou et al., 2021; Lee & Gupta, 2020). Although global frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and the Cloud Security Alliance (CSA) Cloud Controls Matrix provide structured approaches to mitigating these risks, their applicability in emerging economies remains constrained (NIST, 2022; ISO/IEC, 2021; CSA, 2021). These frameworks are largely designed for environments with mature regulatory systems and advanced technical capacity, limiting their effectiveness in contexts characterized by resource constraints and evolving governance structures.

Furthermore, existing research reveals a fragmentation between technical security models and behavioral adoption frameworks. While security-focused studies emphasize technical controls such as encryption and access management (Alqahtani et al., 2020), adoption models such as TAM and UTAUT focus on perceived usefulness and ease of use, neglecting critical dimensions such as governance, compliance, and risk management (Venkatesh et al., 2021; Almulla, 2021). This disconnects results in incomplete models that fail to capture the socio-technical complexity of secure IaaS adoption.

In the Kenyan context, these challenges are exacerbated by regulatory inconsistencies, limited cybersecurity expertise, and low organizational readiness (Mumo et al., 2020; Mutembei et al., 2022). Despite increasing cloud adoption, there remains a lack of empirically validated, context-specific security models that integrate technical, organizational, and regulatory dimensions.

This study addresses this gap by developing a context-aware security model for IaaS adoption in Kenyan organizations. Specifically, it integrates security controls, governance mechanisms, regulatory compliance, organizational readiness, trust, and user awareness into a unified framework. The study contributes to both theory and practice by bridging global cloud security standards with local implementation realities, thereby enabling more secure and sustainable cloud adoption in emerging economies.

2. Literature Review

2.1. Security Risks and Trust in IaaS Adoption

The literature consistently identifies security risk as the dominant barrier to IaaS adoption. Key concerns include data breaches, unauthorized access, and vulnerabilities associated with shared cloud environments (Jaiswal & Rohankar, 2019; Pallavi, 2020). More recent studies further emphasize the growing complexity of securing cloud environments due to evolving threat landscapes and the dissolution of traditional security perimeters (Hay et al., 2020).

However, this body of work is largely technocentric, prioritizing encryption, intrusion detection, and access control mechanisms while underrepresenting trust and organizational dynamics. Trust in cloud service providers has emerged as a critical determinant of adoption, particularly in environments where data sovereignty and jurisdictional concerns are prominent (Chen et al., 2021; Ranjan & Prakash, 2023). Despite this, trust is often treated as an external variable rather than an integrated component of security frameworks.

2.2. Limitations of Existing Security Frameworks

Table 1 Comparison of Technology Adoption Models (TAM and UTAUT) and Their Relevance to IaaS Adoption

Framework	Focus	Strengths	Limitations	Gap Identified
National Institute of Standards and Technology (NIST Cybersecurity Framework)	Risk-based cybersecurity management across Identify, Protect, Detect, Respond, Recover functions	- Flexible and adaptable across sectors - Strong risk management orientation - Widely adopted and practical guidance - Aligns with other standards	- Not certifiable - Requires interpretation for implementation - Limited prescriptive controls	Lacks explicit cloud-context adaptation, particularly for dynamic and context-aware environments in IaaS

ISO/IEC 27001	Establishment of Information Security Management Systems (ISMS)	- Globally recognized certification - Comprehensive control framework - Strong governance and compliance focus - Supports continuous improvement	- Resource-intensive to implement - Can be rigid and documentation-heavy - Limited real-time threat responsiveness	Does not sufficiently address adaptive, real-time security requirements in cloud-native and IaaS environments
Cloud Security Alliance Cloud Controls Matrix (CCM)	Cloud-specific security controls mapped to industry standards	- Tailored for cloud environments - Provides detailed control mappings - Supports multi-framework alignment - Useful for cloud assurance and audits	- Complex and extensive - Implementation can be challenging for SMEs - Focuses more on compliance than dynamic security	Lacks context-aware and behavioral security mechanisms for evolving threats in IaaS
Governance, Risk, and Compliance (GRC)	Integrated approach to aligning IT with business objectives, risk management, and regulatory compliance	- Holistic organizational perspective - Enhances decision-making and accountability - Integrates risk and compliance processes - Supports strategic alignment	- Not a specific technical framework - Can be overly abstract - Implementation varies widely - May lack technical depth in cybersecurity controls	Insufficient technical granularity and lacks real-time, context-aware enforcement mechanisms for cloud security

Global frameworks such as NIST, ISO/IEC 27001, and CSA CCM provide structured approaches to managing cloud security risks (Alhassan, 2021; Kaur et al., 2020). These frameworks emphasize governance, compliance, and risk management, offering standardized guidelines for organizations.

Nevertheless, recent studies highlight several limitations. First, these frameworks are overly generic and resource-intensive, making them difficult to implement in organizations with limited technical capacity (Nwobodo & Maduako, 2023; Mumo et al., 2020). Second, they assume mature regulatory environments, which may not exist in developing countries (Gitau & Rotich, 2023). Third, they prioritize compliance over usability and contextual adaptation, resulting in partial or ineffective implementation.

Additionally, these frameworks inadequately address human and organizational factors, including user awareness, cultural dynamics, and institutional readiness. This limitation reduces their effectiveness as holistic models for secure cloud adoption.

2.3. Adoption Models and Their Limitations

Table 2 Comparison of Technology Adoption Models (TAM and UTAUT) and Their Relevance to IaaS Adoption

Model	**Construct**	**Definition**	**Relevance to IaaS Adoption**
TAM (Technology Acceptance Model)	Perceived Usefulness (PU)	Degree to which a user believes that using a technology will enhance job performance	Helps assess whether employees perceive cloud services (IaaS, PaaS, SaaS) as improving productivity and efficiency (Buyya et al., 2019; Liu et al., 2020)
	Perceived Ease of Use (PEOU)	Degree to which a user believes that using the technology will be free of effort	Evaluates the simplicity of accessing and using cloud services, and integrating them into existing workflows (Alghofaili et al., 2021; Milhem et al., 2025)
UTAUT (Unified Theory of Acceptance and	Performance Expectancy (PE)	Degree to which using the technology provides benefits in job performance	Measures expected benefits of IaaS adoption for organizational tasks and efficiency (Buyya et al., 2019; Moeti, 2024)

Use of Technology)			
	Effort Expectancy (EE)	Degree of ease associated with using the technology	Evaluates how simple it is for employees to adopt and use cloud services (Milhem et al., 2025)
	Social Influence (SI)	Extent to which individuals perceive that important others believe they should use the technology	Captures peer, managerial, and organizational pressure or support in adopting IaaS (Alghofaili et al., 2021)
	Facilitating Conditions (FC)	Degree to which an individual believes that organizational and technical infrastructure exists to support technology use	Highlights the importance of IT support, infrastructure readiness, and policies for successful cloud adoption (Omar & Mwakondo, 2024; Suliman, 2021)
	Moderators	Age, gender, experience, voluntariness of use	Helps contextualize adoption behavior based on individual differences, especially relevant in diverse organizational environments (Milhem et al., 2025)
Comparison: TAM vs UTAUT	Scope & Applicability	TAM focuses on individual perceptions of usefulness and ease of use, while UTAUT incorporates social influence, facilitating conditions, and moderating factors	UTAUT provides a broader organizational and social perspective, making it more suitable for enterprise-level IaaS adoption studies; TAM is simpler and effective for understanding user acceptance at the individual level (Alghofaili et al., 2021; Milhem et al., 2025)

Technology adoption models such as TAM and UTAUT explain user behavior based on perceived usefulness, ease of use, and social influence (Venkatesh et al., 2021; Kabra et al., 2023). While these models provide valuable insights into behavioral intention, they are limited in their applicability to cloud security.

Specifically, these models do not incorporate security risk, governance, or regulatory compliance as core constructs. Empirical studies demonstrate that adoption decisions in cloud environments are significantly influenced by perceived risk and trust rather than usability alone (Dillon et al., 2020). Consequently, these models provide incomplete explanations of IaaS adoption in security-sensitive contexts.

2.4. Contextual Constraints in Emerging Economies

Emerging economies face unique challenges that are insufficiently addressed in existing literature. These include limited cybersecurity skills, regulatory ambiguity, infrastructural disparities, and dependence on foreign cloud providers (Okeyo et al., 2021; Nyakundi & Kihara, 2021).

Additionally, compliance with data protection regulations remains a significant barrier, particularly in contexts where enforcement mechanisms are evolving (Almorsy, 2022; Office of the Data Protection Commissioner, 2022). These factors highlight the need for context-specific frameworks that align with local regulatory and organizational realities.

2.5. Research Gap

The literature reveals a critical gap in the absence of integrated, context-aware security models that combine technical controls, governance, compliance, trust, and organizational readiness. Existing approaches remain fragmented, addressing these dimensions in isolation. This study addresses this gap by proposing a unified framework tailored to the Kenyan context.

3. Conceptual Model / Framework

This study proposes a multi-dimensional conceptual model for secure IaaS adoption, integrating five key constructs: security risk management, governance and compliance, organizational readiness, trust, and user awareness.

Security risk management encompasses technical controls such as encryption, access control, and threat detection (Alqahtani et al., 2020). Governance and compliance capture alignment with regulatory frameworks and international standards (ISO/IEC, 2021). Organizational readiness reflects infrastructure, skills, and institutional capacity (Kumar et al., 2020). Trust represents confidence in cloud providers (Dillon et al., 2020), while user awareness captures human factors influencing security behavior (Wilkins et al., 2021).

The model posits that secure IaaS adoption is achieved through the integration of these dimensions, rather than isolated implementation. This socio-technical approach extends existing frameworks by incorporating contextual realities specific to emerging economies.

3.1. Conceptual Model.

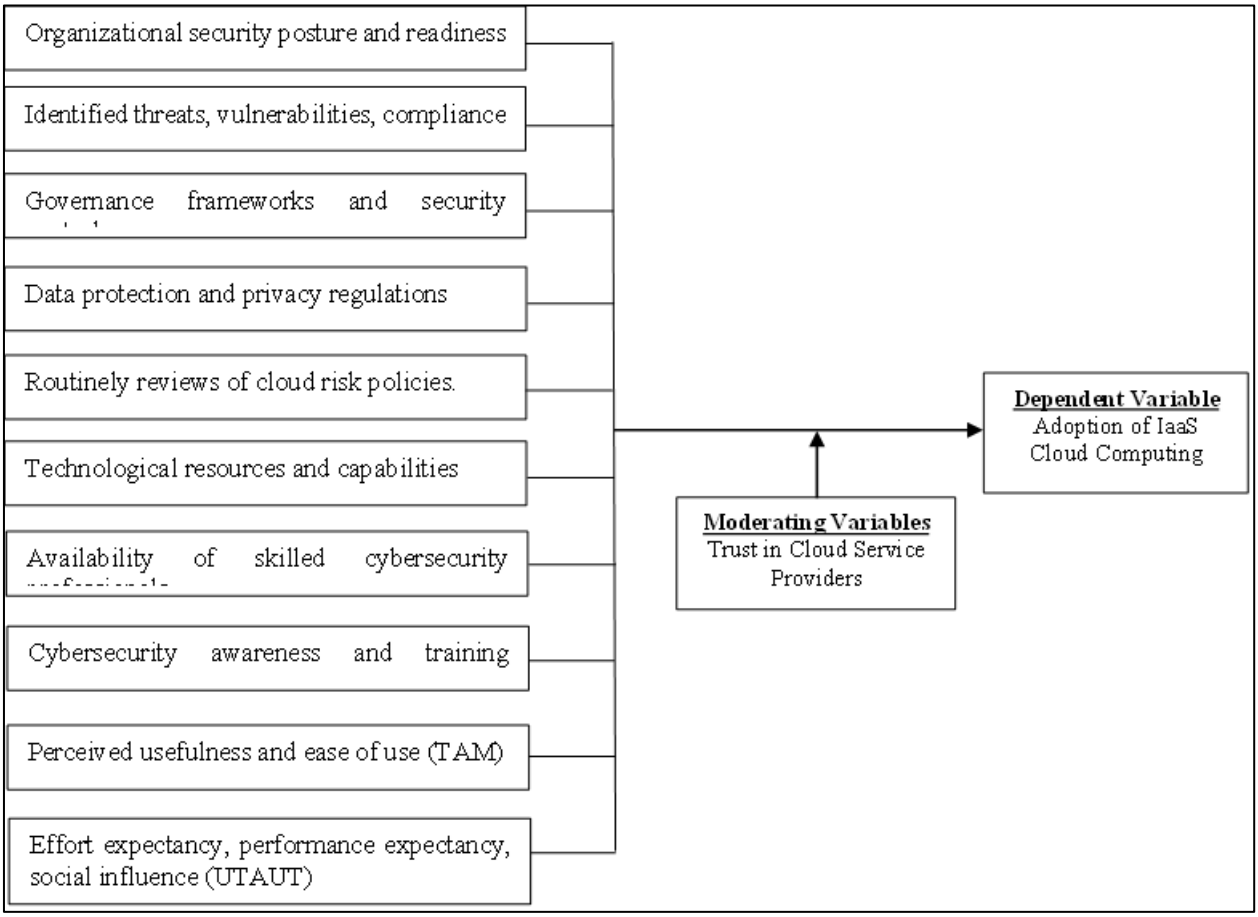

Figure 1 Proposed Conceptual Model for Secure IaaS Adoption

4. Methodology

4.1. Study Design

A quantitative cross-sectional design was employed to examine factors influencing secure IaaS adoption. This approach enabled statistical analysis of relationships between variables and supported empirical validation of the conceptual model (Creswell & Creswell, 2018; Sekaran & Bougie, 2020).

4.2. Population and Sampling

The study targeted organizations in Kenya adopting IaaS, including public institutions, private enterprises, and academic organizations. The unit of analysis comprised IT professionals, security specialists, and decision-makers.

A total population of 240 respondents was identified. Using purposive sampling, participants were selected based on expertise in cloud computing. The sample size of 150 respondents was determined using Yamane's formula (Apuke, 2017; Babbie, 2021).

4.3. Data Collection

Data were collected using a structured questionnaire comprising six sections: demographics, security posture, governance and compliance, awareness, adoption factors, and model relevance. Responses were measured using Likert scales to ensure quantitative analysis.

4.4. Data Analysis

Data analysis included:

- Descriptive statistics (means, frequencies)
- Correlation analysis
- Multiple regression analysis

These techniques enabled evaluation of relationships between independent variables and secure IaaS adoption (Saunders et al., 2019).

4.5. Ethical Considerations

Ethical approval was obtained, and participation was voluntary. Confidentiality and anonymity were maintained throughout the study.

5. Conclusion

The study established that secure adoption of Infrastructure-as-a Service (IaaS) in Kenyan organizations is significantly influenced by an integrated set of factors like security risk management, governance and compliance, organisational readiness, trust and user awareness demonstrating that a holistic, context aware approach is more effective than relying on isolated technical or behavioural models. By empirical validating a unified model tailored to emerging economies, the research bridges the gap between global security standards and local social technical realities offering practical insights for enhancing cloud security adoption in resource constraint environments.

This study benefits organizations by promoting more secure, resilient and trustworthy cloud infrastructures that supports digital transformation and it recommends future work to focus on model development, implementation, policy alignment and continuous adaptation to evolving cybersecurity threats in emerging economies.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest regarding the publication of this paper.

Statement of ethical approval

Ethical approval for this study was obtained from the relevant institutional review body prior to data collection. The study involved human participants (IT professionals and decision-makers), and all procedures complied with ethical standards for research involving human subjects.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Alghofaili, M., Almefleh, A., & Alazab, M. (2021). Evaluating security measures in cloud service providers: A framework approach. Journal of Information Security and Applications, 58, 102709. https://doi.org/10.1016/j.jisa.2021.102709

[2] Alhassan, I. (2021). Enhancing cloud computing security: A review of governance frameworks. Journal of Cloud Computing, 10(1), 15–30.

[3] Almorsy, M. (2022). The impact of privacy and security regulations on cloud computing adoption. IEEE Cloud Computing, 10(1), 37–45.

[4] Almulla, M. (2021). The updated technology acceptance model: Understanding e-learning adoption among university students. International Journal of Educational Technology in Higher Education, 18(1), 1–17. https://doi.org/10.1186/s41239-021-00259-6

[5] Alqahtani, A., Kavakli-Thorne, M., & Kumar, R. (2020). A security risk assessment framework for cloud computing systems. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

[6] Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. Arabian Journal of Business and Management Review, 6(11), 1–8. https://doi.org/10.12816/0040336

[7] Babbie, E. R. (2021). The practice of social research (15th ed.). Cengage Learning.

[8] Buyya, R., Vecchiola, C., & Selvi, S. T. (2019). Mastering cloud computing: Foundations and applications programming. Elsevier.

[9] Chen, X., et al. (2021). Trust management in cloud computing: Challenges and research opportunities. Journal of Cloud Computing, 10(1), 15–27.

[10] Cloud Security Alliance (CSA). (2021). Cloud Controls Matrix (CCM) v4.0. https://cloudsecurityalliance.org

[11] Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

[12] Dillon, T., Wu, C., & Chang, E. (2020). Trust in cloud computing: A systematic literature review. Journal of Cloud Computing, 9(1), 1–24. https://doi.org/10.1186/s13677-020-00156-7

[13] Gitau, M., & Rotich, G. (2023). A framework for cloud computing adoption among public sector organizations in Kenya. International Journal of ICT and Security Research, 15(2), 112–125.

[14] Hay, A., Singh, K., & Prasad, A. (2020). Addressing evolving cloud security challenges in IaaS environments. Cloud Security Journal, 15(3), 33–48. https://doi.org/10.1016/j.csj.2020.100011

[15] ISO/IEC. (2021). ISO/IEC 27001:2022 Information security management systems. International Organization for Standardization. https://www.iso.org/standard/63028.html

[16] Jaiswal, V., & Rohankar, R. (2019). Security challenges in infrastructure as a service (IaaS) cloud models. Journal of Information Security, 8(1), 120–135. https://doi.org/10.4236/jis.2019.81009

[17] Kabra, G., Kaur, K., & Gupta, A. (2023). Exploring the role of cognitive factors in cloud computing adoption using UTAUT. Journal of Cloud Computing, 12(1), 1–14. https://doi.org/10.1186/s13677-023-00334-x

[18] Kaur, A., Gupta, P., & Singh, M. (2020). Implementation of information security management systems in organizations: A review. International Journal of Information Security, 19(2), 113–124. https://doi.org/10.1007/s10207-019-00500-5

[19] Kumar, M., et al. (2020). Cloud adoption maturity models: An organizational readiness perspective. Journal of Information Systems and Technology Management, 17(1), 12–28.

[20] Lee, S., & Gupta, R. (2020). Emerging security challenges in IaaS-based cloud environments. Journal of Security Studies, 14(4), 78–91.

[21] Mumo, M., Wabwoba, F., & Namisango, F. (2020). Factors influencing information security governance in cloud computing: A Kenyan perspective. African Journal of Information Systems, 12(1), 1–15.

[22] Mutembei, J., Mwangi, B., & Kamau, G. (2022). Barriers to cloud computing implementation in SMEs in Kenya. East African Journal of Science, Technology and Innovation, 3(3), 32–44.

[23] National Institute of Standards and Technology (NIST). (2022). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework

[24] Nwobodo, C., & Maduako, J. (2023). Security governance models for cloud computing in emerging economies. Journal of Cloud Computing, 12(1), 18–34. https://doi.org/10.1186/s13677-023-00329-5

[25] Nyakundi, P., & Kihara, A. (2021). Organizational capabilities and cloud computing adoption in Kenya's financial sector. Strategic Journal of Business & Change Management, 8(3), 540–558.

[26] Office of the Data Protection Commissioner. (2022). Annual report 2021/2022. Government of Kenya.

[27] Okeyo, G., Oduor, M., & Mutai, L. (2021). Evaluating trust and risk management in cloud computing adoption: A case of Kenyan government institutions. International Journal of Computer Applications Technology and Research, 10(5), 205–213.

[28] Omar, A. S., & Mwakondo, F. (2024). Evolution of Cloud Computing: Trends, Issues, and Future Directions: A Systematic Literature Review. International Journal of Computer Science Trends and Technology, 12(3), 102-111.

[29] Pallavi, S. (2020). Understanding cloud computing security risks and countermeasures. International Journal of Computer Science and Information Security, 18(5), 48–60.

[30] Ranjan, P., & Prakash, A. (2023). Exploring the role of trust in cloud migration: An empirical investigation. International Journal of Information Management, 68, Article 102394. https://doi.org/10.1016/j.ijinfomgt.2023.102394

[31] Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

[32] Sekaran, U., & Bougie, R. (2020). *Research methods for business: A skill building approach* (8th ed.). Wiley.

[33] Sharma, P., Aggarwal, A., & Goel, S. (2019). IaaS as the foundational layer in cloud computing and its security implications. Journal of Cloud Infrastructure, 7(4), 97–115.

[34] Singh, A. (2020). Cloud computing: Security and privacy challenges. Journal of Cloud Computing and Services, 15(1), 1–17. https://doi.org/10.1007/s13677-020-00245-8

[35] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2021). Unified theory of acceptance and use of technology: A review and research agenda. Journal of Information Technology, 36(3), 227–245. https://doi.org/10.1177/02683962211019564

[36] Wilkins, M., et al. (2021). Bridging the cloud computing skills gap. Journal of Technology and Society, 25(2), 104–118.

[37] Zhou, L., Liu, D., & Zhang, J. (2021). Security challenges and strategies for cloud computing adoption: A systematic review. IEEE Access, 9, 119396–119410. https://doi.org/10.1109/ACCESS.2021.3108917