International Journal of Science, Technology and Society
ISSN: 2395-7395 | Vol. 7 No. 02 (2023), July–December 2023 | pp. 13–23
DOI: https://doi.org/10.18091/ijsts.v7i2-02

RESEARCH ARTICLE

Intelligent Project Risk Prediction Using Natural Language Processing and Historical Project Data

Matqurbonov Omon
Department of History, Mamun University, Khiva, Uzbekistan
Email: omonbekmatqurbonov93@gmail.com | ORCID: 0000-0001-9024-7987

Alijon Esanov
Department of Uzbek Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan
Email: alijon_esanov@tues.uz | ORCID: 0009-0008-1528-5316

Turdiev Abdullo Sagdullaevich
Associate Professor, Department of Finance, Alfraganus University, Tashkent, Uzbekistan
Email: a.turdiyev@afu.uz | ORCID: 0000-0001-7973-5875

Abstract

Project risk prediction remains difficult because emerging hazards are often documented in unstructured meeting minutes, issue logs, change requests and retrospective reports before they appear in quantitative performance indicators. This paper develops an intelligent framework that combines natural language processing of project narratives with temporally aligned historical project attributes to estimate the probability and severity of schedule, cost and delivery risks. The architecture integrates text cleaning, contextual embeddings, structured feature engineering, temporal validation, calibrated classification and explainable decision support. A simulation protocol and fully specified evaluation design demonstrate how the proposed method can be tested without leaking future information. Illustrative numerical tables compare structured-only, text-only and multimodal predictors, including calibration and early-warning utility. The numbers are explicitly synthetic examples rather than outcomes of an implemented empirical study. The framework emphasizes auditability, data governance, operational intervention and external validation. It offers a foundation for future testing using anonymized organizational project repositories.

Keywords: *project risk prediction; natural language processing; historical project data; contextual embeddings; machine learning; risk governance; explainable artificial intelligence.*

1. Introduction

Projects operate within networks of uncertain dependencies involving scope, finance, staffing, suppliers, technology and stakeholder expectations. Conventional risk registers organize these uncertainties but are commonly updated periodically and depend on the judgment of individuals. As a result, weak signals can remain hidden in everyday communication until a milestone is missed. Predictive risk management aims to move from retrospective reporting to timely estimates of adverse outcomes, accompanied by enough evidence for a project manager to act.

Historical project databases contain potentially valuable signals such as planned duration, budget utilization, milestone slippage, change frequency, team turnover, defect density and vendor performance. Yet these structured fields do not always capture why a project is deteriorating. A schedule indicator may remain stable while a team meeting records unresolved architecture disagreements or an urgent change request describes an external dependency. Combining both forms of evidence can therefore improve the completeness of risk assessment.

Natural language processing offers techniques for extracting meaning from issue descriptions, lessons learned, progress notes, emails and project retrospectives. Earlier text mining systems relied on keywords and manually designed dictionaries. Modern contextual language models represent sentences according to

surrounding language and can distinguish a resolved concern from an escalating issue. Nevertheless, such representations may also encode irrelevant organizational style, confidential information or misleading correlations.

The challenge is not simply to classify negative words. A statement such as “the critical defect has been resolved” should not be treated as equivalent to “the critical defect remains unresolved.” Temporal context, negation, ownership, action status and the time at which a statement became available all matter. A prediction made on Monday must never use a retrospective note written on Friday. Failure to respect this distinction produces optimistic evaluations that cannot be replicated in deployment.

Project risk is also multidimensional. A team can meet a deadline by increasing cost or reducing quality; a low-cost project can fail to satisfy contractual requirements. Therefore, an intelligent model should support multiple outcome definitions, such as probability of a material schedule overrun, probability of cost escalation and an aggregate severity score. These outcomes should be defined before modeling, with thresholds linked to organizational policy rather than selected after observing results.

Risk scores are only useful when they influence decisions. Project managers need to know which evidence contributed to an alert, how reliable the probability estimate is and what intervention is proportionate to the expected loss. A model that flags nearly every project can have high sensitivity but create alert fatigue. Conversely, a highly precise model may miss rare but consequential failures. Evaluation must reflect both statistical discrimination and the economic cost of action.

Another important challenge is heterogeneity across projects. Construction, software, public infrastructure and research projects have different lifecycles and reporting practices. Even within one organization, documentation standards evolve. Models trained on historical projects may not generalize to new departments or policy regimes. Group-aware validation, time-based holdouts and monitoring of data drift are therefore essential to trustworthy performance estimates.

This paper proposes a modular prediction architecture linking narrative evidence to historical project data at weekly observation points. The framework uses a contextual encoder for text, a structured learner for project metrics, and a fusion layer that generates calibrated risk probabilities. It additionally includes missingness indicators, text-source provenance, explanations, intervention thresholds and governance checks. Each component can be replaced independently to support comparisons across resource constraints.

The central research questions concern whether narrative features add incremental predictive value beyond conventional project indicators, whether fusion improves the lead time of warnings, and whether probability calibration supports useful decisions. These questions are formulated as hypotheses rather than asserted as demonstrated facts. The paper provides a rigorous test plan and numerical examples to illustrate expected reporting formats without representing the examples as observed empirical evidence.

The contribution is methodological and practical. It specifies data alignment rules, a reproducible training and validation protocol, interpretable equations, a risk-management workflow and a template for cost-sensitive evaluation. It also distinguishes genuine field evidence from synthetic demonstration. Future researchers can instantiate the design on authorized project archives, preregister risk definitions and report uncertainty across organizations and time periods.

2. Literature Review

Project risk management literature has traditionally emphasized identification, qualitative probability-impact matrices, response planning and periodic review. These practices are valuable for accountability but depend on the completeness of the risk register and the consistency of expert assessments. Quantitative prediction complements rather than replaces expert judgment by learning patterns from repeated project observations and systematically comparing predictions with realized outcomes.

Studies of project performance have linked overruns to scope instability, estimation bias, complexity, resource constraints and governance. Such findings motivate structured predictors including earned-value indices, change-request counts, schedule variance and team capacity. However, many published models are developed on narrow datasets or use a single outcome definition, limiting comparison. A robust research design must document label definitions, measurement dates and the distribution of project types.

In machine learning, logistic regression provides an interpretable baseline, while random forests and gradient-boosted trees capture nonlinear relationships and interactions among tabular attributes. Tree ensembles can model complex risk patterns but may overfit small organizational samples. Baseline comparisons are essential because a complicated multimodal architecture is not justified unless it delivers meaningful out-of-time improvements over simple alternatives.

Text mining extends the evidence base beyond numerical project dashboards. Term frequency and inverse document frequency can represent issue logs efficiently, whereas topic models summarize recurring concerns such as staffing, procurement and technical debt. These approaches offer relatively transparent features, yet they struggle with word order, negation and semantic similarity. Domain-specific dictionaries may improve precision but require ongoing maintenance.

Contextual representation learning changed NLP by modeling words in relation to their surrounding text. Transformer-based encoders, including BERT, support sentence and document classification with transfer learning. For project narratives, contextual models may recognize that a delayed supplier approval and a pending external dependency express related concerns. However, pretrained encoders may require adaptation to technical terminology and cannot be assumed accurate on project-management records.

Multimodal fusion combines complementary information sources. Early fusion concatenates embeddings and numeric features before a shared classifier; late fusion aggregates separate model predictions. Intermediate or gated fusion can adapt the contribution of each source when narrative quality varies. Comparing these approaches helps identify whether performance gains arise from new information, increased model capacity or both.

An important methodological issue is temporal leakage. Randomly splitting weekly records from the same project can put highly similar observations into training and test partitions. Notes written after an outcome may accidentally describe the event being predicted. Proper evaluation requires grouping by project, respecting observation cutoffs and reserving later projects for final testing. Without these safeguards, apparent accuracy can be substantially overstated.

Risk prediction also requires probability calibration. A model that assigns a 0.70 risk should experience the outcome in approximately 70% of comparable cases. Reliability curves, Brier scores and calibration error examine this property, while precision-recall analysis is particularly relevant for uncommon failure events. Decision thresholds should be determined using intervention cost and expected loss rather than maximizing accuracy alone.

Explainable AI offers local feature attribution and global sensitivity analysis. SHAP can summarize the influence of structured variables, while text-level explanations may highlight relevant sentences. These explanations are approximations of model behavior, not proof of causal drivers.

Finally, governance research highlights privacy, fairness, security and human oversight. Project communications may include employee names, commercial details and sensitive client information. De-identification, access controls, retention rules and auditing are necessary before model development. The literature suggests a research gap in integrated, temporally rigorous, calibrated and decision-oriented prediction pipelines that combine narrative signals with historical project metrics; the present framework addresses this gap as a testable design.

3. Research Methodology

3.1 Research design and prediction task

The proposed design is a retrospective longitudinal prediction study with a prospective shadow-mode validation phase. Each project is observed at weekly cutoffs. The target is a material adverse event occurring within the following four weeks. The primary binary label is a schedule overrun greater than 15% of the approved baseline; secondary outcomes include cost overrun above 10% and a composite severity measure.

The unit of analysis is a project-week. Project identifiers are used only for grouping, not as predictive features. An observation is eligible only if the project was active at the cutoff and at least four weeks of subsequent outcome data exist. Completed projects contribute no observations after closure. Reporting frequency is normalized to avoid privileging highly documented teams.

3.2 Data sources and governance

Source	Illustrative fields	Timing rule
Project master	type, budget, duration, phase	known by cutoff
Performance history	variance, milestones, burn rate	snapshot at cutoff
Narrative records	issues, meeting notes, change logs	timestamp at or before cutoff
Outcome ledger	final milestone and spend	future label only

Before extraction, obtain organizational approval, remove direct identifiers, restrict access by role, encrypt the research repository and log each data transformation. Narratives must be screened for confidential contracts and personally identifying information.

3.3 Proposed workflow

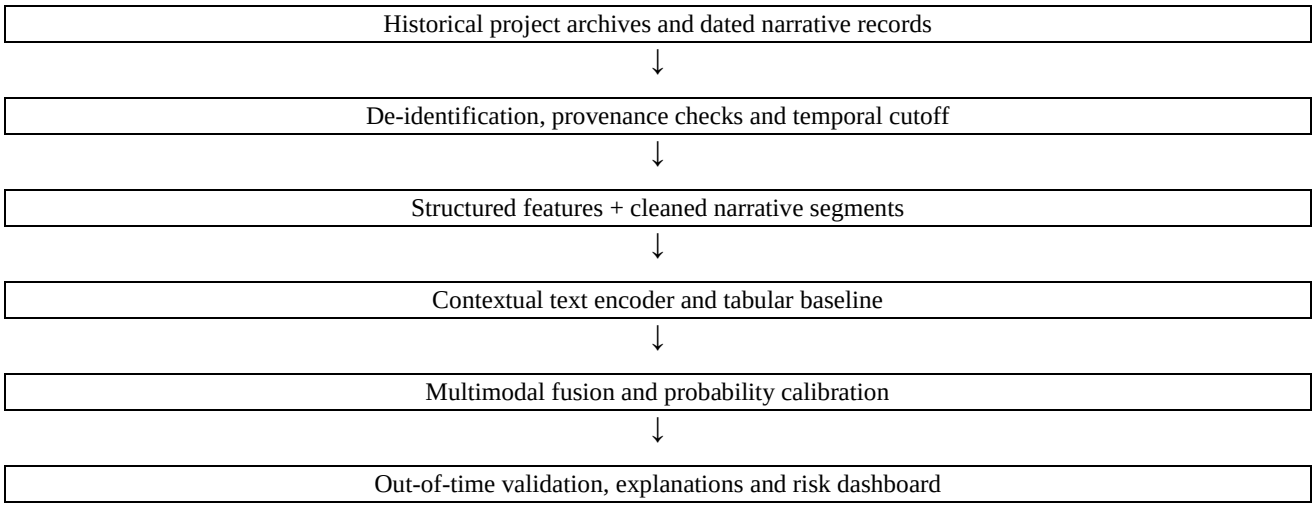


Figure 1. Editable workflow of the proposed prediction framework. Every feature must be available at the prediction cutoff.

3.4 Structured feature preparation

For numeric feature j, estimate the training-set mean and standard deviation only on the training fold. Apply the same transformation to validation and test observations. Missingness indicators preserve information about reporting gaps, while robust winsorization limits the effect of extreme administrative entries.

$$z_j = (x_j - \mu_j) / \sigma_j$$

Here x_j is the observed value of feature j, μ_j is its training mean, σ_j is its training standard deviation and z_j is the standardized feature. No statistics are recomputed on held-out data.

3.5 Text processing and representation

Collect text from issue logs, risk comments, meeting minutes and change requests. Normalize encodings, remove duplicate attachments, retain negation and modal terms, and segment long records by sentence or

document section. Attach source type, author role where legally permissible, record timestamp and resolution status. A document is excluded when its creation timestamp exceeds the prediction cutoff.

A pretrained transformer encoder produces a contextual vector for each narrative segment. Mean pooling across valid tokens yields a segment representation; attention or recency-weighted aggregation then summarizes all segments available for a project-week. To reduce dominance by verbose projects, cap the number of segments per source and include a document-count feature.

$$h_i = Encoder(T_i)$$

$$v = \Sigma_i \alpha_i h_i$$

$$\alpha_i = exp(s_i) / \Sigma_k exp(s_k)$$

T_i denotes segment i, h_i its contextual embedding, s_i its learned attention score, α_i its normalized weight and v the aggregated narrative representation. Attention scores alone should not be interpreted as causal explanations.

3.6 Multimodal risk estimation

Let x represent standardized structured features and v the narrative embedding. A gated fusion network assigns a context-dependent contribution to the two feature groups. The concatenated representation is processed by a feedforward classifier to estimate event probability. A text-only and a structured-only model are trained with equivalent partitions for ablation.

$$g = sigmoid(Wg\,[x\,;\,v] + bg)$$

$$u = g \odot \varphi(Wx\,x) + (1 - g) \odot \varphi(Wv\,v)$$

$$p = sigmoid(w^T u + b)$$

Wg, Wx and Wv are learned weight matrices; bg and b are bias terms; φ is a nonlinear activation; ⊙denotes elementwise multiplication; g is the fusion gate; u is the fused feature vector; and p is the predicted event probability. The projected vectors are constrained to equal dimensionality.

3.7 Objective and class imbalance

Use weighted binary cross-entropy to account for minority risk events. Class weights are computed from training data only. Hyperparameters are selected using a temporally separated validation fold; class weighting, focal loss and resampling should be compared rather than applied simultaneously without evidence.

$$L = -(1/N)\,\Sigma_i\,[w_1\,y_i\,log(p_i) + w_0\,(1 - y_i)\,log(1 - p_i)]$$

N is the number of training observations, y_i is the observed binary outcome, p_i is its predicted probability, and w_1 and w_0 weight positive and negative outcomes. Optimization uses early stopping based on validation loss.

3.8 Validation and leakage prevention

Partition projects by initiation date into training (earliest 65%), validation (next 15%) and final test (latest 20%), ensuring no project appears in multiple partitions. A second leave-one-department-out evaluation probes organizational transfer. Feature selection, text vocabulary adaptation, normalization, calibration and threshold tuning occur without access to final test labels. Confidence intervals should be bootstrapped by project, not by project-week, because repeated observations are correlated.

3.9 Evaluation metrics

$$Precision = TP / (TP + FP)$$

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

$$F1 = 2 \times Precision \times Recall / (Precision + Recall)$$

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

TP, FP and FN denote true positives, false positives and false negatives. Precision measures the fraction of alerts that are genuine; recall measures the fraction of actual adverse events detected. F1 balances both. The Brier score assesses probability accuracy, with smaller values preferred. Also report ROC AUC, PR AUC, calibration plots and the distribution of warning lead times.

3.10 Cost-sensitive alert policy

An alert should trigger a documented review rather than automatic punitive action. Let C_r be the cost of review, C_m the loss from an unmitigated event and q the fraction of event loss avoidable through timely intervention. Under a simplified expected-value assumption, review is justified when its cost is smaller than the expected preventable loss.

$$Review\ if\ p \times q \times C_m > C_r$$

The equation assumes calibrated p and approximately stable intervention efficacy. Real-world evaluation must estimate q and C_m from historical interventions or a controlled pilot. Managers should record whether an alert was accepted, the action taken, and its outcome to support continuous improvement.

3.11 Explainability, fairness and monitoring

Generate SHAP summaries for structured features and source-linked text rationales for individual alerts. Explanations must display the record timestamp and allow authorized users to inspect the underlying evidence. Compare false-positive and false-negative rates by project category and department where lawful and statistically meaningful. Monitor population drift, missingness, document volume, calibration and intervention workload monthly.

3.12 Reproducibility protocol

Freeze dataset versions, record labeling rules, retain random seeds, disclose encoder versions and hyperparameters, and preserve code for extraction and evaluation. Report confidence intervals and baseline comparisons on the untouched test set. A prospective shadow deployment should run for at least one complete reporting cycle before operational alerts are enabled.

4. Illustrative Results and Discussion

IMPORTANT: The following numerical values are constructed to demonstrate analysis and visualization. They are not measured results from an implemented model or a real project dataset. They must be replaced with outputs from an approved empirical study before claims of effectiveness can be made.

4.1 Example test-set classification performance

Model	Precision	Recall	F1	ROC AUC	PR AUC
Logistic regression (structured)	0.74	0.52	0.61	0.77	0.43
Gradient boosting (structured)	0.79	0.61	0.69	0.82	0.48
Transformer (text)	0.76	0.66	0.71	0.83	0.5
Proposed multimodal fusion	0.84	0.73	0.78	0.89	0.59

Table 2. Synthetic performance scenario. The multimodal row is higher across all reported metrics by construction, illustrating the type of incremental-value hypothesis to test. Statistical significance and reproducibility cannot be inferred from this table.

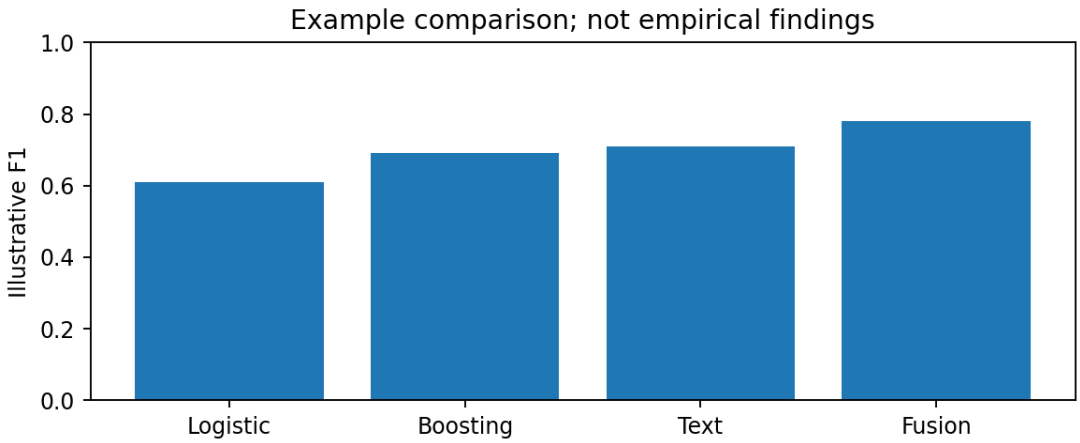


Figure 2. Hypothetical F1 comparison. A real study should add confidence intervals and paired project-level tests.

4.2 Illustrative confusion matrix

Actual / predicted	Risk alert	No alert
Risk event	73	27
No risk event	14	86

Table 3. Synthetic confusion matrix for 200 project observations. It implies precision 73/87 = 0.839, recall 73/100 = 0.730 and F1 ≈ 0.781, consistent with the rounded multimodal example above. These counts are illustrative only.

4.3 Example calibration and decision value

Predicted risk bin	Mean predicted probability	Illustrative observed frequency	Observations
0.0–0.2	0.12	0.1	50
0.2–0.4	0.3	0.28	50
0.4–0.6	0.5	0.54	50
0.6–0.8	0.7	0.72	50

Table 4. Synthetic reliability bins. Observed frequencies are deliberately near the mean predictions to illustrate how calibration is assessed. The gap between prediction and frequency must be calculated on actual held-out observations.

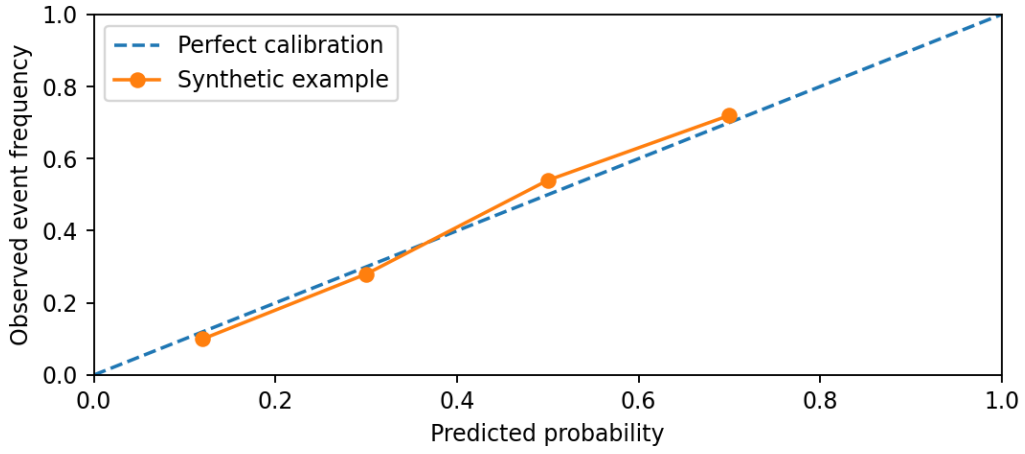


Figure 3. Hypothetical calibration plot. A prospective evaluation should also test whether calibration changes over time and across project categories.

4.4 Ablation and early-warning scenarios

Configuration	Illustrative PR AUC	Median warning lead (days)
Structured features only	0.48	8
Narrative features only	0.5	11
Fusion without calibration	0.58	13
Fusion with calibration	0.59	13

Table 5. Constructed ablation scenario. Calibration ordinarily changes probabilities, not ranking, so PR AUC may remain unchanged; the small difference shown is a scenario rather than a general expected effect. Lead time should be measured only for correctly predicted events at a prespecified alert threshold.

4.5 Interpretation and threats to validity

Potential gains from narrative signals could arise because meeting notes and issue records describe emerging obstacles earlier than milestone metrics. However, documentation intensity, retrospective editing, selection bias and differences in reporting culture can produce spurious associations. Class prevalence, project size and industry mix can also alter precision and calibration. A credible empirical paper must report actual sample characteristics, confidence intervals, failure cases and subgroup analyses.

5. Conclusion

This study develops a testable architecture for intelligent project risk prediction using natural language processing and historical project data. The framework joins time-aligned narrative evidence with structured project metrics, employs contextual text representations and gated fusion, and produces calibrated probabilities for decision support. Its methodological safeguards address project-level dependence, temporal leakage, class imbalance, explanation fidelity and responsible data governance. The numerical tables and figures demonstrate reporting and interpretation only; they do not establish empirical superiority. Future work should evaluate the pipeline on authorized multi-organization datasets, compare it against transparent baselines, quantify uncertainty, assess warning lead time and test whether risk alerts improve real management outcomes. The ultimate objective is not merely to predict failure but to support earlier, proportionate and accountable interventions.

References

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

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.

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

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

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

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

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

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

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

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

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

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

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., & 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

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

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

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

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

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

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

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

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

Khan, S. (2022). The use of artificial intelligence in ESG (environmental, social, and governance) investing: A study on AI models for sustainability analytics in asset and wealth management. International Journal of Multidisciplinary and Scientific Emerging Research, 10(1), 431–439. https://doi.org/10.15662/IJMSERH.2022.1001046

Jain, A., 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

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

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

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

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

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, 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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. (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

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

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

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

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

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

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

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

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