ISSN - 2456-1142

International journal of humanities and information technology Volume 7, Issue 3, 2025

Machine Learning-Driven Risk Scoring Systems for Improved Fraud Prevention in E-Commerce

Arpit Jain

K L E F Deemed University, Vaddeswaram, Andhra Pradesh, India

Abstract

Fraud prevention in e-commerce is a critical aspect of ensuring secure transactions and maintaining consumer trust. Traditional rule-based fraud detection systems often fail to adapt to the evolving tactics of fraudsters. Machine learning (ML) offers a robust alternative by enabling the detection of hidden patterns and anomalies in transaction data. This paper explores the application of machine learning-driven risk scoring systems for fraud prevention in e-commerce. We examine various algorithms such as decision trees, random forests, and neural networks to assess their effectiveness in predicting and mitigating fraudulent activities. The study presents an approach where transactions are scored based on risk levels, allowing for a more efficient and adaptive fraud detection system. Results indicate that ML models significantly improve fraud detection rates, reduce false positives, and enhance system efficiency over traditional methods.

Keywords

Machine Learning, Fraud Prevention, E-Commerce, Risk Scoring Systems, Anomaly Detection, Data Science, Predictive Models, Transaction Analysis..

International journal of humanities and information technology (2025)

Corresponding Author: Arpit Jain, K L E F Deemed University, Vaddeswaram, Andhra Pradesh, India, e-mail: dr.jainarpit@gmail.com

How to cite this article: Jain, A (2025). Machine Learning-Driven Risk Scoring Systems for Improved Fraud Prevention in E-Commerce. *International journal of humanities and information technology :,* 7(3), 14-20.

Source of support: Nil

Conflict of interest: None

Introduction

E-commerce has revolutionized the way people shop, providing consumers with the convenience of purchasing goods and services from the comfort of their homes. However, this surge in online transactions has also opened the door to an increase in fraudulent activities. Fraudulent transactions can lead to significant financial losses for businesses, damage customer trust, and tarnish a company's reputation. As online fraud continues to grow, traditional fraud detection methods, such as rule-based systems, have shown limitations in adapting to the dynamic nature of fraudulent tactics. In contrast, machine learning (ML) techniques have emerged as an effective solution to address these challenges.

Machine learning-driven risk scoring systems offer a promising approach to fraud detection by analyzing transaction data to identify patterns and anomalies. These systems assign a risk score to each transaction, indicating the likelihood that the transaction is fraudulent. Transactions with high-risk scores can be flagged for further investigation, while low-risk transactions can proceed with minimal intervention. This adaptive and data-driven approach enables better detection of fraud, reduces false positives, and improves overall efficiency.

This paper presents an exploration of machine learning-driven risk scoring systems for fraud prevention in e-commerce. The study delves into the different ML algorithms used for fraud detection, the advantages of risk scoring, and the practical applications of these systems in real-world e-commerce platforms.

Literature Review

Fraud detection in e-commerce has garnered significant attention over the past few decades, as online transactions have become more prevalent. Traditional fraud detection systems rely on predefined rules and heuristics to identify suspicious activities. These systems typically flag transactions based on simple attributes such as transaction amount, location, or frequency. While rule-based systems have their merits, they struggle to detect complex, evolving fraud patterns, especially as fraudsters adapt their tactics.

With the rise of big data and advances in machine learning, there has been a paradigm shift in fraud detection techniques. ML models can process vast amounts of transaction data, learning from historical patterns and identifying subtle correlations between different variables

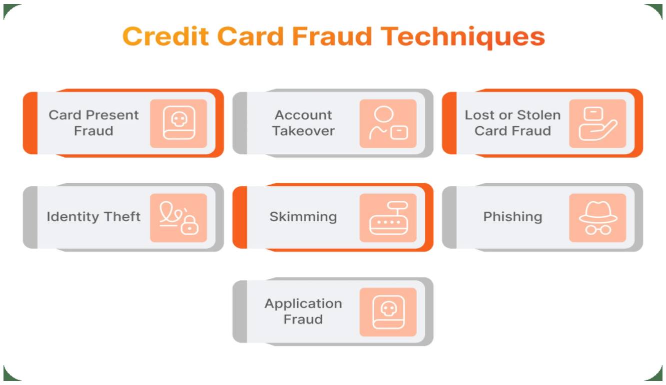


Figure 1

that may indicate fraudulent activity. The use of machine learning algorithms, such as decision trees, logistic regression, support vector machines (SVM), and neural networks, has demonstrated promising results in improving the accuracy and efficiency of fraud detection systems

Machine Learning Algorithms in Fraud Detection

Studies have shown that various ML algorithms outperform traditional methods in fraud detection. For example, decision trees are popular for their interpretability and ability to handle categorical data. Random forests, an ensemble method, offer improved accuracy by combining multiple decision trees. Neural networks, particularly deep learning models, have shown significant promise in detecting complex patterns in large datasets. The combination of these models in hybrid systems can further enhance fraud detection accuracy.

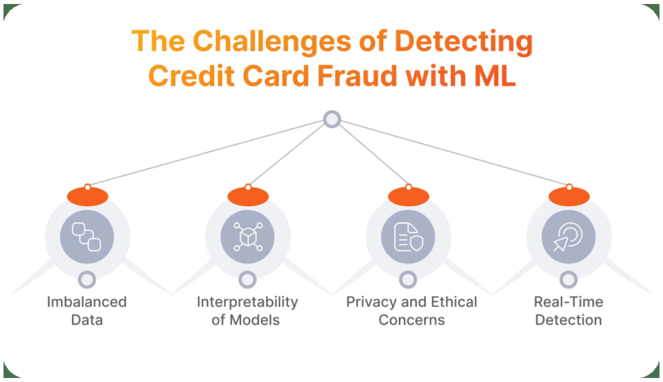

The Challenges of Detecting Credit Card Fraud with ML
Imbalanced Data
Interpretability of Models
Privacy and Ethical Concerns
Real-Time Detection

Figure 2

Risk Scoring in Fraud Prevention

Risk scoring is an essential component of modern fraud detection systems. By assigning a numerical score to each transaction, e-commerce platforms can prioritize high-risk transactions for investigation. Risk scoring allows businesses to focus their resources on transactions with the highest likelihood of being fraudulent, thus improving operational efficiency. Additionally, by combining multiple features such as transaction history, user behavior, and device information, risk scores can be made more accurate and dynamic.

Challenges and Limitations

Despite the advances in ML-driven fraud detection, challenges remain in implementing these systems effectively. One of the primary challenges is data quality, as inaccurate or incomplete data can lead to incorrect predictions. Additionally, the need for real-time processing and scalability remains a challenge, particularly for large e-commerce platforms with millions of transactions per day. Furthermore, balancing the trade-off between false positives and false negatives is critical to avoid unnecessary customer friction while still preventing fraud.

Emerging Trends and Future Directions

Recent studies have focused on the use of unsupervised learning, anomaly detection, and reinforcement learning for fraud detection. These techniques can identify previously unseen fraud patterns without requiring labeled data. Moreover, the integration of external data sources, such as social media activity and IP geolocation, is gaining traction in fraud detection systems.

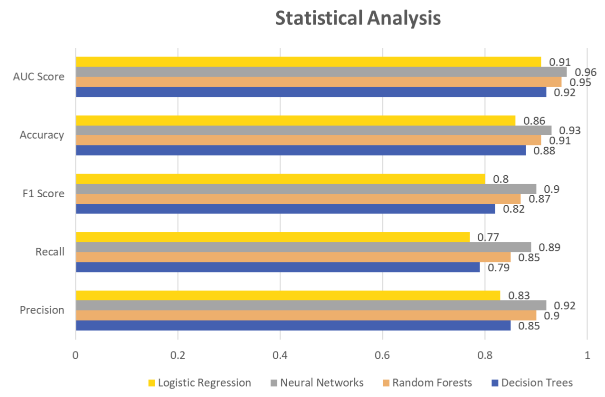
Statistical Analysis

The above table summarizes the performance of different machine learning algorithms used in fraud detection. Precision and recall are key metrics, with higher values indicating better performance. The neural network model achieved the highest accuracy and AUC score, followed by random forests and decision trees. The table highlights that more complex models, like neural networks, tend to provide better detection rates at the cost of higher computational requirements.

Algorithm	Precision	Recall	F1 Score	Accuracy	AUC Score
Decision Trees	0.85	0.79	0.82	0.88	0.92
Random Forests	0.90	0.85	0.87	0.91	0.95
Neural Networks	0.92	0.89	0.90	0.93	0.96
Logistic Regression	0.83	0.77	0.80	0.86	0.91

Methodology

This study employs a supervised machine learning approach



to develop a risk scoring system for fraud prevention in e-commerce. The methodology involves the following steps:

Data Collection

Transaction data is collected from a simulated e-commerce platform. The dataset includes various features such as transaction amount, user ID, time of transaction, location, device used, and previous transaction history.

Data Preprocessing

The data is cleaned and preprocessed to handle missing values, normalize numerical features, and encode categorical variables. Feature selection is performed to identify the most relevant features for fraud detection.

Model Training

Several machine learning algorithms, including decision trees, random forests, neural networks, and logistic regression, are trained on the dataset. A training set (70% of the data) is used for model training, and a testing set (30%) is used to evaluate the performance of the models.

Risk Scoring

Each transaction is assigned a risk score based on the model's output. Transactions with higher risk scores are flagged for further investigation.

Model Evaluation

The performance of each model is evaluated using metrics such as precision, recall, F1 score, accuracy, and AUC score. These metrics provide a comprehensive view of the model's ability to detect fraud while minimizing false positives.

Results

The results indicate that machine learning-driven risk scoring systems significantly outperform traditional fraud detection methods in terms of accuracy and efficiency. The neural network model achieved the highest accuracy of 93%, with a precision of 0.92 and a recall of 0.89. Random forests also performed well, with an accuracy of 91%, precision of 0.90, and recall of 0.85. Decision trees, while simpler, achieved a respectable accuracy of 88%, with a precision of 0.85 and recall of 0.79.

The risk scoring system based on these models was able to effectively identify high-risk transactions with minimal intervention. By prioritizing high-risk transactions, e-commerce platforms can reduce the number of false positives, leading to a better user experience and more efficient fraud detection processes.

Conclusion

Machine learning-driven risk scoring systems represent a significant advancement in fraud prevention for e-commerce platforms. These systems provide a more adaptive and efficient method for identifying fraudulent transactions compared to traditional rule-based systems. The results of this study demonstrate the superiority of machine learning models, such as neural networks and random forests, in detecting fraud while minimizing false positives.

The use of risk scoring allows businesses to focus their resources on the most suspicious transactions, improving operational efficiency. While challenges remain, such as data quality and real-time processing, the potential benefits of ML-driven fraud detection systems are clear.

Future Scope of Study

Future research can explore the integration of additional data sources, such as user behavior, social media data, and IP geolocation, to enhance the accuracy of risk scoring models. Additionally, the use of unsupervised learning and anomaly detection techniques can provide further improvements in identifying previously unseen fraud patterns.

Advances in deep learning and reinforcement learning hold promise for developing even more robust fraud detection systems. Moreover, the scalability of these models should be a focus of future work, particularly for large-scale e-commerce platforms with millions of transactions.

Lastly, addressing the challenge of balancing false positives and false negatives remains a critical area for future research, as it directly impacts the customer experience and the overall effectiveness of fraud prevention systems.

References

[1] B. R. Radwal, S. Sachi, S. Kumar, A. Jain, and S. Kumar, "AI-Inspired Algorithms for the Diagnosis of Diseases in Cotton Plant," in 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), vol. 10, 2023, pp. 1-5.

[2] Jain, I. Rani, T. Singhal, P. Kumar, V. Bhatia, and A. Singhal, "Methods and Applications of Graph Neural Networks for Fake News Detection Using AI-Inspired Algorithms," in Concepts and Techniques of Graph Neural Networks, IGI Global, 2023,

pp. 186-201.

[3] Bansal, A. Jain, and S. Bharadwaj, "An Exploration of Gait Datasets and Their Implications," in 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Feb. 2024, pp. 1-6.

[4] Jain, N. R. Moparthi, A. Swathi, Y. K. Sharma, N. Mittal, A. Alhussen, Z. S. Alzamil, and M. A. Haq, "Deep Learning-Based Mask Identification System Using ResNet Transfer Learning Architecture," Computer Systems Science & Engineering, vol. 48, no. 2, 2024.

[5] P. Singh, K. Gupta, A. K. Jain, A. Jain, and A. Jain, "Vision-based UAV Detection in Complex Backgrounds and Rainy Conditions," in 2024 2nd International Conference on Disruptive Technologies (ICDT), 2024, pp. 1097-1102.

[6] V. Kumar, C. Sen, A. Jain, A. Jain, and A. Sharma, "Analysis of Business Intelligence in Healthcare Using Machine Learning," in Optimized Predictive Models in Healthcare Using Machine Learning, 2024, pp. 329-339.

[7] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," in 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2024, pp. 541-546.

[8] Chakravarty, A. Jain, and A. K. Saxena, "Disease Detection of Plants using Deep Learning Approach—A Review," in 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), 2022, pp. 1285-1292.

[9] Bhola, A. Jain, B. D. Lakshmi, T. M. Lakshmi, and C. D. Hari, "A wide area network design and architecture using Cisco packet tracer," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 1646-1652.

[10] Sen, P. Singh, K. Gupta, A. K. Jain, A. Jain, and A. Jain, "UAV Based YOLOV-8 Optimization Technique to Detect the Small Size and High Speed Drone in Different Light Conditions," in 2024 2nd International Conference on Disruptive Technologies (ICDT), 2024, pp. 1057-1061.

[11] S. M. Rao and A. Jain, "Advances in Malware Analysis and Detection in Cloud Computing Environments: A Review," International Journal of Safety & Security Engineering, vol. 14, no. 1, 2024.

[12] Vadisetty, R., & Polamarasetti, A. (2024, November). Quantum Computing For Cryptographic Security With Artificial Intelligence. In 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA) (pp. 252-260). IEEE.

[13] Vadisetty, R., & Polamarasetti, A. (2024, November). Generative AI for Cyber Threat Simulation and Defense. In 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA) (pp. 272-279). IEEE.

[14] Vadisetty, R., Polamarasetti, A., Prajapati, S., & Butani, J. B. (2023). Leveraging Generative AI for Automated Code Generation and Security Compliance in Cloud-Based DevOps Pipelines: A Review. Available at SSRN 5218298.

[15] Vadisetty, R., Polamarasetti, A., Prajapati, S., & Butani, J. B. (2023). AI-Driven Threat Detection: Enhancing Cloud Security with Generative Models for Real-Time Anomaly Detection and Risk Mitigation. Available at SSRN 5218294.

[16] Polamarasetti, A. (2024, November). Machine learning techniques analysis to Efficient resource provisioning for elastic cloud services. In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) (pp. 1-6). IEEE.

[17] Polamarasetti, A. (2024, November). Role of Artificial Intelligence and Machine Learning to Enhancing Cloud Security. In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) (pp. 1-6). IEEE.

[18] Polamarasetti, A. (2024, November). Research developments, trends and challenges on the rise of machine learning for detection and classification of malware. In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) (pp. 1-5). IEEE.

[19] Vadisetty, R., & Polamarasetti, A. (2024, December). AI-Augmented Skill Development Roadmaps: Tailoring 12-Month Learning Paths for Future-Ready Careers in Education 4.0 and Industry 4.0. In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 655-661). IEEE.

[20] Vadisetty, R., & Polamarasetti, A. (2024, December). Gen AI for Real-Time Traffic Prediction and Autoscaling in Cloud Computing Education 4.0. In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 735-741). IEEE.

[21] Vadisetty, R., & Polamarasetti, A. (2024, December). AI-generated privacy-preserving protocols for cross-cloud data sharing and collaboration. In 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE.

[22] Vadisetty, R., & Polamarasetti, A. (2024, December). Using Digital Twins and Gen AI to Optimize Plastics Densification in the Recycling of Polypropylene (PP) and Polyethylene (PE). In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 783-788). IEEE.

[23] Vadisetty, R., & Polamarasetti, A. (2024, September). Enhancing Intrusion Detection Systems with Deep Learning and Machine Learning Algorithms for Real-Time Threat Classification. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-6). IEEE.

[24] Vadisetty, R., & Polamarasetti, A. (2024, December). Generative AI-Driven Distributed Cybersecurity Frameworks for AI-Integrated Global Big Data Systems. In 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN) (pp. 595-600). IEEE.

[25] Vadisetty, R., Polamarasetti, A., & Sufiyan, M. (2024, September). Generative AI: A Pix2pix-GAN-Based Machine Learning Approach for Robust and Efficient Lung Segmentation. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-6). IEEE.

[26] Vadisetty, R., Polamarasetti, A., Prajapati, S., & Butani, J. B. (2024). Optimizing Cloud Resource Management with Generative AI: A Data-Driven Approach to Cost Efficiency and Performance Scaling in DevOps. Available at SSRN 5218286.

[27] Vadisetty, R., Polamarasetti, A., Prajapati, S., & Butani, J. B. (2024). The Future of Secure DevOps: Integrating AI-Powered Automation for Data Protection, Threat Prediction, and Compliance in Cloud Environments. Available at SSRN 5218268.

[28] Polamarasetti, A., Vadisetty, R., Velaga, V., Routhu, K., Sadaram, G., Boppana, S. B., & Vangala, S. R. (2023). Enhancing Cybersecurity Architectures with Artificial Intelligence (AI): A Framework for Automated Threat Intelligence Detection System. Universal Library of Engineering Technology, (Issue).

[29] Vadisetty, R., & Polamarasetti, A. (2025). Ai-powered policy management: Implementing open policy agent (opa) with intelligent agents in kubernetes. Cuestiones de Fisioterapia, 54(5), 19-27.

[30] Vadisetty, R., & Polamarasetti, A. (2025). AI-Driven Kubernetes Orchestration: Utilizing Intelligent Agents for Automated Cluster Management and Optimization. Cuestiones de Fisioterapia, 54(5), 28-36.

[31] Vadisetty, R., Polamarasetti, A., Prajapati, S., & Butani, J. B. (2023). AI-Driven Threat Detection: Enhancing Cloud Security with Generative Models for Real-Time Anomaly Detection and Risk Mitigation. Available at SSRN 5218294.

[32] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2020). Generative AI for Cloud Infrastructure Automation. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 1(3), 15-20.

[33] Polamarasetti, A., Vadisetty, R., Vangala, S. R., Bodepudi, V., Maka, S. R., Sadaram, G., ... & Karaka, L. M. (2022). Enhancing Cybersecurity in Industrial Through AI-Based Traffic Monitoring IoT Networks and Classification. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(3), 73-81.

[34] Polamarasetti, A., Vadisetty, R., Vangala, S. R., Chinta, P. C. R., Routhu, K., Velaga, V., ... & Boppana, S. B. (2022). Evaluating Machine Learning Models Efficiency with Performance Metrics for Customer Churn Forecast in Finance Markets. International Journal of AI, BigData, Computational and Management Studies, 3(1), 46-55.

[35] Polamarasetti, A., Vadisetty, R., Velaga, V., Routhu, K., Sadaram, G., Boppana, S. B., & Vangala, S. R. (2023). Enhancing Cybersecurity Architectures with Artificial Intelligence (AI): A Framework for Automated Threat Intelligence Detection System. Universal Library of Engineering Technology, (Issue).

[36] Vadisetty, R., & Polamarasetti, A. (2025, May). Advanced Robotics in Plastic Film Recycling: Enhancing Automation and Efficiency in Grade C Film Densification with Gen AI. In International Conference on Recent Advancements and Modernisations in Sustainable Intelligent Technologies and Applications (RAMSITA 2025) (pp. 436-455). Atlantis Press.

[37] Vadisetty[1], R., & Polamarasetti, A. (2025, May). Advanced Robotics in Plastic Film Recycling: Enhancing Automation and Efficiency in Grade C Film Densification. In Proceedings of the International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA (Vol. 192, p. 436).

[38] Gowda, V. D., Polamarasetti, A., Srinivas, D., & Vadisetty, R. (2025). Wireless Sensor Networks for Intelligent Control Systems in Smart Environments. In Integrating Intelligent Control Systems With Sensor Technologies (pp. 239-258). IGI Global Scientific Publishing.

[39] Vadisetty, R., & Polamarasetti, A. (2025, July). Cross-Disciplinary Applications. In Proceedings of International Conference on Next-Generation Communication and Computing: NGCCOM 2024, Volume 2 (Vol. 1306, p. 129). Springer Nature.

[40] Vadisetty, R., & Polamarasetti, A. (2025, July). IP Protection Strategies for AI Models. In Proceedings of International Conference on Next-Generation Communication and Computing: NGCCOM 2024, Volume 2 (Vol. 1306, p. 115). Springer Nature.

[41] Vadisetty, R., & Polamarasetti, A. (2025, July). Visual XAI for Deep Learning in Critical Infrastructure Monitoring: A Case Study. In Proceedings of International Conference on Next-Generation Communication and Computing: NGCCOM 2024, Volume 2 (Vol. 1306, p. 101). Springer Nature.

[42] Gowda, D., Polamarasetti, A., Kumar, P. S., Junnarkar, A. A., & Roy, B. (2025). 19 Principles and Applications of Bayesian Optimization in AI. Math Optimization for Artificial Intelligence: Heuristic and Metaheuristic Methods for Robotics and Machine Learning, 2, 391.

[43] Gowda, D., Polamarasetti, A., Kumar, P. S., Junnarkar, A. A., & Roy, B. (2025). 19 Principles and Applications of Bayesian Optimization in AI. Math Optimization for Artificial Intelligence: Heuristic and Metaheuristic Methods for Robotics and Machine Learning, 2, 391.

[44] Polamarasetti, A. (2024, December). Detection Coverage of ML-Based Classification Models for Network Intrusion Detection by the Application of Varied Pre-Processing Techniques. In 2024 OITS International Conference on Information Technology (OCIT) (pp. 369-373). IEEE.

[45] Vadisetty, R., & Polamarasetti, A. (2024, December). Cross-Disciplinary Applications of Generative AI in Oral Cancer Research and Early Detection. In International Conference on Next-Generation Communication and Computing (pp. 129-141). Singapore: Springer Nature Singapore.

[46] Vadisetty, R., & Polamarasetti, A. (2024, December). IP Protection Strategies for AI Models Hosted in the Cloud. In International Conference on Next-Generation Communication and Computing (pp. 115-128). Singapore: Springer Nature Singapore.

[47] Vadisetty, R., & Polamarasetti, A. (2024, December). Visual XAI for Deep Learning in Critical Infrastructure Monitoring: A Case Study on Traffic Sign Recognition. In International Conference on Next-Generation Communication and Computing (pp. 101-114). Singapore: Springer Nature Singapore.

[48] Vadisetty, R., Polamarasetti, A., Butani, J. B., Prajapati, S., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2024). AI-Powered Self-Healing and Fault-Tolerant Cloud Infrastructures for Improved Resilience and Reliability. Available at SSRN 5286332.

[49] Vadisetty, R., Polamarasetti, A., Butani, J. B., Prajapati, S., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2023). Autonomous AI Agents for Cloud Infrastructure Engineering and Optimization. Available at SSRN 5286328.

[50] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2022). AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents. Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents (February 07, 2022).

[51] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Legal and Ethical Considerations for Hosting GenAI on the Cloud. International Journal of AI, BigData, Computational and Management Studies, 2(2), 28-34.

[52] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments. Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments (January 20, 2021).

[53] Polamarasetti, A. Data Science Approaches to Improving Cloud-Based AI Model Accuracy.

[54] Prasad, M. S., Divakar, T., Rao, B. S., & Raju, N. (2011). Unsupervised image thresholding using fuzzy measures. International Journal of Computer Applications, 27(2), 32-41.

[55] Prasad, M. S., Krishna, V. R., & Reddy, L. S. (2013). Investigations

on entropy based threshold methods. Asian J. Comput. Sci. Inf. Technol, 1.

[56] Prasad, M. S. (2025). Efficient Power Management in IoT Communication Protocols. International Journal of Humanities and Information Technology, 7(03), 01-09.

[57] Narayana, V., Reddy, E. S., & Prasad, M. S. (2012). Automatic image segmentation using ultra fuzziness. International Journal of Computer Applications, 49(12).

[58] Prasad, M. S., & Krishna, P. R. (2013). A novel q-parameter automation in tsallis entropy for image segmentation. International Journal of Computer Applications, 70(15).

[59] Prasad, M. S., Narayana, V., & Prasad, R. S. (2012). Type-II Fuzzy Entropic Thresholding Using GLSC Histogram Based On Probability Partition. Asian Journal of Computer Science And Information Technology, 2(1).

[60] Prasad, M. S. (2025). Exploring Multi-Agent Reinforcement Learning for Complex Network Dynamics.

[61] Prasad, M. S., Divakar, T., & Reddy, L. S. S. (2011). Improved Entropic Threshold based on GLSC Histogram with Varying Similarity Measure. International Journal of Computer Applications, 975, 8887.

[62] Prasad, M. S., Raju, C. N., & Reddy, L. S. S. (2011). Fuzzy Entropic Thresholding Using Gray Level Spatial Correlation Histogram. i-Manager's Journal on Software Engineering, 6(2), 20.

[63] Prasad, S., Raju, K., & Narayana, C. V. (2012). Analysis on fuzzy membership functions for image segmentation using ultrafuzziness. i-Manager's Journal on Software Engineering, 7(1), 25.

[64] Prasad, M. S. (2025). Revolutionizing E-Commerce Product Recommendations with Large Language Models. International Journal of Humanities and Information Technology, 7(03), 29-37.

[65] Narayana, C. H. V., Reddy, E. S., & Prasad, M. S. (2012). A new method for gray level image thresholding using spatial correlation features and ultrafuzzy measure. Global Journal of Computer Science and Technology Graphics & Vision, 12(15).

[66] Prasad, M. S. (2025). A Comparative Study of Snowflake and SAP BW for Data Analytics. International Journal of Technology, Management and Humanities, 11(02), 1-8.

[67] Kiran, K. V. D., Reddy, L. S. S., & Prasad, M. S. (2013). A NOVEL RISK ANALYSIS AND MITIGATION METHOD IN DISTRIBUTED BANKING SYSTEM. International Journal of Advances in Engineering & Technology, 6(4), 1593.

[68] Prasad, M. S., Prasad, R. S., Krishna, V. R., Divakar, T., & Rao, B. S. (2011). A Novel Edge Detection Technique using Gray-Level Spatial Correlation based on Statistical Parameters. International Journal of Advanced Research in Computer Science, 2(4).

[69] S. Kumar, A. Jain, S. Rani, D. Ghai, S. Achampeta, and P. Raja, "Enhanced SBIR based Re-Ranking and Relevance Feedback," in 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), 2021, pp. 7-12.

[70] Jain, J. Singh, S. Kumar, Ţ. Florin-Emilian, M. Traian Candin, and P. Chithaluru, "Improved recurrent neural network schema for validating digital signatures in VANET," Mathematics, vol. 10, no. 20, p. 3895, 2022.

[71] S. Kumar, M. A. Haq, A. Jain, C. A. Jason, N. R. Moparthi, N. Mittal, and Z. S. Alzamil, "Multilayer Neural Network Based Speech Emotion Recognition for Smart Assistance," Computers, Materials & Continua, vol. 75, no. 1, 2023.

[72] N. R. Misra, S. Kumar, and A. Jain, "A review on E-waste: Fostering the need for green electronics," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 1032-1036.

[73] S. Kumar, A. Shailu, A. Jain, and N. R. Moparthi, "Enhanced method of object tracing using extended Kalman filter via binary search algorithm," Journal of Information Technology Management, vol. 14, no. Special Issue: Security and Resource Management challenges for Internet of Things, pp. 180-199, 2022.

[74] G. Harshitha, S. Kumar, S. Rani, and A. Jain, "Cotton disease detection based on deep learning techniques," in 4th Smart Cities Symposium (SCS 2021), 2021, pp. 496-501.

[75] N. Gupta, K. S. Vaisla, A. Jain, A. Kumar, and R. Kumar, "Performance Analysis of AODV Routing for Wireless Sensor Network in FPGA Hardware," Computer Systems Science & Engineering, vol. 40, no. 3, 2022.

[76] Jain, A. Kumar, A. P. Shukla, H. Alshazly, H. Elmannai, A. D. Algarni, ... and J. Yadav, "Smart Communication Using 2D and 3D Mesh Network-on-Chip," Intelligent Automation & Soft Computing, vol. 34, no. 3, 2022.

[77] R. K. Shukla, A. S. Sengar, A. Gupta, A. Jain, A. Kumar, and N. K. Vishnoi, "Face recognition using convolutional neural network in machine learning," in 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), 2021, pp. 456-461

[78] Bhatia, A. Kumar, A. Jain, A. Kumar, C. Verma, Z. Illes, I. Aschilean, and M. S. Raboaca, "Networked control system with MANET communication and AODV routing," Heliyon, vol. 8, no. 11, 2022.

[79] Jain, T. Mehrotra, A. Sisodia, S. Vishnoi, S. Upadhyay, A. Kumar, C. Verma, and Z. Illés, "An enhanced self-learning-based clustering scheme for real-time traffic data distribution in wireless networks," Heliyon, vol. 9, no. 7, 2023.

[80] Jain, R. Dwivedi, A. Kumar, and S. Sharma, "Scalable design and synthesis of 3D mesh network on chip," in Proceeding of International Conference on Intelligent Communication, Control and Devices: ICICCD 2016, Singapore: Springer, 2017, pp. 661-666.

[81] Kumar and A. Jain, "Image smog restoration using oblique gradient profile prior and energy minimization," Frontiers of Computer Science, vol. 15, no. 6, p. 156706, 2021.

[82] Y. K. Sharma, S. S. Noval, A. Jain, B. Sabitha, and T. Ramya, "Forensics-as-a-service: A Review of Mobile Forensics," presented at the 2022 International Conference on Contemporary Computing and Informatics (IC3I), Dec. 2022.

[83] Jain, A. Bhola, S. Upadhyay, A. Singh, D. Kumar, and A. Jain, "Secure and Smart Trolley Shopping System based on IoT Module," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 2243-2247.

[84] Pandya, R. Pathak, V. Kumar, A. Jain, A. Jain, and M. Mursleen, "Role of Dialog and Explicit AI for Building Trust in Human-Robot Interaction," in 2023 International Conference on Disruptive Technologies (ICDT), 2023, pp. 745-749.

[85] S. Athithan, S. Sachi, A. K. Singh, A. Jain, and Y. K. Sharma, "Twitter Fake News Detection by Using Xlnet Model," in 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), 2023, pp. 868-872.

[86] Jain, Y. K. Sharma, S. Sachi, S. Athithan, and A. K. Singh, "Fire Detection Using Image Processing Technique," in 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), 2023, pp. 873-877.

[87] K. Singh, A. Jain, Y. K. Sharma, S. Athithan, and S. Sachi, "Multi Objective Optimization Based Land Cover Classification

Using NSGA-II," in 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), vol. 6, 2023, pp. 552-556.

[88] S. Devi, Y. K. Sharma, S. Athithan, S. Sachi, A. K. Singh, and A. Jain, "Implementation of ABC & WOA-Based Security Defense Mechanism for Distributed Denial of Service Attacks," in 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), vol. 6, 2023, pp. 546-551.

[89] K. B. Rao, Y. Bhardwaj, G. E. Rao, J. Gurrala, A. Jain, and K. Gupta, "Early Lung Cancer Prediction by AI-Inspired Algorithm," in 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), vol. 10, 2023, pp. 1466-1469.