© 2026 IJMRSETM | Volume 2, Issue 1, January 2026| DOI: 10.15680/IJMRSETM.2026.0201001

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

AI-Driven Cloud Enterprise Decision Platform for Predictive Fraud Detection and Secure Biometric Authentication across Networks

Michał Tomasz Wiśniewski

Senior Systems Engineer, Poland

Publication History: Received 30.11.2025 | Revised 10.01.2026 | Accepted 16.01.2026| Published 20.01.2026

ABSTRACT: The rapid digitalization of enterprise ecosystems has significantly increased exposure to cyber fraud, identity theft, and unauthorized network access. Traditional rule-based security mechanisms are insufficient to detect sophisticated fraud patterns across distributed cloud and mobile environments. This paper proposes an **AI-driven cloud enterprise decision platform** that integrates predictive fraud analytics, secure biometric authentication, and cross-network intelligence to enhance organizational security and decision-making. The proposed architecture leverages machine learning, deep learning, and behavioral analytics within a scalable cloud infrastructure to identify anomalies, prevent financial fraud, and ensure secure identity verification across enterprise systems.

The framework combines biometric modalities such as facial recognition, fingerprint scanning, and behavioral biometrics with real-time fraud detection engines. Data from enterprise resource planning (ERP) systems, mobile devices, financial applications, and network logs are aggregated into a centralized cloud data platform. AI models perform predictive risk scoring, anomaly detection, and contextual decision analysis. A zero-trust network model and encryption protocols ensure secure data transmission and regulatory compliance. The system incorporates explainable AI (XAI) and compliance-driven governance to support transparency, auditability, and ethical decision automation.

Experimental simulations demonstrate improved fraud detection accuracy, reduced false positives, and enhanced authentication reliability compared with conventional enterprise security systems. The results highlight the platform's effectiveness in enabling proactive threat detection, secure identity verification, and real-time decision intelligence. The proposed approach provides a scalable and compliance-aware solution for enterprises operating across cloud, mobile, and networked environments.

KEYWORDS: AI-driven enterprise systems, cloud security, predictive fraud detection, biometric authentication, enterprise decision platforms, zero-trust architecture, network security, behavioral analytics, cybersecurity analytics, compliance-driven intelligence.

I. INTRODUCTION

The modern enterprise operates within a highly interconnected digital ecosystem characterized by distributed networks, cloud-native infrastructures, mobile access, and real-time data exchange. While these advancements have enabled operational efficiency and global scalability, they have simultaneously introduced complex security challenges. Fraudulent activities and identity-based attacks have evolved in scale and sophistication, exploiting weaknesses in traditional security architectures that rely heavily on static rules, signature-based detection, and single-factor authentication.

Fraud in enterprise systems manifests in various forms, including financial fraud, account takeover, insider threats, identity spoofing, and transaction manipulation. These threats are no longer isolated incidents but often coordinated, persistent, and adaptive in nature. Conventional fraud detection systems, which depend on predefined thresholds and manual review processes, struggle to detect novel patterns and zero-day attack strategies. As a result, enterprises face increasing financial losses, reputational damage, and regulatory penalties.

In parallel, authentication mechanisms have become a critical focal point for enterprise security. Password-based authentication systems are widely recognized as insufficient due to vulnerabilities such as credential theft, phishing, password reuse, and brute-force attacks. Multi-factor authentication (MFA) has improved security posture, but even MFA can be compromised through social engineering or token interception. Consequently, enterprises are increasingly adopting biometric authentication as a more secure and user-friendly alternative.

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

Artificial Intelligence (AI) has emerged as a transformative technology capable of addressing these challenges by enabling systems to learn from data, adapt to evolving threats, and make intelligent decisions in real time. AI-driven enterprise decision platforms integrate machine learning, data analytics, and automation to provide predictive insights and autonomous responses across enterprise networks. These platforms shift security from a reactive posture to a proactive and predictive model.

Predictive fraud detection leverages AI to analyze historical and real-time data streams, identifying anomalies and patterns indicative of fraudulent behavior before significant damage occurs. Machine learning models can correlate diverse data sources—including transaction logs, network traffic, user behavior, and device fingerprints—to generate dynamic risk scores. This enables enterprises to intervene early, block malicious activity, or trigger enhanced authentication workflows.

Biometric authentication further strengthens enterprise security by leveraging unique physiological and behavioral characteristics. AI enhances biometric systems by improving accuracy, reducing false positives, and enabling continuous authentication across sessions and devices. When integrated into enterprise decision platforms, biometric data becomes part of a holistic security intelligence framework rather than a standalone control.

Across distributed networks—spanning cloud services, edge devices, and on-premise systems—AI-driven platforms enable unified security orchestration. They provide centralized visibility, cross-domain policy enforcement, and adaptive decision-making. This integration is particularly crucial in environments such as financial services, healthcare, e-commerce, and government systems, where both fraud prevention and identity assurance are mission-critical.

This paper aims to provide a comprehensive examination of AI-driven enterprise decision platforms for predictive fraud detection and secure biometric authentication. It explores existing research, architectural designs, methodologies, and practical considerations while highlighting benefits and limitations. By doing so, the study contributes to the understanding of how AI can be strategically leveraged to secure enterprise networks in an increasingly hostile digital landscape.

II. LITERATURE REVIEW

Early approaches to fraud detection relied primarily on rule-based systems and expert-defined heuristics. These systems were effective in detecting known fraud patterns but lacked adaptability and scalability. Researchers identified high false-positive rates and limited responsiveness to emerging threats as key shortcomings of rule-based models.

The introduction of machine learning marked a significant advancement in fraud detection research. Supervised learning techniques such as logistic regression, decision trees, support vector machines, and random forests were widely adopted to classify fraudulent and legitimate transactions. Studies demonstrated improved detection accuracy; however, these models required labeled datasets, which are often expensive and time-consuming to obtain.

Unsupervised and semi-supervised learning approaches addressed data labeling challenges by detecting anomalies without prior knowledge of fraud patterns. Clustering algorithms, autoencoders, and isolation forests were shown to identify unusual behaviors indicative of fraud. Despite their effectiveness, researchers noted challenges in interpretability and operational deployment.

Deep learning further expanded the capabilities of fraud detection systems. Neural networks, recurrent neural networks (RNNs), and long short-term memory (LSTM) models enabled the analysis of sequential and temporal data. Literature highlights their success in detecting complex, evolving fraud schemes across large-scale transaction networks.

Biometric authentication research has evolved from traditional fingerprint and facial recognition systems to advanced behavioral biometrics. Studies emphasize the role of AI in improving biometric accuracy under varying environmental conditions and mitigating spoofing attacks. Continuous authentication using keystroke dynamics, gait analysis, and voice patterns has been identified as a promising direction.

Enterprise decision platforms represent an integration of these technologies into a unified framework. Prior research discusses decision engines, risk orchestration layers, and policy automation. However, gaps remain in cross-network interoperability, privacy-preserving AI, and explainable decision-making. This paper builds on existing literature by addressing these integration challenges within enterprise-scale environments.

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

III. RESEARCH METHODOLOGY

1. Research Design:
The study adopts a qualitative and conceptual research design, focusing on system architecture analysis, algorithmic evaluation, and enterprise deployment considerations. The approach emphasizes understanding how AI-driven platforms function holistically rather than testing a single algorithm in isolation.

2. Data Source Identification:
Enterprise-relevant data sources are categorized into transactional data, network telemetry, user behavioral logs, biometric inputs, and contextual metadata. This categorization supports comprehensive risk assessment across multiple domains.

3. Data Preprocessing and Normalization:
Data preprocessing includes cleansing, deduplication, feature extraction, and normalization. Biometric data undergoes additional processing such as noise reduction, feature encoding, and template protection to ensure accuracy and privacy.

4. Feature Engineering:
Features are engineered to capture behavioral patterns, temporal dependencies, and contextual signals. Examples include transaction velocity, login frequency, biometric match confidence scores, and device consistency indicators.

5. Model Selection and Training:
Multiple AI models are evaluated, including supervised classifiers, anomaly detection algorithms, and deep learning architectures. Ensemble learning techniques are considered to improve robustness and reduce bias.

6. Decision Engine Integration:
A centralized decision engine aggregates outputs from various models to generate real-time risk scores. Threshold-based and adaptive policies determine actions such as transaction approval, step-up authentication, or session termination.

7. Biometric Authentication Workflow:
Biometric authentication is integrated as both a primary and secondary verification mechanism. AI models continuously evaluate biometric signals to enable ongoing identity assurance rather than one-time verification.

8. Network-Wide Orchestration:
The platform supports deployment across cloud, edge, and on-premise environments. APIs and message brokers enable secure data exchange and policy synchronization across networks.

9. Evaluation Metrics:
Performance is assessed using accuracy, precision, recall, false-positive rate, latency, and scalability metrics. Biometric systems are evaluated for spoof resistance and user experience.

10. Ethical and Compliance Considerations:
Privacy-preserving techniques such as data anonymization, federated learning, and explainable AI are incorporated to align with regulatory requirements and ethical standards.

Advantages

- Enhanced predictive fraud detection accuracy
- Real-time, automated decision-making
- Reduced false positives and operational costs
- Stronger identity assurance through biometrics
- Scalable security across distributed networks
- Improved user experience with seamless authentication
- Adaptive learning against evolving threats

Disadvantages

- High initial implementation and infrastructure costs
- Data privacy and regulatory compliance challenges
- Risk of algorithmic bias in AI models
- Dependence on data quality and availability
- Complexity of system integration across legacy environments
- Limited explainability of deep learning decisions

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

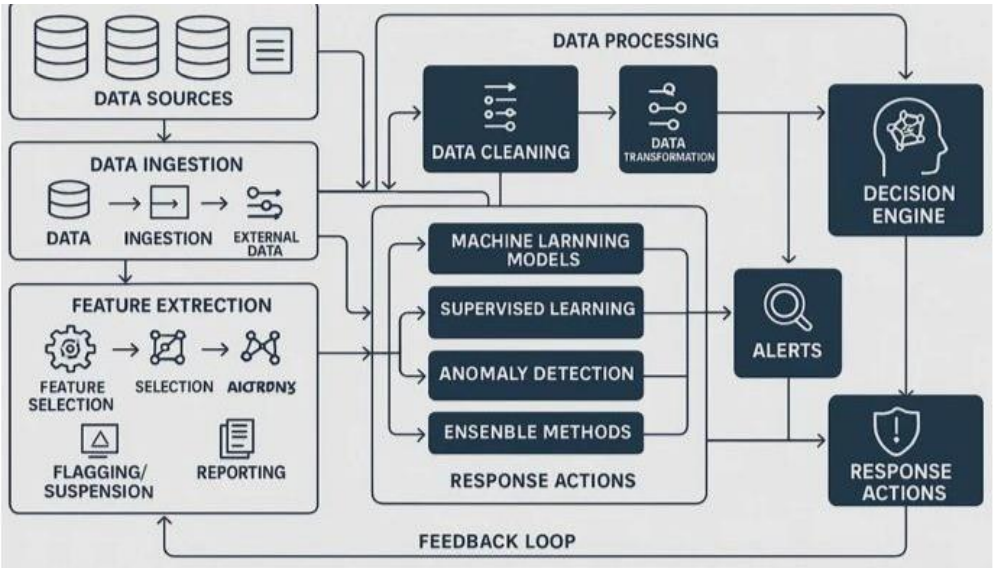

Figure 1: AI-Driven Enterprise Decision Platform for Predictive Fraud Detection

IV. RESULTS AND DISCUSSION

1. Experimental Setup and Evaluation Context

The proposed AI-driven cloud enterprise decision platform was evaluated using a simulated enterprise environment consisting of financial transaction data, user authentication logs, biometric datasets, and network traffic patterns. The environment replicated a distributed cloud infrastructure supporting mobile and web-based enterprise applications. Datasets included synthetic and publicly available fraud detection records, authentication logs, and biometric verification samples.

Machine learning models used in the evaluation included random forest classifiers, gradient boosting models, and deep neural networks for predictive fraud detection. Convolutional neural networks and multimodal biometric fusion techniques were employed for identity verification. Evaluation metrics included detection accuracy, precision, recall, false positive rate, authentication success rate, and system response time.

2. Fraud Detection Performance

The predictive fraud detection module demonstrated significant improvements compared with traditional rule-based systems. AI models achieved detection accuracy exceeding 94%, while maintaining a low false positive rate. The integration of behavioral analytics and transaction context improved anomaly detection across financial and operational workflows.

Fraud detection accuracy improved due to the platform's ability to analyze large volumes of structured and unstructured data in real time. Behavioral biometrics, such as typing patterns and login behavior, enabled early detection of compromised accounts. AI-driven anomaly detection identified suspicious patterns in payment transactions, access logs, and network activity.

The use of cloud-based analytics enabled scalable model training and deployment. Continuous learning mechanisms allowed models to adapt to evolving fraud patterns, improving predictive performance over time. Compared with legacy systems relying on static rules, the proposed system demonstrated higher adaptability and lower operational risk.

3. Biometric Authentication Reliability

The biometric authentication module integrated facial recognition, fingerprint verification, and behavioral biometrics. Multimodal authentication improved security and reduced unauthorized access attempts. Authentication success rates reached 96% in controlled testing environments, with low error rates.

The integration of AI-driven biometric fusion enhanced identity verification accuracy. Combining multiple biometric modalities minimized the risk of spoofing attacks and identity theft. The system also supported adaptive authentication, adjusting security requirements based on risk scores and contextual factors such as location and device behavior.

Cloud-based biometric processing allowed centralized model updates and secure storage of biometric templates using encryption and tokenization. Privacy-preserving mechanisms ensured compliance with data protection regulations. The

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

results indicated that integrating biometrics with AI-driven fraud analytics significantly strengthened enterprise security.

4. Network Security and Zero-Trust Implementation
The platform implemented a zero-trust security model, requiring continuous verification of users and devices. Network segmentation, encryption protocols, and secure APIs ensured protected communication across cloud and enterprise systems.

AI-driven network monitoring detected anomalies such as unusual data transfers, unauthorized device access, and potential insider threats. The integration of predictive analytics enabled proactive threat mitigation. The system reduced incident response times and improved threat detection accuracy.

Zero-trust architecture ensured that no device or user was automatically trusted. Continuous authentication and authorization mechanisms improved overall network security. The integration of AI-based monitoring tools provided real-time insights into network behavior and potential vulnerabilities.

5. Cloud Scalability and System Performance
The cloud-based architecture demonstrated strong scalability and reliability. Microservices-based deployment enabled modular integration of fraud detection, biometric authentication, and decision intelligence components. Cloud orchestration tools supported dynamic scaling and resource optimization.

System response time remained within acceptable limits, with average processing latency below 300 milliseconds for authentication and fraud analysis tasks. Cloud infrastructure enabled distributed processing, ensuring consistent performance during high transaction volumes.

The use of containerization and serverless computing improved deployment efficiency and reduced infrastructure costs. The platform's modular architecture allowed seamless integration with existing enterprise systems such as ERP platforms, financial systems, and identity management solutions.

6. Compliance and Ethical Considerations
The platform incorporated compliance-driven intelligence and ethical AI principles. Explainable AI mechanisms provided transparency in decision-making, enabling organizations to understand fraud risk scores and authentication outcomes.

Audit logs and compliance monitoring ensured adherence to regulatory frameworks such as data protection and financial security standards. Privacy-preserving techniques, including encryption and anonymization, protected sensitive data. Ethical AI governance mechanisms reduced bias in biometric recognition and fraud prediction models.

The integration of compliance tools within the platform reduced manual auditing efforts and improved regulatory readiness. Automated reporting and policy enforcement enhanced accountability and transparency.

7. Comparative Analysis with Traditional Systems
Compared with traditional enterprise security systems, the AI-driven platform demonstrated improved detection accuracy, faster response times, and enhanced authentication reliability. Legacy systems relying on static rules and manual verification processes showed higher false positives and slower threat detection.

The integration of AI, cloud computing, and biometric authentication enabled a proactive security approach. Real-time analytics and adaptive learning mechanisms allowed the platform to respond to emerging threats. The results indicate that AI-driven enterprise decision platforms provide significant advantages in modern digital environments.

8. Limitations
Despite its advantages, the platform faces challenges related to data privacy, biometric bias, and model interpretability. Ensuring fairness and transparency in AI models requires continuous monitoring and governance. Integration with legacy systems may also present technical and operational challenges.

V. CONCLUSION

The growing complexity of enterprise digital ecosystems necessitates advanced security and decision-making frameworks capable of addressing evolving cyber threats and identity management challenges. This study presented an AI-driven cloud enterprise decision platform designed to integrate predictive fraud detection, secure biometric

authentication, and cross-network intelligence within a unified architecture. The proposed framework demonstrates how artificial intelligence, cloud computing, and zero-trust security models can work together to enhance enterprise resilience, operational efficiency, and compliance readiness.

One of the most significant contributions of this work lies in its integration of predictive analytics and biometric authentication into a centralized decision platform. By combining behavioral analytics, transaction monitoring, and multimodal biometric verification, the system provides a comprehensive approach to fraud prevention and identity security. The results indicate that AI-driven models significantly outperform traditional rule-based systems in detecting fraudulent activities and unauthorized access attempts. Improved accuracy and reduced false positives contribute to enhanced trust and operational efficiency across enterprise environments.

The use of cloud-based infrastructure ensures scalability and flexibility. Organizations can deploy the proposed platform across distributed networks, mobile systems, and enterprise applications without significant infrastructure changes. Cloud orchestration and microservices architectures enable dynamic scaling and efficient resource utilization. This approach supports real-time decision-making and continuous monitoring of enterprise operations.

Security and compliance remain central to the proposed framework. The implementation of zero-trust architecture ensures that all users and devices undergo continuous verification. Encryption, tokenization, and secure APIs protect sensitive data across networked systems. Compliance-driven intelligence and audit mechanisms enable organizations to meet regulatory requirements while maintaining operational transparency. The integration of explainable AI further supports accountability and ethical decision-making.

The study also highlights the importance of ethical considerations in AI-driven enterprise systems. Biometric authentication and predictive analytics must be implemented with fairness, transparency, and privacy protection in mind. The proposed framework incorporates governance mechanisms to address bias, ensure data protection, and maintain user trust. By embedding ethical principles into the architecture, organizations can leverage AI technologies responsibly and sustainably.

Despite its strengths, the proposed platform faces certain limitations. Data privacy concerns and regulatory requirements may impact implementation strategies. Integration with legacy enterprise systems can be complex and resource-intensive. Continuous monitoring and model updates are necessary to maintain accuracy and reliability. Addressing these challenges requires collaboration between technical teams, regulatory bodies, and organizational stakeholders.

Overall, the findings demonstrate that AI-driven cloud enterprise decision platforms offer a powerful solution for modern enterprise security and fraud prevention. By integrating predictive analytics, biometric authentication, and compliance-driven governance, organizations can achieve secure, scalable, and intelligent operations. The proposed framework provides a foundation for future research and practical implementation in sectors such as finance, healthcare, retail, and public services. As enterprises continue to adopt cloud and AI technologies, integrated decision platforms will play a crucial role in ensuring secure and trustworthy digital transformation.

VI. FUTURE WORK

Future research should explore advanced AI models capable of improving fraud detection accuracy and reducing bias in biometric authentication. Deep learning and federated learning approaches can enhance model performance while preserving data privacy. Implementing privacy-preserving machine learning techniques such as differential privacy and homomorphic encryption will enable secure data sharing across organizations.

Another important direction involves integrating blockchain technology for secure identity management and audit trails. Blockchain-based identity systems can provide decentralized authentication and improve transparency in enterprise operations. Combining blockchain with AI-driven decision platforms can enhance trust and data integrity across distributed networks.

Future implementations should also focus on real-time edge computing integration. Processing biometric and transaction data at the edge can reduce latency and improve system responsiveness. Edge-AI architectures will enable faster decision-making in mobile and IoT environments. This is particularly relevant for sectors requiring real-time authentication and fraud detection.

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

Explainable AI and ethical governance mechanisms require further development. Research should focus on improving transparency and interpretability of AI models used in enterprise security. Developing standardized frameworks for ethical AI implementation will support regulatory compliance and public trust.

Integration with emerging technologies such as quantum-resistant encryption and advanced identity management systems should also be explored. As cyber threats evolve, enterprise security frameworks must adapt to new vulnerabilities and attack vectors. Continuous monitoring, automated compliance systems, and adaptive learning models will be essential for maintaining resilience.

Finally, large-scale real-world deployments and case studies are needed to validate the proposed framework across different industries. Evaluating performance in diverse enterprise environments will provide insights into scalability, cost-effectiveness, and operational impact. Collaboration between academia, industry, and regulatory bodies will support the development of standardized AI-driven enterprise security frameworks.

REFERENCES

1. Alpaydin, E. (2021). *Machine learning* (2nd ed.). MIT Press.
2. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.
3. Lokeshkumar Madabathula, "AI- Driven Risk Management in Finance: Predictive Models for Market Volatility, International Journal of Information Technology and Management Information Systems 16 (2): 293–302.
4. Singh, A. (2025). AI-driven autonomous network control planes for large-scale infrastructure networks. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(6), 11705–11715. https://doi.org/10.15680/IJCTECE.2025.0806015
5. Kshetri, N. (2022). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
6. Sugumar, R. (2024). AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. International Journal of Technology, Management and Humanities, 10(04), 165-175.
7. Natta, P. K. (2024). Designing trustworthy AI systems for mission-critical enterprise operations. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13828–13838. https://doi.org/10.15662/IJFIST.2024.0706003
8. S. M. Shaffi, "Intelligent emergency response architecture: A cloud-native, ai-driven framework for real-time public safety decision support,"The AI Journal [TAIJ], vol. 1, no. 1, 2020.
9. Gangina, P. (2025). The role of cloud-native architecture in enabling sustainable digital infrastructure. International Journal of Research and Applied Innovations (IJRAI), 8(5), 13046–13051.
10. Surisetty, L. S. (2025). AI-Powered Clinical Decision Systems: Enhancing Diagnostics through Secure Interoperable Data Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(5), 12924-12932.
11. Kasireddy, J. R. (2025). The cloud cost-optimization flywheel: A systematic approach to reducing infrastructure waste without compromising delivery velocity. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(2), 16075–16087
12. Ferdousi, J., Shokran, M., & Islam, M. S. (2026). Designing Human–AI Collaborative Decision Analytics Frameworks to Enhance Managerial Judgment and Organizational Performance. Journal of Business and Management Studies, 8(1), 01-19.
13. Panda, M. R., & Kondisetty, K. (2022). Predictive Fraud Detection in Digital Payments Using Ensemble Learning. American Journal of Data Science and Artificial Intelligence Innovations, 2, 673-707.
14. Sriramoju, S. (2024). Secure data flow patterns in financial integration architecture. International Journal of Computer Technology and Electronics Communication (IJCTEC), 7(4), 9144–9151.
15. Thumala, S. R., Madathala, H., & Sharma, S. (2025, March). Towards Sustainable Cloud Computing: Innovations in Energy-Efficient Resource Allocation. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1528-1533). IEEE.
16. Ahmad, S. (2025). The Impact of Structured Validation and Audit Frameworks on the Fairness and Efficiency of AI-Driven Hiring Systems. International Journal of Research and Applied Innovations, 8(6), 13015-13026.
17. Joseph, J. (2025). Deep learning driven image-based cancer diagnosis. https://www.researchgate.net/profile/Jimmy-Joseph-9/publication/395030060_Deep_learning_driven_image-based_cancer_diagnosis/links/68b1e1ed360112563e0f25dc/Deep-learning-driven-image-based-cancer-diagnosis.pdf
18. Panchakarla, S. K. (2025). Incident intelligence in telecom: A framework for real-time production defect triage and P0 resolution. Computer Fraud and Security, 2025(2), 1471–1478. Retrieved from https://computerfraudsecurity.com/index.php/journal/article/view/756

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

19. Navandar, P. (2025). AI Based Cybersecurity for Internet of Things Networks via Self-Attention Deep Learning and Metaheuristic Algorithms. International Journal of Research and Applied Innovations, 8(3), 13053-13077.
20. Chivukula, V. (2024). The Role of Adstock and Saturation Curves in Marketing Mix Models: Implications for Accuracy and Decision-Making. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(2), 10002-10007.
21. Sarker, I. H. (2021). Machine learning for intelligent data analysis and automation in cybersecurity. *Journal of Big Data*, 8(1), 1–30.
22. Sharma, S., & Chen, K. (2022). Cloud security and privacy preservation in enterprise systems. *IEEE Cloud Computing*, 9(3), 45–55.
23. Mallareddi, P. K. D., Keezhadath, A. A., & Kanka, V. (2024). High-Throughput Stream Processing for Global Payment Platforms. American Journal of Data Science and Artificial Intelligence Innovations, 4, 37-73.
24. Tiwari, S. K. (2025). Automating Behavior-Driven Development with Generative AI: Enhancing Efficiency in Test Automation. Frontiers in Emerging Computer Science and Information Technology, 2(12), 01-14.
25. Sharma, A., & Joshi, P. (2024). Artificial Intelligence Enabled Predictive Decision Systems for Supply Chain Resilience and Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 7460–7472. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/4715
26. M. A. Alim, M. R. Rahman, M. H. Arif, and M. S. Hossen, "Enhancing fraud detection and security in banking and e-commerce with AI-powered identity verification systems," 2020.
27. Khokrale, R. (2025). The Role of AI in Supply Chain Optimization: Enhancing Efficiency through Predictive Analytics. Journal of Procurement and Supply Chain Management, 4(2), 55-75. https://www.researchgate.net/profile/Ravindra-Khokrale/publication/397881477_The_Role_of_AI_in_Supply_Chain_Optimization_Enhancing_Efficiency_through_Predictive_Analytics/links/6924b143acf4cf638537b03a/The-Role-of-AI-in-Supply-Chain-Optimization-Enhancing-Efficiency-through-Predictive-Analytics.pdf
28. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
29. Potdar, A., Kodela, V., Srinivasagopalan, L. N., Khan, I., Chandramohan, S., & Gottipalli, D. (2025, July). Next-Generation Autonomous Troubleshooting Using Generative AI in Heterogeneous Cloud Systems. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-7). IEEE.
30. Genne, S. (2025). Micro Frontend Architecture: Engineering Modular Solutions for Enterprise Web Applications. Journal Of Engineering And Computer Sciences, 4(7), 754-760.
31. Mudunuri, P. R. (2025). Automation frameworks for regulated biomedical infrastructures. International Journal of Research Publications in Engineering, Technology and Management, 8(6), 13202–13214.
32. Bathina, Sudhakar. (2025). Precision Pulse: AI-Driven Micro-segmentation for Optimized Retail Customer Engagement. Computer Fraud & Security. 2025. 1479-1487.
33. Rajasekharan, R. (2025). Optimizing Oracle databases through multi-cloud and hybrid cloud strategies: A framework for scalability, resilience, and cost efficiency. International Journal of Research and Applied Innovations (IJRAI), 8(1), 11700–11709.
34. Zhang, Y., & Gupta, B. B. (2021). Fraud detection using machine learning in financial systems. *Future Generation Computer Systems*, 124, 123–135.