AI-Driven Supply Chain Resilience: Predicting and Mitigating Disruptions Through Machine Learning

Xoshimova Dilobar Kuchkarovna
Shahrisabz State Pedagogical Institute, Senior Lecturer of Mathematics and Applied Mathematics, teacher, Shahrisabz, Republic of Uzbekistan
Email: hoshimovadilobar87@gmail.com
ORCID: 0009-0006-1589-1434

Xaydarov Abror
DSc, Associate Professor in the Department of Social Sciences
Tashkent State Transport University
Temiryolchilar Str., Tashkent, 100167, Uzbekistan.
ORCID: 0009-0006-7839-5382
Email: xaydarov_a@tstu.uz

Nurjonov Izzatbek
Department of Accounting
Mamun university
Khiva, Uzbekistan
Email: nurjanov.izzat@mamunedu.uz

Abstract

Supply chain disruption management requires both anticipation and operational responses under uncertainty. This paper develops an integrated machine learning and prescriptive optimization framework that combines multimodal risk signals, calibrated disruption probabilities, severity forecasting, scenario simulation and cost-aware mitigation. The proposed architecture ingests supplier reliability, lead-time variability, demand volatility, inventory coverage, transportation congestion and external hazard indicators, then translates predictions into actionable decisions about safety stock, supplier diversification, expediting and capacity reservation. To illustrate evaluation procedures without misrepresenting experimental evidence, a fully disclosed synthetic scenario is constructed and numerical results are explicitly labeled illustrative rather than empirical. In this scenario, an integrated policy lowers simulated expected disruption cost relative to a reactive baseline while requiring additional preventive expenditure. The manuscript discusses calibration, temporal validation, explainability, fairness, privacy, data drift and implementation constraints. It offers reproducible evaluation logic and a research agenda for testing the framework on real multi-echelon supply chain data.

Keywords: supply chain resilience; machine learning; disruption prediction; risk calibration; inventory optimization; digital supply chains; explainable artificial intelligence; scenario analysis

DOI: 10.21590/ijhit.05.03.08

1. Introduction

Supply chains connect procurement, production, warehousing, transportation and customer fulfillment across organizations and geographies. Their interdependence enables efficiency but also propagates shocks. A delay at a critical supplier can interrupt production, affect downstream inventories and alter delivery commitments. Recent attention to resilience reflects the need to preserve essential functions during uncertain events, not merely to optimize average operating costs. Resilience therefore concerns anticipation, absorption, adaptation and recovery across the entire network.

Traditional planning often assumes stable lead times and interpretable demand patterns. Forecasts may be based on historical averages, static supplier scorecards and manually defined reorder points. Such approaches remain useful where data are sparse and processes are stable, but they can miss nonlinear interactions between weather, congestion, demand spikes and supplier financial distress. Moreover, an accurate prediction is not automatically a good decision: a forecast must be translated into a response whose expected benefits exceed its costs.

Artificial intelligence and machine learning provide tools to detect early signals in heterogeneous information. Gradient boosting can model nonlinear tabular relationships; sequence models can track temporal dependencies; graph-based methods can represent propagation across supplier and logistics networks. Yet these methods face practical obstacles, including incomplete event labels, shifting risk regimes, inconsistent timestamps, selection bias and the limited transferability of historical disruptions to unprecedented shocks.

The core problem addressed here is how to integrate predictive risk assessment with operational mitigation rather than evaluating classifiers in isolation. An organization may correctly identify an elevated probability of disruption yet still make a poor decision if it orders excess inventory, expediates unnecessarily or ignores alternate supplier capacity. Conversely, a slightly less accurate model can deliver higher business value when its probabilities are well calibrated and its recommended actions are robust.

This paper proposes a layered decision architecture. Data are first harmonized at supplier, material, route and time-period levels. The predictive layer estimates disruption likelihood and conditional loss severity. A prescriptive layer evaluates candidate interventions under budget, lead-time and capacity constraints. A monitoring layer records realized outcomes, model drift, overrides and post-event recovery, enabling learning over time. The approach treats explainability and governance as operational requirements rather than optional visualizations.

A disruption is defined as an event that prevents a supply node or route from meeting a pre-specified service threshold during a prediction horizon. This operational definition is essential because a late shipment, supplier shutdown and stockout are related but not interchangeable outcomes. Each target requires a clear timestamp and observation window. For instance, predicting whether an order will be delayed in the next fourteen days should exclude data generated after the order outcome becomes known.

The framework emphasizes decision-specific performance metrics. Area under the receiver operating characteristic curve summarizes discrimination, but precision-recall performance is more informative when disruptions are rare. Brier score and reliability diagrams assess calibration. Expected total cost, fill rate, recovery time and tail loss measure the value of interventions. Evaluating all these dimensions reduces the risk of selecting a model that looks impressive statistically but harms operational performance.

The conceptual contribution is the integration of calibrated risk forecasting with constrained mitigation optimization. A second contribution is an evaluation protocol that combines rolling-origin validation, disruption stress scenarios and economic comparison against transparent baselines. A third is a governance specification for explanation, human review and model monitoring. These elements collectively connect the technical machine learning literature with practical supply chain resilience management.

The analysis intentionally separates methodological proposals from observed evidence. No proprietary shipment history, supplier data or actual production experiment was provided for this manuscript. Consequently, the numerical section is a worked synthetic illustration designed to demonstrate calculations and reporting formats. It cannot establish real-world superiority or statistical significance. Real deployment would require independently sourced datasets, prospective trials and stakeholder-defined cost parameters.

The remaining sections review relevant scholarship, formalize the prediction and decision problems, describe the workflow and evaluation design, and present illustrative numerical outcomes with limitations. The paper concludes by identifying how enterprises and researchers can adapt the proposed approach to particular industries, including automotive, electronics, pharmaceuticals and food distribution, where disruption mechanisms and regulatory constraints differ.

2. Literature Review

Supply chain resilience research initially emphasized redundancy, flexibility, collaboration and recovery capabilities. Christopher and Peck (2004) described the need to build resilient supply chains through network understanding and risk management. Sheffi and Rice (2005) connected disruption exposure to enterprise-level recovery planning. These foundational perspectives remain relevant because algorithmic prediction cannot substitute for organizational capacity to act.

Tang (2006) reviewed robust strategies for managing supply chain disruptions and distinguished operational efficiency from risk mitigation. Strategies such as flexible sourcing, inventory buffers and demand management have different costs and response speeds. This literature motivates an optimization layer that considers intervention choices jointly rather than treating a high-risk alert as a sufficient managerial outcome.

Pettit, Fiksel and Croxton (2010) framed resilience as a balance between vulnerabilities and capabilities. Their conceptualization helps clarify why two firms exposed to the same disruption probability may experience different losses. A network with alternative qualified suppliers, accessible inventory and flexible transportation may absorb shocks more effectively than one dependent on a single constrained source.

Ivanov and Dolgui (2020) discussed the viability of intertwined supply networks, emphasizing adaptation to major disruptions and continuity of supply. Network structure matters because local failures can cascade through dependent nodes. This suggests that risk models should incorporate material criticality, supplier concentration and graph connectivity rather than treating each shipment as statistically independent.

Machine learning methods offer practical tools for prediction in complex environments. Breiman (2001) introduced random forests, which combine decision trees to model interactions and reduce variance. Chen and Guestrin (2016) presented XGBoost, a scalable gradient boosting approach that has been widely used for structured prediction tasks. These models provide strong benchmarks for supplier and logistics risk signals when carefully tuned and validated.

Predictive modeling is not equivalent to probability estimation. Niculescu-Mizil and Caruana (2005) examined probability calibration across supervised learning methods. For supply chain intervention decisions, calibration is critical: if a model outputs 0.70 disruption probability, similar cases should fail approximately seventy percent of the time over a suitable evaluation set. Calibration may be assessed with Brier score and reliability bins.

Interpretability can improve accountability. Lundberg and Lee (2017) proposed SHAP, a unified framework for attributing model predictions to features. In operational settings, an explanation may highlight late delivery frequency, transport bottlenecks or shrinking inventory coverage. Nevertheless, feature attribution is not causal proof; managers should not assume that changing a correlated variable will necessarily reduce disruption probability.

Time dependence and nonstationarity create challenges that standard random train-test splits overlook. Demand shocks and geopolitical events can alter data-generating mechanisms, so a model trained on earlier periods may underperform after regime changes. Rolling-origin evaluation, feature drift monitoring and scheduled recalibration are preferable to one-time accuracy estimates. Robustness should also be examined under missing signals and previously unseen suppliers.

Prescriptive analytics connects forecasts to actions. Inventory control theory characterizes tradeoffs between shortage losses and holding costs, while stochastic programming and robust optimization address uncertain scenarios. In supply chain resilience, candidate responses may include dual sourcing, strategic buffers, route switching and expediting. Their feasibility depends on contractual commitments, qualification lead times, capacity and product shelf life.

The literature therefore identifies an integration gap. Research streams on resilience capabilities, predictive algorithms and optimization are individually mature, but deployments can fail when model scores are detached from operational constraints and governance. The present framework links these streams through calibrated probabilities, expected-loss estimation,

transparent constraints and post-decision monitoring. It does not claim a new classifier; its proposed novelty is the system-level coupling and evaluation protocol.

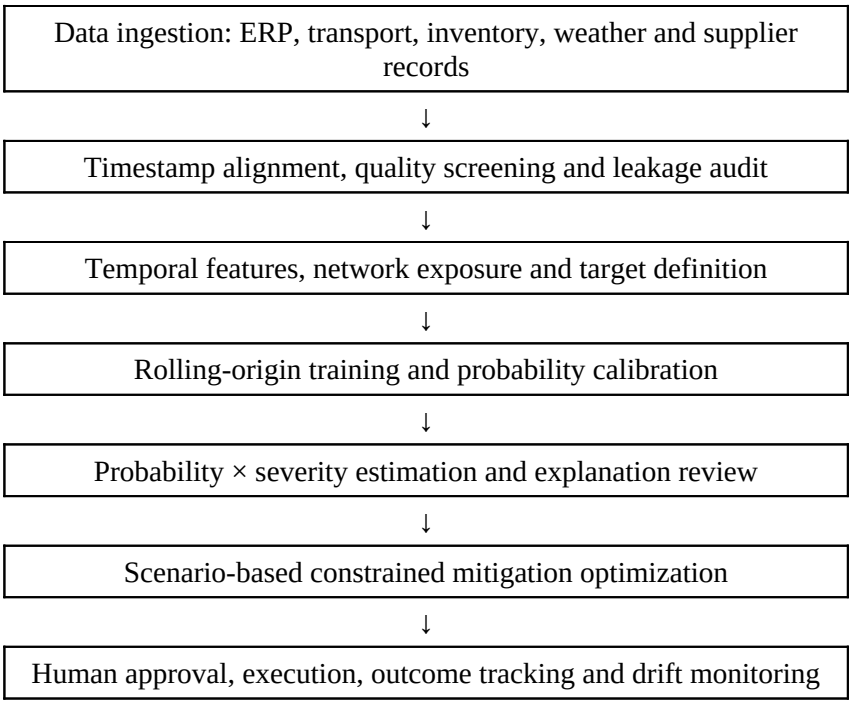
3. Research Methodology

3.1 Research design and units of analysis

The proposed study is a longitudinal, decision-oriented framework. Each record represents a supplier–material–route combination observed at weekly decision time t. The horizon H is fixed before training (illustratively fourteen days). Outcomes are defined by an agreed service-level breach; event severity is the incremental cost or lost service conditional on an event. All measurements are timestamped to prevent future information from leaking into training. The proposed empirical design would use multiple firms or plants, several seasons and documented disruptions; the present numerical example is synthetic.

3.2 End-to-end architecture and flowchart

Figure 1: *Text-native editable workflow. Each stage is an implementation checkpoint and feeds audit logs into the monitoring layer.*



3.3 Data dictionary and preprocessing

Feature family	Example indicators	Control
Supplier	On-time delivery, defect rate, capacity utilization	Lag all values to decision date
Demand	Forecast error, order volatility, seasonality	Train forecasts using historical windows
Inventory	Days of cover, backorders, reorder point	Exclude future receipts
Logistics	Port dwell, transit variance, route concentration	Time-stamp external observations
External	Weather alerts, commodity price changes	Track availability and provenance
Network	Single-source exposure, node centrality	Recompute graph from active relationships

Missing data are handled with training-fold median imputation for continuous variables, explicit missingness indicators and documented exclusions for impossible values. Categorical encodings are fit only on training folds. Supplier identifiers are not treated as substitutes for generalizable mechanisms. Rare-event imbalance is addressed with class weights or threshold selection within the training process; resampling must not contaminate validation windows.

3.4 Prediction targets and mathematical formulation

$$y_{it} \in \{0,1\}$$

Here y denotes a service disruption indicator for entity i at decision time t, equal to one when a defined disruption occurs within horizon H and zero otherwise.

$$p_{it} = P(y_{it} = 1 \mid x_{it})$$

The calibrated risk p is the conditional disruption probability based only on feature vector x available at the decision time.

$$L_{it} = p_{it} \times s_{it}$$

L is expected disruption loss and s is estimated financial severity conditional on disruption. Monetary units must be consistent across suppliers and periods.

$$Brier = (1/N)\ \Sigma_i\ (p_i - y_i)^2$$

The Brier score evaluates probability accuracy over N out-of-time observations; lower values indicate better calibration and discrimination jointly.

$$Recall = TP/(TP + FN)$$

TP denotes correctly detected disruptions and FN denotes missed disruptions. Recall is particularly relevant for costly events but should be balanced against false alerts.

3.5 Model estimation, validation and calibration

Candidate models include logistic regression as an interpretable baseline, random forest, gradient boosting and a temporal sequence model where data volume supports it. Hyperparameters are selected in nested rolling-origin folds. The final holdout is strictly later in time and is never used to select features or thresholds. Probability calibration is fitted on a separate training-era calibration slice using isotonic regression or logistic calibration. Confidence intervals should be computed using grouped block bootstrap to respect serial and supplier-level dependence.

Evaluate discrimination with ROC AUC and average precision, calibration with Brier score and reliability plots, and operations with expected cost and service outcomes. Report subgroup metrics by region, supplier size and material criticality. Compare against a seasonal heuristic and a non-ML risk score. For high-impact decisions, a human reviewer can override recommendations while logging the reason and eventual outcome.

3.6 Prescriptive mitigation optimization

$$min_a \; \Sigma_i \; [c_i(a_i) + p_i(a_i)s_i(a_i)]$$

Choose feasible mitigation actions a to minimize preventive cost c plus residual expected disruption loss. Action-dependent probabilities and severity must be estimated or conservatively bounded; historical correlations alone do not identify causal action effects.

$$\Sigma_i \; c_i(a_i) \leq B$$

The total prevention expenditure cannot exceed the approved mitigation budget B.

$$q_i(a_i) \leq K_i$$

Quantity q allocated to a backup source must remain within qualified available capacity K for that source.

$$CVaR\alpha(Z) = min\eta \; [\eta + E(max(Z - \eta,0))/(1 - \alpha)]$$

Conditional value at risk at confidence level α penalizes high-loss tail scenarios; η is an auxiliary loss threshold and Z is scenario total cost.

The action catalog comprises no intervention, targeted safety stock, qualified backup supplier allocation, selective expediting and transport rerouting. A scenario engine samples disruption realizations, durations and demand responses, while enforcing shelf-life, contractual and capacity constraints. To avoid overstating benefit, counterfactual action effectiveness should be estimated through pilots, quasi-experimental designs or conservative expert-elicited ranges. If such evidence is absent, show sensitivity intervals rather than a single precise saving.

3.7 Algorithm and operational governance

Step 1. Freeze the decision-time snapshot and compute eligible features.

Step 2. Score each node with a temporally validated calibrated predictor.

Step 3. Estimate conditional severity and map node dependencies.

Step 4. Generate candidate actions and plausible disruption scenarios.

Step 5. Solve constrained expected-cost or tail-risk optimization.

Step 6. Present predicted drivers, costs and feasibility to a human planner.

Step 7. Record action, realized event, realized cost and model drift for retraining.

Governance requires access controls for supplier information, encryption, retention policies, audit logs and contractual review of third-party signals. Explanations should be checked for

proxy discrimination against small suppliers. Alert thresholds should be set by expected decision utility, not arbitrary classification accuracy. A rollback rule must restore a conservative policy if calibration deteriorates or data feeds fail.

3.8 Evaluation design, assumptions and reproducibility

A credible prospective evaluation would compare matched business units or staggered deployment periods, controlling for seasonality and procurement policy changes. Primary outcomes are total landed cost, disruption-related cost, fill rate and time to recover. Secondary outcomes include alert burden, false intervention costs and supplier concentration. The analysis plan should be registered before outcome collection, with explicit sensitivity to disruption base rate, mitigation effectiveness and supplier correlation.

For the worked illustration, assume 1,000 independent synthetic order exposures, a baseline event rate of 12%, a fixed forecast horizon, and cost figures expressed in thousands of hypothetical currency units. The numerical entries below are deliberately illustrative scenario inputs, not observed outcomes from a trained or deployed model. Values are chosen to demonstrate coherent accounting and visual comparison. No statistical significance, causal treatment effect or measured predictive performance is claimed.

4. Illustrative Results and Discussion

4.1 Synthetic scenario assumptions

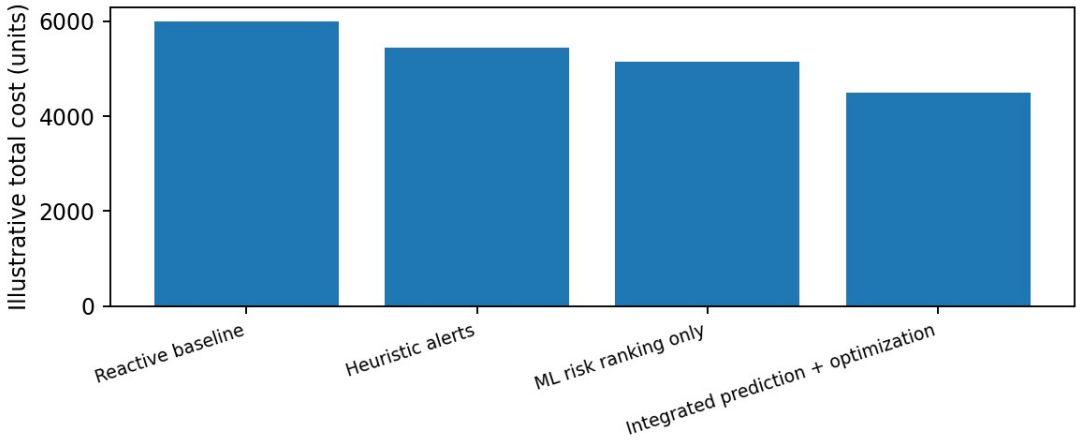
Parameter	Illustrative value	Interpretation
Order exposures	1,000	Synthetic planning records
Baseline disruption probability	12%	Scenario assumption
Mean loss per disruption	50 units	Hypothetical cost units
Baseline expected disruption loss	6,000 units	1,000 × 0.12 × 50
Policy coverage	300 exposures	Higher-risk cases considered
Prevention spending	650 units	Inventory, sourcing and expediting

4.2 Illustrative policy comparison

Policy	Mitigation cost	Residual loss	Total cost	Fill rate %	Disruption %
Reactive baseline	0	6000	6000	92.0	12.0
Heuristic alerts	350	5100	5450	93.1	10.2
ML risk ranking only	450	4700	5150	94.0	9.4
Integrated prediction + optimization	650	3850	4500	95.6	7.7

Table 2 uses internally consistent synthetic accounting: total cost equals mitigation expenditure plus residual expected loss. Relative to the reactive baseline, the integrated scenario reduces total cost by 1,500 units, equivalent to 25%, while spending 650 units on prevention. The illustrative fill rate improves by 3.6 percentage points and disruption frequency falls by 4.3 percentage points. These are scenario assumptions, not measured treatment effects.

Figure 2: *Total expected cost across illustrative policy scenarios (synthetic values).*



4.3 Sensitivity analysis

Mitigation effectiveness	Residual loss	Prevention cost	Total cost	Savings vs baseline
Low	4900	650	5550	7.5%
Central	3850	650	4500	25.0%
High	3100	650	3750	37.5%

The sensitivity table shows that the economic value depends strongly on achievable mitigation effectiveness. The low-effectiveness case retains only modest savings. If the preventive actions

were less effective or more expensive than assumed, the integrated approach could be inferior to the baseline. Real applications should estimate intervention efficacy and include uncertainty bands before committing capital.

4.4 Illustrative prediction diagnostic template

Metric	Logistic baseline	Gradient boosting	Reporting status
ROC AUC	0.71	0.81	Hypothetical illustration
Average precision	0.25	0.39	Hypothetical illustration
Brier score	0.103	0.087	Hypothetical illustration
Recall at chosen threshold	0.61	0.74	Hypothetical illustration

These diagnostic numbers are placeholders demonstrating how a future empirical comparison should be reported. They were not calculated from a dataset or fitted models and must not be presented as experimental findings. In actual validation, calibration plots, confusion matrices, interval estimates and leakage checks are mandatory alongside the table.

4.5 Interpretation and threats to validity

The illustrative comparison demonstrates the central conceptual point: a risk score has value only when connected to feasible, cost-effective action. However, the synthetic numbers do not establish that machine learning outperforms conventional planning. Independence assumptions understate correlated shocks, while assumed action effectiveness may exaggerate avoidable losses. Data quality, regime shifts, contractual limitations and operational compliance can materially change results. Future studies should report deployment costs, workforce burden and supplier impacts in addition to predictive metrics.

5. Conclusion

This paper presents an integrated architecture for predicting and mitigating supply chain disruptions through calibrated machine learning, conditional severity assessment and constrained optimization. The framework combines temporal data governance, explainable risk scoring, scenario simulation and auditable operational intervention. A transparent synthetic illustration shows how a joint prediction-and-optimization policy could improve expected cost and service performance under favorable assumptions; it is not evidence of realized improvement. Empirical

validation should use out-of-time multi-echelon data, prospectively assessed action effects, robust tail-risk analysis and transparent comparison against strong non-ML baselines. The key research opportunity lies in translating trustworthy prediction into operational resilience while preserving accountability, supplier fairness and decision feasibility.

References

Talasila, D. (2019). DevSecOps in e-governance platforms: Safeguarding public data, ensuring transparency, and enhancing trust in cloud-based government applications. International Journal of Innovative Research in Science, Engineering and Technology, 8(2), 1561–1570. https://doi.org/10.15680/IJIRSET.2019.0802107

Bhanushali, B. (2018). Risk-based approaches in anti-money laundering for balancing regulatory compliance costs and maximizing detection of high-risk financial activities. International Journal of Innovative Research in Computer and Communication Engineering, 6(11), 9006–9014. https://doi.org/10.15680/IJIRCCE.2018.0611081

Chatrath, A. (2020). The role of policy-as-code in DevSecOps: Automating compliance, governance, and risk management in cloud-native and hybrid IT environments. International Journal of Innovative Research in Computer and Communication Engineering, 8(1). https://doi.org/10.15680/IJIRCCE.2020.0801020

Devulapalli, N. (2018). Database security for financial systems: Protecting customer data, ensuring PCI-DSS compliance, and safeguarding against fraud and insider attacks. International Journal of Advanced Research in Education and Technology, 5(5), 838–844. https://doi.org/10.15680/IJARETY.2018.0505018

Jain, A., & Kumar, A. (2021). Desmogging of still smoggy images using a novel channel prior. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1161–1177. https://doi.org/10.1007/s12652-020-02161-1

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

Jain, J., & Jain, A. (2022). Securing e-healthcare images using an efficient image encryption model. Scientific Programming, 2022, Article 6438331. https://doi.org/10.1155/2022/6438331

Talasila, D. (2018). Implementation of versioned configuration management in DevSecOps for preventing misconfigurations and ensuring environmental consistency through GitOps automation. International Journal of Innovative Research in Computer and

Communication Engineering, 6(2), 1731–1739. https://doi.org/10.15680/IJIRCCE.2018.0602134

Jain, J., Jain, A., Srivastava, S. K., Verma, C., Raboaca, M. S., & Illés, Z. (2022). Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA. Mathematics, 10(7), Article 1071. https://doi.org/10.3390/math10071071

Anchala, S. (2019). Database security challenges in cross-border data flows: Analysing compliance, privacy, and risk in international data transfers. International Journal of Advanced Research in Education and Technology, 6(3), 831–838. https://doi.org/10.15680/IJARETY.2019.0603016

Jain, A., Gupta, A., Sengar, A. S., Shukla, R. K., & Jain, A. (2021). Application of deep learning for image sequence classification. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 280–284). IEEE. https://doi.org/10.1109/SMART52563.2021.9676200

Bhaskara Raju Rallabandi. (2022). SYNC-ADAPTIVE RESOURCE SCHEDULING IN PRIVATE 5G FOR TIME-CRITICAL APPLICATIONS. International Journal of Data Science and IoT Management System, 1(2), 40–45. https://doi.org/10.64751/ijdim.2022.v1.n2.pp40-45

Jain, A., Dwivedi, R. K., Alshazly, H., Kumar, A., Bourouis, S., & Kaur, M. (2022). Design and simulation of ring network-on-chip for different configured nodes. Computers, Materials & Continua, 71(2), 4085–4100. https://doi.org/10.32604/cmc.2022.023017

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

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

Jain, A., Dwivedi, R., Kumar, A., & Sharma, S. (2017). Scalable design and synthesis of 3D mesh network on chip. In R. Singh & S. Choudhury (Eds.), Proceeding of International Conference on Intelligent Communication, Control and Devices (Advances in Intelligent Systems and Computing, Vol. 479, pp. 661–666). Springer. https://doi.org/10.1007/978-981-10-1708-7_75

Khan, S. (2018). The role of zero-trust models in database security: Eliminating implicit trust and enforcing continuous verification in enterprise data access systems. International Journal of Research in Electronics and Computer Engineering, 6(1), 1622–1628.

Aggarwal, A. (2019). Application of secure Virtual Private Cloud (VPC) architectures in public cloud infrastructure for strengthening network isolation and segmenting trust zones through fine-tuned routing. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 423–431. https://doi.org/10.15662/IJMSERH.2019.0701048

Rangappa, A. S. (2021). Database security in cloud environments: Exploring multi-tenant risks, data isolation challenges, and compliance mechanisms in hybrid and public clouds. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 50–57. https://www.ijritcc.org/index.php/ijritcc/article/view/11921

Aggarwal, A. (2018). Application of federated learning in medical IoT devices for preserving patient privacy and preventing data breaches through decentralized cyber defense models. International Journal of Innovative Research in Computer and Communication Engineering, 6(3), 2654–2660. https://doi.org/10.15680/IJIRCCE.2018.0603167

Anchala, S. (2018). Adoption of infrastructure as code security validation in cloud-native environments for reducing configuration drifts and compliance violations through automated template scanning. International Journal of Innovative Research in Science, Engineering and Technology, 7(10), 8305–8313. https://doi.org/10.15680/IJIRSET.2018.0710087

Mahadasu, S. S., & Rallabandi, B. R. (2023). Federated learning for privacy-preserving RAN optimization across multi-site enterprise 5G networks. International Journal of Engineering Science and Advanced Technology, 23(4), 53–57. https://doi.org/10.64771/ijesat.2023.v23.i04.pp3847

Talasila, D. (2018). Utilization of runtime application self-protection (RASP) in production environments for real-time vulnerability mitigation and behavioral enforcement through embedded monitoring agents. International Journal of Advanced Research in Education and Technology, 5(3), 831–840. https://doi.org/10.15680/IJARETY.2018.0503017

Aggarwal, A. (2018). Implementation of quantum cryptography in financial transactions for enhancing data confidentiality and resisting future quantum attacks through secure key distribution mechanisms. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 7(7), 3196–3204. https://doi.org/10.15662/IJAREEIE.2018.0707016

Kumar, S., Jain, A., Shukla, A. P., Singh, S., Raja, R., Rani, S., Harshitha, G., AlZain, M. A., & Masud, M. (2021). A comparative analysis of machine learning algorithms for detection of organic and nonorganic cotton diseases. Mathematical Problems in Engineering, 2021, Article 1790171. https://doi.org/10.1155/2021/1790171

Talasila, D. (2018). Integration of identity federation in multi-cloud access management for streamlining user authentication and reducing credential sprawl through centralized SSO protocols. International Journal of Multidisciplinary and Scientific Emerging Research, 6(4), 2017–2025. https://doi.org/10.15662/IJMSERH.2018.0604046

Jain, A., Kumar, A., & Sharma, S. (2015). Comparative design and analysis of mesh, torus and ring NoC. Procedia Computer Science, 48, 330–337. https://doi.org/10.1016/j.procs.2015.04.190

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

Bhaskara Raju Rallabandi. (2020). PRIVATE 5G SLICING DRIVEN BY INTENT USING MEC AND SD-WAN FOR SUPPORTING MULTITNTARY COMMUNICATIONS. International Journal of Engineering Research and Science & Technology, 16(4), 49–54. https://doi.org/10.62643/ijerst.2020.v16.n4.pp49-54

Jain, A., Gahlot, A. K., Dwivedi, R., Kumar, A., & Sharma, S. K. (2018). Fat tree NoC design and synthesis. In R. Singh, S. Choudhury, & A. Gehlot (Eds.), Intelligent communication, control and devices (Advances in Intelligent Systems and Computing, Vol. 624, pp. 1749–1756). Springer. https://doi.org/10.1007/978-981-10-5903-2_180

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

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

Chatrath, A. (2018). The impact of containerization on DevSecOps: Security considerations for Docker, Kubernetes, and microservices architectures in continuous deployment pipelines. International Journal of Advanced Research in Education and Technology, 5(6). https://doi.org/10.15680/IJARETY.2018.0506019

Ahuja, R. (2019). A comparative study of traditional DevOps and DevSecOps: Examining the cultural, technical, and organizational shifts required to embed security into software engineering practices. International Journal of Innovative Research in Science, Engineering and Technology, 8(8), 8561–8569. https://doi.org/10.15680/IJIRSET.2019.0808096

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

Gupta, N., Jain, A., Vaisla, K. S., Kumar, A., & Kumar, R. (2021). Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and

machine learning. Multimedia Tools and Applications, 80(14), 22301–22319. https://doi.org/10.1007/s11042-021-10820-4

Rangappa, A. S. (2020). Integration of behavioral analytics in developer workflows for detecting insider threats and malicious activities through activity monitoring and contextual profiling. International Journal of Innovative Research in Science, Engineering and Technology, 9(1), 13375–13383. https://doi.org/10.15680/IJIRSET.2020.0901064

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

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

Gupta, A. (2020). Utilization of homomorphic encryption in healthcare data sharing for ensuring confidentiality and compliance through secure computation without data exposure. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(10). https://doi.org/10.15680/IJMRSET.2020.0310011

Ahuja, R. (2023). The role of artificial intelligence and machine learning in DevSecOps: Leveraging predictive analytics, automated threat detection, and anomaly identification for secure software delivery pipelines. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 381–389. https://www.ijritcc.org/index.php/ijritcc/article/view/11946

Bhanushali, B. (2019). Graph-based network analysis for identifying complex money laundering typologies, detecting suspicious transaction chains, and tracing illicit financial flows. International Journal of Multidisciplinary and Scientific Emerging Research, 7(4), 2007–2014. https://doi.org/10.15662/IJMSERH.2019.0704047

Kumar, A., & Jain, A. (2021). Image smog restoration using oblique gradient profile prior and energy minimization. Frontiers of Computer Science, 15(6), Article 156706. https://doi.org/10.1007/s11704-020-9305-8

Chatrath, A. (2019). A multi-layered DevSecOps framework: Integrating secure coding, automated testing, vulnerability scanning, and incident response into end-to-end software development lifecycles. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 8(3). https://doi.org/10.15662/IJAREEIE.2019.0803102

Aggarwal, A. (2018). Implementation of cloud security automation in continuous integration pipelines for accelerating DevSecOps adoption and minimizing manual misconfigurations through security-as-code. International Journal of Innovative Research

in Science, Engineering and Technology, 7(11). https://doi.org/10.15680/IJIRSET.2018.0711083

Mahadasu, S. S. (2022). Cross-domain service assurance for private 5G networks using streaming telemetry and dependency-aware event correlation. International Journal of Data Science and IoT Management System, 1(3), 51–56. https://doi.org/10.64751/ijdim.2022.v1.n3.1290

Ahuja, R. (2020). Adoption of secure API development practices in microservice architectures for preventing unauthorized access and data leakage through OAuth2 and input throttling. Journal of Critical Reviews, 7(9), 4063–4069. https://doi.org/10.69980/jcr.v7:i9.13404

Bhanushali, B. (2019). Integration of biometric authentication with AML systems for strengthening know-your-customer (KYC) processes and reducing identity fraud in financial institutions. International Journal of Advanced Research in Education and Technology, 6(5), 853–860. https://doi.org/10.15680/IJARETY.2019.0605019

Ahuja, R. (2020). Database security in smart cities: Protecting interconnected infrastructure data, ensuring citizen privacy, and managing large-scale IoT data streams. International Journal of Multidisciplinary and Scientific Emerging Research, 8(1), 410–418. https://doi.org/10.15662/IJMSERH.2020.0801047

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

Anchala, S. (2018). Deployment of container image scanning in DevSecOps pipelines for mitigating open-source vulnerabilities and ensuring runtime safety through CVE-based detection mechanisms. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 7(3), 1546–1554. https://doi.org/10.15662/IJAREEIE.2018.0703058

Bhanushali, B. (2020). Effective sanctions screening and false positive identification. International Journal of Innovative Research in Science, Engineering and Technology, 9(4), 8306–8313. https://doi.org/10.15680/IJIRSET.2020.0904179

Ghai, D., Gianey, H. K., Jain, A., & Uppal, R. S. (2020). Quantum and dual-tree complex wavelet transform-based image watermarking. International Journal of Modern Physics B, 34(4), Article 2050009. https://doi.org/10.1142/S0217979220500095

Chatrath, A. (2019). DevSecOps in Agile and Lean development: Examining the alignment of security, speed, and scalability in rapid iteration and continuous delivery environments. International Journal of Multidisciplinary and Scientific Emerging Research, 7(3), 1506–1513. https://doi.org/10.15662/IJMSERH.2019.0703046

Rangappa, A. S. (2018). Deployment of immutable infrastructure in Dev Sec Ops practices for minimizing configuration drift and recovery time through ephemeral build environments. International Journal of Multidisciplinary and Scientific Emerging Research, 6(4), 2026–2034. https://doi.org/10.15662/IJMSERH.2018.0604047

Dwivedi, D. (2023). Integration of secure file upload mechanisms in user-facing applications for preventing malware injections and file-based exploits through content-type validation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 768–775. https://www.ijritcc.org/index.php/ijritcc/article/view/11940