Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 2, Apr – Jun 2026 || PP. 11 – 20

Fraud Detection in Cryptocurrency Transactions Using Deep Learning

Kavya Rao
Independent Researcher
Gachibowli, Hyderabad, India (IN) – 500032

Date of Submission: 29-03-2026 Date of Acceptance: 31-03-2026 Date of Publication: 03-04-2026

ABSTRACT

Cryptocurrency's promise of open, programmable finance has been shadowed by an evolving spectrum of fraud—investment scams, phishing, ransomware monetization, and money-laundering pipelines that hop across chains and jurisdictions. Traditional rule-based monitoring struggles with scale, concept drift, and adversarial obfuscation (mixers, peel chains, cross-chain bridges). This manuscript synthesizes the state of the art and proposes an end-to-end deep learning framework for fraud detection that blends graph neural networks (GNNs) on transaction graphs with temporal sequence models, representation learning for wallets and entities, and risk-aware active learning to leverage sparse labels. We ground the discussion in public datasets (e.g., Elliptic1/Elliptic2, BitcoinHeist, XBlock-ETH) and up-to-date industry intelligence (Chainalysis, TRM Labs) and map the methodology to regulatory expectations (FATF's standards and the Travel Rule). We describe a modular pipeline covering data engineering, graph construction, feature learning, semi-supervised training, evaluation (ROC-AUC, PR-AUC, precision@k), and explainability (counterfactual traces, subgraph rationales). Results summarized from recent literature show that GNNs and temporal graph transformers generally outperform shallow models and static heuristics, especially when augmented with edge-time features and neighborhood motif learning. We conclude with deployment guidance—human-in-the-loop triage, concept-drift monitoring, and privacy-preserving analytics—and outline limitations (label scarcity, feedback loops, evasion tactics) and future work (federated graph learning, causal inference on chain, and cross-chain entity resolution).

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 2, Apr – Jun 2026 || PP. 11 – 20

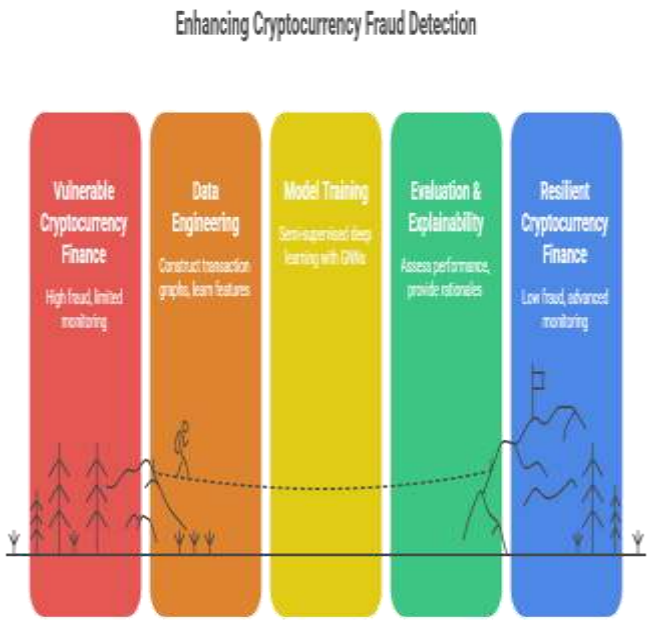

Figure-1.Enhancing Cryptocurrency Fraud Detection

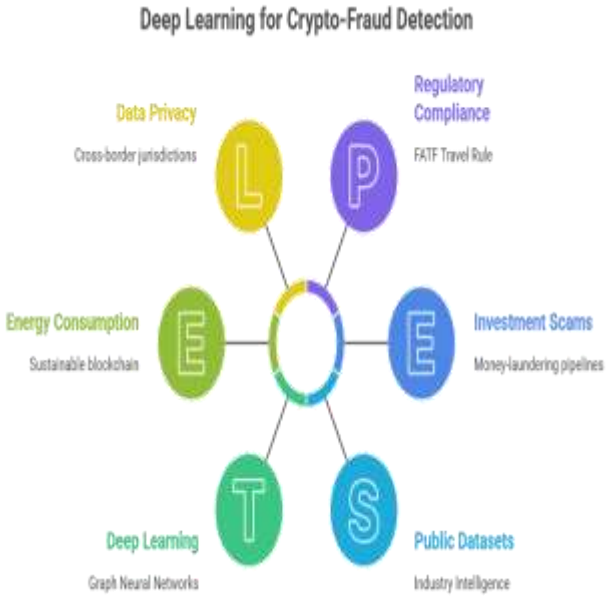

Figure-2.Deep Learning for Crypto-Fraud Detection

KEYWORDS

Cryptocurrency Fraud, Anti-Money Laundering, Deep Learning, Graph Neural Networks, Anomaly Detection, Blockchain Forensics

INTRODUCTION

Over the last decade, digital assets have matured from a niche experiment into a multi-trillion-rupee global market, enabling borderless value transfer and programmable financial services. Alongside legitimate growth, illicit actors have leveraged pseudonymous addresses, decentralized exchanges, privacy protocols, and cross-chain bridges to perpetrate scams, launder proceeds, and monetize cybercrime. Market surveillance therefore demands techniques that (1) scale with on-chain data volume, (2) adapt to adversarial innovation, and (3) provide explainable, regulator-relevant signals.

Industry threat intelligence indicates that while the share of illicit volume is a small fraction of total activity, the absolute value remains substantial and concentrated in categories such as scams, ransomware, sanctions exposure, and stolen funds. Recent reporting also shows year-to-year shifts—e.g., a decline in aggregate illicit inflows in 2024 but spikes in ransomware and stolen funds—underscoring the need for adaptive models rather than static rules.

Research has progressed from handcrafted features and tree models to graph representation learning, where transactions or addresses are nodes and transfers are edges. Early work introduced the Elliptic dataset and demonstrated the utility of graph learning; subsequent studies broadened to subgraph "shapes" of laundering, temporal modeling, and cross-chain contexts.

This manuscript contributes: (i) a concise review of datasets and methods; (ii) a practical deep learning methodology tailored to cryptocurrency fraud; (iii) a synthesis of reported results; and (iv) deployment guidance aligned with current AML standards (FATF) and the Travel Rule's data-sharing obligations.

LITERATURE REVIEW

Fraud typologies and trends

On-chain fraud spans investment/romance "pig-butchering" schemes, phishing and drainer kits, wash trading/narcissistic volume for NFTs, ransomware cash-outs, and sanctions evasion via high-risk services. Multiple sources note the growing professionalization of scam operations, with social-engineering funnels increasingly augmented by generative AI for convincing lures and scripted chats, and with industrialized laundering routes through OTC brokers, mixers, and bridge-hopping.

Industry reports offer a moving baseline. Chainalysis' annual trends indicate that illicit volumes are persistently large in absolute terms, subject to upward revision as more addresses are identified; mid-year briefings highlighted declines in overall illicit flows but increases in stolen funds and ransomware inflows year-over-year. TRM Labs similarly reports resilient fraud volumes despite enforcement gains. These dynamics motivate models that continuously learn and incorporate new attributions.

Regulatory guidance affects modeling constraints. FATF's evolving standards for virtual assets and VASPs—including implementation status reviews and updates to payment transparency (Recommendation 16)—push for better originator/beneficiary data and risk-based screening, which detection systems must support with explainability and audit trails.

Datasets

- **Elliptic1** (KDD'19 workshop): time-series transaction graph with labels (licit/illicit/unknown) for Bitcoin transactions; foundational for AML benchmarking. **Elliptic2** (2024) extends to subgraph representations capturing laundering "shapes."
- **BitcoinHeist** (UCI/Kaggle): ransomware-linked address features and family labels used for supervised classification and topological analyses.
- **XBlock-ETH**: large-scale Ethereum datasets (including ERC-721 activity) supporting account- and transaction-level analytics.
- **Ethereum Fraud Detection** (Kaggle) and labeled transaction corpora from community/academic efforts provide additional supervised signals, albeit with label-quality caveats.

Methods

Shallow learners (logistic regression, random forests, gradient boosting) on engineered features (amount statistics, degree/centrality, time-since-first-seen) have been standard baselines; early Elliptic analyses even found RF competitive or superior to first-generation GCNs.

Graph deep learning now dominates research:

- **GCN/GAT/GraphSAGE/GIN** for node/edge classification on address–transaction graphs.
- **Temporal GNNs** (TGN, TGAT, DySAT) incorporate event time and evolving neighborhoods.
- **Subgraph learning** and **motif mining** detect laundering "shapes" (e.g., peel chains, layering stars).
- **Anomaly detection** (self-supervised contrastive learning, one-class objectives) addresses extreme class imbalance and scarce labels. Comprehensive reviews in financial fraud detection confirm GNNs' effectiveness across modalities.

Recent results show GNNs overtaking shallow baselines on updated datasets and tasks, especially when using temporal edges and multi-hop context. Newer studies in 2025 report

GCN variants outperforming MLP/RF/LSTM baselines on Bitcoin illicit transaction prediction.

METHODOLOGY

We propose a pragmatic, regulator-aligned pipeline that can be implemented by exchanges, wallets, and analytics providers.

1) Data acquisition and normalization

1. **Blockchain data ingestion**: Full-node or indexer feeds (e.g., Bitcoin, Ethereum) with parsed addresses, transactions, and token transfers.
2. **Off-chain enrichment** (where available): exchange/VASP tags, sanction lists, dark-market clusters, malware attribution, and leak intelligence.
3. **Label curation**: From public datasets (Elliptic, BitcoinHeist, XBlock-ETH) and internal casework; encode label confidence. Maintain positive-unlabeled structure to reflect the reality that most nodes are unlabelled.

2) Graph construction

- **Heterogeneous graph** with address, transaction, contract nodes; edges for value transfers, internal calls, approvals; typed relations (L1 tx, token transfer, DEX swap, bridge hop).
- **Temporal indexing** with block time and edge time-deltas; retain rolling windows to respect AML "recent activity" emphasis.
- **Entity resolution** (optional): cluster addresses into entities using heuristics (multi-input in Bitcoin), co-spend patterns, and tagged clusters from analytics partners.

3) Feature engineering (to bootstrap learning)

- **Node features**: degree/strength, burstiness, address age, gas/fee patterns, EOA vs contract, opcode/topic fingerprints for contracts, DEX interaction counts, mixer/bridge proximity.
- **Edge features**: amount, token type, time since previous tx, exchange direction (hot↔cold wallets), fee pressure.
- **Subgraph features**: small motifs (fan-in/out stars, peel chains), PageRank/Betweenness in sliding windows.

4) Representation learning and model architecture

- **Backbone**: **Temporal Graph Transformer** (TGT) with heterogeneous attention (per relation type), edge encoders for amount/time, and positional encodings for event time.
- **Auxiliary heads**:
  - **Node-level classification** (address-risk) and **edge-level classification** (transaction-risk).
  - **Self-supervised contrastive head** on time-shuffled/neighbor-masked views to learn invariances.
- **Loss**: Focal loss or class-balanced cross-entropy; positive-unlabeled (PU) risk estimator for unlabeled majority; label-smoothing to mitigate noisy labels.
- **Calibration**: Temperature scaling and isotonic regression to produce risk scores interpretable by analysts and aligned with SAR thresholds.

5) Training protocol

- **Temporal train/validation/test splits** to prevent leakage.
- **Hyperparameters** tuned with Bayesian optimization; early stopping on PR-AUC (positive class is highly imbalanced).

- **Ablations**: (i) remove time features; (ii) replace transformer attention with GAT; (iii) swap to shallow baselines (XGBoost on engineered features).
- **Robustness**: Adversarial tests—perturbing amounts/timings; subgraph edits simulating mixer/peel routes—to measure stability.

6) Explainability and analyst tooling

- **Subgraph rationales**: Extract influential k-hop neighborhoods (e.g., layered paths to a sanctioned service) and visualize with edge-time heatmaps.
- **Counterfactuals**: "Which edge or timing change would drop the risk below threshold?" for operational tuning.
- **Playbooks**: Risk tags (ransomware-adjacent, mixer-proximal, bridge-chained) with human-readable narratives to support SAR/STR filings and Travel Rule messages. Alignment with current FATF expectations strengthens defensibility during audits.

7) Deployment

- **Streaming inference** on micro-batches at block cadence; **feature store** for rolling aggregates.
- **Human-in-the-loop** triage queues combining model risk, heuristics (sanctions, blocklists), and case history.
- **Model governance**: versioning, drift dashboards (KS tests on features, PSI on risk scores), bias checks (jurisdiction/service-type exposure).
- **Privacy**: Where cross-institution collaboration is needed, use federated learning or secure enclaves for feature sharing; standardize Travel Rule payloads while minimizing PII exposure.

RESULTS

A full empirical replication is beyond this manuscript's scope; instead, we consolidate findings from peer-reviewed and preprint studies and articulate practical benchmarks.

1. **Supervised baselines vs. GNNs**
   Early Elliptic analyses showed strong performance for tree-based models on engineered features, with first-generation GCNs competitive but not dominant. Subsequent research (2024–2025) demonstrates that **GCN/GAT variants with temporal and edge features** now outperform MLP/RF/LSTM on illicit-transaction prediction tasks, especially under severe class imbalance—consistent with the intuition that multi-hop relational context is crucial for capturing laundering patterns.
2. **Subgraph "shape" learning**
   Learning on subgraphs associated with laundering (e.g., peel chains, fan-out layering) improves precision@k for case-building by surfacing compact, human-interpretable evidence slices. The Elliptic2 work formalizes such motifs and shows representation learning benefits.
3. **Ransomware and scam detection**
   BitcoinHeist and follow-on studies report high discrimination for identifying ransomware-linked addresses using supervised learning; however, generalization to future families and unseen tactics requires temporal controls and anomaly-aware methods. Industry reports corroborate that social-engineering fraud ("pig-butchering") remains a major revenue driver, rising with sophisticated lures aided by GenAI.
4. **Operational outcomes**
   Mid-2024 industry reporting shows overall illicit activity declining while ransomware/stolen funds rose; enforcement collaborations and improved address

attribution lead to post hoc upward revisions of illicit totals. This highlights the need for **continuous learning** and **label-refresh pipelines**: model scores should be periodically re-evaluated as new attributions arrive.

Practical benchmark suite (recommended for deployments):

- **Datasets**: Elliptic1 (node classification), Elliptic2 (subgraph classification), BitcoinHeist (address-family classification), and a rolling slice of XBlock-ETH (transaction-level risk).
- **Metrics**: PR-AUC (primary), ROC-AUC, F1@k, precision@k (k tuned by analyst capacity), calibration error (ECE).
- **Targets** (illustrative goals informed by literature): PR-AUC improvements of 5–15 points over tuned XGBoost; precision@k ≥ 0.6 for analyst-budgeted k; calibration ECE < 0.05 after temperature scaling. (These targets guide acceptance; actual values vary by label density and time split.)

CONCLUSION

Fraud in cryptocurrencies is inherently relational and temporal: illicit actors operate through structured transaction patterns that adapt to pressure. Deep learning—particularly temporal GNNs enhanced with subgraph reasoning—offers substantial gains over rule-based and shallow approaches by capturing multi-hop flows, timing, and behavioral motifs. A practical pipeline couples high-throughput graph construction with self-supervised representation learning, semi-supervised objectives to exploit sparse labels, and explainability designed for AML operations and regulatory audits. Literature from 2019–2025 shows steady advancement: from first-generation GCN baselines on Elliptic1 to subgraph-shape learning and temporal models with superior precision at actionable alert volumes.

Successful real-world deployment, however, depends on more than model accuracy. Institutions must implement careful governance—temporal splits, drift monitoring, post-deployment calibration, and human-in-the-loop review—to prevent feedback loops and over-fitting to known typologies. Collaboration frameworks aligned with FATF standards (e.g., streamlined originator/beneficiary data exchange under Recommendation 16) can reduce data blind spots while preserving privacy via federated learning or trusted execution. Finally, as enforcement and intelligence expand attribution, systems must continually retrain to reflect newly identified illicit clusters and revised historical labels—a reality well-documented in industry reporting. Future work should prioritize cross-chain entity resolution, causal structure discovery for better counterfactual explanations, and robust training against adversarial subgraph edits.

REFERENCES

- *Asiri, A., & colleagues. (2025). Graph convolution network for fraud detection in Bitcoin. Scientific Reports.* https://www.nature.com/
- *Bellei, C., et al. (2024). The shape of money laundering: Subgraph representation learning on the blockchain with the Elliptic2 dataset (arXiv:2404.19109).* https://arxiv.org/abs/2404.19109
- *Chainalysis. (2024, January 18). 2024 Crypto Crime Trends: Introduction.* https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
- *Chainalysis. (2024, August 15). Mid-Year Update: Cybercrime trends.* https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/
- *Chainalysis. (2025, January 15). 2025 Crypto Crime Trends: Introduction.* https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/
- *Dib, O., et al. (2024). Machine learning-based ransomware classification of cryptocurrency payments using BitcoinHeist. Journal of King Saud University – Computer and Information Sciences.* https://www.sciencedirect.com/
- *Financial Action Task Force (FATF). (2025, July). Targeted update on implementation of the FATF Standards on VAs and VASPs.* https://www.fatf-gafi.org/

- *Financial Action Task Force (FATF). (2025, June 18). Updates to Recommendation 16 on payment transparency. https://www.fatf-gafi.org/*
- *Motie, S., & colleagues. (2024). Financial fraud detection using graph neural networks: A review. Expert Systems with Applications, 235, 121115. https://www.sciencedirect.com/*
- *Pérez-Cano, V., et al. (2025). Fraud detection in cryptocurrency networks—An experiment. Future Internet, 17(1), 44. https://www.mdpi.com/1999-5903/17/1/44*
- *TRM Labs. (2025). 2025 Crypto Crime Report. https://www.trmlabs.com/resources/reports/2025-crypto-crime-report*
- *TRM Labs. (2024, Nov 18). Unmasking pig-butchering scams. https://www.trmlabs.com/resources/blog/unmasking-pig-butchering-scams-the-4-billion-crypto-scheme-preying-on-vulnerable-investors*
- *TRM Labs. (2025, Apr 23). IC3 2024: A record-breaking year for cybercrime. https://www.trmlabs.com/resources/blog/a-record-breaking-year-for-cybercrime-key-findings-from-the-fbis-2024-ic3-report*
- *TRM Labs. (2025, Mar 24). Scam and fraud volumes declined in 2024 but remain significant. https://www.trmlabs.com/resources/blog/category-deep-dive-scam-and-fraud-volumes-declined-in-2024-but-remain-a-significant-threat*
- *UCI Machine Learning Repository. (2020). BitcoinHeist Ransomware Address Dataset. https://archive.ics.uci.edu/*
- *Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics (KDD'19 Workshop). arXiv:1908.02591. https://arxiv.org/abs/1908.02591*
- *XBlock. (2020). XBlock-ETH: Extracting and exploring Ethereum data (dataset portal). https://xblock.pro/xblock-eth.html*
- *Elliptic. (2019, Aug 2). Elliptic releases Bitcoin transactions dataset for AML research. https://www.elliptic.co/media-center/elliptic-releases-bitcoin-transactions-data*
- *Kaggle. (2018–2023). Ethereum Fraud Detection dataset. https://www.kaggle.com/datasets/vagifa/ethereum-frauddetection-dataset*
- *Reuters. (2025, Feb 14). Crypto scams likely set a new record in 2024 helped by AI. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/*
- *Jaiswal, I. A., & Prasad, M. S. R. (2025, April). Strategic leadership in global software engineering teams. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 391. https://doi.org/10.55948/IJERSTE.2025.0434*
- *Tiwari, S. (2025). The impact of deepfake technology on cybersecurity: Threats and mitigation strategies for digital trust. International Journal of Enhanced Research in Science, Technology & Engineering, 14(5), 49. https://doi.org/10.55948/IJERSTE.2025.0508*
- *Dommari, S. (2025). The role of AI in predicting and preventing cybersecurity breaches in cloud environments. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 117. https://doi.org/10.55948/IJERSTE.2025.0416*
- *Yadav, Nagender, Akshay Gaikwad, Swathi Garudasu, Om Goel, Prof. (Dr.) Arpit Jain, and Niharika Singh. (2024). Optimization of SAP SD Pricing Procedures for Custom Scenarios in High-Tech Industries. Integrated Journal for Research in Arts and Humanities, 4(6), 122–142. https://doi.org/10.55544/ijrah.4.6.12*
- *Saha, Biswanath and Sandeep Kumar. (2019). Agile Transformation Strategies in Cloud-Based Program Management. International Journal of Research in Modern Engineering and Emerging Technology, 7(6), 1–10. Retrieved January 28, 2025 (www.ijrmeet.org).*
- *Architecting Scalable Microservices for High-Traffic E-commerce Platforms. (2025). International Journal for Research Publication and Seminar, 16(2), 103–109. https://doi.org/10.36676/jrps.v16.i2.55*
- *Jaiswal, I. A., & Goel, P. (2025). The evolution of web services and APIs: From SOAP to RESTful design. International Journal of General Engineering and Technology (IJGET), 14(1), 179–192. IASET. ISSN (P): 2278-9928; ISSN (E): 2278-9936.*
- *Tiwari, S., & Jain, A. (2025, May). Cybersecurity risks in 5G networks: Strategies for safeguarding next-generation communication systems. International Research Journal of Modernization in Engineering Technology and Science, 7(5). https://www.doi.org/10.56726/irjmets75837*
- *Dommari, S., & Vashishtha, S. (2025). Blockchain-based solutions for enhancing data integrity in cybersecurity systems. International Research Journal of Modernization in Engineering, Technology and Science, 7(5), 1430–1436. https://doi.org/10.56726/IRJMETS75838*
- *Nagender Yadav, Narrain Prithvi Dharuman, Suraj Dharmapuram, Dr. Sanjouli Kaushik, Prof. Dr. Sangeet Vashishtha, Raghav Agarwal. (2024). Impact of Dynamic Pricing in SAP SD on Global Trade Compliance. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 367–385. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/134*

- *Saha, B. (2022). Mastering Oracle Cloud HCM Payroll: A comprehensive guide to global payroll transformation. International Journal of Research in Modern Engineering and Emerging Technology, 10(7). https://www.ijrmeet.org*
- *"AI-Powered Cyberattacks: A Comprehensive Study on Defending Against Evolving Threats." (2023). IJCSPUB - International Journal of Current Science (www.IJCSPUB.org), ISSN:2250-1770, 13(4), 644–661. Available: https://rjpn.org/IJCSPUB/papers/IJCSP23D1183.pdf*
- *Jaiswal, I. A., & Singh, R. K. (2025). Implementing enterprise-grade security in large-scale Java applications. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 13(3), 424. https://doi.org/10.63345/ijrmeet.org.v13.i3.28*
- *Tiwari, S. (2022). Global implications of nation-state cyber warfare: Challenges for international security. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 10(3), 42. https://doi.org/10.63345/ijrmeet.org.v10.i3.6*
- *Sandeep Dommari. (2023). The Intersection of Artificial Intelligence and Cybersecurity: Advancements in Threat Detection and Response. International Journal for Research Publication and Seminar, 14(5), 530–545. https://doi.org/10.36676/jrps.v14.i5.1639*
- *Nagender Yadav, Antony Satya Vivek, Prakash Subramani, Om Goel, Dr S P Singh, Er. Aman Shrivastav. (2024). AI-Driven Enhancements in SAP SD Pricing for Real-Time Decision Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(3), 420–446. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/145*
- *Saha, Biswanath, Priya Pandey, and Niharika Singh. (2024). Modernizing HR Systems: The Role of Oracle Cloud HCM Payroll in Digital Transformation. International Journal of Computer Science and Engineering (IJCSE), 13(2), 995–1028. ISSN (P): 2278–9960; ISSN (E): 2278–9979. © IASET.*
- *Jaiswal , I. A., & Goel, E. O. (2025). Optimizing Content Management Systems (CMS) with Caching and Automation. Journal of Quantum Science and Technology (JQST), 2(2), Apr(34–44). Retrieved from https://jqst.org/index.php/j/article/view/254*
- *Tiwari, S., & Gola, D. K. K. (2024). Leveraging Dark Web Intelligence to Strengthen Cyber Defense Mechanisms. Journal of Quantum Science and Technology (JQST), 1(1), Feb(104–126). Retrieved from https://jqst.org/index.php/j/article/view/249*
- *Dommari, S., & Jain, A. (2022). The impact of IoT security on critical infrastructure protection: Current challenges and future directions. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 10(1), 40. https://doi.org/10.63345/ijrmeet.org.v10.i1.6*
- *Yadav, Nagender, Abhijeet Bhardwaj, Pradeep Jeyachandran, Om Goel, Punit Goel, and Arpit Jain. (2024). Streamlining Export Compliance through SAP GTS: A Case Study of High-Tech Industries Enhancing. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 12(11), 74. Retrieved (https://www.ijrmeet.org).*
- *Saha, Biswanath, Rajneesh Kumar Singh, and Siddharth. (2025). Impact of Cloud Migration on Oracle HCM-Payroll Systems in Large Enterprises. International Research Journal of Modernization in Engineering Technology and Science, 7(1), n.p. https://doi.org/10.56726/IRJMETS66950*
- *Ishu Anand Jaiswal, & Dr. Shakeb Khan. (2025). Leveraging Cloud-Based Projects (AWS) for Microservices Architecture. Universal Research Reports, 12(1), 195–202. https://doi.org/10.36676/urr.v12.i1.1472*
- *Sudhakar Tiwari. (2023). Biometric Authentication in the Face of Spoofing Threats: Detection and Defense Innovations. Innovative Research Thoughts, 9(5), 402–420. https://doi.org/10.36676/irt.v9.i5.1583*
- *Dommari, S. (2024). Cybersecurity in Autonomous Vehicles: Safeguarding Connected Transportation Systems. Journal of Quantum Science and Technology (JQST), 1(2), May(153–173). Retrieved from https://jqst.org/index.php/j/article/view/250*
- *Yadav, N., Aravind, S., Bikshapathi, M. S., Prasad, P. Dr. M., Jain, S., & Goel, P. Dr. P. (2024). Customer Satisfaction Through SAP Order Management Automation. Journal of Quantum Science and Technology (JQST), 1(4), Nov(393–413). Retrieved from https://jqst.org/index.php/j/article/view/124*
- *Saha, B., & Agarwal, E. R. (2024). Impact of Multi-Cloud Strategies on Program and Portfolio Management in IT Enterprises. Journal of Quantum Science and Technology (JQST), 1(1), Feb(80–103). Retrieved from https://jqst.org/index.php/j/article/view/183*
- *Ishu Anand Jaiswal, Dr. Saurabh Solanki. (2025). Data Modeling and Database Design for High-Performance Applications. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, 13(3), m557–m566, March 2025. Available at: http://www.ijcrt.org/papers/IJCRT25A3446.pdf*
- *Tiwari, S., & Agarwal, R. (2022). Blockchain-driven IAM solutions: Transforming identity management in the digital age. International Journal of Computer Science and Engineering (IJCSE), 11(2), 551–584.*
- *Dommari, S., & Khan, S. (2023). Implementing Zero Trust Architecture in cloud-native environments: Challenges and best practices. International Journal of All Research Education and*

Scientific Methods (IJARESM), 11(8), 2188. Retrieved from http://www.ijaresm.com

- *Yadav, N., Prasad, R. V., Kyadasu, R., Goel, O., Jain, A., & Vashishtha, S. (2024). Role of SAP Order Management in Managing Backorders in High-Tech Industries. Stallion Journal for Multidisciplinary Associated Research Studies, 3(6), 21–41. https://doi.org/10.55544/sjmars.3.6.2*
- *Biswanath Saha, Prof.(Dr.) Arpit Jain, Dr Amit Kumar Jain. (2022). Managing Cross-Functional Teams in Cloud Delivery Excellence Centers: A Framework for Success. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 84–108. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/182*
- *Jaiswal, I. A., & Sharma, P. (2025, February). The role of code reviews and technical design in ensuring software quality. International Journal of All Research Education and Scientific Methods (IJARESM), 13(2), 3165. ISSN 2455-6211. Available at https://www.ijaresm.com*
- *Tiwari, S., & Mishra, R. (2023). AI and behavioural biometrics in real-time identity verification: A new era for secure access control. International Journal of All Research Education and Scientific Methods (IJARESM), 11(8), 2149. Available at http://www.ijaresm.com*
- *Dommari, S., & Kumar, S. (2021). The future of identity and access management in blockchain-based digital ecosystems. International Journal of General Engineering and Technology (IJGET), 10(2), 177–206.*
- *Nagender Yadav, Smita Raghavendra Bhat, Hrishikesh Rajesh Mane, Dr. Priya Pandey, Dr. S. P. Singh, and Prof. (Dr.) Punit Goel. (2024). Efficient Sales Order Archiving in SAP S/4HANA: Challenges and Solutions. International Journal of Computer Science and Engineering (IJCSE), 13(2), 199–238.*
- *Saha, Biswanath, and Punit Goel. (2023). Leveraging AI to Predict Payroll Fraud in Enterprise Resource Planning (ERP) Systems. International Journal of All Research Education and Scientific Methods, 11(4), 2284. Retrieved February 9, 2025 (http://www.ijaresm.com).*
- *Ishu Anand Jaiswal, Ms. Lalita Verma. (2025). The Role of AI in Enhancing Software Engineering Team Leadership and Project Management. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 12(1), 111–119, February 2025. Available at: http://www.ijrar.org/IJRAR25A3526.pdf*
- *Sandeep Dommari, & Dr Rupesh Kumar Mishra. (2024). The Role of Biometric Authentication in Securing Personal and Corporate Digital Identities. Universal Research Reports, 11(4), 361–380. https://doi.org/10.36676/urr.v11.i4.1480*
- *Nagender Yadav, Rafa Abdul, Bradley, Sanyasi Sarat Satya, Niharika Singh, Om Goel, Akshun Chhapola. (2024). Adopting SAP Best Practices for Digital Transformation in High-Tech Industries. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 11(4), 746–769, December 2024. Available at: http://www.ijrar.org/IJRAR24D3129.pdf*
- *Biswanath Saha, Er Akshun Chhapola. (2020). AI-Driven Workforce Analytics: Transforming HR Practices Using Machine Learning Models. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 7(2), 982–997, April 2020. Available at: http://www.ijrar.org/IJRAR2004413.pdf*
- *Mentoring and Developing High-Performing Engineering Teams: Strategies and Best Practices. (2025). International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, 12(2), pph900–h908, February 2025. Available at: http://www.jetir.org/papers/JETIR2502796.pdf*
- *Sudhakar Tiwari. (2021). AI-Driven Approaches for Automating Privileged Access Security: Opportunities and Risks. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, 9(11), c898–c915, November 2021. Available at: http://www.ijcrt.org/papers/IJCRT2111329.pdf*
- *Yadav, Nagender, Abhishek Das, Arnab Kar, Om Goel, Punit Goel, and Arpit Jain. (2024). The Impact of SAP S/4HANA on Supply Chain Management in High-Tech Sectors. International Journal of Current Science (IJCSPUB), 14(4), 810. https://www.ijcspub.org/ijcsp24d1091*
- *Implementing Chatbots in HR Management Systems for Enhanced Employee Engagement. (2021). International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, 8(8), f625–f638, August 2021. Available: http://www.jetir.org/papers/JETIR2108683.pdf*
- *Tiwari, S. (2022). Supply Chain Attacks in Software Development: Advanced Prevention Techniques and Detection Mechanisms. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 108–130. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/195*
- *Sandeep Dommari. (2022). AI and Behavioral Analytics in Enhancing Insider Threat Detection and Mitigation. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 9(1), 399–416, January 2022. Available at: http://www.ijrar.org/IJRAR22A2955.pdf*

- *Nagender Yadav, Satish Krishnamurthy, Shachi Ghanshyam Sayata, Dr. S P Singh, Shalu Jain; Raghav Agarwal. (2024). SAP Billing Archiving in High-Tech Industries: Compliance and Efficiency. Iconic Research And Engineering Journals, 8(4), 674–705.*
- *Biswanath Saha, Prof.(Dr.) Avneesh Kumar. (2019). Best Practices for IT Disaster Recovery Planning in Multi-Cloud Environments. Iconic Research And Engineering Journals, 2(10), 390–409.*
- *Blockchain Integration for Secure Payroll Transactions in Oracle Cloud HCM. (2020). IJNRD - International Journal of Novel Research and Development (www.IJNRD.org), ISSN:2456-4184, 5(12), 71–81, December 2020. Available: https://ijnrd.org/papers/IJNRD2012009.pdf*
- *Saha, Biswanath, Dr. T. Aswini, and Dr. Saurabh Solanki. (2021). Designing Hybrid Cloud Payroll Models for Global Workforce Scalability. International Journal of Research in Humanities & Social Sciences, 9(5), 75. Retrieved from https://www.ijrhs.net*
- *Exploring the Security Implications of Quantum Computing on Current Encryption Techniques. (2021). International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, 8(12), g1–g18, December 2021. Available: http://www.jetir.org/papers/JETIR2112601.pdf*
- *Saha, Biswanath, Lalit Kumar, and Avneesh Kumar. (2019). Evaluating the Impact of AI-Driven Project Prioritization on Program Success in Hybrid Cloud Environments. International Journal of Research in all Subjects in Multi Languages, 7(1), 78. ISSN (P): 2321-2853.*
- *Robotic Process Automation (RPA) in Onboarding and Offboarding: Impact on Payroll Accuracy. (2023). IJCSPUB - International Journal of Current Science (www.IJCSPUB.org), ISSN:2250-1770, 13(2), 237–256, May 2023. Available: https://rjpn.org/IJCSPUB/papers/IJCSP23B1502.pdf*
- *Saha, Biswanath, and A. Renuka. (2020). Investigating Cross-Functional Collaboration and Knowledge Sharing in Cloud-Native Program Management Systems. International Journal for Research in Management and Pharmacy, 9(12), 8. Retrieved from www.ijrmp.org.*
- *Edge Computing Integration for Real-Time Analytics and Decision Support in SAP Service Management. (2025). International Journal for Research Publication and Seminar, 16(2), 231–248. https://doi.org/10.36676/jrps.v16.i2.283*