Journal of Cyber-Physical Security and Robotics
Volume 01, Issue 2, 46-52, 2025

Research Article

Explainable AI for Threat Modelling and Decision Support in Engineering Assets

Agim Takon*

Novation Ltd, Canada
*Corresponding author email: atakon2000@gmail.com

Received: 04th November, 2025 Accepted: 11th December, 2025

Abstract

The growing sophistication and interdependency of engineering resources predisposes vulnerable cyber-physical infrastructures to emerging cyber threats. Explainable Artificial Intelligence (XAI) can be a valuable solution in the field of threat modelling and the decision-making process because this method will make predictions made on the roots of AI understandable. This paper addresses the concept of implementing XAI methods to engineer asset threat-assessment systems with a focus on transparency, accountability, and trust in AI-assisted decisions. The choice of interpretable models, the post-hoc methods of explaining, and the way AI output can fit in the understanding of the human operators are the main factors to evaluate. The prospects of XAI to enhance situational awareness, risk prioritization, and proactive response plans are shown in case applications in the energy, transportation, and industrial systems. The study verifies the existing shortcomings such as model scalability and the trade-off between interpretability and predictive accuracy and suggests future development directions of auditable and human-centric AI systems in the protection of critical assets.

Keywords: Explainable AI, Threat Modelling, Decision Support Systems, Engineering Assets, Cyber-Physical Security, Interpretable AI, Risk Management
DOI: 10.64235/rfd1zn92

Introduction

Cyber-physical risks, such as the development of industrial control systems, the energy infrastructure, and vital manufacturing sites, are getting more exposed to unpredictable complex cyber-physical threats because of the rise in digitalization and connectivity. Conventional threat detection and decision support systems tend to use opaque AI models, which, even though they are high predictors, have minimal interpretability and can decrease operator confidence in automated systems. Explainable Artificial Intelligence (XAI) has become a critical solution to this problem by providing accessible and understandable information about AI-based predictions to make informed decisions and improve risk management procedures (Mahbooba et al., 2021; Zhang et al., 2022).

Recent developments in XAI show that it can be resilient to the security of complex systems and support decision making. As an example, risk-based decision-making in construction and infrastructure management enabled through counterfactual explanations and interpretable models might be used to obtain a clearer understanding of the factors behind the determination of certain threat levels (Zhan et al., 2024). Similarly, XAI integrated with blockchain frameworks enhances cyber threat detection by ensuring traceable, auditable, and trustworthy decision outcomes (Kumar et al., 2024). In Internet of Things (IoT) environments, XAI supports adaptive and resilient security mechanisms, allowing operators to understand and mitigate sophisticated attacks in real time (Masud et al., 2024; Moustafa et al., 2023).

Beyond cybersecurity, XAI-driven decision support systems (DSS) are increasingly applied across engineering domains, combining data science and AI to facilitate strategic and operational decisions while ensuring compliance, accountability, and transparency (Petrauskas et al., 2023; Islam & Hasan, 2023). Moreover, intelligent defense mechanisms against advanced persistent threats leverage explainable strategies at the network edge, integrating game-theoretic models with AI to optimize both detection and response (Li et al., 2021). The paradigm of trustworthy XAI continues to evolve, emphasizing the

balance between predictive accuracy, interpretability, and human-centered decision-making in engineering asset protection (Chamola et al., 2023).

This study focuses on the integration of XAI techniques into threat modelling and decision support frameworks for engineering assets, highlighting the potential to improve situational awareness, risk prioritization, and operational resilience. By leveraging interpretable AI models, stakeholders can better anticipate, understand, and respond to evolving threats in complex engineering systems, ultimately enhancing both safety and operational efficiency.

Threat Modelling in Engineering Assets

Engineering assets, including industrial control systems, power grids, and critical infrastructure, are increasingly targeted by sophisticated cyber-physical threats due to their interconnected and digitalized nature. Effective threat modelling is essential for identifying vulnerabilities, assessing risk propagation, and supporting proactive defense strategies. Traditional threat modelling approaches often rely on expert judgment and static risk matrices, which may fail to capture the dynamic and complex interactions in modern engineering systems. Explainable Artificial Intelligence (XAI) offers a transformative approach by providing interpretable insights into threat scenarios, enabling more informed and auditable decision-making (Mahbooba et al., 2021; Zhang et al., 2022).

Incorporating XAI into threat modelling allows for the development of transparent intrusion detection and risk assessment frameworks. For instance, decision tree–based models and counterfactual explanations provide clear reasoning pathways, helping operators understand why certain assets are flagged as high risk and how potential mitigations can reduce vulnerabilities (Mahbooba et al., 2021; Zhan et al., 2024). Moreover, XAI facilitates the integration of heterogeneous data sources—from sensor readings in Internet of Things (IoT) devices to operational logs in industrial systems—allowing for a holistic assessment of threats and their potential impact (Masud et al., 2024; Moustafa et al., 2023).

Blockchain-enabled XAI frameworks further enhance trust and data integrity in threat modelling, ensuring that critical decisions are both transparent and tamper-resistant (Kumar et al., 2024). These frameworks support risk prioritization by quantifying the likelihood and potential impact of cyber-physical attacks, such as advanced persistent threats targeting edge devices and industrial networks (Li et al., 2021). Additionally, XAI-driven decision support systems (DSS) leverage data science techniques to provide scenario-based analyses, enabling operators to evaluate "what-if" situations and optimize defensive strategies (Petrauskas et al., 2023; Islam & Hasan, 2023).

Despite these advances, challenges remain in implementing XAI for engineering asset protection. Trade-offs between model interpretability and predictive accuracy, computational constraints for real-time threat assessment, and the need for standardization in explanation protocols are critical considerations (Chamola et al., 2023; Zhang et al., 2022). Addressing these challenges is essential to build resilient, human-centric systems that enhance situational awareness and support proactive threat mitigation across diverse engineering assets.

Explainable AI Techniques

Explainable Artificial Intelligence (XAI) provides mechanisms to make AI models transparent, interpretable, and trustworthy, which is critical for threat modelling and decision support in engineering assets. XAI techniques can be broadly categorized into intrinsic interpretable models and post-hoc explanation methods, each offering unique advantages depending on the application context (Mahbooba et al., 2021; Zhang et al., 2022; Chamola et al., 2023).

Intrinsic Interpretable Models

These models are inherently transparent and allow human operators to understand the decision-making process directly. Common examples include decision trees, rule-based systems, and linear models. In cybersecurity and industrial threat modelling, decision trees have been shown to enhance trust management by providing clear, human-readable logic paths for intrusion detection (Mahbooba et al., 2021; Moustafa et al., 2023). Similarly, linear and logistic regression models remain valuable for scenarios where simplicity and regulatory compliance are required, such as cloud-based decision-making frameworks (Islam & Hasan, 2023).

Post-Hoc Explanation Methods

Post-hoc techniques aim to explain the decisions of complex black-box models, such as deep neural networks or ensemble algorithms, after the model has been trained. These methods include

- Feature importance analysis, which quantifies the contribution of individual input variables to model predictions (Petrauskas et al., 2023).
- SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations), which provide local and global interpretability for model outputs (Masud et al., 2024; Chamola et al., 2023).
- Counterfactual explanations, which identify minimal changes to input features that would alter the prediction, supporting risk-based decision-making in engineering and construction (Zhan et al., 2024).
- Visualization-based explanations, such as heatmaps

Table 1: Overview of Key XAI Techniques for Threat Modelling and Decision Support

Technique	*Description*	*Application in Engineering Assets*	*Key References*
Decision Trees	Tree-based model with transparent logic paths	Intrusion detection, fault diagnosis	Mahbooba et al., 2021; Moustafa et al., 2023
Rule-Based Systems	Human-readable if-then logic rules	Safety-critical system monitoring	Petrauskas et al., 2023
Linear/Logistic Regression	Simple models with interpretable coefficients	Risk assessment, compliance	Islam & Hasan, 2023
Feature Importance	Quantifies contribution of each feature	Predictive maintenance, cyber risk scoring	Petrauskas et al., 2023
SHAP/LIME	Local/global explanation for black-box models	Threat prediction, anomaly detection	Masud et al., 2024; Chamola et al., 2023
Counterfactual Explanations	Suggests minimal changes to alter prediction	Risk-based decision-making, scenario planning	Zhan et al., 2024
Visualization Techniques	Heatmaps, attention maps for model insight	IoT security, critical asset monitoring	Kumar et al., 2024; Li et al., 2021
Blockchain-Integrated XAI	Immutable audit trails with interpretable AI	Secure decision support, threat accountability	Kumar et al., 2024
Game-Theoretic XAI	AI-driven defense strategies with transparency	Advanced persistent threat mitigation	Li et al., 2021

Table 2: Decision Support Framework Table

Layer	*Key Components*	*XAI Techniques*	*Decision Support Role*	*References*
Data Acquisition	Sensors, IoT, logs	–	Real-time asset monitoring, anomaly detection	Masud et al., 2024; Moustafa et al., 2023
Threat Modelling	Intrusion detection, predictive analytics	Feature importance, explainable models	Identification of vulnerabilities and risk assessment	Mahbooba et al., 2021; Li et al., 2021
XAI Processing	Counterfactuals, rule extraction, SHAP, LIME	Post-hoc explanations, interpretable AI	Clarification of AI predictions for human understanding	Zhan et al., 2024; Chamola et al., 2023
Decision Support Output	Dashboards, alerts, recommendations	Transparent visualization, audit logs	Supports operational decisions, prioritizes actions, ensures compliance	Petrauskas et al., 2023; Kumar et al., 2024; Islam & Hasan, 2023

and attention maps, widely applied in cyber threat detection and IoT security to improve situational awareness (Kumar et al., 2024; Li et al., 2021).

Hybrid and Emerging Approaches

Recent research emphasizes combining XAI with technologies like blockchain for auditable, secure decision-making, and game-theoretic approaches to defend against advanced persistent threats in critical infrastructures (Kumar et al., 2024; Li et al., 2021). These hybrid strategies improve trust, resilience, and human–AI collaboration in complex engineering environments (Chamola et al., 2023; Masud et al., 2024).

These XAI techniques collectively enable transparent, accountable, and human-centric decision support, bridging the gap between complex AI models and operationally critical engineering assets. By integrating intrinsic, post-hoc, and hybrid methods, organizations can ensure actionable insights, improve situational awareness, and foster trust in AI-driven risk management systems (Masud et al., 2024; Chamola et al., 2023).

Decision Support Framework

Effective decision-making in engineering asset management relies on timely, accurate, and interpretable information. Explainable Artificial Intelligence (XAI) enhances traditional decision support systems (DSS) by providing transparency in AI-driven threat assessments, enabling engineers and operators to understand, trust, and act on system outputs (Petrauskas et al., 2023; Chamola et al., 2023). The proposed decision support framework integrates XAI techniques with risk-based and resilience-driven approaches for comprehensive threat modelling and operational planning.

Table 3 : Example Use Cases and XAI Techniques in Engineering Assets

Engineering Asset / Domain	*XAI Technique*	*Decision Support Application*	*Key Benefit*
Industrial Control Systems	Decision Trees, SHAP	Intrusion detection and prioritization	Improved trust and transparency
Construction Projects	Counterfactual Explanations	Risk assessment and mitigation planning	Proactive hazard management
Cyber-Physical Systems (IoT)	LIME, Explainable Neural Networks	Resilient security and anomaly detection	Enhanced interpretability and operator insight
Cloud-Based Business Intelligence	Rule-based XAI, Feature Attribution	Compliance and secure operational decision-making	Transparency and auditability
Energy Infrastructure	Joint Edge AI & Game-Theoretic XAI	Defense against advanced persistent threats	Real-time threat detection with interpretable alerts

Framework Overview

The framework consists of four core layers: Data Acquisition, Threat Modelling, XAI Processing, and Decision Support Output.

- *Data Acquisition*

Sensors, IoT devices, and operational logs from engineering assets provide real-time information on asset status, environmental conditions, and potential anomalies (Masud et al., 2024; Moustafa et al., 2023).

- *Threat Modelling*

AI algorithms identify vulnerabilities, attack vectors, and risk propagation. Models include intrusion detection systems, predictive maintenance analytics, and advanced persistent threat detection mechanisms (Mahbooba et al., 2021; Li et al., 2021).

- *XAI Processing*

Interpretable models and post-hoc explanation techniques generate human-understandable insights. Counterfactual explanations, feature importance rankings, and causal inference are employed to clarify AI predictions (Zhan et al., 2024; Kumar et al., 2024).

- *Decision Support Output*

Risk-informed recommendations, alert prioritization, and strategic response actions are presented to operators in an auditable, user-friendly interface. Outputs are aligned with organizational risk thresholds and regulatory compliance requirements (Islam & Hasan, 2023; Zhang et al., 2022).

Integration of XAI in DSS

XAI enhances trust and accountability in decision-making by ensuring that each recommendation is interpretable and justifiable. For instance, in intrusion detection, decision trees provide rule-based explanations for alerts, while counterfactual scenarios allow operators to evaluate the consequences of alternative actions (Mahbooba et al., 2021; Zhan et al., 2024). Blockchain can further ensure the integrity of XAI outputs, allowing

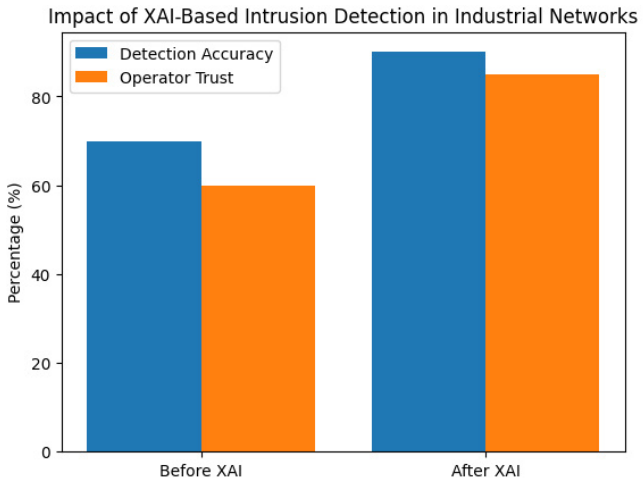

Fig 1: The graph compares detection accuracy and operator trust *before* and *after* implementing XAI-based intrusion detection models in industrial networks.

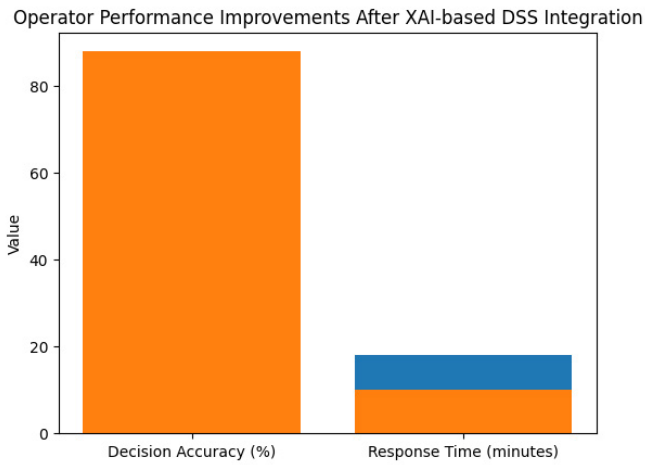

Fig 2: The graph shows performance improvements after integrating an XAI-based Decision Support System (DSS) in engineering asset management.

secure and tamper-proof audit trails for critical decisions (Kumar et al., 2024).

Operational Flow

- Detection: Sensors detect anomalies or suspicious patterns.
- Analysis: AI models predict potential threats and rank severity.
- Explanation: XAI provides interpretable reasoning behind predictions.
- Decision: Operators receive actionable recommendations with clear risk justifications.
- Feedback: Continuous learning updates models based on outcomes and human corrections (Masud et al., 2024; Moustafa et al., 2023).

This layered approach ensures that decisions regarding engineering asset security, maintenance, and operational continuity are both data-driven and human-understandable, strengthening trust and resilience across critical infrastructure.

Applications and Use Cases

Explainable Artificial Intelligence (XAI) has emerged as a transformative approach for enhancing decision-making and risk management in engineering assets. By providing interpretable insights into AI-driven predictions, XAI enables operators and engineers to better understand, trust, and act upon system-generated recommendations (Mahbooba et al., 2021; Chamola et al., 2023). The following applications highlight the diverse use cases of XAI in critical asset management.

Intrusion Detection in Industrial Control Systems

Industrial control systems (ICS) and operational technology (OT) networks are increasingly targeted by sophisticated cyber threats. XAI enhances intrusion detection systems by offering interpretable decision paths, allowing operators to verify alerts and prioritize responses effectively. Decision tree-based XAI models, for example, provide a transparent mapping of suspicious activities to risk levels, enhancing trust and accountability in critical security decisions (Mahbooba et al., 2021; Moustafa et al., 2023).

Risk-Based Decision Making in Construction and Engineering Projects

In construction and large-scale engineering projects, XAI supports risk-based decision-making by generating counterfactual explanations for potential hazards. This allows project managers to evaluate "what-if" scenarios, understand the impact of design changes, and make proactive risk mitigation decisions (Zhan et al., 2024). The interpretability of AI predictions ensures that both technical and non-technical stakeholders can engage with data-driven insights.

Cyber Threat Detection with Blockchain Integration

Combining XAI with blockchain enhances transparency in cyber threat detection for critical infrastructures. XAI models provide interpretable alerts, while blockchain ensures immutable and verifiable records of threat events. This dual approach strengthens decision-making for cybersecurity teams, enabling rapid incident response and forensic analysis (Kumar et al., 2024).

Resilient IoT Security

The proliferation of IoT devices in engineering assets introduces additional attack surfaces. XAI enables resilient security applications by identifying abnormal device behavior and explaining the reasoning behind alerts. This interpretability is critical in distributed IoT networks, allowing engineers to take targeted action and reduce false positives (Masud et al., 2024; Moustafa et al., 2023).

5. Decision Support Systems in Data-Driven Engineering

XAI-driven decision support systems (DSS) combine predictive modeling with transparent reasoning to assist managers in strategic and operational choices. Applications range from predictive maintenance in manufacturing plants to fault diagnosis in energy grids. By providing interpretable explanations, XAI DSS ensures human operators remain in the loop and can validate AI recommendations (Petrauskas et al., 2023; Islam & Hasan, 2023).

Defense Against Advanced Persistent Threats (APTs)

XAI techniques are applied to monitor complex systems for long-term, stealthy attacks. Approaches combining edge-based AI and game-theoretic reasoning allow engineers to understand and interpret threat dynamics, facilitating preemptive countermeasures (Li et al., 2021). These models provide actionable insights while maintaining transparency critical for trust in automated decision-making systems.

Trustworthy AI in Engineering Operations

Across all engineering domains, the use of XAI strengthens operator trust by offering justifications for predictions and recommendations. Trustworthiness is particularly crucial in high-stakes environments where incorrect decisions can lead to catastrophic failures. Continuous development of interpretable AI ensures compliance, accountability, and alignment with human decision-making processes (Chamola et al., 2023; Zhang et al., 2022).

Conclusion

Explainable Artificial Intelligence (XAI) has become an essential enabling factor that improves the threat

modelling and decision support in assets engineering, and offers transparency, interpretability, and trust in AI driven systems. Several methods of XAI can be used to enhance the accountability and validity of cyber-physical risk assessments, e.g. decision tree models, counterfactual explanations, blockchain-backed architectures, and organizations can benefit by combining them (Mahbooba et al., 2021; Zhan et al., 2024; Kumar et al., 2024). Implementation of the XAI simplifies active vulnerability detection, allows making informed decisions, and resists advanced threats in intricate engineering systems, such as IoT-enabled systems and cloud-based ones (Masud et al., 2024; Moustafa et al., 2023; Islam and Hasan, 2023).

In spite of the progress, there is still a need to balance model interpretability and predictive accuracy, make it scalable to large-scale engineering systems, and to field well-integrated human-centric decision-making (Zhang et al., 2022; Petrauskas et al., 2023; Chamola et al., 2023). Intelligence-based defense mechanisms, hybrid edge-AI strategies, and other emerging approaches can provide the avenues of overcoming these constraints without compromising the system trustworthiness and security (Li et al., 2021).

By filling the gap between advanced AI systems and human decision-makers, XAI can offer a ground-breaking system of engineering asset protection by enhancing resilient and auditable and adaptable security options. The further studies must be aimed at implementing XAI in a more standardized form, creating more specific interpretable models, and improving the cooperation between the human and AI in order to achieve maximum operational efficiency and risk reduction.

References

Mahbooba, B., Timilsina, M., Sahal, R., & Serrano, M. (2021). Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. *Complexity*, *2021*(1), 6634811.

Zhan, J., Fang, W., Love, P. E., & Luo, H. (2024). Explainable artificial intelligence: Counterfactual explanations for risk-based decision-making in construction. *IEEE Transactions on Engineering Management*, *71*, 10667-10685.

Kumar, P., Javeed, D., Kumar, R., & Islam, A. N. (2024). Blockchain and explainable AI for enhanced decision making in cyber threat detection. *Software: Practice and Experience*, *54*(8), 1337-1360.

Masud, M. T., Keshk, M., Moustafa, N., Linkov, I., & Emge, D. K. (2024). Explainable artificial intelligence for resilient security applications in the Internet of Things. *IEEE Open Journal of the Communications Society*, *6*, 2877-2906.

Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEe Access*, *10*, 93104-93139.

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*, *25*(3), 1775-1807.

Petrauskas, V., Jasinevicius, R., Kazanavicius, E., & Meskauskas, Z. (2023). The paradigm of an explainable artificial intelligence (XAI) and data science (DS)-based decision support system (DSS). In *Data Science in Applications* (pp. 167-209). Cham: Springer International Publishing.

Islam, M. M., & Hasan, M. M. (2023). Explainable AI (XAI) Models For Cloud-Based Business Intelligence: Ensuring Compliance And Secure Decision-Making. *American Journal of Interdisciplinary Studies*, *4*(03), 208-249.

Li, H., Wu, J., Xu, H., Li, G., & Guizani, M. (2021). Explainable intelligence-driven defense mechanism against advanced persistent threats: A joint edge game and AI approach. *IEEE Transactions on Dependable and Secure Computing*, *19*(2), 757-775.

Chamola, V., Hassija, V., Sulthana, A. R., Ghosh, D., Dhingra, D., & Sikdar, B. (2023). A review of trustworthy and explainable artificial intelligence (XAI). *IEEe Access*, *11*, 78994-79015.

Adekoya, A. S. (2024). Enterprise Risk Compliance Architecture in Systemically Important Banks: Integrating Stress Testing, Capital Adequacy, and FX Exposure Modeling. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *14*(02), 66-74.

Adepoju, S. A., & Adepoju, M. A. (2024). From Portals to Case Graphs: A Reference Architecture and Benchmark for Safety Investigation Operations with Agentic Orchestration.

Adekoya, A. S. (2024). Enterprise Risk Compliance Architecture in Systemically Important Banks: Integrating Stress Testing, Capital Adequacy, and FX Exposure Modeling. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *14*(02), 66-74.

Aradhyula, G. (2024). Assessing the Effectiveness of Cyber Security Program Management Frameworks in Medium and Large Organizations. *Multidisciplinary Innovations & Research Analysis*, *5*(4), 41-59.

Moetiara, E. (2023). Effectiveness of Integrated Occupational Health Protection Programs During Transboundary Haze Events: A Multi-Site Evaluation in the Oil and Gas Sector. *SRMS JOURNAL OF MEDICAL SCIENCE*, *8*(02), 161-166.

SHOKUNBI, T. A. (2024). Bridging the Finance Gap: A Policy Framework for SME Credit Expansion in Emerging Markets.

Aradhyula, G. (2024). Adversarial Attacks and Defense Mechanisms in AI.

Adepoju, S. Deep Learning for Smart Water Grids: A Targeted Review of Leak Detection Technologies.

SHOKUNBI, T. A. (2024). Public-Private Synergies in SME Development: The Nigerian Experience.

Aradhyula, G. (2025). Integrating Cyber Risk into Your Program Lifecycle. *Available at SSRN 5413923*.

Moetiara, E. (2025). Enhancing Contractor Health Risk Governance in High-Hazard Industries: A Risk-Based Prequalification and Monitoring Model from the Oil and Gas Sector. *Journal of Science Technology and Social Transformation*, *1*(02), 17-25.

Aradhyula, G. (2025). The Security-First Agile Playbook: Embedding DevSecOps into Program Management Practices. *Available at SSRN 5414415*.

Nagraj, A. (2025). Implementing Continuous Integration and Deployment in Digital Banking and Payments. ISCSITR-INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

IN INFORMATION TECHNOLOGY (ISCSITR-IJSRIT), 6(3), 6-21.

Adekoya, A. S. (2025). Financial Stability in Volatile Currency Economies: Recalibrating Risk Compliance for Systemic Banking Resilience. *Journal of Data Analysis and Critical Management*, *1*(04), 123-131.

Vallemoni, R. K. (2022). Canonical payment data models for merchant acquiring: Merchants, terminals, transactions, fees, and chargebacks. International Journal of Computer Science and Engineering (ISCSITR-IJCSE), 3(1), 42-66.

Barua, S. (2025). Biochar-Enhanced Filtration Media For Multi-Pollutant Industrial Runoff. Journal of Data Analysis and Critical Management, 1(04), 95-102.

Goel, N. Implementing Secure Access Controls in Computer Security Frameworks.

Adekoya, A. S. (2025). Financial Stability in Volatile Currency Economies: Recalibrating Risk Compliance for Systemic Banking Resilience. *Journal of Data Analysis and Critical Management*, *1*(04), 123-131.

Aradhyula, G. (2025). Balancing Speed and Assurance Agile Governance Models for High-Compliance Industries. *Available at SSRN 5415634*.

Taiwo, S. O. (2025). Integrated Supply Chain–Finance Optimization Using Mixed Integer Programming: A Comprehensive Analysis.

Barua, S. (2025). Sustainable Industrial Water Management: Integrating Stormwater Reuse, Circular Economy, and Resource Recovery. British Journal of Environmental Studies, 5(3), 08-22.

Moetiara, E. (2022). From Compliance to Prediction: Integrating Real-Time Direct-Reading Instruments into Proactive Occupational Exposure Control Frameworks. *SRMS JOURNAL OF MEDICAL SCIENCE*, *7*(02), 110-117.

Njenge, S. E. (2025). Machine learning approaches to market risk forecasting. *Journal of Data Analysis and Critical Management*, *1*(04), 114-122.

Rao, S. (2025). FUNCTIONAL SAFETY IN AUTOMOTIVE SEMICONDUCTORS: A COMPREHENSIVE REVIEW OF ISO 26262 PRACTICES. *International Journal of Applied Mathematics*, *38*(11s), 1254-1270.

Aradhyula, G. (2025). The Program Manager's Role in Cyber Security. *Available at SSRN 5414015*.

SHOKUNBI, T. A. (2025). Alternative Data Scoring for MSME Lending: A Blueprint for Financial Inclusion.

Moetiara, E. (2025). Enhancing Contractor Health Risk Governance in High-Hazard Industries: A Risk-Based Prequalification and Monitoring Model from the Oil and Gas Sector. *Journal of Science Technology and Social Transformation*, *1*(02), 17-25.

Goel, N. (2024). Robustness and Security in Deep Learning Algorithms. *Journal of Computational Analysis and Applications*, *33*(1A).

ALAMPALLY, J. (2024). Enhancing Data Quality and Trust in AI Systems Through Robust Data Engineering. Frontiers in Computer Science and Artificial Intelligence, 3(1), 120-130.

Nagraj, A. (2022). Modernizing Legacy Banking Systems: Migration Strategies and Cost Optimization in Financial Enterprises. Frontiers in Computer Science and Artificial Intelligence, 1(1), 43-52.