

Articles

Blockchain Adoption in Supply Chain Management: A Multi-Criteria Decision Analysis

Toshov Kamoliddin

Department of Social Sciences Education, Termez University of Economics and Service, Termez, Uzbekistan.

*Corresponding author email: kamoliddin_toshov@tues.uz

Abstract

Firms considering blockchain for their supply chains face a decision with several alternatives and conflicting criteria: traceability and data integrity argue for distributed ledgers, while cost, integration effort and partner readiness argue against them, and non-blockchain traceability platforms offer a middle path. This paper structures the decision as a multi-criteria decision analysis (MCDA). Four alternatives, the status quo of ERP and electronic data interchange, a permissioned blockchain consortium, public blockchain anchoring and a cloud traceability platform without blockchain, are evaluated on six criteria, traceability, cost, integration effort, scalability, partner readiness and data privacy, using TOPSIS with weights elicited in an AHP-style procedure. Under baseline weights that place 30% on traceability, the permissioned consortium ranks first with a closeness coefficient of 0.72, ahead of public anchoring (0.64), the cloud platform (0.53) and the status quo (0.33). Sensitivity analysis over the traceability weight shows that the consortium remains first across the range from 0.1 to 0.5, with public anchoring overtaking the cloud platform only above 0.2, and Monte Carlo sampling of weights ranks the consortium first in 90% of draws. The paper discusses what the analysis reveals about when blockchain is warranted, how the criteria should be scored from evidence rather than vendor claims, and how the method supports consortium decision-making in which partners hold different weights.

Keywords: Blockchain adoption; supply chain management; multi-criteria decision analysis; TOPSIS; AHP; sensitivity analysis.

Introduction

Blockchain has been proposed for supply chains on the strength of traceability, shared records and automated settlement [1], [2], and has been implemented in food, pharmaceuticals, shipping and luxury goods with mixed results. Some consortia have delivered traceability at scale; others have been wound down after partners failed to join or costs exceeded benefits. The pattern suggests that blockchain is warranted in some supply chains and not in others, and that firms need a disciplined way to decide.

The decision is multi-criteria. Traceability, provenance and data integrity favour distributed ledgers; implementation cost, integration with existing systems, scalability and the readiness of partners to participate often do not; and data privacy cuts both ways, since shared ledgers expose data to partners while cryptographic designs can protect it. The alternatives are also more than binary: a firm can retain its ERP and electronic data interchange (EDI) arrangements, join or form a permissioned consortium,

anchor records to a public chain, or adopt a cloud traceability platform that delivers much of the visibility without a ledger.

Multi-criteria decision analysis provides the structure. This paper applies the Analytic Hierarchy Process (AHP) for weighting and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) for ranking [3], [4], evaluates the four alternatives, and examines how the ranking responds to the weight on traceability and to uncertainty in weights generally. The analysis is a worked application with illustrative scores; its contribution is the structure and the sensitivity findings.

Background

Blockchain in supply chains

Reviews identify traceability, transparency, disintermediation and automation as the principal benefits claimed for blockchain in supply chains, and cost, scalability, interoperability, governance and partner

adoption as the principal barriers [1], [2], [5]. Empirical adoption studies find that relative advantage, partner pressure and top-management support drive adoption and that complexity and uncertainty deter it, consistent with technology–organisation–environment reasoning.

Multi-criteria decision analysis

MCDA methods structure decisions with multiple objectives by defining criteria, scoring alternatives, weighting criteria and aggregating. AHP [3] elicits weights through pairwise comparison with a consistency check; TOPSIS [4] ranks alternatives by their distance from ideal and anti-ideal solutions. Both are widely used for technology selection in operations management, comparative studies find their rankings broadly consistent [6], and their combination lets weights reflect stakeholder judgement while scores reflect evidence.

The alternatives

The status quo retains ERP and EDI, with traceability limited to bilateral records. A permissioned consortium establishes a shared ledger among known partners with governed access. Public anchoring stores hashes of records on a public chain for integrity while keeping data off-chain. A cloud traceability platform centralises records with a provider, offering visibility without decentralisation. The alternatives differ in which criteria they serve.

Why structure matters for this decision

Blockchain adoption decisions are vulnerable to two failures that MCDA is designed to prevent. The first is technology-led reasoning, in which the decision begins with the technology and searches for a justification; MCDA begins with criteria and treats the technology as one alternative among several. The second is single-criterion reasoning, in which traceability or cost dominates the discussion according to who is in the room; MCDA forces all criteria onto the table with explicit weights. The sensitivity analysis adds a third protection: it shows how much the ranking depends on contested weights, so that decision-makers can see whether their disagreements matter to the outcome.

Methodology

Criteria and weights

Six criteria are used: traceability (benefit), cost (cost), integration effort (cost), scalability (benefit), partner readiness (benefit) and data privacy (benefit). Baseline weights, representing a firm for which traceability is the primary objective, are 0.30, 0.20, 0.15, 0.10, 0.15 and 0.10. The weights are illustrative of an AHP elicitation; in application they would be derived from pairwise comparisons by the decision group.

Scoring

Alternatives are scored 1–10 on each criterion: status quo (3, 9, 9, 7, 9, 6), permissioned consortium (8, 5, 4, 6, 5, 7), public anchoring (9, 6, 5, 4, 3, 4) and cloud platform (6, 7, 7, 8, 7, 6). The scores encode the qualitative properties in Section 2.3; higher is better for benefit criteria and for cost criteria scored as favourability (so a score of 9 on cost means low cost).

TOPSIS and sensitivity

TOPSIS normalises the decision matrix, weights it, identifies the ideal and anti-ideal solutions, and computes each alternative's closeness coefficient:

$$C_i = d_i^- / (d_i^+ + d_i^-), \quad (1)$$

where d_i^+ and d_i^- are the Euclidean distances to the ideal and anti-ideal solutions. Sensitivity is examined by varying the traceability weight from 0.1 to 0.5 with the other weights rescaled proportionally, and by Monte Carlo sampling of 2,000 weight vectors from a Dirichlet distribution centred on the baseline.

Results

Baseline ranking

Under baseline weights, the permissioned consortium has the highest closeness coefficient (0.723), followed by public anchoring (0.636), the cloud platform (0.534) and the status quo (0.330). The consortium leads because it scores well on traceability and privacy while avoiding the worst partner-readiness and privacy scores of public anchoring; the status quo trails because its traceability is poor and traceability carries the largest weight.

Sensitivity to the traceability weight

Figure 1 and Table 1 show the ranking across traceability weights. The consortium ranks first throughout. At low traceability weight (0.1), the cloud platform is second and public anchoring falls to fourth, nearly tied with the status quo; the cloud platform overtakes the consortium only if the traceability weight falls below about 0.05, outside the examined range. As the traceability weight rises, public anchoring climbs rapidly and nearly matches the consortium at 0.5. The status quo declines monotonically and is never competitive once traceability carries meaningful weight.

Monte Carlo over weights

Sampling weight vectors around the baseline, the consortium ranks first in 89.7% of draws, the cloud platform in 5.6%, public anchoring in 3.5% and the status quo in 1.1%. The consortium's lead is robust to moderate disagreement among decision-makers about weights.

Table 1. TOPSIS closeness coefficients under baseline weights and across traceability weights

<i>Alternative</i>	<i>Baseline (0.30)</i>	<i>Traceability weight 0.10</i>	<i>0.20</i>	<i>0.40</i>	<i>0.50</i>
Status quo (ERP + EDI)	0.330	0.461	0.404	0.257	0.194
Permissioned blockchain consortium	0.723	0.655	0.683	0.762	0.792
Public blockchain anchoring	0.636	0.463	0.544	0.719	0.789
Cloud traceability platform	0.534	0.569	0.553	0.519	0.510

Sensitivity to scores

Although weights were the focus of the sensitivity analysis, the ranking also depends on scores. Raising the consortium's partner-readiness score from 5 to 7, as would happen once anchor partners commit, widens its lead; lowering it to 3, as in a fragmented industry, brings the cloud platform within reach at moderate traceability weights. Public anchoring's position depends chiefly on its privacy score, which improves with zero-knowledge and selective-disclosure designs. Decision groups should therefore treat the scores on partner readiness and privacy as the most consequential to verify.

Discussion

When blockchain is warranted

The analysis locates the conditions. Blockchain alternatives dominate when traceability carries substantial weight and partners are ready enough to participate; the permissioned form dominates the public form unless traceability is nearly the only criterion, because it preserves privacy and partner control. When traceability matters little, the cloud platform offers most of the visibility at lower cost and integration effort, and the status quo is adequate only where traceability is immaterial. The decision therefore turns on how much the firm and its partners value traceability and on partner readiness, which the MCDA makes explicit.

Scoring from evidence

The scores used here are illustrative. In application, traceability should be scored from the granularity and latency of provenance data each alternative delivers; cost from vendor quotes and consortium fees; integration effort from system inventories; scalability from transaction volumes and platform benchmarks; partner readiness from partner surveys; and privacy from the data-exposure analysis of each design. Scoring from evidence rather than vendor claims is where most of the analytical effort should go, since the sensitivity analysis shows that ranking is stable to weights but would respond to score changes.

Consortium decision-making

Blockchain consortia require several firms to agree. MCDA supports this by making each partner's weights explicit, computing rankings under each, and identifying

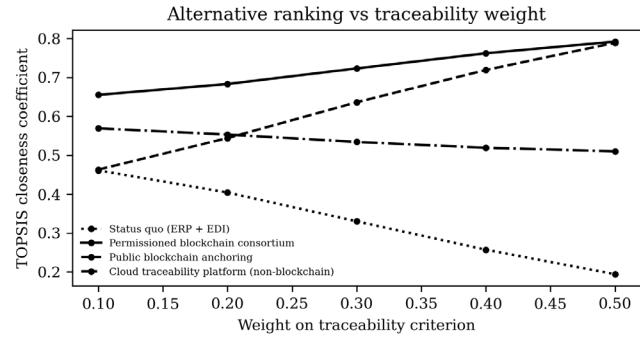


Figure 1: TOPSIS closeness coefficients of the four alternatives as the weight on traceability varies

the alternatives that rank acceptably under all. The Monte Carlo analysis is the formal version of this exercise, and its 90% agreement on the consortium alternative suggests that partners with moderately different priorities would converge.

Beyond the ranking

The analysis identifies the consortium alternative's weaknesses, cost and integration effort, as the criteria on which it scores worst. These are the areas where consortium design, such as shared infrastructure, standard interfaces and phased onboarding, should focus to raise the alternative's standing further and to address the partners for whom cost weighs heavily.

Applying the method in practice

A practical application proceeds in five steps. Convene the decision group, including supply chain, IT, finance and representatives of key partners. Elicit weights by pairwise comparison, checking consistency and recording disagreements. Score alternatives from evidence gathered through pilots, vendor assessments and partner surveys, with scoring rationales documented. Compute rankings under the group weights and under each member's weights, and run the sensitivity analyses. Report the ranking, its robustness and the criteria on which the preferred alternative is weakest, as inputs to a decision that remains the group's.

Revisiting the decision

Scores change: platform costs fall, partner readiness rises as consortia mature, and privacy techniques improve. The analysis should be repeated at intervals or when

scores move materially, since an alternative that ranks second today may rank first once a barrier such as partner readiness is overcome. Maintaining the decision matrix as a living document converts a one-time adoption decision into a monitored strategy.

Extensions of the method

Where criteria interact, for instance when scalability limits traceability at volume, outranking methods or fuzzy extensions of AHP–TOPSIS can represent the dependence. Where scores are uncertain, interval or fuzzy scores propagate the uncertainty into the closeness coefficients. Where the decision is sequential, with a pilot preceding full adoption, real-options reasoning can value the information the pilot provides. The baseline method presented here is deliberately simple so that decision groups can apply and audit it; the extensions are available where the decision warrants them.

Limitations

The scores are illustrative and the weights hypothetical; the analysis demonstrates the method and the sensitivity structure, not a recommendation for any firm. TOPSIS assumes criteria are independent and compensatory, and alternatives are treated as fixed rather than designable. Dynamic considerations such as option value, switching costs and the evolution of partner readiness are outside the model. All reported values are outputs of the illustrative analysis.

Conclusion

Blockchain adoption in supply chains is a multi-criteria decision in which traceability competes with cost, integration, scalability, partner readiness and privacy. An AHP–TOPSIS analysis of four alternatives ranked a permissioned consortium first under baseline weights and across a wide range of traceability weights, with public anchoring competitive only when traceability dominates and the cloud platform preferred only when it matters little. The method's value lies in making the trade-offs explicit, scoring from evidence and supporting agreement among partners whose priorities differ.

References

- 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 hyperchaotic system along with RSA." *Mathematics* 10, no. 7 (2022): 1071.
- Talasila, D. (2023). Enhancing cloud security with intrusion detection and prevention systems (IDPS): Comparative evaluation of signature-based, anomaly-based, and AI-powered detection models. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(3), 828–836. <https://www.ijritcc.org/index.php/ijritcc/article/view/11945>
- Dwivedi, D. (2022). Application of AI-powered vulnerability scanners in legacy applications for identifying unpatched security flaws and weak dependencies through semantic code analysis. *International Journal on Recent and Innovation Trends in Computing and Communication*, 10(12), 617–623. <https://www.ijritcc.org/index.php/ijritcc/article/view/11918>
- Mahadasu, S. S. (2024). Open RAN-based on-demand 6G agricultural networks: Adaptive edge infrastructure for autonomous farming systems. *International Journal of Data Science and IoT Management System*, 3(4), 96–102. <https://doi.org/10.64751/ijdim.2024.v3.n4.1289>
- Devulapalli, N. (2020). Implementation of compliance-as-code in regulated DevSecOps environments for automating audit readiness and reducing human error through scripted control validation. *Journal of Critical Reviews*, 7(1), 2651–2657. <https://doi.org/10.69980/jcr.v7:i1.13405>
- Mahajan, R. A., Dey, R., Khan, M., Mohd Su'ud, M., Alam, M. M., & Jadhav, P. (2025). Enhancing personalization in IoT-based health monitoring via generative AI and transfer learning. *Egyptian Informatics Journal*, 32, Article 100788. <https://doi.org/10.1016/j.eij.2025.100788>
- Chatrath, A. (2021). Integration of AI-powered forensic analysis in cloud breach investigations for accelerating root cause identification and evidence collection through log correlation techniques. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 10(8). <https://doi.org/10.15662/IJAREEIE.2021.1008051>
- Bhaskara Raju Rallabandi. (2019). Enhancing 5G NSA Performance with Lightweight Network Data Analytics Loops. *International Journal of Engineering Research and Science & Technology*, 15(4), 57–61. <https://doi.org/10.62643/ijerst.2019.v15.n4.pp57-61>
- Gupta, A. (2021). Deployment of advanced endpoint detection in remote work environments for preventing malware intrusions and data exfiltration through behavioral analytics and AI-driven responses. *NeuroQuantology*, 19(9), 1206–1224. <https://doi.org/10.48047/nq.2021.19.9.NQ21199>
- Chatrath, A. (2024). The role of encryption and key management in cloud security: Balancing performance, scalability, and confidentiality in multi-tenant and distributed data storage systems. *International Journal of Innovative Research in Science, Engineering and Technology*, 13(7). <https://doi.org/10.15680/IJIRSET.2024.1307187>
- Khan, S. (2022). Sales force security in mobile and remote work environments: Addressing authentication

- challenges, secure synchronization, and device-level threats. *International Journal of Innovative Research in Computer and Communication Engineering*, 10(12), 8735–8743. <https://doi.org/10.15680/IJIRCCCE.2022.1012040>
- Rangappa, A. S. (2021). Database security in cloud environments: Exploring multi-tenant risks, data isolation challenges, and compliance mechanisms in hybrid and public clouds. *International Journal on Recent and Innovation Trends in Computing and Communication*, 9(2), 50–57. <https://www.ijritcc.org/index.php/ijritcc/article/view/11921>
- Aggarwal, A. (2021). Utilization of continuous vulnerability scanning in DevSecOps pipelines for preemptive threat detection and secure code deployment through automated security checks. *NeuroQuantology*, 19(1), 427–442. <https://doi.org/10.48047/nq.2021.19.1.NQ21055>
- Dwivedi, D. (2020). Adoption of secure software updates in application lifecycle for preventing supply chain tampering and maintaining trust through cryptographically signed patches. *Journal of Critical Reviews*, 7(10), 6974–6980. <https://doi.org/10.69980/jcr.v7.i10.13406>
- Gupta, A. (2021). Application of cyber deception strategies in military networks for enhancing operational security and misleading attackers through adaptive honeypots and decoy systems. *NeuroQuantology*, 19(4), 317–333. <https://doi.org/10.48047/nq.2021.19.4.NQ21068>
- 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.
- Rangappa, A. S. (2020). Integration of behavioral analytics in developer workflows for detecting insider threats and malicious activities through activity monitoring and contextual profiling. *International Journal of Innovative Research in Science, Engineering and Technology*, 9(1), 13375–13383. <https://doi.org/10.15680/IJIRSET.2020.0901064>
- 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>
- 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.
- Mahadasu, S. S. (2025). Distributed AI-RAN inference placement for joint radio optimization and edge workload acceleration. *International Journal of AI Electronics and Nexus Energy*, 1(1), 39–44. <https://doi.org/10.64751/7ep35m50>
- Anchala, S. (2023). Utilization of blockchain technology in cloud storage systems for enhancing data integrity and preventing unauthorized modifications through decentralized validation. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(5), 629–637. <https://www.ijritcc.org/index.php/ijritcc/article/view/11942>
- Jain, Arpit, Nageswara Rao Moparthy, 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.
- 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>
- Anchala, S. (2020). Cloud security challenges in supply chain systems: Addressing vendor risks, data integrity, and third-party service provider vulnerabilities. *Journal of Critical Reviews*, 7(2). <https://doi.org/10.69980/jcr.v7.i2.13401>
- Mahadasu, S. S. (2025). AI-enhanced service management and orchestration for rApp and xApp lifecycle automation in Open RAN. *Communications on Applied Nonlinear Analysis*, 32(2s), 794–807. <https://doi.org/10.52783/cana.v32.6716>
- Rangappa, A. S. (2020). Deployment of cross-platform code scanning tools in polyglot DevSecOps projects for uniform security testing and language-agnostic vulnerability coverage. *Journal of Critical Reviews*, 7(11), 5000–5006. <https://doi.org/10.69980/jcr.v7.i11.13402>
- Bhanushali, B. (2023). Blockchain for trade finance: Enhancing cross-border payment transparency, reducing processing time, and mitigating fraud through distributed ledger systems. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 5690–5697. <https://www.ijritcc.org/index.php/ijritcc/article/view/11932>
- Aggarwal, A. (2022). Cloud security in artificial intelligence workloads: Protecting model training, data confidentiality, and AI-generated insights in cloud-based machine learning pipelines. *NeuroQuantology*, 20(3), 1367–1382. <https://doi.org/10.48047/nq.2022.20.3.NQ23004>
- Bhaskara Raju Rallabandi. (2019). *Comprehensive Design and Field Performance Assessment of Early 5G NSA*

- Private Networks for Industrial IoT Campuses. *International Journal of Engineering Research and Science & Technology*, 15(1), 22–26. <https://doi.org/10.62643/ijerst.2019.v15.n1.pp22-26>
- 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.
- Talasila, D. (2020). Deployment of dynamic data masking in cloud-based applications for protecting sensitive information and enhancing privacy controls through contextual access filtering. *Journal of Critical Reviews*, 7(9), 4056–4062. <https://doi.org/10.69980/jcr.v7.i9.13403>
- Kumar, S., Jain, A., & Moparthy, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
- Chatrath, A. (2021). Implementation of AI in recruitment platforms for improving candidate screening and diversity inclusion through bias-free resume parsing and skill matching. *International Journal of Innovative Research in Computer and Communication Engineering*, 9(12). <https://doi.org/10.15680/IJIRCC.2021.0912046>
- Anchala, S. (2023). Integration of confidential computing in multi-cloud environments for enhancing data privacy and regulatory compliance through encrypted processing and isolated execution. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 5698–5709. <https://www.ijritcc.org/index.php/ijritcc/article/view/11933>
- Talasila, D. (2023). Implementation of cloud-based disaster recovery models for minimizing business downtime and ensuring operational continuity through geographically distributed backup systems. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(8), 867–874. <https://www.ijritcc.org/index.php/ijritcc/article/view/11934>
- Devulapalli, N. (2019). Post-quantum cryptography for database security: Preparing for the impact of quantum computing on encrypted data storage and secure queries. *Journal of Critical Reviews*, 6(1), 614–620. <https://doi.org/10.69980/jcr.v6.i1.13396>
- Khan, S. (2022). The use of artificial intelligence in ESG (environmental, social, and governance) investing: A study on AI models for sustainability analytics in asset and wealth management. *International Journal of Multidisciplinary and Scientific Emerging Research*, 10(1), 431–439. <https://doi.org/10.15662/IJMSERH.2022.1001046>
- 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.
- Mahadasu, S. S. (2024). Real-time network digital twin synchronization for predictive capacity planning in multi-vendor private 5G systems. *International Journal of Engineering Research and Science & Technology*, 20(4), 483–488. <https://doi.org/10.62643/ijerst.2024.v20.n4.4405>
- Bhanushali, B. (2022). Blockchain-driven carbon credit trading systems for improving environmental transparency, reducing double counting, and ensuring accountability in climate finance. *International Journal on Recent and Innovation Trends in Computing and Communication*, 10(11), 292–300. <https://www.ijritcc.org/index.php/ijritcc/article/view/11927>
- Khan, S. (2019). Sales force security compliance: An in-depth study of GDPR, HIPAA, and PCI-DSS enforcement in cloud-based CRM systems and their implications for global enterprises. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 8(9), 2211–2219. <https://doi.org/10.15662/IJAREEIE.2019.0809010>
- 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>
- Bhanushali, B. (2024). Tokenization of real-world assets through block chain for improving liquidity, enabling fractional ownership, and reducing transaction costs in global financial markets. *International Journal of Advanced Research in Education and Technology*, 11(4), 1809–1816. <https://doi.org/10.15680/IJARETY.2024.1104071>
- Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." *Procedia Computer Science* 48 (2015): 330–337.
- Bhaskara Raju Rallabandi. (2024). 6G Cross-Layer Intent Engine: Automated Translation from Business Requirements to Network Policies and Real-Time Scheduling Controls. *International Journal of Data Science and IoT Management System*, 3(1), 44–48. <https://doi.org/10.64751/ijdim.2024.v3.n1.pp44-48>
- 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.
- Aggarwal, A. (2021). Implementation of machine learning in cloud SIEM solutions for enhancing threat detection accuracy and reducing alert fatigue through correlation-based anomaly detection.

- NeuroQuantology, 19(10). <https://doi.org/10.48047/nq.2021.19.10.NQ21226>
- Devulapalli, N. (2020). The evolution of database security from centralized architectures to distributed cloud-native systems: A comparative and historical perspective. *Turkish Online Journal of Qualitative Inquiry*, 11(4), 2954–2963. <https://doi.org/10.69980/j1064z97>
- Dwivedi, D. (2019). The use of homomorphic encryption in cloud security: Enabling secure data processing, confidential query execution, and privacy-preserving cloud applications. *International Journal of Innovative Research in Science, Engineering and Technology*, 8(4), 4690–4698. <https://doi.org/10.15680/IJIRSET.2019.0804136>
- Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. *Scientific Programming*, 2022(1), 6438331.
- Pandit, T., Raval, M., & Upadhyay, D. (2025). Multi-domain ABSA conversation dataset generation via LLMs for real-world evaluation and model comparison (arXiv:2505.24701). *arXiv*. <https://arxiv.org/abs/2505.24701>
- Gupta, A. (2021). Implementation of cyber threat hunting in hybrid cloud environments for early breach detection and threat containment through behavior-based analysis tools. *NeuroQuantology*, 19(12), 1312–1329. <https://doi.org/10.48047/nq.2021.19.12.NQ21342>
- Bhaskara Raju Rallabandi. (2023). AGENTIC-AI xAPPS: O-RANMULTI-AGENTCONTROLFORENTERPRISE POLICY, SCHEDULING & SPECTRUM. *International Journal of Data Science and IoT Management System*, 2(4), 54–58. <https://doi.org/10.64751/ijdim.2023.v2.n4.pp54-58>