IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141122

Cyber Threat and Fraud Detection using AI/ML

Chaitrali Shinde[1], Bhakti Nannaware[2], Sakshi Harnawal[3], Priyanka Gadhe[4],

Mr. Jaybhay D. S[5]

Department of Computer Engineering, Dattakala Group of Institutions, Faculty of Engineering Savitribai Phule Pune University[1-4]

Guide, Department of Computer Engineering, Dattakala Group of Institutions, Faculty of Engineering Savitribai Phule Pune University[5]

Abstract: Cyber threats and online fraud have become critical challenges in the digital era. Traditional security systems such as firewalls and signature-based methods are insufficient to counter increasingly sophisticated attacks including malware, phishing, ransomware, and fraudulent transactions in online shopping platforms. Artificial Intelligence (AI) and Machine Learning (ML) offer predictive, adaptive, and intelligent solutions capable of detecting cyber threats in real-time. This paper provides a comprehensive review of AI/ML techniques for cyber threat and fraud detection, explores their applications in online shopping platforms, discusses commonly used datasets and evaluation metrics, and highlights emerging trends and future directions for research.

Keywords: Cybersecurity, Fraud Detection, Artificial Intelligence, Machine Learning, Online Shopping, Anomaly Detection, Predictive Security.

I. INTROCUCTION

In the modern digital world, cyber threats and online fraud have become widespread, affecting individuals, busi- nesses, and critical infrastructures. With increasing reliance on online transactions, cloud computing, and dig- ital communication, traditional security methods are often inadequate against sophisticated attacks such as ran- somware, phishing, malware, and identity theft.

Online shopping platforms are particularly vulnerable, as fraudulent transactions and account takeovers can result in significant financial and reputational losses. Fraud detection is thus a crucial component in safeguard- ing both customers and businesses.

Artificial Intelligence (AI) and Machine Learning (ML) provide automated, intelligent, and predictive so- lutions capable of monitoring vast datasets, identifying anomalies, and detecting cyber threats in real-time. By leveraging historical and streaming data, AI/ML models can adapt to evolving attack patterns and provide early warnings for potential breaches. This review explores various AI/ML techniques, datasets, and evaluation meth- ods used in cyber threat detection and fraud prevention, with particular emphasis on online shopping platforms, highlighting current trends and challenges in the field.

II. LITERATURE SURVEY

Traditional cybersecurity techniques, such as signature-based detection, rule-based systems, and firewalls, are limited because they only detect known threats and fail against emerging, sophisticated attacks. To overcome these limitations, researchers have increasingly applied AI/ML approaches for cyber threat and fraud detection.

Supervised learning models, including Decision Trees, Random Forests, Support Vector Machines (SVM), and Neural Networks, are widely used for classifying and predicting malicious activities. Unsupervised learning techniques, such as K-Means clustering, DBSCAN, and anomaly detection algorithms, help identify unusual pat- terns in network traffic and user behavior. Deep learning models, such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Autoencoders, are capable of learning complex relationships in data and detecting advanced cyber attacks.

In online shopping platforms, AI/ML techniques are extensively used for fraud detection. Transaction patterns, user behavior, account activity, and payment details are analyzed in real-time to identify suspicious trans- actions and abnormal activity. Hybrid approaches combining rule-based systems and ML models have shown higher accuracy and

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141122

reduced false positives. Several datasets, such as CICIDS, KDDCup99, UNSW-NB15, and e-commerce transaction datasets, are commonly used for research and model training, though many lack full real- world complexity. Recent studies demonstrate that AI/ML-based solutions significantly improve detection speed, accuracy, and overall cybersecurity effectiveness for both IT systems and online shopping environments.

III. METHODOLOGY

The methodology for AI/ML-based cyber threat and fraud detection involves several stages. First, data is collected from multiple sources, including network traffic logs, system audit logs, and online transaction histories. For e-commerce applications, data may include user registration details, purchase history, IP addresses, and device information. Data preprocessing involves cleaning, normalization, feature selection, and handling class imbalance, which is critical as fraudulent events are far less frequent than legitimate transactions.

Next, AI/ML models are selected based on problem type. Supervised learning algorithms, such as Random Forests, SVM, and Neural Networks, are used for classification tasks, while unsupervised learning methods like K-Means and anomaly detection identify unusual behavior without prior labels. Deep learning models, including CNNs and RNNs, are effective in detecting complex and temporal patterns. Models are trained and validated using cross-validation techniques, and performance is evaluated using metrics like accuracy, precision, recall, F1-score, and ROC-AUC. For online shopping platforms, these models enable real-time monitoring of transactions, identify- ing potential fraud immediately and improving platform security. Tools such as Python, Scikit-learn, TensorFlow, and Keras are widely employed for implementation.

IV. FINDINGS AND TRENDS

AI/ML models significantly enhance the accuracy and efficiency of cyber threat and fraud detection compared to traditional methods. Real-time detection systems powered by streaming data analytics allow proactive mitigation of potential threats. Deep learning techniques outperform classical ML models in detecting sophisticated attack patterns. Hybrid approaches that combine supervised and unsupervised learning improve detection rates and reduce false positives. In online shopping, AI/ML systems successfully detect fraudulent transactions, fake accounts, and abnormal purchasing patterns. Emerging trends include reinforcement learning for adaptive threat mitigation, federated learning for distributed data privacy, and AI-driven threat intelligence systems. Challenges remain, including high computational requirements, need for large and diverse datasets, and susceptibility to adversarial attacks.

V. FIGURES AND TABLES

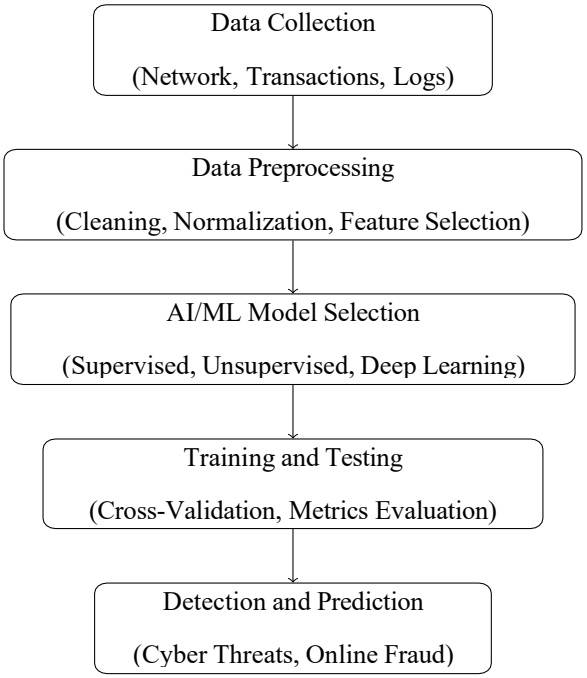

Figure 1: Workflow of Cyber Threat and Fraud Detection using AI/ML

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141122

Table 1: Common Datasets for Cyber Threat and Fraud Detection

Dataset	Type	Use Case
CICIDS	Network	Intrusion Detection
KDDCup99	Network	Anomaly Detection
UNSW-NB15	Network	Cybersecurity Research
E-Commerce Transactions	Transaction	Fraud Detection in Online Shopping

Table 2: Popular AI/ML Models for Cyber Threat and Fraud Detection

Model	Type	Application
Decision Tree	Supervised	Classification of Threats
Random Forest	Supervised	Fraud Detection, Anomaly Detection
SVM	Supervised	Intrusion Detection
K-Means	Unsupervised	Pattern Clustering, Anomaly Detection
CNN/RNN	Deep Learning	Complex Cyber Attack Detection
Autoencoder	Deep Learning	Anomaly Detection, Fraud Detection

VI. CONCLUSION

AI and ML have revolutionized cyber threat and fraud detection by providing intelligent, automated, and predic- tive solutions. Their applications in IT systems and online shopping platforms enhance security, detect anomalies in real-time, and reduce financial and reputational losses. This paper reviewed various AI/ML models, datasets, and methodologies, highlighting hybrid approaches, deep learning models, and real-time monitoring as key con- tributors to effective cybersecurity. Future research should focus on adaptive, robust systems capable of handling evolving threats, minimizing false positives, and maintaining privacy in online transactions. Integration of AI/ML into real-world e-commerce and IT infrastructures ensures safer digital environments for both organizations and users.

REFERENCES

[1] Kim, J., & Lee, S. (2021). AI-based Cybersecurity: Threat Detection and Prevention. *Journal of Information Security*.

[2] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A Survey of Network Anomaly Detection Techniques. *Journal of Computer Networks*.

[3] Javaid, A., et al. (2016). A Deep Learning Approach for Network Intrusion Detection System. *IEEE Access*.

[4] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *ICISSP*.

[5] Sahoo, B., & Tripathy, B. K. (2020). Machine Learning Techniques for Fraud Detection: A Review. *International Journal of Computer Applications*.