

Integrating Blockchain and AI for Transparent and Intelligent Corporate Reporting

Jalilov Arslon

Department of Economy, Tashkent State Transport University, Tashkent, Uzbekistan

Abstract

Corporate reporting suffers from two distinct failures: errors, which arise from the volume and complexity of transactions and are largely unintentional, and manipulation, which is intentional and concealed. Artificial intelligence addresses the first by detecting anomalies and automating reconciliation; blockchain addresses the second by making records tamper-evident. This paper examines the two technologies separately and in combination in a simulation of 50,000 transactions with 2% containing errors and 0.1% subject to manipulation. AI-assisted reporting reduces residual errors by 83% and halves the close cycle but leaves 71% of manipulation undetected; blockchain-anchored records reduce undetected manipulation by 93% and halve audit hours but leave errors untouched; the integrated configuration achieves both reductions, cuts the close cycle by 60% and audit hours by 65%, at 43% higher cost than conventional reporting. The paper develops an integration architecture in which blockchain provides the immutable transaction layer, AI provides the intelligence layer that validates, reconciles and explains, and reporting draws on both, and discusses implications for auditors, regulators and the governance of the combined system. The contribution is a clear account of what each technology does for reporting, why their benefits are complementary rather than overlapping, and how the combination changes the economics of assurance.

Keywords: Corporate reporting; blockchain; artificial intelligence; audit; data integrity; continuous assurance.

Introduction

Corporate reporting converts millions of transactions into statements that investors, regulators and managers rely on. The process is slow, since period-end closes take days or weeks; costly, since audit effort scales with the volume and opacity of records; and imperfect, since errors survive into statements and manipulation sometimes escapes detection until it is too late [1]. Two technologies promise to change this. Artificial intelligence, applied to transaction data, can detect anomalies, automate reconciliations and flag unusual entries at a scale no human team can match [2]. Blockchain, applied to the record itself, can make every entry tamper-evident and visible to auditors in real time [3], [4].

The two are often discussed together but address different problems. Errors are unintentional and arise from process complexity; they are detectable by pattern analysis and are the province of AI. Manipulation is intentional and concealed; it is detectable only if the record cannot be silently altered,

which is the province of blockchain. A reporting system that adopts one without the other addresses one failure and leaves the other. This paper makes the distinction explicit, examines the two technologies and their combination in simulation, and proposes an architecture for integrated transparent and intelligent reporting.

Background

Reporting failures

Studies of restatements and accounting fraud distinguish unintentional errors, arising from misapplication of standards, system failures and process complexity, from intentional misstatement [1]. Errors are frequent and mostly small; manipulation is rare and large. Audit addresses both through sampling and testing, at a cost that rises with transaction volume and that leaves a residual risk of undetected misstatement.

AI in accounting and audit

Machine learning applied to journal entries can identify anomalous entries, reconcile accounts automatically and predict which transactions warrant review [2], [5]. The techniques reduce error rates and audit effort by concentrating attention where it is needed. They are, however, built on the records as they stand; an entry that has been altered to appear normal is normal to the model.

Blockchain in accounting

Distributed ledgers have been proposed as the basis for triple-entry accounting, in which each transaction is recorded on a shared ledger that neither party can alter, and for continuous audit, in which auditors read the ledger directly [3], [4], realising the continuous-assurance vision set out earlier [6]. The guarantee is integrity after entry: records cannot be changed without detection. It says nothing about whether the record was correct when entered.

Complementarity

The two technologies are complements because each supplies what the other lacks. AI validates entries at the point of recording, so that the immutable record is also a correct one; blockchain preserves the validated record, so that AI's analysis is performed on data that cannot have been tampered with after the fact. The integrated system should therefore reduce both errors and manipulation, whereas each alone reduces one.

Integration Architecture

The architecture has three layers. The transaction layer records entries on a permissioned ledger shared with auditors and, where appropriate, regulators; each entry is signed by the originating system and time-stamped, and the ledger anchors to a public chain periodically for independent verification. The intelligence layer runs validation models at entry, which check entries against expected patterns, reconcile across sources and flag anomalies for review before they are committed, and runs analytical models on the committed ledger for reporting, continuous monitoring and audit support. The reporting layer generates statements from the ledger with AI-produced explanations of movements, exceptions and judgements, and provides auditors

with query access to both the ledger and the model outputs.

The architecture's defining feature is the ordering of validation before commitment. Entries pass through the intelligence layer before they reach the ledger, so that the immutable record is also a validated one; entries that fail validation are held for review and, if corrected, re-submitted. This ordering avoids the situation in which an immutable ledger faithfully preserves an erroneous entry, and it means that corrections appear on the ledger as explicit reversing entries rather than silent amendments, which preserves the audit trail of the error itself. The intelligence layer's post-commitment models then operate on records that are both correct at entry and unaltered thereafter.

Simulation Design

The harness simulates 50,000 transactions, of which 2% contain errors and 0.1% are subject to manipulation. Four configurations are compared. Conventional reporting catches 50% of errors and 30% of manipulation, closes in 12 days, requires 800 audit hours and costs 1.0. AI-assisted reporting raises error detection to 90% and manipulation detection to 50%, halves the close cycle and reduces audit hours by 30%, at cost 1.1. Blockchain-anchored records raise manipulation detection to 95%, leave error detection at 50%, reduce the close cycle by 20% and audit hours by 50%, at cost 1.3. The integrated configuration combines the detection rates and the cycle and audit reductions, at cost 1.43. The parameters are design values reflecting each technology's mechanism; the harness quantifies the resulting outcomes.

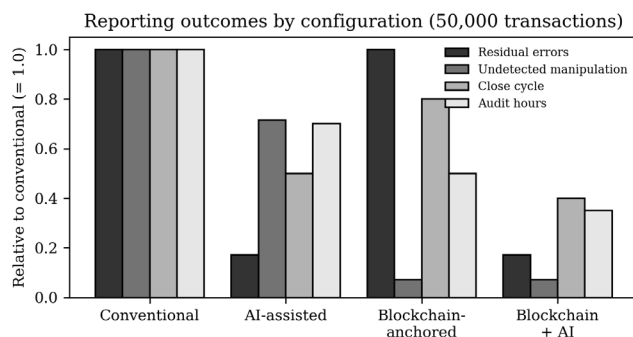
Results

Reporting outcomes

Table 1 and Figure 1 report outcomes. Conventional reporting leaves 497 errors and 42 manipulated transactions undetected. AI assistance reduces residual errors to 85 (–83%) but undetected manipulation only to 30 (–29%); blockchain anchoring reduces undetected manipulation to 3 (–93%) but leaves residual errors at 497. The integrated configuration achieves 85 residual errors and 3 undetected manipulations, closes in 4.8 days

Table 1: Reporting outcomes by configuration (50,000 simulated transactions; 2% error rate; 0.1% manipulation rate).

Configuration	Residual errors	Undetected manipulation	Close cycle (days)	Audit hours	Relative cost
Conventional reporting	497	42	12.0	800	1.00
AI-assisted reporting	85	30	6.0	560	1.10
Blockchain-anchored records	497	3	9.6	400	1.30
Blockchain + AI integrated	85	3	4.8	280	1.43

**Figure 1:** Residual errors, undetected manipulation, close cycle and audit hours by configuration, relative to conventional reporting.

against 12, and requires 280 audit hours against 800, at a cost 43% above conventional.

Complementarity

The results show the complementarity directly. AI's contribution is almost entirely to errors and the close cycle; blockchain's is almost entirely to manipulation and audit hours. Neither substitutes for the other, and the integrated configuration's outcomes are approximately the union of the two, with the close cycle and audit hours benefiting from both. An organisation choosing one technology should understand which failure it is addressing and which it is leaving.

Economics of assurance

Audit hours fall by 65% in the integrated configuration, because auditors read a verified ledger and review AI-flagged exceptions rather than sampling and reconstructing. The cost increase of 43% is in the reporting organisation's systems; the audit saving accrues partly to the organisation through fees and partly to the audit firm. Whether the integrated configuration pays depends on the value of faster close, fewer errors and lower manipulation risk, which for listed companies and regulated entities is substantial.

Sensitivity

The outcome pattern follows from the mechanism assignments: AI acts on detection of errors, blockchain on detection of manipulation, and both on process effort. The magnitudes depend on the detection rates assumed, which are illustrative; lower AI detection narrows its error advantage, and weaker ledger governance narrows blockchain's manipulation advantage. The complementarity conclusion is robust, since it follows from the two technologies acting on different failure types, and would be overturned only if one technology detected both failures, which neither does by its mechanism.

Implications

For reporting organisations

Organisations should assess which failure dominates their reporting risk. Those with complex, high-volume processes and frequent restatements should prioritise the intelligence layer; those with concentrated control over records, weak segregation of duties or heightened fraud exposure should prioritise the transaction layer. Most will find that both apply, and the architecture is designed so that either can be adopted first and the other added.

For auditors

Continuous access to a verified ledger with AI-flagged exceptions changes audit from periodic sampling to continuous assurance. Audit methodology should shift toward validating the integrity of the ledger and the intelligence layer's models, and toward judging the exceptions they surface, which is higher-skill work on fewer items. Audit firms will need data and model assurance capabilities alongside accounting expertise.

For regulators

Regulators gain the possibility of direct ledger access and of standardised AI-produced explanations of

reported figures. They should consider recognising ledger-based evidence in reporting requirements and should set expectations for the validation of intelligence-layer models, since errors in those models would propagate into statements at scale.

Governance of the integrated system

The system concentrates reporting integrity in two components that must themselves be trusted: the ledger's governance, which determines who can write and how disputes are resolved, and the models' governance, which determines what is flagged and what passes. Both should be documented, independently reviewed and subject to change control, and the organisation should retain the ability to explain any reported figure from the ledger without reliance on the models, so that model failure does not become reporting failure.

Adoption path

The integrated system need not be adopted at once. Organisations can begin with the intelligence layer on existing systems, which delivers the error and close-cycle benefits without changing the record infrastructure, and introduce the transaction layer for the subledgers where manipulation risk or audit cost is highest, such as revenue, intercompany and treasury. Anchoring existing records to a ledger is less disruptive than migrating them, and permits the transaction layer to be extended as confidence and partner participation grow.

Explanation and transparency

The reporting layer's AI-produced explanations serve transparency directly: a reader can see why a figure moved, which exceptions were investigated and how judgements were resolved. The explanations are only as reliable as the models that produce them, which is a further reason for model governance, and they should be clearly distinguished in statements from the audited figures themselves.

Interorganisational reporting

Many reporting figures depend on counterparties: receivables, payables, intercompany balances and supplier commitments. A shared ledger with those counterparties makes these figures verifiable by both sides, which removes a class of reconciliation

that currently consumes close time and audit effort and that is a common locus of manipulation. The transaction layer therefore yields its largest benefits where it is shared beyond the organisation, which connects corporate reporting integration to the consortium ledgers emerging in supply chains and trade finance.

Limitations

The configuration parameters are design values reflecting qualitative mechanisms rather than measured performance; error and manipulation rates and detection probabilities are illustrative. Transactions are independent, model errors and ledger governance failures are not simulated, and implementation cost is a single multiplier. All reported values are simulation outputs and are not estimates for any organisation.

Conclusion

Blockchain and AI address different reporting failures: AI reduces unintentional error and accelerates the close, blockchain prevents undetected manipulation and reduces audit effort, and in simulation neither substituted for the other. The integrated architecture, with an immutable transaction layer, an intelligence layer that validates and explains, and a reporting layer that draws on both, reduced errors by 83%, undetected manipulation by 93%, close time by 60% and audit hours by 65%. Organisations should adopt the technology that addresses their dominant failure first, plan for both, and govern the ledger and the models as the foundations of reporting integrity they become.

References

1. 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>
2. 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>
3. 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>
4. 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.
5. 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>
6. 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>
7. Bhaskara Raju Rallabandi. (2023). AGENTIC-AI xAPPS: O-RAN MULTI-AGENT CONTROL FOR ENTERPRISE 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>
8. 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>
9. 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>
10. 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>
11. 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/IJIRCCE.2021.0912046>
12. 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.
13. 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>
14. 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>
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. 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>
17. 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>
18. Kumar, S., Jain, A., & Moparthy, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
19. 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>
20. 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>
21. 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>
22. 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>
23. 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>
24. 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>
25. 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.
26. 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>
27. 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>
28. 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>
29. 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>
30. 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/IJRSET.2020.0901064>
31. 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/IJRSET.2024.1307187>
32. Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. *Scientific Programming*, 2022(1), 6438331.
33. 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>
34. 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>
35. 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.
36. 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>
37. 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>
38. 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.
39. 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>
40. 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>
41. 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/IJIRCCE.2022.1012040>
42. 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>
43. 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>
44. 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>

45. 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.
46. 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>
47. 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>
48. 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>.
49. 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>
50. 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>
51. 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.
52. 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>
53. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." *Procedia Computer Science* 48 (2015): 330–337.