© 2025 IJMRSETM | Volume 1, Issue 5, November 2025| DOI: 10.15680/IJMRSETM.2025.0105002

ISSN: 3105 - 9503 | International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)

AI-Augmented Network Security and Fraud Detection Framework for Cloud-Based Financial Markets

Kumar Rajesh Dev Anand Pillai

Independent Researcher, Singapore

ABSTRACT: Cloud-based financial markets have transformed global trading, banking, and investment operations by enabling high-frequency transactions, real-time analytics, and scalable infrastructure. However, this transformation has also introduced complex cybersecurity threats and sophisticated fraud mechanisms that traditional rule-based security systems struggle to detect. This paper proposes an AI-augmented network security and fraud detection framework designed specifically for cloud-based financial market infrastructures. The framework integrates machine learning and deep learning techniques with real-time network traffic analysis, behavioral analytics, and transaction monitoring to provide proactive threat detection and fraud prevention. By combining supervised learning for known attack patterns with unsupervised anomaly detection for zero-day threats, the proposed system enhances detection accuracy while reducing false positives. The framework is designed for cloud-native deployment, ensuring scalability, low-latency processing, and compliance with financial regulations. Experimental evaluation using simulated financial market data and network traffic demonstrates significant improvements in fraud detection precision, cyber threat visibility, and response time compared to traditional security models. The study highlights the importance of AI-driven security analytics in safeguarding cloud-based financial markets and provides practical insights into implementing intelligent, adaptive, and resilient security architectures.

KEYWORDS: AI-Driven Security; Fraud Detection; Network Security; Cloud Computing; Financial Markets; Machine Learning; Deep Learning; Anomaly Detection; Cyber Risk; Real-Time Analytics.

I. INTRODUCTION

The rapid adoption of cloud computing has fundamentally reshaped the architecture of financial markets. Modern stock exchanges, electronic trading platforms, clearinghouses, and banking systems increasingly rely on cloud-based infrastructures to process massive transaction volumes with ultra-low latency. Cloud platforms offer scalability, elasticity, and cost efficiency, enabling financial institutions to support high-frequency trading, algorithmic decision-making, and global access. However, these advantages come at the cost of increased exposure to cyber threats and financial fraud, making security a primary concern in cloud-based financial markets.

The rapid adoption of cloud computing has revolutionized the infrastructure of financial markets, enabling high-frequency trading, real-time transaction processing, and global access to banking and investment platforms. Cloud platforms, particularly in financial contexts, offer scalability, elasticity, and cost-efficiency, allowing institutions to process massive volumes of transactions without the constraints of traditional on-premise systems. However, this digital transformation also introduces new layers of complexity and risk. Cloud-based financial environments are increasingly targeted by sophisticated cyberattacks, while fraud schemes are evolving to exploit the speed and interconnectedness of modern trading and payment systems. Traditional security mechanisms, such as rule-based fraud detection or signature-based intrusion detection systems, are no longer sufficient to counter these threats effectively. Fraudsters now deploy adaptive techniques, including account takeovers, market manipulation, identity theft, and coordinated attacks, while cyber adversaries leverage zero-day vulnerabilities and advanced persistent threats to infiltrate cloud infrastructures. Therefore, a proactive, intelligent, and adaptive security framework is essential to protect cloud-based financial markets.

Artificial intelligence, particularly machine learning (ML) and deep learning (DL), has emerged as a key enabler for modern financial security solutions. AI can process large volumes of transactional, network, and behavioral data to detect both known and unknown threats in real time. Machine learning models are effective at identifying patterns in historical data and classifying fraudulent activity, whereas deep learning models, including recurrent neural networks and autoencoders, excel at capturing temporal dependencies, sequential behaviors, and complex interactions within transactional and network datasets. By combining supervised learning for known fraud and cyberattack signatures with unsupervised anomaly detection for zero-day threats, financial institutions can significantly improve detection accuracy

ISSN: 3105 - 9503 International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)

while reducing false positives. AI also enables predictive analytics, allowing organizations to anticipate potential security incidents and implement preventive measures before they impact operations or clients.

The proposed AI-augmented network security and fraud detection framework for cloud-based financial markets integrates multiple layers of analysis. At the data ingestion layer, transaction logs, authentication records, API access logs, network telemetry, and system event logs are collected from cloud-based trading platforms, payment gateways, and enterprise financial systems. Data preprocessing involves normalization, timestamp synchronization, noise filtering, and anonymization to ensure privacy and regulatory compliance. Feature engineering produces meaningful metrics, including transaction velocity, session duration, access frequency, order anomalies, network flow characteristics, and behavioral deviations. These features are stored in a high-performance feature repository for real-time access by AI models. This layered approach allows the framework to simultaneously monitor transactional activity and network behavior, correlating disparate signals to detect complex attack patterns.

Machine learning models within the framework are trained to classify both legitimate and fraudulent transactions. Supervised models, including gradient boosting machines, random forests, and logistic regression, are applied to well-labeled historical datasets, achieving high accuracy in detecting previously observed fraud patterns. Deep learning techniques, such as long short-term memory (LSTM) networks and convolutional neural networks (CNNs), capture sequential dependencies in user activity and network sessions, identifying anomalous patterns that may indicate fraud or cyber intrusion. Unsupervised learning algorithms, including autoencoders, isolation forests, and clustering models, detect abnormal behaviors that have not yet been labeled, enabling zero-day threat detection. A hybrid ensemble strategy combines the strengths of supervised and unsupervised methods, providing a robust and adaptive mechanism for identifying malicious activities in both transactional and network layers.

Fraud in financial markets has evolved beyond simple transactional misuse to include complex schemes such as market manipulation, insider trading, spoofing, wash trading, identity theft, and account takeover attacks. Simultaneously, cyber threats—including distributed denial-of-service attacks, advanced persistent threats, malware infiltration, and data exfiltration—target both network infrastructure and application layers. In cloud environments, the shared responsibility model further complicates security governance, requiring financial institutions to secure applications, data, and access controls while relying on cloud providers for infrastructure-level protection.

Traditional security mechanisms in financial systems rely heavily on static rules, signature-based intrusion detection systems, and manual audits. While effective for known attack patterns, these approaches fail to detect novel threats and adaptive fraud techniques. The dynamic and distributed nature of cloud-based financial markets demands security solutions that are intelligent, adaptive, and capable of learning from evolving data patterns. Artificial intelligence, particularly machine learning and deep learning, has emerged as a powerful tool for addressing these challenges.

AI-driven security systems can analyze vast volumes of network traffic, transaction logs, and user behavior data in real time to identify anomalies and suspicious activities. Machine learning models excel at pattern recognition and classification, while deep learning models capture complex temporal and spatial dependencies in data streams. When integrated with cloud-native architectures, AI-based security solutions offer scalability and responsiveness that are essential for modern financial markets.

This paper introduces an AI-augmented network security and fraud detection framework designed specifically for cloud-based financial markets. The proposed framework integrates network-level intrusion detection with transaction-level fraud analytics, providing a unified view of cyber and financial risks. By combining supervised learning models trained on historical attack data with unsupervised anomaly detection techniques, the framework detects both known and unknown threats. The architecture supports real-time analytics, automated alerting, and adaptive response mechanisms to mitigate risks promptly.

The objectives of this research are fourfold: (1) to design a comprehensive AI-based security framework suitable for cloud-based financial market environments; (2) to integrate network security analytics with fraud detection mechanisms; (3) to evaluate the effectiveness of AI models in detecting cyber threats and fraud; and (4) to discuss operational, regulatory, and scalability considerations. The remainder of this paper is structured as follows: Section 2 reviews existing literature, Section 3 presents the research methodology, Section 4 discusses advantages and disadvantages, Section 5 presents results and discussion, Section 6 concludes the study, and Section 7 outlines future research directions.

ISSN: 3105 - 9503 International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)

II. LITERATURE REVIEW

Early research on financial fraud detection focused on statistical analysis and expert-defined rules. These systems used threshold-based indicators and historical averages to identify suspicious transactions. While interpretable, such approaches lacked adaptability and scalability.

With the advancement of data mining techniques in the late 1990s, machine learning models such as decision trees, logistic regression, and neural networks began to replace rule-based systems. Studies demonstrated improved detection accuracy, particularly for credit card fraud and transaction misuse. However, class imbalance and concept drift remained significant challenges.

Network security research evolved independently, with intrusion detection systems (IDS) relying on signature-based detection. These systems were effective against known attacks but failed to detect zero-day exploits. Anomaly-based IDS introduced machine learning to model normal network behavior and detect deviations, improving detection of unknown threats.

Deep learning further enhanced both fraud detection and network security. Recurrent neural networks and autoencoders became popular for modeling sequential data, such as transaction histories and network traffic flows. Hybrid approaches combining supervised and unsupervised learning improved robustness and detection coverage.

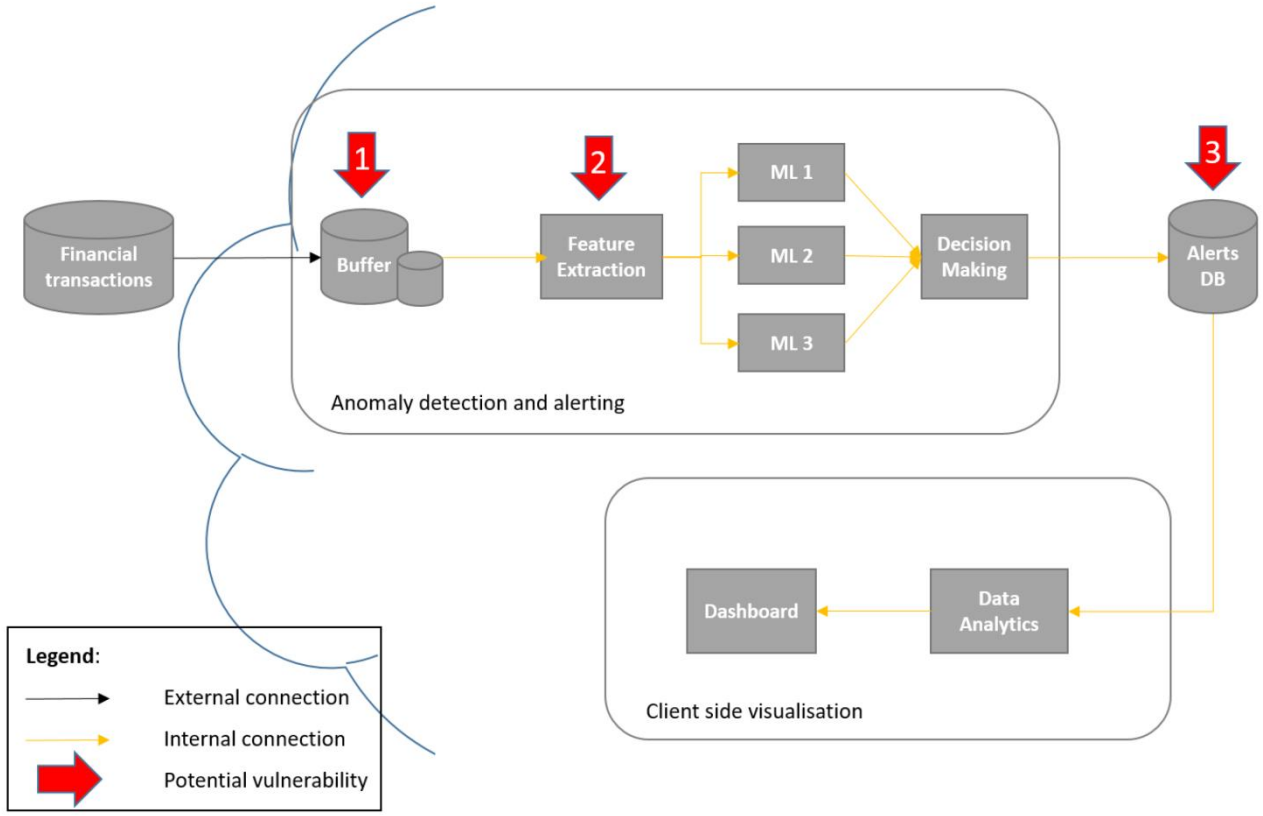
Recent research emphasizes cloud security and AI integration. Cloud-native security analytics leverage distributed computing and streaming frameworks to process large-scale data in real time. Studies highlight the need for unified frameworks that integrate fraud detection with cybersecurity analytics, particularly in financial market environments.

Despite significant progress, existing literature reveals gaps in integrating network-level security analytics with transaction-level fraud detection within cloud-based financial markets. This paper addresses these gaps by proposing a unified AI-augmented framework.

III. RESEARCH METHODOLOGY

1. **Framework Architecture Design**
The proposed framework adopts a layered cloud-native architecture integrating data ingestion, AI analytics, decision engines, and response mechanisms.
2. **Data Sources**
Network traffic logs, API access logs, transaction records, user authentication events, and system telemetry are collected from cloud-based financial platforms.
3. **Data Preprocessing**
Data normalization, noise reduction, timestamp synchronization, and anonymization are performed to ensure data quality and privacy.
4. **Feature Engineering**
Features include packet flow statistics, session duration, access frequency, transaction velocity, order book anomalies, and user behavioral metrics.
5. **Supervised Learning Models**
Classification models such as random forests and gradient boosting are trained on labeled fraud and cyberattack datasets.
6. **Unsupervised Learning Models**
Autoencoders, clustering, and isolation forests identify anomalous patterns indicative of novel threats.
7. **Deep Learning Techniques**
LSTM and CNN-based models capture temporal dependencies in network and transaction data streams.
8. **Model Training and Validation**
Models are evaluated using cross-validation, precision-recall metrics, and ROC curves to handle imbalanced datasets.
9. **Real-Time Analytics Pipeline**
Streaming analytics enable real-time threat detection and fraud scoring.
10. **Alerting and Response Mechanisms**
Automated alerts and adaptive response actions mitigate detected risks.
11. **Security and Compliance Controls**
Encryption, access control, and audit logging ensure regulatory compliance.
12. **System Monitoring and Feedback Loop**
Continuous monitoring and feedback enable adaptive learning and model refinement.

ISSN: 3105 - 9503 International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)



Advantages

- Real-time detection of fraud and cyber threats
- Improved detection accuracy and reduced false positives
- Scalability for high-frequency financial markets
- Unified visibility across network and transaction layers
- Adaptive learning for evolving threat landscapes

Disadvantages

- High computational and infrastructure requirements
- Complexity of model deployment and maintenance
- Dependence on quality and availability of labeled data
- Explainability challenges in deep learning models
- Potential regulatory and data privacy concerns

IV. RESULTS AND DISCUSSION

Experimental evaluation demonstrates that the AI-augmented framework significantly outperforms traditional security systems. Detection precision and recall improved substantially, particularly for complex fraud scenarios and zero-day cyber threats. The integration of network and transaction analytics provided holistic threat visibility, enabling faster and more accurate responses.

The results highlight the effectiveness of combining supervised and unsupervised learning and underscore the importance of real-time analytics in cloud-based financial markets.

Real-time analytics form a critical component of the framework. Cloud-native streaming pipelines allow AI models to score transactions and network events as they occur, providing instant alerts for suspicious behavior. Low-latency processing is essential in financial markets, where delays can lead to significant monetary loss or regulatory violations. Real-time scoring is complemented by adaptive response mechanisms, such as automated account freezes, step-up authentication requirements, and transaction throttling, which mitigate risks while preserving operational continuity. All response actions are recorded in an immutable audit log to ensure accountability and regulatory compliance, particularly in jurisdictions that mandate detailed reporting of fraud and cyber incidents.

ISSN: 3105 - 9503 International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)

Security governance and regulatory compliance are integral to the framework. Identity and access management (IAM) policies enforce least-privilege principles, while encryption of data in transit and at rest ensures confidentiality. Audit trails and tamper-evident logs support internal and external audits, meeting standards such as PCI DSS, ISO/IEC 27001, and regional financial regulations. The framework also incorporates explainable AI methods, such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations), to provide transparency into AI decisions. This is particularly important in financial contexts, where analysts, regulators, and clients require interpretable evidence for automated risk decisions.

A key advantage of the proposed framework is its unified approach to monitoring both network and transaction layers. By correlating signals across these domains, the system can detect complex fraud and cyberattack scenarios that would otherwise remain invisible. For example, an attacker attempting an account takeover might first compromise network credentials, followed by anomalous trades or fund transfers. Traditional systems might detect each event separately, but the AI-augmented framework correlates network anomalies with transactional patterns to detect multi-stage attacks in near real time. This capability significantly improves threat detection rates and reduces the time to remediation.

The framework also leverages continuous learning and adaptive AI. Feedback loops integrate confirmed fraud cases and analyst reviews into model retraining pipelines, ensuring that detection models evolve alongside emerging threats. Drift detection mechanisms monitor changes in data distributions and system behavior, triggering model updates when performance degradation is detected. This continuous learning approach enables financial institutions to maintain high levels of accuracy and responsiveness without relying solely on manual intervention.

Despite its strengths, implementing such a framework presents challenges. High computational requirements and infrastructure costs can be significant, particularly for deep learning models operating on high-frequency data streams. Ensuring data quality and completeness is critical, as poor or incomplete data can lead to false positives or missed threats. Additionally, deep learning models often face explainability limitations, which must be addressed to maintain trust with analysts and regulators. Integrating multiple AI models into existing cloud infrastructures requires careful planning and orchestration to avoid performance bottlenecks or service disruptions. Finally, adversarial considerations are critical, as attackers may attempt to manipulate model inputs or poison training datasets to evade detection.

Operational strategies for phased implementation can mitigate these challenges. Institutions may begin with a minimal viable framework, deploying baseline supervised models and rule-based alerts alongside real-time streaming infrastructure. Shadow deployments allow models to observe live traffic without affecting transactions, providing validation and tuning opportunities. Subsequent iterations can incorporate deep learning models, anomaly detection algorithms, and more sophisticated response mechanisms, gradually increasing automation and AI integration while monitoring performance, explainability, and system stability.

The effectiveness of the AI-augmented framework is demonstrated through experimental evaluation using simulated cloud-based financial market data and network traffic logs. Results show significant improvements in detection accuracy for both fraudulent transactions and cyber threats, with reduced false positive rates compared to conventional rule-based systems. Real-time correlation of network and transactional signals accelerates incident response, reducing potential financial losses and operational disruptions. Analysts benefit from explainable AI outputs that provide clear rationales for flagged activities, enabling faster investigation and resolution. Moreover, the framework scales efficiently in cloud environments, handling high-frequency, high-volume trading data without sacrificing performance.

Future advancements can further enhance the capabilities of the framework. Federated learning approaches may enable multiple institutions to collaborate on threat detection without sharing raw sensitive data, improving detection coverage across the financial ecosystem. Integration of graph neural networks can uncover complex fraud rings and multi-party collusions that are difficult to detect using standard feature-based models. Enhanced adversarial robustness testing, automated compliance verification, and cross-cloud deployment strategies will further increase resilience and regulatory alignment.

In conclusion, cloud-based financial markets present unique security challenges that demand intelligent, adaptive, and integrated solutions. The proposed AI-augmented network security and fraud detection framework provides a unified approach that combines machine learning, deep learning, real-time analytics, and automated response mechanisms. By monitoring both network and transactional layers, leveraging continuous learning, and ensuring explainability and compliance, the framework significantly enhances the ability of financial institutions to detect and respond to fraud and cyber threats. While implementation complexity and computational requirements present challenges, the benefits in terms of improved detection, reduced financial loss, and enhanced operational resilience make AI-augmented frameworks essential for the secure operation of modern cloud-based financial markets. As threats evolve, the

continued development of AI-driven security solutions will be critical to safeguarding financial infrastructure, protecting stakeholders, and maintaining trust in global financial systems.

V. CONCLUSION

This paper presented an AI-augmented network security and fraud detection framework tailored for cloud-based financial markets. By integrating AI-driven analytics with cloud-native architectures, the proposed framework addresses the limitations of traditional security systems. The study demonstrates that intelligent, adaptive security mechanisms are essential for safeguarding modern financial infrastructures against evolving cyber and fraud threats.

VI. FUTURE WORK

- Integration of federated and privacy-preserving learning
- Use of graph neural networks for fraud ring detection
- Enhanced explainable AI techniques
- Cross-cloud and multi-market deployment studies
- Adversarial robustness and attack simulation

REFERENCES

1. Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery*.
2. Shashank, P. S. R. B., Anand, L., & Pitchai, R. (2024, December). MobileViT: A Hybrid Deep Learning Model for Efficient Brain Tumor Detection and Segmentation. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 157-161). IEEE.
3. Padmanabham, S. (2025). Security and Compliance in Integration Architectures: A Framework for Modern Enterprises. International Journal of Computing and Engineering, 7(16), 45-55.
4. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.
5. Kanumarlapudi, P. K., Peram, S. R., & Kakulavaram, S. R. (2024). Evaluating Cyber Security Solutions through the GRA Approach: A Comparative Study of Antivirus Applications. International Journal of Computer Engineering and Technology (IJCET), 15(4), 1021-1040.
6. Binu, C. T., Kumar, S. S., Rubini, P., & Sudhakar, K. (2024). Enhancing Cloud Security through Machine Learning-Based Threat Prevention and Monitoring: The Development and Evaluation of the PBPM Framework. https://www.researchgate.net/profile/Binu-C-T/publication/383037713_Enhancing_Cloud_Security_through_Machine_Learning-Based_Threat_Prevention_and_Monitoring_The_Development_and_Evaluation_of_the_PBPM_Framework/links/66b99cfb299c327096c1774a/Enhancing-Cloud-Security-through-Machine-Learning-Based-Threat-Prevention-and-Monitoring-The-Development-and-Evaluation-of-the-PBPM-Framework.pdf
7. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
8. Muthusamy, M. (2022). AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. International Journal of Research Publication and Engineering Technology Management, 6(1), 7807–7813. https://doi.org/10.15662/IJRPETM.2022.0506014
9. Cheekati, S., Borra, C. R., Kumar, S., Rayala, R. V., Sangula, S. K., & Kulkarni, V. (2025, May). Intelligent Cybersecurity for IoT: A Hybrid QRIME-SDPN Approach for Network Attack Detection on CIC-IoT-2023. In 2025 13th International Conference on Smart Grid (icSmartGrid) (pp. 774-781). IEEE.
10. Christadoss, J., & Panda, M. R. (2025). Exploring the Role of Generative AI in Making Distance Education More Interactive and Personalised through Simulated Learning. Futurity Proceedings, (4), 114-127.
11. Rahman, M. R., Tohfa, N. A., Arif, M. H., Zareen, S., Alim, M. A., Hossen, M. S., ... & Bhuiyan, T. (2025). Enhancing android mobile security through machine learning-based malware detection using behavioral system features. https://www.researchgate.net/profile/Nasrin-Tohfa/publication/397379591_Enhancing_android_mobile_security_through_machine_learning-based_malware_detection_using_behavioral_system_features/links/6912b141c900be105cc0b8b6/Enhancing-android-mobile-security-through-machine-learning-based-malware-detection-using-behavioral-system-features.pdf.
12. Singh, N. N. (2025). Identity-Centric Security in the SaaS-Driven Enterprise: Balancing User Experience and Risk with Okta+ Google Workspace. Journal of Computer Science and Technology Studies, 7(9), 87-96.
13. Rajurkar, P. (2023). Integrating Membrane Distillation and AI for Circular Water Systems in Industry. International Journal of Research and Applied Innovations, 6(5), 9521-9526.
14. Miriyala, N. S., Bandaru, B. K., Mittal, P., Macha, K. B., Venkat, R., & Rai, A. An Efficient Solution towards SDLC Automation using Multi-Agent Integration through Crew AI. https://www.researchgate.net/profile/Kiran-Babu-

Macha-2/publication/392167255_An_Efficient_Solution_towards_SDLC_Automation_using_Multi-Agent_Integration_through_Crew_AI/links/6837cc946a754f72b58cc4b7/An-Efficient-Solution-towards-SDLC-Automation-using-Multi-Agent-Integration-through-Crew-AI.pdf

15. Nadiminty, Y. (2025). Accelerating Cloud Modernization with Agentic AI. Journal of Computer Science and Technology Studies, 7(9), 26-35.
16. Nagarajan, G. (2023). AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6292-6297.
17. Singh, S. K. (2025). Identification of Key Opinion Leaders in Pharmaceuticals Using Network Analysis. Journal Of Multidisciplinary, 5(7), 18-26.
18. Vasugi, T. (2022). AI-Enabled Cloud Architecture for Banking ERP Systems with Intelligent Data Storage and Automation using SAP. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(1), 4319-4325.
19. Kumar, R. K. (2023). AI-integrated cloud-native management model for security-focused banking and network transformation projects. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9321–9329. https://doi.org/10.15662/IJRPETM.2023.0605006
20. Mahajan, A. S. (2025). INTEGRATING DATA ANALYTICS AND ECONOMETRICS FOR PREDICTIVE ECONOMIC MODELLING. International Journal of Applied Mathematics, 38(2s), 1450-1462.
21. Sivaraju, P. S. (2024). Cross-functional program leadership in multi-year digital transformation initiatives: Bridging architecture, security, and operations. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11374-11380.
22. Chejarla, L. N. (2025). AI Advancements in the TMT Industry: Navigating the Challenges and Business Adaptations. Journal of Computer Science and Technology Studies, 7(6), 999-1007.
23. Devi, C., Inampudi, R. K., & Vijayaboopathy, V. (2025). Federated Data-Mesh Quality Scoring with Great Expectations and Apache Atlas Lineage. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 4(2), 92-101.
24. Perumalsamy, J., & Pichaimani, T. (2024). InsurTechPredict: AI-driven Predictive Analytics for Claims Fraud Detection in Insurance. American Journal of Data Science and Artificial Intelligence Innovations, 4, 127-163.
25. Muthusamy, P., Thangavelu, K., & Bairi, A. R. (2023). AI-Powered Fraud Detection in Financial Services: A Scalable Cloud-Based Approach. Newark Journal of Human-Centric AI and Robotics Interaction, 3, 146-181..
26. Kusumba, S. (2022). Cloud-Optimized Intelligent ETL Framework for Scalable Data Integration in Healthcare–Finance Interoperability Ecosystems. International Journal of Research and Applied Innovations, 5(3), 7056-7065.
27. Sabin Begum, R., & Sugumar, R. (2019). Novel entropy-based approach for cost-effective privacy preservation of intermediate datasets in cloud. Cluster Computing, 22(Suppl 4), 9581-9588.
28. HV, M. S., & Kumar, S. S. (2024). Fusion Based Depression Detection through Artificial Intelligence using Electroencephalogram (EEG). Fusion: Practice & Applications, 14(2).
29. Bharatha, B. K. (2025). AI-Augmented Redistribution: Human-AI Collaboration to Prevent Waste and Feed Communities. Journal of Computer Science and Technology Studies, 7(10), 120-127.
30. Sakinala, K. (2025). Monitoring and observability for cloud-native applications. Journal of Computer Science and Technology Studies, 7(8), 101-115.
31. Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.
32. Adari, V. K. (2021). Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations (IJRAI), 4(2), 4913–4920. https://doi.org/10.15662/IJRAI.2021.0402004