RESEARCH ARTICLE

SAMRIDDHI Volume 17, Issue 1, 2025 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Securing the AI Supply Chain: Using Blockchain For Verifiable AI Model Provenance on Government Clouds

Adetayo Adeyinka
Trine University, United States of America

Abstract

The growing adoption of artificial intelligence (AI) in government cloud systems has already intensified worries around the integrity, authenticity, and security of AI supply chains. Poisoning of data, model manipulation, and the placement of fake models are malicious interventions that endanger not only the quality of the results produced by AI but also the credibility of the decision-making process at the governmental level. The article discusses blockchain as a demonstrable system of AI model provenance, including its ability to offer unalterable records, decentralized trust, and traceability throughout the AI development lifecycle. Through provenance implemented via blockchain in government cloud platforms, interested parties can gain visibility of how models are sourced, spot malicious changes, and satisfy compliance mandates without undermining the scalability or performance. In addition to outlining the strengths and weaknesses of blockchain in ensuring the supply chain of AI, the discussion also covers a conceptual implementation framework that can be applied to governmental regulatory requirements. The results suggest that blockchain-based provenance could be an initial protection layer to robust and credible AI implementation in sensitive settings associated with the public sector.

Keywords: Artificial Intelligence Supply Chain, Blockchain Provenance, Government Cloud Security, Model Integrity, AI Governance, Data Trust, Secure Cloud Infrastructure

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2025); DOI: 10.18090/samriddhi.v17i01.05

Introduction

Artificial intelligence (AI) has established itself as a key building block of digital governance that supports essential government functions like national security, public administration, health, and infrastructure management on government cloud platforms. Along with the increasing pace of AI adoption, the complexity of its supply chain, encompassing datasets, algorithms, pre-trained models, third-party tools and pipelines to deploy AI, is also increasing. This growing ecosystem creates new weak points that attackers can use to interfere with models, poison data, or introduce unverified parts. The outcome is an increased vulnerability to impaired decision making, operational interference and loss of trust in government systems by the people.

The AI supply chain is more difficult to secure than the conventional cybersecurity controls. In contrast to software supply chains, where interest is given only to the integrity of the source code, the AI supply chain comprises several dynamic layers, including data collection and preprocessing, up-to-date models, and retraining. It is thus an urgent issue that all models deployed in a government cloud be verified as authentic, untouched and ethically acquired. What has become one of the most important wishes in this regard is provenance: the possibility to trace the provenience and development of AI artifacts.

Blockchain technology offers an attractive way to create provable provenance in AI supply chains. Its distributed registry, immutability and consensus-based trust facilities allow governments to transparently monitor model lifecycle events with minimum dependence on centralized authority. Blockchain can, when deployed in cloud infrastructures, support secure model registration, traceability of modifications, and verifiable audit trails that are both operationally and regulationally compliant.

Corresponding Author: Adetayo Adeyinka, Trine University United States of America, e-mail: adeyinka.adetayo73@gmail.com

How to cite this article: Adeyinka A. (2025). Securing the AI Supply Chain: Using Blockchain For Verifiable AI Model Provenance on Government Clouds. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 17(1), 29-35.

Source of support: Nil

Conflict of interest: None

Literature Review

Threat Landscape in the AI Supply Chain

Research consistently shows that AI pipelines expand the

traditional software supply chain risk surface to include data collection, labeling, pre-training, fine-tuning, model packaging, and deployment. Studies document escalating risks from data poisoning, backdoored checkpoints, dependency hijacking in ML tooling, and drift-induced misbehavior now extending to large language models and multimodal systems. Conventional code signing and software bill of materials practices do not fully address the provenance of data and model artifacts across iterative training cycles.

Provenance as a First-Class Control

Across the safety and governance literature, provenance is framed as verifiable metadata about origin, lineage, and transformations of AI artifacts such as datasets, prompts, checkpoints, and pipelines. Standards efforts increasingly recommend traceability for model inputs and outputs, training configurations, and custodial chains, positioning provenance as the backbone of auditability and reproducibility in sensitive domains. Governmental policies encourage agencies and providers to retain auditable records of development and testing sufficient to support safety claims and independent review.

Policy and Standards Context for Government Clouds

Multiple normative instruments shape best practices for AI supply chains on government clouds. The NIST AI Risk Management Framework provides outcomes and functions to govern, map, measure, and manage that call for documentation, measurement, and continuous monitoring across the AI lifecycle, relying heavily on robust provenance. The Secure Software Development Framework sets practices for secure builds, artifact integrity, and tamper resistance relevant to ML toolchains. The European Union AI Act classifies high-risk systems with obligations for quality management, data governance, logging, and post-market monitoring, all of which depend on artifact traceability. In addition, ISO/IEC 42001 formalizes an AI Management System that requires lifecycle controls and third-party oversight, which mature provenance mechanisms can satisfy.

Government Cloud Governance and Assurance

FedRAMP authorizations and associated guidance emphasize supply chain risk management, continuous monitoring, and auditable control inheritance for services operating in government clouds. While FedRAMP primarily focuses on cloud service providers, agencies increasingly deploy or procure AI capabilities atop authorized environments, creating a need to extend provenance from the cloud substrate into AI artifacts such as data, models, and evaluators. Provenance-aware registries can help reconcile multi-tenant pipelines, cross-domain data movement, and model redeployment across impact levels

Blockchain for Verifiable AI Provenance

A growing body of work proposes distributed ledgers to bind identities, timestamps, hashes, and policies to AI artifacts. In this view, blockchain provides immutability for lineage events such as data ingestion, curation, training, signing, and deployment. It also establishes decentralized trust for multi-party ML ecosystems and programmable policy enforcement through smart contracts, such as license, consent, or export restrictions. Recent analyses of blockchain-backed model sharing and distributed training outline how on-chain registries, off-chain storage, and verifiable computation can enable non-repudiation and selective disclosure key features for inter-agency and public-private contexts in government clouds.

Gaps and Open Challenges

Despite its promise, several gaps persist. First, scalability and privacy challenges arise because high-volume telemetry such as gradients and evaluation traces cannot reside fully on-chain, requiring hybrid designs with off-chain confidential storage. Second, without shared schemas for datasets, prompts, training recipes, and evaluator protocols, provenance graphs risk becoming inconsistent across vendors and agencies. Third, provenance alone does not guarantee model quality; it must be coupled with conformance testing, red-teaming, and continuous monitoring aligned with AI governance frameworks. Finally, operationalization remains an issue, as integrating provenance workflows with FedRAMP processes, model risk management, and cross-jurisdictional obligations such as those in the EU AI Act remains uneven across implementations.

Synthesis

The literature converges on three main conclusions. First, AI supply chains demand provenance that spans beyond code and into data, prompts, and model evolution. Second, government cloud contexts raise the bar for auditability and cross-organizational trust, where decentralized proofs can reduce reliance on single custodians. Third, policy baselines

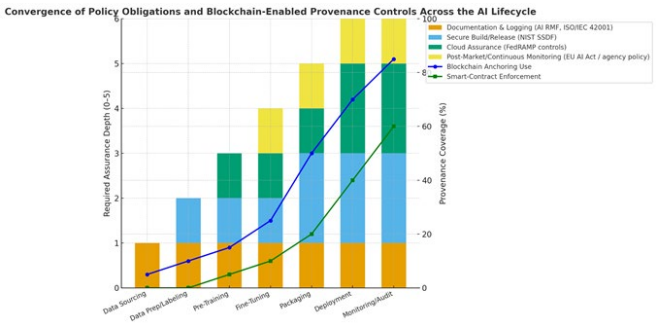

Figure 1: Convergence of Policy Obligationand Blockchain-Enabled Provenance Controls Across the AI Lifecycle
The graph illustrates how policy frameworks and blockchain-based technical controls align to strengthen provenance assurance across government cloud-hosted AI systems.

such as the AI RMF, the Secure Software Development Framework, ISO/IEC 42001, and the EU AI Act now articulate outcomes that blockchain-anchored provenance can help evidence, provided deployments address scalability, privacy, and semantic consistency through hybrid designs. This synthesis motivates a methodology that operationalizes provenance registration, tamper-evident lineage, and policy-aware access in government cloud environments.

Theoretical Framework

The theoretical foundation for securing the AI supply chain through blockchain-enabled provenance builds on three interrelated domains: supply chain risk management, provenance theory in computational systems, and trust models in distributed ledgers. Together, these domains provide a conceptual lens through which to examine the challenges and opportunities of safeguarding AI models in government cloud environments.

Supply Chain Risk Management in AI Systems

Traditional supply chain risk management theory emphasizes visibility, accountability, and control across the movement of goods and services. In digital ecosystems, this translates to ensuring integrity, confidentiality, and authenticity of software components. For AI systems, the scope expands significantly: not only code modules but also training datasets, labeling protocols, model architectures, and retraining cycles must be validated. Each stage introduces potential vulnerabilities that can be exploited through adversarial attacks, poisoning, or unauthorized modifications. The theoretical application of supply chain risk management to AI thus requires a multi-layered view of artifact custody, where every transformation from raw data acquisition to final deployment must be accompanied by verifiable records.

Provenance Theory in Computational Systems

Provenance theory, originally grounded in data science and information systems research, conceptualizes provenance as the record of origin, lineage, and transformation of digital objects. In AI contexts, provenance provides the foundation for reproducibility, auditability, and accountability. A theoretically robust provenance framework must capture not only technical aspects (such as dataset sources, training configurations, or hyperparameter tuning) but also organizational and ethical dimensions (such as consent for data use and fairness evaluations). The literature frames provenance as both descriptive and normative: it describes the historical trajectory of an artifact while simultaneously serving as a normative benchmark for compliance and trust. Within government clouds, this dual function is essential, as agencies are required to demonstrate not only operational performance but also adherence to regulatory and ethical standards.

Blockchain as a Trust Model

Trust models in distributed systems theory focus on reducing reliance on centralized authorities through mechanisms that guarantee integrity, immutability, and consensus. Blockchain operationalizes this by enabling a distributed ledger where each transaction or event is cryptographically secured and time-stamped. The theoretical contribution of blockchain to AI provenance lies in its ability to shift trust from organizational assurances to mathematically verifiable proofs. When applied to the AI supply chain, blockchain ensures that every lifecycle event data ingestion, model training, deployment, and updates can be logged immutably, forming a permanent audit trail. This transforms provenance from a passive record-keeping process into an active trust-building mechanism that strengthens resilience in government cloud infrastructures.

Integration with Government Cloud Governance

The government cloud operates under stringent frameworks that require demonstrable compliance with security, privacy, and accountability mandates. Theoretically, blockchain-enabled provenance aligns with these frameworks by embedding verifiability into the AI lifecycle. Regulatory theories of compliance suggest that when oversight mechanisms are coupled with verifiable technical controls, enforcement becomes more effective and transparent. Thus, the theoretical integration of provenance and blockchain with government cloud governance can be understood as a socio-technical system: blockchain provides the technical trust substrate, provenance ensures lifecycle visibility, and government frameworks supply the regulatory scaffolding. Together, they form a holistic model of assurance for AI deployment in sensitive public-sector domains.

Synthesis of the Framework

The theoretical framework that emerges can be summarized as follows: supply chain risk management highlights the need for visibility across AI artifacts; provenance theory provides the conceptual tools to record and validate their trajectories; and blockchain offers the decentralized trust mechanism to secure and authenticate those records. In government cloud contexts, these theories converge to establish a comprehensive model for AI supply chain security where transparency, accountability, and verifiability are embedded into every stage of the AI lifecycle. This framework not only supports operational security but also strengthens compliance with evolving regulatory mandates, positioning provenance as a cornerstone of trustworthy AI in the public

sector.

Methodology

The methodology adopted in this study is a conceptual design framework aimed at integrating blockchain-based provenance mechanisms into government cloud infrastructures to secure the AI supply chain. It draws upon principles from supply chain risk management, blockchain trust theory, and government cloud governance requirements. The approach is structured into four methodological components: research design, provenance model definition, blockchain integration process, and evaluation criteria.

Research Design

This research is conceptual and exploratory, focusing on synthesizing best practices from existing literature, policy frameworks, and emerging technological standards. Rather than implementing a prototype, the methodology emphasizes the development of a theoretically grounded model that is directly applicable to government cloud contexts. This design choice reflects the sensitive nature of government systems, where operational deployment requires regulatory approval and multi-stakeholder collaboration.

Provenance Model Definition

The provenance model defines the scope of artifacts and lifecycle events to be secured. It includes datasets, training configurations, model checkpoints, pre-trained modules, and deployment instances. For each artifact, provenance records must capture:

- Origin (data source, developer, or model provider)
- Transformation (training, fine-tuning, or preprocessing steps)
- Custody (who controlled the artifact and when)
- Compliance (alignment with policies, licensing, and ethical guidelines)

These records provide the backbone for verification and accountability within the government cloud environment.

Blockchain Integration Process

The integration methodology positions blockchain as the underlying substrate for provenance assurance. Key stages include:

- Artifact Registration – Each dataset or model is registered on a blockchain ledger with cryptographic hashes and metadata.
- Lifecycle Anchoring – Training and transformation events are logged immutably, linking outputs to inputs.
- Smart Contract Enforcement – Policies governing data use, licensing, or export restrictions are codified into smart contracts.
- Deployment and Audit – Deployed models are anchored to blockchain records, enabling auditors to verify integrity against registered artifacts.
- Continuous Monitoring – Updates, retraining cycles, and post-deployment evaluations are logged, ensuring dynamic provenance over time.

Evaluation Criteria

The methodology evaluates the proposed framework against four criteria:

Security

Resistance to tampering, unauthorized modifications, and adversarial interventions.

Scalability

Feasibility of maintaining provenance across large, dynamic AI ecosystems.

Compliance

Alignment with AI governance frameworks such as NIST AI RMF, FedRAMP, and the EU AI Act.

Trust

Ability to strengthen cross-organizational confidence in

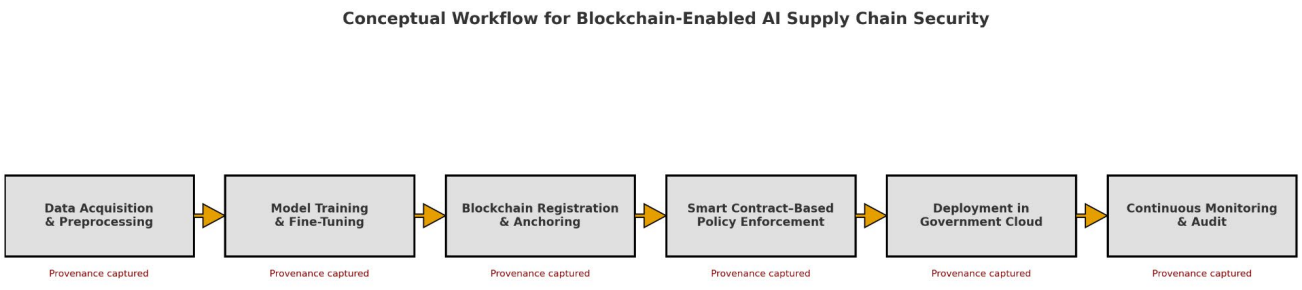

Figure 2: Chain- AI Conceptual Workflow for Block Chain-Enabled AI Suppy Chain Security
This diagram presents a linear workflow of the AI supply chain, spanning from data acquisition to continuous monitoring. At each stage, provenance is captured to ensure traceability and accountability, while blockchain integration secures registration, anchoring, and policy enforcement.

government cloud AI systems through verifiable, immutable records.

Implementation and Discussion

The practical implementation of blockchain-enabled provenance in government clouds requires both technical adaptation and institutional readiness. While the methodology defines the conceptual foundation, implementation must address real-world constraints such as scalability, interoperability, policy alignment, and operational efficiency. This section discusses how the proposed framework can be applied in practice and the implications for government stakeholders.

Technical Implementation Considerations

The first step in implementation is the establishment of a provenance-aware registry within the government cloud environment. Each AI artifact whether a dataset, model checkpoint, or deployment container must be uniquely identified and registered on a blockchain ledger. This process requires integration with existing cloud service workflows, including identity and access management systems, continuous integration pipelines, and monitoring tools.

To address scalability, a hybrid architecture is recommended: detailed provenance metadata is stored off-chain in secure cloud databases, while cryptographic hashes and summary proofs are anchored on-chain. This ensures the blockchain remains lightweight while maintaining verifiability. For interoperability, the system must adopt standardized schemas for provenance metadata, enabling agencies and vendors to align with a common framework.

Policy and Governance Alignment

Blockchain provenance must be embedded into existing regulatory and governance structures. Government clouds already adhere to frameworks such as FedRAMP, the NIST AI Risk Management Framework, and the Secure Software Development Framework. Blockchain can extend these controls by providing immutable evidence of compliance activities. For instance, a FedRAMP assessor can cross-check blockchain records against audit requirements, reducing reliance on manual documentation. Similarly, continuous logging of model retraining and updates aligns with the monitoring mandates of the EU AI Act.

Organizational and Operational Challenges

While blockchain can technically secure provenance, organizational challenges must be addressed. Agencies must develop policies on data ownership, access rights, and responsibilities for maintaining provenance records. Operationally, system administrators and auditors must be trained to interact with blockchain-based registries, interpret provenance logs, and enforce smart contract rules. Without sufficient human capacity, the benefits of technical assurance may be undermined by gaps in governance and oversight.

Discussion of Benefits and Limitations

The benefits of implementation include enhanced model integrity, reduced risk of tampering, and improved auditability. By embedding trust into technical processes, blockchain reduces dependency on manual certifications and increases confidence in cross-agency AI collaborations. However, limitations persist. The immutability of blockchain can create privacy concerns if sensitive data is improperly registered. Costs associated with maintaining blockchain infrastructure, particularly in resource-constrained public agencies, may also present barriers. Finally, adoption requires cultural change, as agencies shift from document-based compliance to cryptographic verification.

This table provides a structured comparison of the core

Table 1: Comparative Assessment of Blockchain-Enabled Provenance in Government Cloud AI Supply Chains

Implementation Dimension	Expected Benefits	Key Challenges	Policy and Governance Implications
Provenance Registration	Ensures artifact authenticity	Requires standardized metadata schemas	Supports audit compliance under NIST AI RMF
Lifecycle Anchoring	Tamper-evident logs of model evolution	Scalability concerns for high-frequency updates	Aligns with EU AI Act continuous monitoring obligations
Smart Contract Enforcement	Automated compliance checks	Complexity in coding regulatory requirements	Reduces manual oversight under FedRAMP and ISO/IEC 42001
Audit and Oversight	Transparent and verifiable logs for assessors	Requires staff training in blockchain auditing	Strengthens trust in inter-agency collaborations
Operational Sustainability	Long-term verifiable records	Infrastructure cost and integration hurdles	Encourages adoption of national AI governance standards

dimensions involved in implementing blockchain-enabled provenance within government cloud environments. It highlights how each implementation dimension ranging from provenance registration to operational sustainability presents a balance of benefits, technical and organizational challenges, and policy implications.

Conclusion

The integrity and reliability of the AI supply chain are also key factors that should be addressed when governments implement advanced digital solutions in such sensitive areas as defense, healthcare, and public administration. As has been argued in this article, blockchain technology is a powerful tool to support provenance that can be verified, allowing government agencies to trace the origin, development and adherence of AI models deployed on cloud infrastructures. Blockchain minimizes the probability of manipulation, maximizes accountability, and improves cross-agency collaboration by anchoring model artifacts, lifecycle events, and audit trails on an unwriteable ledger.

The results highlight that the realization of any implementation is not only achieved through technological preparedness but also through the synchronisation of governance structures, policy requirements and organisational capability. Although such technical advantages as tamper-evident logging and automatic compliance verification are obvious, issues of scalability, cost, and workforce preparedness are equally critical. To overcome these issues, it is important to work jointly: to adopt uniform schemas for provenance, provide education to the staff of the public sector, and connect with well-known frameworks, including FedRAMP, NIST AI RMF, and EU AI Act.

References

[1] Soldatos, J., Despotopoulou, A., Kefalakis, N., & Ipektsidis, B. (2021). Blockchain based data provenance for trusted artificial intelligence. *Trusted Artificial Intelligence in Manufacturing: A Review of the Emerging Wave of Ethical and Human Centric AI Technologies for Smart Production*, 1-29.

[2] Dedeoglu, V., Malik, S., Ramachandran, G., Pal, S., & Jurdak, R. (2023). Blockchain meets edge-AI for food supply chain traceability and provenance. In *Comprehensive analytical chemistry* (Vol. 101, pp. 251-275). Elsevier.

[3] Umer, M. A., Belay, E. G., & Gouveia, L. B. (2024). Leveraging Artificial Intelligence and Provenance Blockchain Framework to Mitigate Risks in Cloud Manufacturing in Industry 4.0. *Electronics*, *13*(3), 660.

[4] Tyagi, A. K. (2024). Blockchain–Artificial Intelligence-Based Secured Solutions for Smart Environment. *Digital Twin and Blockchain for Smart Cities*, 547-577.

[5] Anthony Kendall, A. D., & Bruce Nagy, A. G. (2021). Blockchain Data Management Benefits by Increasing Confidence in Datasets Supporting Artificial Intelligence (AI) and Analytical Tools using Supply Chain Examples. Acquisition Research Program.

[6] Aramide, O. O. (2025). Quantum-Safe Networking for Critical AI/ML Infrastructure. *Journal of Data Analysis and Critical Management*, *1*(03), 19-29.

[7] Shaik, Kamal Mohammed Najeeb. (2024). Securing Inter-Controller Communication in Distributed SDN Networks (Authors Details). International Journal of Social Sciences & Humanities (IJSSH). 10. 2454-566. 10.21590/ijtmh.10.04.06.

[8] Sanusi, B. Design and Construction of Hospitals: Integrating Civil Engineering with Healthcare Facility Requirements.

[9] Vethachalam, S. (2024). Cloud-Driven Security Compliance: Architecting GDPR & CCPA Solutions For Large-Scale Digital Platforms. *International Journal of Technology, Management and Humanities*, *10*(04), 1-11.

[10] Hasan, N., Riad, M. J. A., Das, S., Roy, P., Shuvo, M. R., & Rahman, M. (2024, January). Advanced retinal image segmentation using u-net architecture: A leap forward in ophthalmological diagnostics. In *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)* (pp. 1-6). IEEE.

[11] Onoja, M. O., Onyenze, C. C., & Akintoye, A. A. (2024). DevOps and Sustainable Software Engineering: Bridging Speed, Reliability, and Environmental Responsibility. *International Journal of Technology, Management and Humanities*, *10*(04).

[12] Riad, M. J. A., Debnath, R., Shuvo, M. R., Ayrin, F. J., Hasan, N., Tamanna, A. A., & Roy, P. (2024, December). Fine-Tuning Large Language Models for Sentiment Classification of AI-Related Tweets. In *2024 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 186-191). IEEE.

[13] Shaik, Kamal Mohammed Najeeb. (2025). SDN-based detection and mitigation of botnet traffic in large-scale networks. World Journal of Advanced Research and Reviews. 10.30574/wjarr.2025.25.2.0686.

[14] Ashraf, M. S., Akuthota, V., Prapty, F. T., Sultana, S., Riad, J. A., Ghosh, C. R., ... & Anwar, A. S. (2025, April). Hybrid Q-Learning with VLMs Reasoning Features. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-6). IEEE.

[15] Shuvo, M. R., Debnath, R., Hasan, N., Nazara, R., Rahman, F. N., Riad, M. J. A., & Roy, P. (2025, February). Exploring Religions and Cross-Cultural Sensitivities in Conversational AI. In *2025 International Conference on Artificial Intelligence and Data Engineering (AIDE)* (pp. 629-636). IEEE.

[16] Aramide, O. (2025). Explainable AI (XAI) for Network Operations and Troubleshooting. In *International Journal for Research Publication and Seminar* (Vol. 16, pp. 533-554).

[17] Sultana, S., Akuthota, V., Subarna, J., Fuad, M. M., Riad, M. J. A., Islam, M. S., ... & Ashraf, M. S. (2025, June). Multi-Vision LVMs Model Ensemble for Gold Jewelry Authenticity Verification. In *2025 International Conference on Computing Technologies (ICOCT)* (pp. 1-6). IEEE.

[18] Riad, M. J. A., Roy, P., Shuvo, M. R., Hasan, N., Das, S., Ayrin, F. J., ... & Rahman, M. M. (2025, January). Fine-Tuning Large Language Models for Regional Dialect Comprehended Question answering in Bangla. In *2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-6). IEEE.

[19] Aramide, O. O. (2025). Advanced Network Telemetry for AI-Driven Network Optimization in Ultra Ethernet and InfiniBand Interconnects. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(01).

[20] Kumar, K. (2023). Dynamic Asset Allocation in an Inflationary

Macro Regime. *International Journal of Technology, Management and Humanities*, *9*(02), 1-21.

[21] Aramide, O. O., Goel, N., & Dildora, M. (2025). Zero-Trust Architecture for Shared AI Infrastructure: Enforcing Security at the Storage-Network Edge. *Well Testing Journal*, *34*(S3), 327-344.

[22] Oni, O. Y., & Oni, O. (2017). Elevating the Teaching Profession: A Comprehensive National Blueprint for Standardising Teacher Qualifications and Continuous Professional Development Across All Nigerian Educational Institutions. *International Journal of Technology, Management and Humanities*, *3*(04).

[23] Adebayo, I. A., Olagunju, O. J., Nkansah, C., Akomolafe, O., Godson, O., Blessing, O., & Clifford, O. (2019). Water-Energy-Food Nexus in Sub-Saharan Africa: Engineering Solutions for Sustainable Resource Management in Densely Populated Regions of West Africa.

[24] Kumar, K. (2020). Using Alternative Data to Enhance Factor-Based Portfolios. *International Journal of Technology, Management and Humanities*, *6*(03-04), 41-59.

[25] Vethachalam, S., & Okafor, C. Architecting Scalable Enterprise API Security Using OWASP and NIST Protocols in Multinational Environments For (2020).

[26] Arefin, N. T. Z. S. (2025). AI vs Cyber Threats: Real-World Case Studies on Securing Healthcare Data.

[27] Adebayo, I. A., Olagunju, O. J., Nkansah, C., Akomolafe, O., Godson, O., Blessing, O., & Clifford, O. (2020). Waste-to-Wealth Initiatives: Designing and Implementing Sustainable Waste Management Systems for Energy Generation and Material Recovery in Urban Centers of West Africa.

[28] Shaik, Kamal Mohammed Najeeb. (2022). Security Challenges and Solutions in SD-WAN Deployments. SAMRIDDHI A Journal of Physical Sciences Engineering and Technology. 14. 2022. 10.18090/samriddhi.v14i04..

[29] SANUSI, B. O. (2022). Sustainable Stormwater Management: Evaluating the Effectiveness of Green Infrastructure in Midwestern Cities. *Well Testing Journal*, *31*(2), 74-96.

[30] Arefin, N. T. Z. S. (2025). Future-Proofing Healthcare: The Role of AI and Blockchain in Data Security.

[31] Kumar, K. (2020). Innovations in Long/Short Equity Strategies for Small-and Mid-Cap Markets. *International Journal of Technology, Management and Humanities*, *6*(03-04), 22-40.

[32] Vethachalam, S., & Okafor, C. Accelerating CI/CD Pipelines Using .NET and Azure Microservices: Lessons from Pearson's Global Education Infrastructure For (2020).

[33] Kumar, K. (2021). Comparing Sharpe Ratios Across Market Cycles for Hedge Fund Strategies. *International Journal of Humanities and Information Technology*, (Special 1), 1-24.

[34] Arefin, S., & Zannat, N. T. (2025). Securing AI in Global Health Research: A Framework for Cross-Border Data Collaboration. *Clinical Medicine And Health Research Journal*, *5*(02), 1187-1193.

[35] Vethachalam, S. (2021). DevSecOps Integration in Cruise Industry Systems: A Framework for Reducing Cybersecurity Incidents. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *13*(02), 158-167.

[36] Shaik, Kamal Mohammed Najeeb. (2024). SDN-BASED TRAFFIC ENGINEERING FOR DATA CENTER NETWORKS: OPTIMIZING PERFORMANCE AND EFFICIENCY. International Journal of Engineering and Technical Research (IJETR). 08. 10.5281/zenodo.15800046.

[37] Kumar, K. (2022). Investor Overreaction in Microcap Earnings Announcements. *International Journal of Humanities and Information Technology*, *4*(01-03), 11-30.

[38] Roy, P., Riad, M. J. A., Akter, L., Hasan, N., Shuvo, M. R., Quader, M. A., ... & Anwar, A. S. (2024, May). Bilstm models with and without pretrained embeddings and bert on german patient reviews. In *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)* (pp. 1-5). IEEE.

[39] Kumar, K. (2022). How Institutional Herding Impacts Small Cap Liquidity. *Well Testing Journal*, *31*(2), 97-117.

[40] Arefin, M. A. O. S. (2025). Advancements in AI-Enhanced OCT Imaging for Early Disease Detection and Prevention in Aging Populations.

[41] Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, *70*(2), 713-739.

[42] Far, A. Z., Far, M. Z., Gharibzadeh, S., Naeini, H. K., Amini, L., Zangeneh, S., ... & Asadi, S. (2024). Artificial intelligence for secured information systems in smart cities: Collaborative iot computing with deep reinforcement learning and blockchain. *arXiv preprint arXiv:2409.16444*.

[43] Harris, L. (2024). The Role of Artificial Intelligence in Advancing Blockchain Technology.

[44] Arefin, S., & Zannat, N. T. (2024). The ROI of Data Security: How Hospitals and Health Systems Can Turn Compliance into Competitive Advantage. *Multidisciplinary Journal of Healthcare (MJH)*, *1*(2), 139-160.