International Journal of Recent Advances in Science and Technology, 2026; 12(1):17-24

DOI: 10.30750/ijarst.120104

Developing an AI Readiness Framework for Digital Transformation in Emerging Economies

Temirova Svetlana

Department of Social Subjects, Tashkent State Transport University, Tashkent, Uzbekistan

Abstract

Organisations in emerging economies face distinctive constraints when adopting artificial intelligence as part of digital transformation: infrastructure is uneven, data are fragmented, skills are scarce and governance frameworks are nascent. Readiness assessments imported from advanced economies average dimension scores into an index and assume that strengths offset weaknesses, which misrepresents conditions in which a single missing prerequisite can block transformation. This paper develops an AI readiness framework with six dimensions, namely infrastructure, data, skills, governance, finance and leadership, in which infrastructure is a floor condition, the dimensions are complements, and readiness is reported through a balance-sensitive composite and the binding dimension. The framework is examined in a simulation of 800 organisations whose transformation success depends on balanced readiness and on the infrastructure floor. Organisations below the infrastructure floor succeed 12% of the time against 49% above it; among organisations with above-median average readiness, those with no dimension below 0.3 succeed 94% of the time against 49% for those with a weak dimension; and the weakest-dimension and geometric-mean composites predict success better (AUC 0.81) than the additive mean (0.80). The paper translates the framework into an assessment procedure and a sequencing logic for organisations and policymakers, emphasising infrastructure and data as prerequisites and the identification of binding constraints over aggregate scores.

Keywords: AI readiness; digital transformation; emerging economies; readiness assessment; complementarity; binding constraints.

Introduction

Artificial intelligence is increasingly central to digital transformation, and organisations in emerging economies are under pressure from competitors, customers and governments to adopt it. Their conditions differ from those in which most AI readiness frameworks were developed. Connectivity and power are unreliable in many regions; organisational data are often paper-based, fragmented across systems or absent; AI and data skills are scarce and expensive; regulatory and governance frameworks for AI are still forming; and finance for long-horizon technology investment is constrained [1], [2]. Readiness assessments designed for advanced-economy firms assume that these prerequisites are broadly in place and focus on strategy and culture.

A further problem is the scoring logic of readiness instruments. Most average dimension scores into an index, which implies that a strong score on leadership offsets a weak score on data. In emerging-economy conditions this is implausible: an organisation without reliable infrastructure cannot run AI systems regardless of its leadership, and one without usable data cannot train them regardless of its skills. Readiness is better understood as a configuration with floor conditions and complementarities, in which the weakest dimension determines what is possible [3], [4].

This paper develops an AI readiness framework for emerging-economy contexts that embeds these ideas, examines its behaviour in a simulation in which the success process is known, and derives an assessment procedure and sequencing guidance for organisations and policymakers.

Background

Digital transformation in emerging economies

Institutional voids, meaning gaps in market-supporting institutions and infrastructure, shape

firm strategy in emerging economies [1]. Digital transformation in such settings often requires firms to internalise functions, such as data infrastructure, that advanced-economy firms source externally [2]. AI adds dependence on data and specialised skills, intensifying the constraint.

Readiness frameworks

Technology readiness and maturity models typically define dimensions and stages and aggregate scores additively. Reviews of digital transformation research note limited theoretical grounding in many maturity models and untested links to outcomes [5]. AI-specific readiness instruments add dimensions for data and ethics, drawing on capability frameworks that treat data, technology and human resources as a bundle [6], but they generally retain additive scoring.

Complementarity and necessary conditions

Complementarity theory holds that the return to one practice rises with the presence of others, so that balanced configurations outperform unbalanced ones at the same average [3]. Necessary-condition reasoning adds that some conditions must be present for an outcome to be possible at all; their absence cannot be compensated [4]. Both ideas motivate composites that are sensitive to the weakest dimension.

The Framework

Dimensions

The framework assesses six dimensions on a 0–1 scale with context-specific descriptors. Infrastructure: reliability of power and connectivity, availability of computing (including cloud access), and resilience to outages. Data: existence, digitisation, quality, accessibility and governance of operational data. Skills: availability of data, analytics and AI competencies, internally or through partners. Governance: policies for data protection, AI risk, accountability and ethics, and alignment with emerging regulation. Finance: capacity to fund multi-year AI investment and to absorb failed pilots. Leadership: executive understanding, commitment and the ability to translate AI into business priorities.

Structural assumptions

Three assumptions distinguish the framework. Infrastructure is a floor condition: below a threshold, success probability is sharply reduced regardless of other dimensions. The dimensions are complements: success depends on the balanced configuration, approximated by the geometric mean, rather than on the average. The weakest dimension binds: the marginal return to improvement is highest for the lowest-scoring dimension.

Reporting

Readiness is reported as the dimension profile, the additive mean R_{add}, the geometric mean R_{geo}, the weakest dimension R_{min} with its identity, and an infrastructure-floor flag. The pair (R_{geo}, R_{min}) is the primary readiness statement; R_{add} is reported for comparability with other instruments.

Context-specific descriptors

Descriptors imported from advanced-economy instruments misrate emerging-economy organisations. An infrastructure descriptor that asks about bandwidth will miss an organisation whose constraint is power reliability; a data descriptor that asks about data warehouses will miss one whose operational records are on paper; a skills descriptor that assumes an internal data team will miss the common pattern of skills accessed through consultancies, universities or vendors. The framework therefore specifies that descriptors be calibrated to the local range of conditions, with the lowest level describing the constraints that actually occur, so that the scale discriminates where organisations are rather than compressing them at the bottom.

Simulation Design

The harness generates 800 organisations with six dimension scores drawn from a Beta(2, 3) distribution plus a shared organisational factor, so that scores are right-skewed and positively correlated, as is typical of emerging-economy samples. Transformation success follows

$$\text{logit } P(\text{success}) = -3 + 6\,R_{geo} + 2\cdot \mathbb{1}[R_{min} > 0.3] - 1.5\cdot \mathbb{1}[\text{infrastructure} < 0.25], \quad (1)$$

encoding complementarity, a balance bonus and the infrastructure floor. Success is drawn from this

probability. Logistic regressions on each composite are compared by AUC, success rates are tabulated by floor status and by balance among organisations with above-median additive readiness, and a regression on the six dimensions estimates their relative weights. The parameters are design values encoding the framework's structural assumptions; the harness examines whether the proposed composites capture them.

Results

Composites as predictors

The weakest-dimension composite predicts success with an AUC of 0.81, the geometric mean 0.81 and the additive mean 0.80. The margins are small because dimensions are correlated in the simulated population, which limits the divergence between composites; the ordering nevertheless favours the balance-sensitive composites, consistent with the framework.

The infrastructure floor and the balance effect

Table 1 reports success rates by floor status and balance. Organisations below the infrastructure floor succeed 11.6% of the time against 48.9% above it. Among organisations with above-median additive readiness, those with no dimension below 0.3 succeed 93.5% of the time; those with at least one weak dimension succeed 49.2% of the time, roughly the same as the population average, despite their high average score. Figure 1 shows the pattern across the additive index: balanced profiles succeed at high rates throughout the range in which they occur, whereas unbalanced profiles rise only slowly with the average.

Dimension weights

A logistic regression on the six dimensions gives coefficients of 2.08 for infrastructure, 1.84 for data, 1.56 for finance, 1.49 for skills, 1.35 for governance and 1.34 for leadership. Infrastructure and data carry the largest weights, reflecting the floor condition and their role as prerequisites for the others; the remaining dimensions matter but cannot substitute for the first two.

Table 1: Transformation success rates by infrastructure floor and profile balance (800 simulated organisations; overall success rate 38.9%).

Group	*Success rate*
Infrastructure below floor (< 0.25)	11.6%
Infrastructure above floor	48.9%
Above-median additive readiness, no dimension below 0.3	93.5%
Above-median additive readiness, at least one dimension below 0.3	49.2%

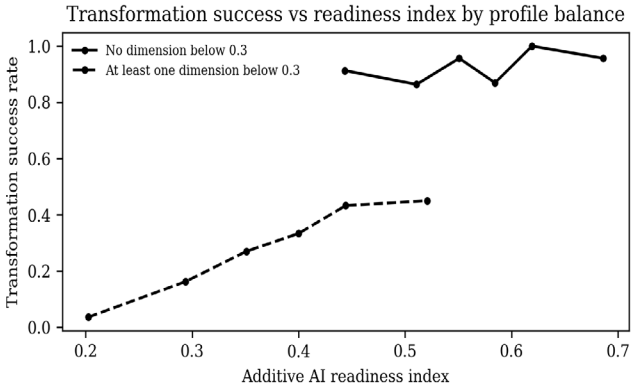


Figure 1: Transformation success rate against the additive readiness index for balanced and unbalanced profiles.

Applying the Framework

Assessment procedure

Assess each dimension with multiple informants and documentary evidence, using descriptors calibrated to local conditions (for instance, infrastructure descriptors that distinguish grid reliability and mobile from fixed connectivity). Compute the composites and the floor flag. Report the profile with the binding dimension identified. Translate into a sequenced plan that addresses the floor first, then the binding dimension, then broad improvement.

Sequencing for organisations

Organisations below the infrastructure floor should invest in resilience, including backup power, mobile and offline-capable systems and cloud services accessed through redundant connectivity, before investing in AI applications. Those above the floor but with weak data should digitise and consolidate operational data before building models. Only when infrastructure and data clear their thresholds does investment in skills, governance and leadership yield the returns that advanced-economy frameworks promise.

Implications for policy

Governments and development agencies supporting AI adoption should recognise that aggregate readiness indices mask binding constraints. Programmes that fund skills training for organisations without data, or AI pilots for organisations without reliable infrastructure, will show low success rates not because the programmes are poorly run but because the prerequisites are absent. Diagnostic assessment with the framework before programme enrolment, and targeting of support to the binding dimension, would raise success rates.

Validation

The framework's propositions are testable with cross-sectional or panel data on organisations undertaking AI-enabled transformation. The key tests are whether success is better predicted by balance-sensitive composites than by the additive mean, whether an infrastructure floor is observable, and whether improvements in the previously weakest dimension are followed by larger gains than improvements elsewhere. Emerging-economy samples, with their greater dispersion across dimensions, are well suited to these tests.

Sector and ecosystem variation

Readiness is partly a property of the organisation's ecosystem. Infrastructure and skills availability vary by region and sector within an economy; an organisation in a metropolitan technology cluster faces different floors from one in a rural manufacturing region. Assessments should record ecosystem conditions separately from organisational conditions, since the remedies differ: an organisation can build its own data but can only partially substitute for regional infrastructure. Policymakers can use the aggregate of organisational assessments to locate ecosystem-level floors that merit public investment.

Readiness over time

Readiness is not static. Organisations that begin AI adoption with a balanced but low profile tend to raise all dimensions together as projects succeed, whereas those that begin with an unbalanced profile often invest further in strong dimensions because that is where capability and advocacy sit. Periodic reassessment with the framework, reported as a trajectory of profiles, allows organisations to see whether they are closing the gap on the binding dimension or widening it.

Limitations

The simulation encodes the framework's structural assumptions and demonstrates the behaviour of its composites under them; it does not test the assumptions. The six dimensions, the floor threshold and the balance threshold are design choices. Dimension scores in practice are subject to measurement error and informant bias. All reported values are simulation outputs and are not estimates for any population of organisations.

Conclusion

AI readiness in emerging economies is a configuration with a floor and complements, not an average. A framework with six dimensions, an infrastructure floor and balance-sensitive composites was developed and examined in simulation, where the floor cut success rates by three-quarters, balanced profiles succeeded almost twice as often as unbalanced ones at the same average readiness, and infrastructure and data carried the largest weights. Organisations and policymakers should assess readiness by its weakest dimension, sequence investment to relieve binding constraints, and treat infrastructure and data as prerequisites rather than as dimensions among equals.

References

1. Chatrath, A. (2021). Bias, fairness, and ethics in artificial intelligence: A comprehensive study of algorithmic discrimination, transparency challenges, and governance frameworks. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 4(1). https://doi.org/10.15680/IJMRSET.2021.0401014
2. Aggarwal, A. (2020). Deployment of multi-factor authentication in cloud-based enterprise applications for preventing credential theft and unauthorized access through adaptive verification layers. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(8). https://doi.org/10.15680/IJMRSET.2020.0308009

3. Gupta, A. (2024). Cloud security in the era of big data: Protecting large-scale storage systems, ensuring query privacy, and safeguarding data lakes against emerging threats. International Journal of Innovative Research in Science, Engineering and Technology, 13(11). https://doi.org/10.15680/IJIRSET.2024.131100217
4. Khan, S. (2018). The role of zero-trust models in database security: Eliminating implicit trust and enforcing continuous verification in enterprise data access systems. International Journal of Research in Electronics and Computer Engineering, 6(1), 1622–1628.
5. Jain, Jaishree, Arpit Jain, Saurabh Kumar Srivastava, Chaman Verma, Maria Simona Raboaca, and Zoltán Illés. "Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA." Mathematics 10, no. 7 (2022): 1071.
6. Ahuja, R. (2022). Application of static application security testing (SAST) in CI/CD pipelines for early detection of insecure coding practices through syntax tree analysis and custom rule sets. International Journal on Recent and Innovation Trends in Computing and Communication, 10(2), 80–87. https://www.ijritcc.org/index.php/ijritcc/article/view/11922
7. Khan, S. (2017). The role of privacy-preserving techniques in database security: Secure multi-party computation, differential privacy, and homomorphic encryption. The Research Journal, 3(4), 29–35.
8. Jain, Arpit, Nageswara Rao Moparthi, A. Swathi, Yogesh Kumar Sharma, Nitin Mittal, Ahmed Alhussen, Zamil S. Alzamil, and MohdAnul Haq. "Deep Learning-Based Mask Identification System Using ResNet Transfer Learning Architecture." Computer Systems Science & Engineering 48, no. 2 (2024): 341.
9. Khan, S. (2016). A study of data provenance and integrity in database security: Ensuring authenticity, non-repudiation, and accountability in data lifecycle management. International Journal of Research in Electronics and Computer Engineering, 4(3), 180–186.
10. Bhanushali, B. (2020). Enhancing alert investigation process with feedback loop to increase efficiently and model tuning. International Journal of Innovative Research in Computer and Communication Engineering, 8(8), 3366–3373. https://doi.org/10.15680/IJIRCCE.2020.0808100
11. Rangappa, A. S. (2023). An analytical study of role-based access control (RBAC) and attribute-based access control (ABAC) in database security for multi-tenant and cloud-based architectures. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 812–819. https://www.ijritcc.org/index.php/ijritcc/article/view/11943
12. Jadhav, P. V., Krishnan, S. B., Dey, R., & Chakrabarti, P. (2026). Combining deep learning and statistical models: LSTM-ARIMA ensemble for financial forecasting. IAENG International Journal of Computer Science, 53(1), 236–246. https://www.iaeng.org/IJCS/issues_v53/issue_1/IJCS_53_1_24.pdf
13. Ahuja, R. (2023). Implementation of AI-driven input validation in user interfaces for preventing injection attacks and ensuring data sanitation through adaptive filtering and pattern recognition. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8), 884–891. https://www.ijritcc.org/index.php/ijritcc/article/view/11936
14. Devulapalli, N. (2024). The role of homomorphic encryption in database security: Enabling confidential query processing, secure data sharing, and privacy-preserving analytics. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(8), 14319–14326. https://doi.org/10.15680/IJMRSET.2024.0708082
15. Ahuja, R. (2023). The role of artificial intelligence and machine learning in DevSecOps: Leveraging predictive analytics, automated threat detection, and anomaly identification for secure software delivery pipelines. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 381–389. https://www.ijritcc.org/index.php/ijritcc/article/view/11946
16. Kumar, Ashok, and Arpit Jain. "Image smog restoration using oblique gradient profile prior and energy minimization." Frontiers of Computer

Science 15, no. 6 (2021): 156706.
17. Mahadasu, S. S. (2022). Cross-domain service assurance for private 5G networks using streaming telemetry and dependency-aware event correlation. International Journal of Data Science and IoT Management System, 1(3), 51–56. https://doi.org/10.64751/ijdim.2022.v1.n3.1290
18. Chatrath, A. (2020). DevSecOps for financial services: An in-depth study of secure CI/CD practices, regulatory compliance, and real-time threat monitoring in cloud-based FinTech applications. International Journal of Innovative Research in Science, Engineering and Technology, 9(11). https://doi.org/10.15680/IJIRSET.2020.0911098
19. Rangappa, A. S. (2024). Generative AI in human-machine collaboration: Exploring co-creation dynamics, shared agency, and the role of human oversight in AI-augmented creative and analytical tasks. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 13(4), 985–992. https://doi.org/10.15662/IJAREEIE.2024.1304077
20. Bhaskara Raju Rallabandi. (2022). SYNC-ADAPTIVE RESOURCE SCHEDULING IN PRIVATE 5G FOR TIME-CRITICAL APPLICATIONS. International Journal of Data Science and IoT Management System, 1(2), 40–45. https://doi.org/10.64751/ijdim.2022.v1.n2.pp40-45
21. Jain, A. (2024, December). Energy-Efficient Signal Processing Architectures for IoT Networks Design. In 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN) (pp. 362–367). IEEE.
22. Anchala, S. (2019). Database security in e-governance systems: Protecting citizen records, ensuring transparency, and managing public trust in cloud-based platforms. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 2(11), 2268–2276. https://doi.org/10.15680/IJMRSET.2019.0211014
23. Kaur, M., AlZubi, A. A., Jain, A., Singh, D., Yadav, V., & Alkhayyat, A. (2023). DSCNet: deep skip connections-based dense network for ALL diagnosis using peripheral blood smear images. Diagnostics, 13(17), 2752.
24. Bhaskara Raju Rallabandi. (2023). CLOSED-LOOP DIGITAL-TWIN MANAGEMENT FOR HYBRID 5G-NTN NETWORKS. American Journal of Management and IOT Medical Computing, 2(3), 30–35. https://doi.org/10.64751/ajmimc.2023.v2.n3.pp30-35
25. Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, 2022(1), 6438331.
26. Mahadasu, S. S. (2024). AI-native wireless digital twins for precision agriculture: Edge intelligence and predictive farm operations in 6G ecosystems. International Journal of Data Science and IoT Management System, 3(1), 65–72. https://doi.org/10.64751/ijdim.2024.v3.n1.1287
27. Gupta, A. (2022). The role of artificial intelligence in transforming healthcare delivery: A critical analysis of machine learning models, predictive diagnostics, and ethical challenges in medical decision-making. NeuroQuantology, 20(3), 1383–1399. https://doi.org/10.48047/nq.2022.20.3.NQ23005
28. Mahadasu, S. S. (2024). Closed-loop sustainability orchestration for energy-aware RAN, edge, and data-center workloads in 5G-Advanced networks. International Journal of Engineering Research and Science & Technology, 20(2), 1392–1398. https://doi.org/10.62643/ijerst.2024.v20.n2.4407
29. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." Procedia Computer Science 48 (2015): 330–337.
30. Aggarwal, A. (2019). Application of secure Virtual Private Cloud (VPC) architectures in public cloud infrastructure for strengthening network isolation and segmenting trust zones through fine-tuned routing. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 423–431. https://doi.org/10.15662/IJMSERH.2019.0701048
31. Kumar, S., Jain, A., & Moparthi, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
32. Mahajan, R., Kanabar, K., Dey, R., Jadhav, P. V., Khan, M., & Ghantasala, G. S. P. (2026). Exploring big tech vulnerabilities: Transparent blockchain harvesting. In A. K. Singh, S. Saxena, & A. K.

Haghi (Eds.), Cybernetic shield: Securing the future of machine intelligence (pp. 167–174). CRC Press. https://doi.org/10.1201/9781003567585-15

33. Anchala, S. (2019). The evolution of DevSecOps in software supply chain security: Addressing dependencies, open-source vulnerabilities, and the prevention of software supply chain attacks. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 415–422. https://doi.org/10.15662/IJMSERH.2019.0701047
34. Kumar, S., Sharma, K., Kumar, P. A., Jain, A., Bhagat, S. K., & Singh, P. (2024, September). An improved particle swarm approach for energy-aware location-aided routing in mobile ad-hoc network. In 2024 7th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 7, pp. 1119–1124). IEEE.
35. Bhanushali, B. (2020). Effective sanctions screening and false positive identification. International Journal of Innovative Research in Science, Engineering and Technology, 9(4), 8306–8313. https://doi.org/10.15680/IJIRSET.2020.0904179
36. Dwivedi, D. (2023). The technical and ethical challenges of building safe agentic AI systems: Balancing autonomy, predictability, alignment, and human oversight in next-generation AI models. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 2024–2031. https://www.ijritcc.org/index.php/ijritcc/article/view/11928
37. Talasila, D. (2021). A risk-based framework for database security: Identifying, classifying, and prioritizing threats for adaptive security policy enforcement. International Journal on Recent and Innovation Trends in Computing and Communication, 9(1), 54–61. https://www.ijritcc.org/index.php/ijritcc/article/view/11919
38. Dwivedi, D. (2024). Deployment of AI-based CAPTCHA systems in web applications for preventing automated bot attacks and brute force attempts through adaptive human verification. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(7), 13529–13536. https://doi.org/10.15680/IJMRSET.2024.0707292
39. Talasila, D. (2020). Deployment of shift-left security practices in agile development for embedding security controls early in the lifecycle and reducing technical debt through dev-centric training. Turkish Online Journal of Qualitative Inquiry, 11(1), 643–651. https://doi.org/10.69980/jzqq0t93
40. Devulapalli, N. (2023). Database security and big data analytics: Protecting large-scale data warehouses, ensuring query privacy, and mitigating emerging threats in real-time analytics systems. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7), 622–629. https://www.ijritcc.org/index.php/ijritcc/article/view/11939
41. Harshitha, G., Kumar, S., Rani, S., & Jain, A. (2021, November). Cotton disease detection based on deep learning techniques. In 4th Smart Cities Symposium (SCS 2021) (Vol. 2021, pp. 496–501). IET.
42. Gupta, A. (2024). Containerization, virtualization, and cloud security: Analyzing vulnerabilities in Kubernetes, Docker, and hypervisor-based architectures with mitigation strategies. International Journal of Advanced Research in Education and Technology, 11(3), 1322–1331. https://doi.org/10.15680/IJARETY.2024.1103067
43. Talasila, D. (2024). Adoption of data loss prevention strategies in SaaS platforms for safeguarding confidential information and preventing unauthorized transfers through real-time content inspection. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(7), 13537–13545. https://doi.org/10.15680/IJMRSET.2024.0707293
44. Rangappa, A. S. (2022). The use of blockchain for auditable and tamper-proof database security logs: Enhancing transparency and trust in data access monitoring. International Journal on Recent and Innovation Trends in Computing and Communication, 10(9), 254–261. https://www.ijritcc.org/index.php/ijritcc/article/view/11925
45. Chatrath, A. (2020). The role of policy-as-code in DevSecOps: Automating compliance, governance, and risk management in cloud-native and hybrid IT environments. International

Journal of Innovative Research in Computer and Communication Engineering, 8(1). https://doi.org/10.15680/IJIRCCE.2020.0801020

46. Bhaskara Raju Rallabandi. (2024). DESIGNING NTN–TERRESTRIAL 6G EXPERIMENTS FOR AGRICULTURE AND SMART GRIDS. American Journal of Management and IOT Medical Computing, 3(3), 27–32. https://doi.org/10.64751/ajmimc.2024.v3.n3.pp27-32
47. Kanabar, K., Dey, R., Mahajan, R., Jadhav, P. V., Khan, M., & Karimullah, S. (2026). Comprehensive guide to blockchain technology: Ecosystems, implementation, governance, and innovations. In A. K. Singh, S. Saxena, & A. K. Haghi (Eds.), Cybernetic shield: Securing the future of machine intelligence (pp. 175–182). CRC Press. https://doi.org/10.1201/9781003567585-16
48. Bhanushali, B. (2020). The industry needs a validated model to justify the immense cost of migrating from manual, periodic KYC (know your customer) to automated. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(11), 1799–1805. https://doi.org/10.15680/IJMRSET.2020.0311009
49. Dwivedi, D. (2023). Integration of secure file upload mechanisms in user-facing applications for preventing malware injections and file-based exploits through content-type validation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 768–775. https://www.ijritcc.org/index.php/ijritcc/article/view/11940
50. Aggarwal, A. (2026). Adoption of end-to-end encryption in cloud communication channels for ensuring data confidentiality and trustworthiness through secure protocol enforcement. Journal of Critical Reviews, 7(12), 5493–5499. https://doi.org/10.69980/jcr.v7:i12.13407
51. Anchala, S. (2020). Adoption of secure access service edge (SASE) in distributed enterprises for ensuring cloud application protection and network optimization through unified security frameworks. Turkish Online Journal of Qualitative Inquiry, 11(4), 2964–2973. https://doi.org/10.69980/60m26411
52. Mahadasu, S. S., & Rallabandi, B. R. (2023). Federated learning for privacy-preserving RAN optimization across multi-site enterprise 5G networks. International Journal of Engineering Science and Advanced Technology, 23(4), 53–57. https://doi.org/10.64771/ijesat.2023.v23.i04.pp3847
53. Devulapalli, N. (2023). Database security in disaster recovery and business continuity planning: Ensuring data availability, backup integrity, and secure failover mechanisms. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 820–827. https://www.ijritcc.org/index.php/ijritcc/article/view/11944