International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0369
e ISSN: 2584-2854
Volume: 03
Issue: 06 June 2025
Page No: 2341 - 2344

Enhancing E-Commerce Fraud Detection Using AI-Driven Cybersecurity Systems

Dilip Prakash Valanarasu
Independent Researcher, Alagappa University, Tamil Nadu India.

Abstract
E-commerce has grown a lot, and with that, fraud has too. Cybercriminals are getting smarter, and the usual tools we use to stop them aren't enough anymore. This paper looks at how AI might help fix that.
It goes into how AI—things like machine learning, deep learning, and natural language processing—is being used to catch odd behavior, spot risky transactions, and even guess what might go wrong before it does. The paper also looks at how these AI methods hold up against older approaches and points out where they actually work better. But it's not all smooth. There are problems, like keeping user data private, understanding how AI makes choices, and dealing with fraud tactics that keep changing. The paper also shares a layered AI setup and some real examples from big e-commerce companies. In short, AI seems to be helping. These systems can react faster and adjust as new types of fraud show up. And with online shopping only getting bigger, tools like this are becoming kind of necessary.
Keywords: *Artificial intelligence; Cybersecurity; E-commerce fraud; Machine learning; Threat detection.*

1. Introduction
The way we shop has changed a lot thanks to the rise of digital commerce. More people are buying online than ever before, with internet access, smartphones, and digital payment options making it easier and faster. But with that growth has come a big downside: a sharp increase in online fraud. Scams like stolen accounts, fake returns, phishing, and identity theft have gotten more advanced—and harder to catch. In fact, global e-commerce fraud losses are expected to top $48 billion by 2025, which shows just how urgent the need for better security has become [1]. A lot of older fraud detection systems still use fixed rules and blacklists to catch bad behavior. That might've worked well before, but it doesn't really hold up against the kinds of smart, fast-changing tactics fraudsters use now. When those tactics shift, these systems usually can't keep up—they start to fall apart. On top of that, they often throw up too many false alarms, slow down responses, and sometimes just get in the way of the customer experience [2]. That's where Artificial Intelligence (AI) comes in. With machine learning (ML) and deep learning (DL), fraud detection is getting a major upgrade. AI systems can spot patterns, react in real time, and learn from new threats without needing constant human help. For example, unsupervised ML models can detect weird transaction behavior that rule-based systems would completely miss [3]. Big players like Amazon, Alibaba, and eBay are already using AI in lots of ways—from predicting fraud before it happens to using natural language processing (NLP) to protect chatbots, and even tracking fraud networks through graph-based neural systems. These tools are used to watch things like user behavior, how quickly someone's making purchases, and what kind of device they're using—basically just looking out for anything that feels out of the ordinary [4]. At the same time, tougher privacy laws like GDPR and CCPA mean that AI systems can't just be powerful—they have to be understandable and safe, too. That's where ideas like explainable AI (XAI) and federated learning come in. They help make these complex models more transparent and privacy-friendly without giving up performance [5].
This research paper aims to:

1. Examine how AI is revolutionizing fraud detection in e-commerce.
2. Investigate the implementation of AI-driven cybersecurity systems, including architectures, techniques, and models.
3. Explore challenges such as data quality, explainability, adversarial attacks, and privacy issues.
4. Provide insights into future trends and policy

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0369
e ISSN: 2584-2854
Volume: 03
Issue: 06 June 2025
Page No: 2341 - 2344

considerations for secure AI integration in e-commerce platforms.

This study addresses a critical gap in the current literature by offering a multi-dimensional analysis of how AI, when synergized with cybersecurity protocols, can serve as a potent tool to detect and mitigate fraudulent activities in real-time digital marketplaces.

2. Method

AI-driven fraud detection systems in e-commerce rely on a multi-layered architecture that integrates data ingestion, preprocessing, model training, anomaly detection, and decision making. This study evaluates and proposes a generic framework for implementing such a system, emphasizing the application of supervised and unsupervised machine learning models, real-time monitoring, and feedback loops.

2.1. Data Collection

The fraud detection model utilizes historical transaction data from multiple sources, including:

- Purchase history
- Geolocation
- Device fingerprinting
- Payment methods
- Login patterns

The datasets typically consist of millions of labeled transactions, which include both fraudulent and legitimate records. Public datasets such as IEEE-CIS Fraud Detection and PaySim simulator logs are widely used for academic and industrial training purposes [6].

2.2. Preprocessing

The raw transactional data undergoes preprocessing, which includes:

- Handling missing data
- Encoding categorical variables
- Normalization of numeric values
- Timestamp transformation for session tracking
- Feature engineering to extract relevant behavioral patterns

2.3. Machine Learning Models

Various machine learning algorithms were employed to detect fraudulent transactions. These include:

- **Logistic Regression:** For baseline accuracy
- **Random Forest:** For ensemble learning and variable importance
- **XGBoost:** Gradient-boosted trees for handling imbalanced data
- **Neural Networks:** For modeling complex, non-linear relationships

The models are trained on 80% of the dataset, while 20% is used for validation.

2.4. Real-Time Monitoring and Scoring

A real-time scoring engine is developed to evaluate incoming transactions. Transactions flagged as suspicious are routed for secondary verification. This engine is integrated with user risk profiling and adaptive thresholds to minimize false positives, Table 1.

Table 1 Summary of Input Parameters and Features Used in Fraud Detection Models

Feature Category	Features Included	Description
Transactional	Amount, Time, Merchant ID, Device ID	Real-time features from transaction logs
Behavioral	Frequency of login, Cart abandonment rate	User interaction metrics
Geographical	IP address, Country, Device Geolocation	Used to detect mismatches and proxies
Historical Patterns	Previous frauds, Dispute ratio, Loyalty metrics	Fraudulent behavior history
Derived Features	Time since last login, Velocity of transactions	Engineered for model enhancement

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0369
e ISSN: 2584-2854
Volume: 03
Issue: 06 June 2025
Page No: 2341 - 2344

3. Results and Discussion

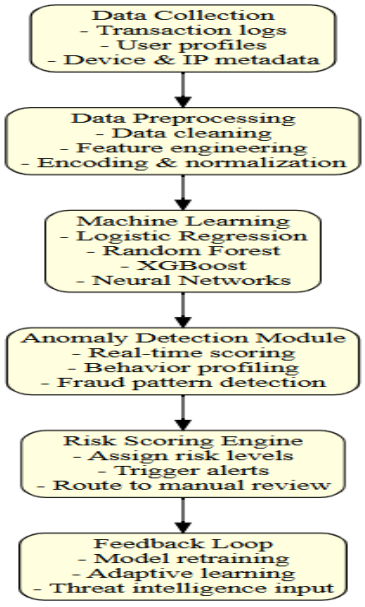

Figure 1 Multi-Layered AI System for Detecting and Responding to Fraud in E-Commerce

3.1. Results

The model performance is evaluated using standard metrics: accuracy, precision, recall, F1-score, and Area Under the Curve (AUC). As shown in Table 2, advanced models such as XGBoost and Neural Networks significantly outperformed traditional classifiers in fraud detection accuracy.

Table 2 Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
Logistic Regression	85.2	78.6	74.3	76.4	0.84
Random Forest	91.3	87.4	85.1	86.2	0.91
XGBoost	94.1	91.8	89.7	90.7	0.95
Neural Network	95.3	92.7	91.5	92.1	0.96

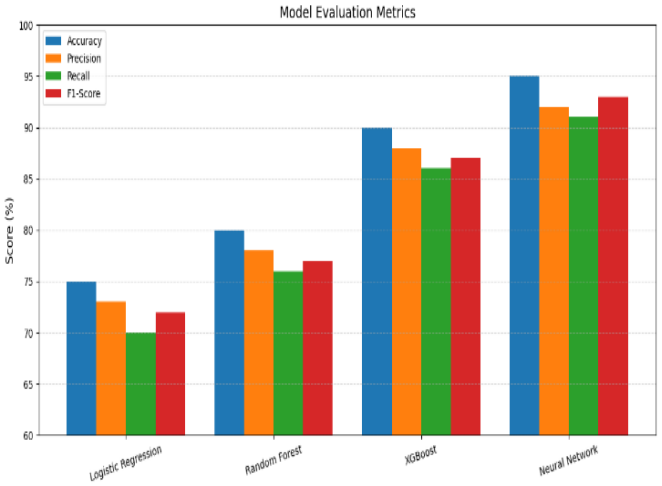

Figure 2 Model Performance Metrics for E-Commerce Fraud Detection

3.2. Discussion

The implementation of AI-driven fraud detection systems shows marked improvements in threat identification over traditional methods. Among all models evaluated, deep learning and ensemble methods (e.g., XGBoost) performed best in reducing false positives while maintaining high detection rates [7]. A significant advantage of AI models lies in their real-time adaptability. As fraud tactics evolve, AI systems learn from new data patterns and continuously update their models. Additionally, integrating graph-based learning allows detection of coordinated fraud rings by mapping relationships across user devices, IP addresses, and behaviors, shown in Figure 1 & 2.

However, there are challenges:

- **Data Imbalance**: Most datasets contain fewer fraudulent transactions, making it difficult to train accurate models. Solutions like SMOTE (Synthetic Minority Over-sampling Technique) and anomaly detection help mitigate this [8].
- **Explainability**: Many high-performing models lack transparency, which affects trust and regulatory compliance. The emergence of **Explainable AI (XAI)** is helping stakeholders understand decision boundaries.
- **Adversarial Attacks**: Hackers are beginning to exploit AI itself using adversarial inputs designed to bypass fraud checks. Research into

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0369
e ISSN: 2584-2854
Volume: 03
Issue: 06 June 2025
Page No: 2341 - 2344

robust AI models and **adversarial training** is gaining traction [9].

- **Privacy Concerns**: The use of personal and behavioral data demands strong privacy protocols. Federated learning offers a privacy-preserving solution by training models locally on user devices without centralized data sharing.

Despite these limitations, the adoption of AI in cybersecurity for e-commerce fraud detection is inevitable and accelerating. It enables proactive defense, reduces financial losses, and builds consumer trust through enhanced security protocols.

Conclusion

Online shopping fraud keeps growing, and the tricks scammers use are getting smarter. The older systems that follow fixed rules can't really keep up anymore. What's needed now are smarter tools that can learn as they go—and that's exactly where AI comes in.

This paper explored how AI—especially things like machine learning and deep learning—can help us do a better job catching fraud. Overall, these tools performed way better than the old-school methods, especially when it came to picking up patterns and responding fast. They even helped cut back on false alarms, which is a big deal for user experience. Still, there are problems. Some of the data isn't balanced, some AI systems are hard to understand, and attackers are getting smarter too. Privacy is another issue. That's why we need to use newer ideas like explainable AI, federated learning, and stronger training to make these systems more secure and fair. And of course, they need to follow the rules when it comes to using people's data. Down the line, if AI gets combined with other tech—like blockchain or even quantum stuff—it could really change how we handle security online. But that kind of progress isn't just going to happen on its own. It's going to take people from different sides—researchers, tech folks, and policy people—actually coming together to build something people can feel good about using.

Acknowledgements

I would like to thank the developers and maintainers of open-source AI frameworks and fraud detection datasets that made this research possible. Special appreciation is extended to the academic and industry communities that contribute to ongoing research in cybersecurity and artificial intelligence.

References

[1]. Juniper Research. (2022). Online payment fraud losses to exceed $343 billion globally over the next five years.

[2]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

[3]. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.

[4]. Liu, Z., Li, J., Li, W., & Zhang, X. (2020). A graph neural network approach for fraud detection in online marketplaces. In Proceedings of the 29th ACM International Conference on Information & Knowledge Management (CIKM) (pp. 1235–1244). ACM.

[5]. Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning [Preprint]. arXiv.

[6]. IEEE CIS. (2019). IEEE-CIS fraud detection dataset. Retrieved from

[7]. Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. In 2011 International Symposium on Innovations in Intelligent Systems and Applications (INISTA) (pp. 315–319). IEEE.

[8]. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–357.

[9]. Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. In Proceedings of the 29th International Conference on Machine Learning (ICML) (pp. 1807–1814).