

Governance at the Edge: Navigating Regulatory, Cloud, and Network-Level Failures in Modern Digital Transformation

Ibrahim A. D. Garba ¹, Tokhirova Sarvinoz Gayratjon kizi ²

¹ Department of Mathematics and Statistics, Federal Polytechnic Mubi, Adamawa State, Nigeria

² Senior Lecturer at Fergana State Technical University, Uzbekistan

Email: ² sarvinozmuxammadjonova2@gmail.com

ARTICLE INFO

Keywords:

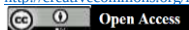
Edge Governance,
Cloud Governance,
Network Security,
Regulatory Compliance,
Digital Resilience.

Vol.01, No.05, 2026

<https://doi.org/10.5281/zenodo.23096280>

Copyright © 2026 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CCBY4.0).

<http://creativecommons.org/licenses/by/4.0/>



ABSTRACT

Digital transformation has moved the organizations from centralized environments to distributed infrastructures that include cloud platforms, edge computing, connected networks, and even more automated services. This shift has brought new challenges in governance and governance issues that go beyond the traditional compliance with regulations, and need to be managed together with security, reliability, operational risk and accountability. This review is a new approach to governance at the edge which combines regulatory, cloud, network, reliability engineering and edge level controls under one roof. Special focus is placed on policy, risk and assurance, which are fundamental governance activities, along with a clear and acceptable framework of accountability, ongoing monitoring, measurable service targets and automated policy enforcement. Shared responsibility models, data lifecycle management, incident governance, routing integrity, service level objectives, and policy as code are emphasized as key concepts in keeping distributed infrastructures reliable and compliant. The regulatory aspects related to cyber security, data protection, operational resilience, and cross border data management are taken into account along with organisational aspects like responsibility matrices, risk assessment, audit evidence and continuous assurance. The examination also includes model driven validation and automated governance, which can be used to enhance consistency and minimize operational gaps in complex environments. But, regulatory evolution, data sovereignty, complexity of automation, lack of transparency, and lack of coordination across organizational boundaries are still major issues. Overall, edge governance should be a coordinated, agile strategy that links technical solutions with accountability and regulatory duties to enable safe and sustainable digital transformation.

Introduction

Governance at the edge (GatE) is the convergence of policy, risk management, security, and operational controls in cloud, edge and networked environments as organizations strive for digital transformation. With distributed digital infrastructures, the governance needs to cover cyber security, data privacy, resilience, compliance and operational accountability in the whole computing environment [1]. Edge computing, combined with cloud services, enables real-time processing, greater geographic reach, and higher reliability, especially in places with connectivity and latency issues and local processing demands. Design and operation of cloud and edge infrastructures are significantly shaped by regulatory governance. The EU's NIS2 Directive and other cybersecurity and cyber resilience frameworks highlight cybersecurity, incident response, risk management, organizational accountability, and fundamental cyber hygiene [2]. Such conditions have an impact on architectural considerations, supplier management, cross border transferring of data, reporting incidents and auditing. This has led to the growing recognition of cybersecurity as a business function instead of one that can be limited to a technical team. Governance, at the organizational level, provides clear ownership and accountability for

information, infrastructure, and risk [3]. Defining data standards, documenting centrally, tracking and assigning roles promote compliance and increase transparency in complex environments. Governance models like three lines of defence and RACI maps can help to define who is responsible within key executive, legal, information technology, security, and operations roles. These mechanisms can aid in facilitating the translation of a general policy goal into specific responsibilities and routine operations [4]. Edge environments pose extra governance risks as infrastructure is spread out across a diverse set of devices, locations, networks and operating conditions. Centralized cloud controls are still relevant for consistency and distributed governance mechanisms must be considered to meet local needs and operational variation. Edge to cloud orchestration and monitoring platforms can help ensure consistent deployment, security management, workload update and policy enforcement at distributed sites [5]. Policy enforcement and automated security and privacy controls can also be built into system development and operations.

1. Conceptual Framework and Regulatory Governance

Proper governance in the modern digital transformation takes an integrated approach in aligning governance, risk management and compliance throughout regulatory, cloud, edge and network environments. The framework aims to break these functions down from their isolation and defines a single system for developing the policy, assessing risk, verifying compliance, and managing operation to ensure ongoing coordination [6]. This ensures continuity, consistency, accountability, and auditability of decisions in hybrid and multi-cloud environments. The conceptual framework is three-fold, namely policy setting, risk management and policy compliance. The creation of policy establishes the requirements and acceptable practices for an organization, risk assessment can be used to identify assets, threats, vulnerabilities and potential impacts, and assurance can be used to determine if controls are effective and conform to regulatory requirements [7]. These functions need to embrace dynamic workloads, distributed infrastructure, the evolving threat landscape, and the need for temporary computing resources in cloud and edge environments. This adaptation can be facilitated by policy as code, automated controls, continuous monitoring and transparent governance (Figure 1) [8]. Defining accountability means having clear ownership and auditable responsibilities. Visibility of policy, configuration and operational decisions is improved. Consistency minimizes misconfigurations through common procedures. Governance mechanisms are flexible and can change as technology and regulations change [9]. Manual errors are minimized, and policies are enforced uniformly throughout distributed systems. These principles interrelate regulatory obligations and security, privacy and operational controls. The European Union has placed growing focus on the cybersecurity, cyber-resilience, incident reporting and risk management of digital and critical infrastructure in its regulatory governance [10]. The NIS2 Directive offers a significant basis for such requirements, which are expanded to other sectors and digital services. It focuses on risk management, incident response, organisational accountability and cyber security requirements relevant to the relevant cloud and digital service providers.

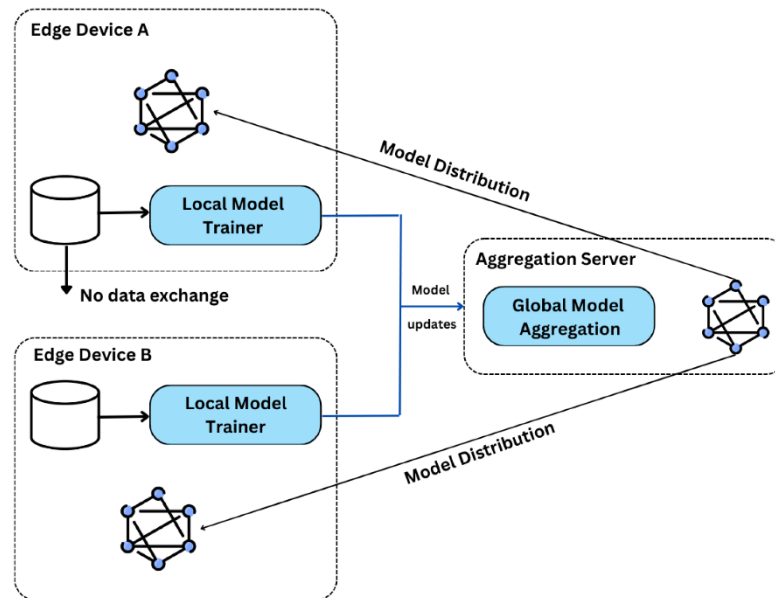


Figure 1. An overview of a federated learning architecture showing distribution between edge devices and an aggregation server [41]

2. Incident and Failure Governance Across Layers

To manage incidents and failures effectively, there needs to be coordination between technical controls, organizational controls and regulatory controls. Technological protections are not the only drivers of resilience, the alignment of people, processes, responsibilities and policies is also important (Table 1) [11]. It is therefore important that the roles are clearly defined to avoid conflicts between security, development, platform, compliance and management. Architects consider security when designing systems, security teams handle security risks, FinOps teams control resource costs, compliance specialists understand regulatory requirements, platform engineers maintain infrastructure, and program managers arrange activities. Frequent cooperation and mutual goals contribute to keeping key tasks on the radar and on task. Configuration problems, unauthorized access, lack of monitoring and policy enforcement are all failure modes that must be addressed by governance across cloud and edge environments [11]. Often, cloud failures occur due to environments that change too quickly and resources that have not been properly configured. These risks can be mitigated with automated discovery, configuration monitoring and policy enforcement and can be documented for ongoing compliance. Gap analysis and posture assessments also enable organisations to translate regulatory requirements into technical and operational controls and prioritise and systematically implement the identified gaps [12]. Edge to cloud environments add on top of that governance needs, as infrastructure is spread out across devices, gateways, local processing systems, edge platforms, and centralized cloud services. Overall, the governance of incidents and failures at layers should be integrated, technical safeguards, the organisation's responsibilities and the regulatory requirements complement each other. Proactive quality controls, ongoing monitoring, automated enforcement, accountability structures, and audit trails are essential to building resilience in today's cloud, edge, and networked digital world [13].

Table 1. Core Governance Domains and Focus Areas in Distributed Infrastructures

Governance Domain	Key Focus & Operational Scope	Reference
Regulatory Compliance	Alignment with cybersecurity directives (e.g., NIS2), data protection standards, incident response, and cross-border data management.	[5]
Organizational Accountability	Defining clear ownership via RACI maps, the three lines of defense model, and aligning cross-functional teams (security, legal, IT, operations).	[6]
Cloud Governance	Managing multi-cloud environments through shared responsibility models, cost optimization (FinOps), compliance monitoring, and backup/recovery.	[7],[8]
Reliability & Network Governance	Establishing Service Level Indicators (SLIs), Service Level Objectives (SLOs), Service Level Agreements (SLAs), and balancing error budgets with innovation.	[9]

3. Cloud Governance

Cloud governance is a strategic approach that combines people, processes, policies and technologies to deliver repeatable results in a hybrid and multi cloud world. It maps out organizational goals and regulatory obligations into actionable controls that help manage security, compliance, cost, performance and operational risk [14]. The development of organization specific governance models can be based on the standards and practices like COBIT, ITIL and ISO 27001. A cloud governance operating model also links the strategic policies to regular operational activities, maintaining measurable, consistent and scalable governance (Figure 2). Another key aspect of cloud governance is clarity regarding the shared responsibility between cloud service provider and customer [15]. Providers will typically handle the security of the underlying infrastructure, and customers will be responsible for compliance, access control, data protection, identity management and other aspects of the customer's environment. New governance capabilities are available on most cloud platforms to enable centralized policies, resource policy and restrictions, compliance monitoring, and automated remediation [16]. This allocation of responsibilities demands organisations to be aware of exactly what security and compliance responsibilities are theirs. The goal of cloud governance is to ensure that the cost of cloud services, security, compliance, performance and operational efficiency are aligned to organizational goals. It covers everything from managing costs to minimising security threats, ensuring compliance with regulation, optimising processes and defining who owns what on the cloud [17]. Backup and recovery are another governance topic that comes into play as it is a part of many regulatory and security requirements to ensure that critical data can be recovered and that the process has been tested. Governance needs to take account of both availability and what can practically be done.

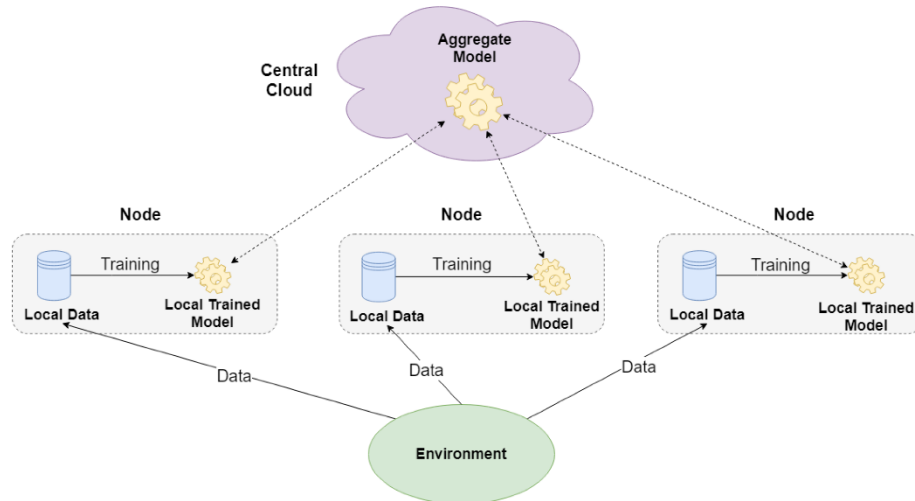


Figure 2. An architecture of distributed data processing and model aggregation [42]

4. Reliability and Network Governance

Network governance and reliability offer a unified approach to ensuring secure, compliant, and reliable digital services in the cloud, edge, and distributed network. Reliability governance establishes a set of service level indicators, service level objectives, and service level agreements to ensure that business, legal, operational and engineering parties have a common understanding of service expectations [18]. These measures offer a shared metric for monitoring system health, performance and availability and help organizational leaders ensure that services are operating within their requirements. SRE is about ongoing measurement and cross functional cooperation, and about continuous improvement. Service owners and business stakeholders can define reliability boundaries together and automated monitoring can be used to provide consistent measures of system performance [19]. Infrastructure as code tools can also help to enhance visibility by illustrating the impact of infrastructure elements and services on reliability. Repeatable and testable configurations eliminate the need for manual processes and institutional knowledge, and help ensure uniform deployment across regions and environments. An error budget offers another way of balancing reliability with the development of a system and innovation. The definition of an acceptable level of failure or service degradation will give organizations more clear guidance for introducing changes to their services and prioritize reliability improvements [20]. Root analysis can then be used to uncover technical or organizational issues that are likely to be causing the failure to meet reliability goals and inform corrective actions when reliability goals are consistently not being met. These ideas are extended to the commitments that are made to customers through service level agreements and can result in formal accountability if service levels are not met as agreed [21]. Reliability and network governance are elements that, when combined, relate measurable service objectives to secure infrastructure management. Reliable cloud, edge and network operations are built on continuous monitoring, automated controls, explicit accountability, auditable configurations, incident response and routing oversight.

5. Edge Governance and Cross Cutting Governance Mechanisms

Edge governance puts in place rules to govern changes at the internet facing edge of digital services, such as managing DNS records, Web Application Firewall rules, redirects, certificates, content delivery settings, and traffic routing. Governance needs to integrate change management, access accountability, approval processes, monitoring and recovery procedures as a relatively small edge modification can affect an entire service path [22]. Identities and permissions that can change edge configurations are especially critical as they can alter trust paths within a chain or route sensitive traffic without changing the basic application logic. There is also a cross-over of edge governance with data

sovereignty and regulatory requirements. Sovereign edge approaches aim to maintain computing, data and AI-based operations in specific jurisdictions or organizational perimeter [23]. These can enable local control, continuity and security in the event of a cloud connectivity disruption or regulatory requirements that limit data movement. Technical performance is only part of the equation for governance; issues of jurisdiction, data location, access rights and independence of operations are all relevant (Table 2). The importance of audit readiness and evidence based governance. Organizations should keep good documentation of data flows, retention policies, breach protocol, third party relationships, processing procedures and security measures [24]. Records of processing activities, data protection assessments, processor agreements, access records, system logs etc. attest that governance requirements are being put in place and monitored. Last but not least, centralized identity and access management should integrate on-premise, cloud and edge environments via consistent least privilege controls. The application of data classification, data encryption, monitoring and change management should be based upon risk and regulatory considerations [25]. Automated policies, roles of governance, continuous improvement, audit evidence, data stewardship and integrated access controls create a coordinated governance approach that enables governance of distributed edge environments.

Table 2. Implementation Mechanisms, Tools, and Challenges in Edge-Cloud Systems

Framework Aspect	Description & Implementation Strategy	Reference
Edge-to-Cloud Orchestration	Synchronizing distributed edge devices, gateways, and centralized cloud services to maintain uniform security deployment and workload updates.	[15]
Model-Driven Validation	Utilizing UML-based interaction and infrastructure models combined with formal constraints to detect design and configuration inconsistencies prior to deployment.	[17]
Policy as Code & Automation	Automating policy enforcement, configuration monitoring, and continuous compliance verification to minimize manual errors.	[19]
Data Sovereignty & Audit Readiness	Maintaining local control, encryption, data classification, and comprehensive processing records to ensure compliance across different jurisdictional perimeters.	[20]

6. Implementation, Operating Model and Limitations

Governance implementation in cloud and edge environments can be modeled, and a model-driven approach can link system modeling, regulatory requirements, validation and operational controls. UML based interaction and infrastructure models can establish relationships between users, services, data and technical components then formal constraints can be applied to detect inconsistencies before deployment of the application [26]. This enables the inclusion of privacy, security and regulatory compliance features within system design and engineering, as opposed to compliance being a standalone process. The stages of a practical implementation lifecycle can be divided into three parts: modeling, validation, and recommendation. In modeling, the interaction of the systems, the infrastructure, data policies and regulatory requirements are specified [27]. The errors, inconsistencies or prohibited actions identified through the validation process are then corrected and the process returns to the modeling stage as needed. The last step converts the approved requirements into suitable cloud configurations and operating

procedures. Case studies and use cases should show the governance in practice with realistic conditions of regulations, technology, and organization [28]. Cross border transfers, health research, clinical collaboration, data minimization, contractual measures to protect data transfer, and transfer risk assessments are examples of relevant cases. Other good examples might show continuous governance improvement, compliance with cloud governance standards, sovereign cloud and edge needs, distribution of workloads and multi cloud approaches with containerization, standardized interfaces and data residency controls [29]. Cases should also illustrate the value of governance in improving organizational outcomes like better decision making, risk management, and technology and business goals coordination. Finally, there are also maintenance needs with policy automation and policy as code. Automated controls need to be regularly checked and revised to account for new threats, new technology and revisions to the rules [30]. To ensure effective implementation, it is important to continually validate, assign responsibilities, update controls and coordinate overall governance, security, technical and business functions.

7. Discussion

The modern digital transformation has moved organisations away from a relatively centralised way of working, to a connected approach to cloud, edge and network architectures. While this shift has helped organisations to scale, process in "real time", deliver services distributedly and be flexible in their operations, it has also added to the governance challenges they need to be able to solve [31]. Traditional compliance-related governance and centralized information technology controls are no longer adequate. Rather, it is required to tie regulatory needs, risk management, cybersecurity, reliability, data stewardship, infrastructure management and operational accountability together in increasingly distributed settings. The key idea is that the governance at the edge is not about the control of a single technique but is a part of an integrated organizational capability [32]. The approach to conceptual development developed in this context assumes the three basic functions of governance: setting rules, handling risks, and verifying compliance. These functions offer a common framework to translate regulatory requirements and organizational goals into operational controls. In times of cloud and edge, where infrastructure, workloads, identities and data flows can shift quickly, this relationship is especially significant. Such static governance processes can thus become ineffective if they are not embedded in continuously evolving technical contexts [33]. Policy-driven automation and ongoing validation bring in a mechanism to ensure governance requirements and reality are aligned. The discussion also shows that accountability is an integral part of good governance. Cloud and edge environments are a collection of teams that have overlapping responsibilities ranging from security, development, infrastructure, compliance, legal, finances, and business operations [34]. Failing to have explicit ownership of the important controls can lead to important controls slipping between the cracks. Role based structures like RACI mappings and the three Lines of Defence can be used to define roles and responsibilities and to distinguish operational activity from risk oversight and independent assurance. A governance program manager may then be able to facilitate these functions by ensuring communication between governance strategic leadership and operational teams [35]. These arrangements minimise uncertainty and help to provide more uniform decision-making in the event of incidents, changes in legislation or infrastructure failures. Another key aspect of the framework is regulatory governance. Increasingly, European and UK regulatory developments have focused on cybersecurity resilience, incident management, data protection, supply chain risk, and organizational accountability [36]. However, as regulatory change is increasingly moving beyond documentation, requirements linked to NIS2, data protection laws, operational resilience plans and sector specific requirements are a testament to this. Organizations should have realistic processes in place to identify risks, monitor systems and processes, respond to incidents,

protect data and keep records of compliance. This establishes an immediate link between regulatory governance and technical architecture. Compliance requirements need to be converted to access control, logging and monitoring, encryption, retention period, incident procedures, supplier controls, and auditable evidence [37]. Cloud governance is the operational backbone to address these requirements in hybrid and multi cloud environments. It is designed to benefit in areas of cost management, security, compliance, performance, resource allocation, accountability and more. The shared responsibility model is important because the responsibilities of security are split between the customer and the cloud provider. Providers own the underlying infrastructure, customers are responsible for data, identities, permissions, configurations, and much more in terms of compliance [38]. This separation implies that you can't take it for granted that provider security automatically results in organizational security. Governance needs to determine which controls will be inherited from providers, and which must be put in place and monitored on an ongoing basis by the organization. Effective governance of data throughout its life cycle is also essential to cloud governance. The same applies to financial governance; distributed infrastructure can result in resource consumption that cannot be controlled. Budgeting, tagging, monitoring, rightsizing and resource ownership are thus part of a larger governance framework, not just a financial dimension. Reliability governance is a form of governance that extends this and relates to service performance and operational resilience [39]. Service level indicators, service level objectives and service level agreements are measurable expectations of availability and performance. The importance of their value is not just to measure uptime but to establish a common understanding of what reliable service is for the technical teams, the management, the customers, and others involved in the service. Along with the balancing of development activity and reliability requirements, error budgets offer another mechanism of balancing [40]. If reliability goals are continually not met, RCA may be used to determine if the issues are due to infrastructure, deployment, configuration, capacity or organizational issues. Overall, governance at the edge is an integrated governance way of managing the risks generated by distributed digital transformation. Good governance ensures that the following activities are related to one another and that they all operate in a unified fashion and framework: Regulation, Cloud Management, Reliability Engineering, Network Security, Edge Controls, Data Stewardship, and Organizational Accountability.

8. Conclusion

Governance at the edge provides an integrated framework for managing regulatory, cloud, network, reliability, and security challenges across distributed digital environments. Effective governance requires clear accountability, risk based controls, continuous monitoring, automated policy enforcement, and reliable evidence of compliance. Cloud and edge infrastructures must be governed through coordinated technical and organizational processes rather than isolated controls. Model driven validation, policy as code, structured responsibility mapping, and continuous improvement can strengthen resilience and regulatory alignment. Despite challenges involving regulatory change, automation, cross border data, and operational complexity, integrated governance provides a practical foundation for secure, reliable, and sustainable digital transformation..

References

1. V. Venkatesh and H. Bala, "Technology acceptance model 3 and a research agenda on interventions," *Decis. Sci.*, vol. 39, no. 2, pp. 273–315, 2008. doi: 10.1111/j.1540-5915.2008.00192.x.
2. N. Nawaz, H. Arunachalam, B. K. Pathi, and V. Gajenderan, "The adoption of artificial intelligence in human resources management practices," *Int. J. Inf. Manag. Data Insights*, vol. 4, no. 1, p. 100208, 2024. doi: 10.1016/j.jjime.2023.100208.

3. A. T. Shama, "AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management," *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.
4. G. Waja, G. Patil, C. Mehta, and S. Patil, "How AI can be used for governance of messaging services: A study on spam classification leveraging multi-channel convolutional neural network," *Int. J. Inf. Manag. Data Insights*, vol. 3, no. 1, p. 100147, 2023. doi: 10.1016/j.jjime.2022.100147.
5. A. Mohammed and M. Mohammad, "How AI algorithms are being used in applications," in *Soft Computing and Signal Processing*, V. S. Reddy, V. K. Prasad, J. Wang, and K. T. V. Reddy, Eds., Singapore: Springer Nature Singapore, 2023, vol. 313, pp. 41–53. doi: 10.1007/978-981-19-8669-7_5.
6. B. Deng and Y. Qiu, "Comment on 'Analytical solutions to one-dimensional advection-diffusion equation with variable coefficients in semi-infinite media' by A. Kumar, D. K. Jaiswal, N. Kumar, *J. Hydrol.*, 2010, 380: 330–337," *J. Hydrol.*, vol. 424–425, pp. 278–279, 2012. doi: 10.1016/j.jhydrol.2011.12.045.
7. J. Jha, A. K. Vishwakarma, C. N, A. Nithin, A. Sayal, A. Gupta, and R. Kumar, "Artificial intelligence and applications," in *Proc. 2023 1st Int. Conf. Intell. Comput. Res. Trends (ICRT)*, Roorkee, India, 2023, pp. 1–4. doi: 10.1109/ICRT57042.2023.10146698.
8. J. Bajwa, U. Munir, A. Nori, and B. Williams, "Artificial intelligence in healthcare: Transforming the practice of medicine," *Future Healthc. J.*, vol. 8, no. 2, pp. e188–e194, 2021. doi: 10.7861/fhj.2021-0095.
9. J. Yang, Y. Blount, and A. Amrollahi, "Artificial intelligence adoption in a professional service industry: A multiple case study," *Technol. Forecast. Soc. Change*, vol. 201, p. 123251, 2024. doi: 10.1016/j.techfore.2024.123251.
10. A. T. Shama, "Third-Party Risk Management in API-Driven Ecosystems: Continuous Vendor Security Practices and Emerging Challenges," *American Journal of Technology Advancement*, vol. 1, no. 4, pp. 42–50, 2024. doi: 10.31149/ajta.v1i4.4322.
11. C. Van Noordt and G. Misuraca, "Exploratory insights on artificial intelligence for government in Europe," *Soc. Sci. Comput. Rev.*, vol. 40, no. 2, pp. 426–444, 2022. doi: 10.1177/0894439320980449.
12. S. Akter, K. Michael, M. R. Uddin, G. McCarthy, and M. Rahman, "Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics," *Ann. Oper. Res.*, vol. 308, pp. 7–39, 2022. doi: 10.1007/s10479-020-03620-w.
13. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-145, 2011. doi: 10.6028/NIST.SP.800-145.
14. F. J. G. Peñalvo, A. Sharma, A. Chhabra, S. K. Singh, S. Kumar, V. Arya, and A. Gaurav, "Mobile cloud computing and sustainable development: Opportunities, challenges, and future directions," *Int. J. Cloud Appl. Comput.*, vol. 12, pp. 1–20, 2022. doi: 10.4018/IJCAC.312583.
15. R. P. Singh, A. Haleem, M. Javaid, R. Kataria, and S. Singhal, "Cloud computing in solving problems of COVID-19 pandemic," *J. Ind. Integr. Manag.*, vol. 6, no. 2, pp. 209–219, 2021. doi: 10.1142/S2424862221500044.
16. P. Modisane and O. Jokonya, "Evaluating the benefits of Cloud Computing in Small, Medium and Micro-sized Enterprises (SMMEs)," *Procedia Comput. Sci.*, vol. 181, pp. 784–792, 2021. doi: 10.1016/j.procs.2021.01.231.

17. A. M. Talib, R. Atan, R. Abdullah, and M. A. A. Murad, "Formulating a security layer of cloud data storage framework based on multi-agent system architecture," *GSTF Int. J. Comput.*, vol. 1, no. 1, p. 120, 2010. doi: 10.5176/2010-2283_1.1.20.
18. S. Z. Alismaili, M. Li, J. Shen, P. Huang, Q. He, and W. Zhan, "Organisational-level assessment of cloud computing adoption: Evidence from the Australian SMEs," *J. Glob. Inf. Manag.*, vol. 28, no. 2, pp. 73–89, 2020. doi: 10.4018/JGIM.2020040104.
19. S. Zhou, B. Yuan, K. Xu, M. Zhang, and W. Zheng, "The impact of pricing schemes on cloud computing and distributed systems," *J. Knowl. Learn. Sci. Technol.*, vol. 3, no. 4, pp. 193–205, 2024. doi: 10.60087/jklst.v3.n4.p68.
20. W. Sutherland, D. Paine, and C. P. Lee, "'The Cloud is Not Not IT': Ecological Change in Research Computing in the Cloud," *Comput. Support. Coop. Work*, vol. 33, pp. 1037–1069, 2024. doi: 10.1007/s10606-024-09490-1.
21. M. M. Hossain and A. T. Shama, "GRC Accountability Gap in AI and Cloud Security: Limitations of Automated Compliance and Risk Control Mechanisms," *International Journal on Orange Technologies*, vol. 7, no. 1, pp. 56–63, 2025. doi: 10.31149/ijot.v7i1.5798.
22. V. Raja, "Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns," *J. Artif. Intell. Gen. Sci.*, vol. 4, no. 1, pp. 121–144, 2024. doi: 10.60087/jaigs.v4i1.86.
23. R. Nagahawatta, M. Warren, S. Salzman, and S. Lokuge, "Towards an Understanding of Cloud Computing Adoption in SMEs: The Role of Security and Privacy Factors," *Int. J. Cyber Warf. Terror.*, vol. 14, no. 1, pp. 1–13, 2024. doi: 10.4018/IJCWT.343315.
24. X. L. Wang, L. Wang, Z. Bi, Y. Y. Li, and Y. Xu, "Cloud computing in human resource management (HRM) system for small and medium enterprises (SMEs)," *Int. J. Adv. Manuf. Technol.*, vol. 84, no. 1-4, pp. 485–496, 2016. doi: 10.1007/s00170-016-8493-8.
25. B. H. Malik, J. Asad, S. Kousar, F. Nawaz, F. Hayder, S. Bibi, and A. Raza, "Cloud Computing Adoption in Small and medium-sized enterprises (SMEs) of Asia and Africa," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 1–8, 2019. doi: 10.14569/IJACSA.2019.0100565.
26. A. Khayer, N. Jahan, M. N. Hossain, and M. Y. Hossain, "The adoption of cloud computing in small and medium enterprises: A developing country perspective," *VINE J. Inf. Knowl. Manag. Syst.*, vol. 51, no. 1, pp. 64–91, 2021. doi: 10.1108/VJIKMS-05-2019-0064.
27. K. Ramchand, M. Baruwat Chhetri, and R. Kowalczyk, "Enterprise adoption of cloud computing with application portfolio profiling and application portfolio assessment," *J. Cloud Comput.*, vol. 10, art. no. 1, 2021. doi: 10.1186/s13677-020-00210-w.
28. A. Uddin, D. Cetindamar, I. Hawryszkiewicz, and O. Sohaib, "The Role of Dynamic Cloud Capability in Improving SME's Strategic Agility and Resource Flexibility: An Empirical Study," *Sustainability*, vol. 15, no. 11, p. 8467, 2023. doi: 10.3390/su15118467.
29. A. Mohammad and Y. Abbas, "Key Challenges of Cloud Computing Resource Allocation in Small and Medium Enterprises," *Digital*, vol. 4, no. 2, pp. 372–388, 2024. doi: 10.3390/digital4020018.
30. C. Sayginer and A. Ercan, "Multi-perspective decision-making cloud computing adoption model for small and medium enterprises (SMEs)," *Emerg. Sci. J.*, vol. 4, pp. 141–153, 2020. doi: 10.28991/esj-2021-SP1-010.
31. E. Erturk, "An incremental model for cloud adoption: Based on a study of regional organizations," *TEM J.*, vol. 6, no. 4, pp. 868–876, 2017. doi: 10.18421/TEM64-29.

32. V. M. Dincă, A. M. Dima, and Z. Rozsa, "Determinants of cloud computing adoption by Romanian SMEs in the digital economy," *J. Bus. Econ. Manag.*, vol. 20, no. 4, pp. 798–820, 2019. doi: 10.3846/jbem.2019.9856.
33. T. S. Afsara and C. Proggo, "Privacy Governance Challenges in AI-Enabled Banking Surveillance Systems: From Compliance to Accountability," *Journal of Knowledge Learning and Science Technology*, vol. 5, no. 2, pp. 131–141, 2026. doi: 10.60087/jklst.vol5.n2.009.
34. K. Mousa, Z. Zhang, E. Sumarlia, and I. K. Hamdan, "The impact of cloud computing adoption on firm performance among SMEs in Palestine: A machine learning approach," *Int. J. Intell. Inf. Technol.*, vol. 20, pp. 1–24, 2024. doi: 10.4018/IJIT.338715.
35. N. H. M. Daud and S. A. Rahmann, "Advantages of using cloud computing by knowledge management personnel," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 7, no. 11, pp. 908–916, 2017. doi: 10.6007/IJARBSS/v7-i11/3525.
36. H. Hassan, M. H. Mohd Nasir, N. Khairudin, and I. Adon, "Factors influencing cloud computing adoption in small and medium enterprises," *J. Inf. Commun. Technol.*, vol. 16, no. 1, pp. 21–41, 2017. doi: 10.32890/jict2017.16.1.2.
37. M. S. Aksoy and D. Algawiaz, "Knowledge management in the cloud: Benefits and risks," *Int. J. Comput. Appl. Technol. Res.*, vol. 3, no. 11, pp. 718–720, 2014. doi: 10.7753/IJCATR0311.1013.
38. R. Hentschel, C. Leyh, and A. Petznick, "Current cloud challenges in Germany: The perspective of cloud service providers," *J. Cloud Comput.*, vol. 7, art. no. 5, 2018. doi: 10.1186/s13677-018-0107-6.
39. A. T. Shama, "AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management," *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.
40. O. Gibreel, A. R. Alsaber, S. Mahenthiran, and L. Tahat, "Factors and Barriers to Cloud Computing Adoption for Small and Medium-Sized Enterprises in Kuwait," *World J. Sci. Technol. Sustain. Dev.*, vol. 19, no. 3-4, pp. 233–246, 2024. doi: 10.47556/J.WJSTSD.19.3-4.2024.9.
41. A. I. Neicu, A. C. Radu, G. Zaman, I. Stoica, and F. Răpan, "Cloud computing usage in SMEs. An empirical study based on SMEs employees perceptions," *Sustainability*, vol. 12, no. 12, p. 4960, 2020. doi: 10.3390/su12124960.
42. B. A. Buhari, B. S. Muhammad, B. A. Bodinga, and M. D. Sifawa, "Adoption of cloud computing by IT based small and medium scale enterprises in Northwestern Nigeria," *Int. J. Adv. Netw. Appl.*, vol. 13, no. 5, pp. 5119–5127, 2022. doi: 10.35444/IJANA.2022.13505.