WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Need for Real-Time Fraud Detection in E-Commerce Using Machine Learning

V. Manideep[1], Mrs. T. Anusha[2]

[1] Student, CSE, UG student, GMRIT Deemed to be University, Rajam.
[2]Assistant professor, CSE, GMRIT Deemed to be University, Rajam.

ABSTRACT:

The rapid growth of e-commerce and digital payment systems has significantly increased the risk of online fraud, leading to substantial losses for businesses and customers. Most traditional fraud detection systems identify fraudulent transactions only after payment completion, making it difficult to prevent financial damage. A real-time fraud detection framework based on Machine Learning is proposed to evaluate every transaction before it is approved. The system collects transaction information such as payment amount, transaction time, user location, device details, IP address, and customer purchasing behavior. These features are processed using feature engineering techniques and analyzed by Machine Learning algorithms such as Random Forest, XGBoost, or LightGBM to calculate a fraud probability score within milliseconds. Based on the calculated risk score, the system approves legitimate transactions, requests additional authentication for suspicious transactions, or blocks fraudulent activities. The framework also supports continuous model retraining using newly generated transaction data, enabling the system to adapt to evolving fraud patterns. By integrating realtime data processing, intelligent risk assessment, and automated decision-making, the proposed solution enhances transaction security, reduces financial losses, minimizes false alarms, and improves customer trust. This approach provides a scalable, accurate, and efficient fraud prevention mechanism suitable for modern e-commerce platforms handling millions of online transactions every day.

Keywords: Real-Time Fraud Detection, Machine Learning, E-Commerce Security, Transaction Monitoring, XGBoost, Risk Scoring, Feature Engineering.

Introduction:

The rapid growth of e-commerce has transformed the way people buy and sell products and services. Online shopping offers convenience, faster transactions, and global accessibility, but it has also increased the risk of online fraud. Fraudulent activities such as payment fraud, account takeover, identity theft, and phishing attacks cause significant financial losses and reduce customer trust. Traditional fraud detection systems mainly rely on predefined rules and manual verification, making them less effective against new and evolving fraud techniques.

Machine Learning has emerged as an effective solution for detecting fraudulent activities by analyzing historical transaction data and identifying suspicious patterns. Unlike traditional methods, Machine Learning models can learn from new data, adapt to changing fraud strategies, and provide accurate predictions in real time. This enables fraudulent transactions to be detected before payment approval, reducing the risk of financial loss.

This study proposes a real-time fraud detection framework based on Machine Learning to evaluate every transaction before it is approved. The framework analyzes transaction details such as payment amount, transaction time, user location, device information, IP address, and customer purchasing behavior to calculate a fraud risk score. Based on this score, the system can approve legitimate transactions, request additional verification for suspicious activities, or block fraudulent transactions. Continuous model retraining enables the framework to adapt to evolving fraud patterns, making it a scalable, accurate, and efficient solution for enhancing transaction security and improving customer trust in modern e-commerce platforms.

Literature:

The reviewed studies cover several approaches to fraud detection. Mutemi and Bação (2024) reviewed Machine Learning techniques for e-commerce fraud detection and identified research challenges and emerging trends. Manoharan et al. (2024) considered supervised, unsupervised, and semi-supervised learning approaches, emphasizing the importance of feature engineering and model selection.

Research on feature engineering and ensemble methods provides further direction. Sánchez-Paniagua et al. (2026) focused on comparing features to improve Machine Learning-based fraud detection. Gupta et al. (2025) considered feature engineering and ensemble models for credit card fraud detection, including the challenge of class imbalance. These approaches highlight the importance of selecting relevant transaction features and handling imbalanced datasets when training fraud classification models.

Other studies explore hybrid and specialized techniques. Vasant et al. (2025) examined a hybrid

Machine Learning approach involving techniques such as SMOTE and Linear Discriminant Analysis. Immanuel et al. (2025) focused on payment fraud detection in e-commerce and considered the KNearest Neighbors algorithm. Jayalakshmi and Priya (2025) reviewed techniques for detecting synthetic fraud and discussed research gaps in existing systems. Together, these works reflect the range of Machine Learning approaches being explored for online fraud prevention.

Graph-based approaches provide another direction. Chen et al. (2019) presented InfDetect, a graphbased fraud detection system for e-commerce insurance. Sarwosri et al. (2026) investigated Graph Neural Network-based feature embedding combined with Machine Learning methods for e-commerce transaction fraud detection. These approaches consider relationships among transactions and related entities, which can help identify suspicious connections that may not be apparent from individual transaction attributes alone.

Comparative studies also examine the performance of different classification algorithms. Aggarwal et al. (2023) compared Logistic Regression, K-Nearest Neighbors, Support Vector Machine, and Decision Tree models for credit card fraud detection. Aditi et al. (2022) studied advanced Machine Learning techniques for the same domain, while Boutaher et al. (2020) reviewed existing methods and their limitations. Research by A. K. et al. (2021) also considered several classification algorithms, including Decision Tree, Logistic Regression, K-Nearest Neighbors, Support Vector Machine, and Random Forest, for e-commerce fraud detection.

Based on these research directions, the present paper proposes a real-time fraud detection framework using Random Forest, XGBoost, and LightGBM as candidate algorithms. The framework collects transaction details, user information, device and location data, and behavioural features. After preprocessing and feature engineering, the selected model estimates a fraud risk score to support transaction approval, additional authentication, or blocking for further investigation. Model monitoring and retraining are included to help address evolving fraud patterns.

The literature indicates the importance of combining suitable features, effective classification techniques, and appropriate handling of class imbalance. However, detecting fraud before payment completion also requires rapid processing and reliable decision-making. Therefore, the proposed framework focuses on real-time risk assessment alongside fraud classification. Experimental evaluation is required to compare the candidate algorithms using precision, recall, F1-score, ROCAUC, and processing latency, and to determine their suitability for practical deployment.

Table 1: Comprehensive Comparative Literature Survey on E-Commerce Fraud Detection.

Ref & Citation	Year	Research Focus	Core Methodology	Key Academic Contribution	Identified Limitation / Gap
[1] Sánchez-Paniagua et al. (2026)	2026	Feature Analysis in E-Commerce	Feature extraction (50 attributes), XGBoost, RF, LR	Achieved >96% F1-score; proved critical role of rich feature engineering	High feature extraction computation; focused on website fraud
[2] Sarwosri et al. (2026)	2026	GNN Relational Embeddings	GraphSAGE GNN embeddings + ANN, RF, Gradient Boost	Captured coordinated fraud syndicates across transaction entity graphs	High graph inference latency (>200 ms); limits real-time gateway deployment
[3] Gupta et al. (2025)	2025	Feature Eng. & Ensemble Fraud	WoE encoding, log transform, SMOTE, RF, XGBoost	Demonstrated ensemble superiority with temporal velocity features	Evaluated on static offline data; no streaming latency benchmarking
[4] Jayalakshmi & Priya (2025)	2025	Synthetic Fraud Survey	Systematic literature survey across ML, DL, and NLP methods	Synthesized structured taxonomy for detecting synthetic identity fraud	Qualitative survey only; no empirical implementation or framework
[5] Vasant et al. (2025)	2025	Hybrid Deep Learning	SMOTE class balancing, LDA feature selection, Hybrid ANN–DNN	Proved hybrid neural networks capture complex non-linear fraud patterns	High training overhead; lacks sub-second streaming validation
[6] Immanuel et al. (2025)	2025	Payment Fraud Verification	KNN behavioral anomaly detection + Face Verification	Integrated behavioral scoring with dynamic biometric identity check	Single classifier (KNN); does not scale to high-throughput streaming
[7] Mutemi & Bação (2024)	2024	Systematic Review on Fraud VOSviewer	PRISMA protocol, algorithmic adoption, and bibliometrics across 101	Mapped research trends, concrete operational structural challenges	Secondary review only; no architecture papers
[8] Manoharan et al. (2024)	2024	ML Transaction Perspective	Stacking ensemble, stratified crossvalidation, supervised ML	Demonstrated stacking heterogeneous classifiers enhances robustness	Evaluated on limited datasets; did not test production streaming latency SLAs

Ref & Citation	Year	Research Focus	Core Methodology	Key Academic Contribution	Identified Limitation / Gap
[9] Aggarwal et al. (2023)	2023	Performance of Four ML Models LR, KNN, SVM, Decision Tree	Comparative analysis: Proved non-linear classifiers (SVM, DT) outperform linear baselines	Small sample (1,136 records); lacks boosting models and class rebalancing	
[10] Aditi et al. (2022)	2022	Advanced ML Credit Card Fraud	Random Forest, Logistic Regression, Decision Tree	Demonstrated ensemble efficacy on European credit card transaction data	Basic classification; lacks advanced feature engineering and threshold tuning
[11] A. K. et al. (2021)	2021	E-Commerce ML Techniques	Standard scaling, under-sampling, DT, LR, evaluated on KNN, SVM, RF	Proved Random Forest achieves highest multi-model classification accuracy	Under-sampling discards majority data; static Kaggle dataset
[12] Boutaher et al. (2020)	2020	Cloud-Based Fraud Review	Literature survey of cloud ML: LR, RF, SVM, Neural Networks	Synthesized evaluation metrics and cloud scalability trade-offs	Qualitative review only; lacks architecture for preauthorization gateway
[13] Chen et al. (2019)	2019	InfDetect: Graph Fraud System	Heterogeneous graph, DeepWalk, GeniePath GNN, PSMART	Detected organized fraud rings in e-commerce insurance applications	High computational complexity; requires distributed graph processing clusters
[14] Jhangiani et al. (2019)	2019	End-to-End ML Pipeline	SMOTE / Undersampling, Gradient Boost, AdaBoost, RF, SVM	Formulated end-to-end pipeline showing boosting superiority on imbalanced data	Batch-oriented processing; lacks online retraining and step-up auth
[15] Saputra & Suharjito (2019)	2019	ML in E-Commerce Fraud	PCA preprocessing, SMOTE class balancing, DT, NB, RF, NN	Showed SMOTE class balancing dramatically elevates recall and G-Mean	Evaluated on static dataset; no streaming drift or latency tests

Methodology:

Research Design

This paper adopts a comparative and analytical research design based on a review of existing studies on Machine Learning-based fraud detection in e-commerce. The main objective is to examine existing detection techniques, understand their advantages and limitations, and propose a conceptual framework for identifying fraudulent transactions in real time.

The study considers different approaches, including feature engineering, ensemble learning, hybrid Machine Learning methods, and Graph Neural Networks. These approaches are analysed based on the transaction features used, detection techniques, evaluation metrics, and research challenges.

Based on the literature review, a conceptual framework is proposed that includes data preprocessing, feature engineering, model training, fraud risk prediction, and risk-based transaction decisions. Random Forest, XGBoost, and LightGBM are considered candidate algorithms for future comparative evaluation using precision, recall, F1-score, ROC-AUC, and processing latency.

Data Sources and Selection Criteria

The study is based on secondary data collected from research papers published in academic journals and conference proceedings, including publications available through IEEE Xplore and other scholarly databases. The literature review focuses on studies related to e-commerce fraud detection, credit card fraud detection, feature engineering, ensemble learning, and graph-based fraud detection.

Research published between 2019 and 2026 is considered to understand the development of fraud detection techniques and recent research directions. The selected studies are examined according to their relevance to e-commerce transactions, Machine Learning methods, transaction features, evaluation approaches, and identified limitations.

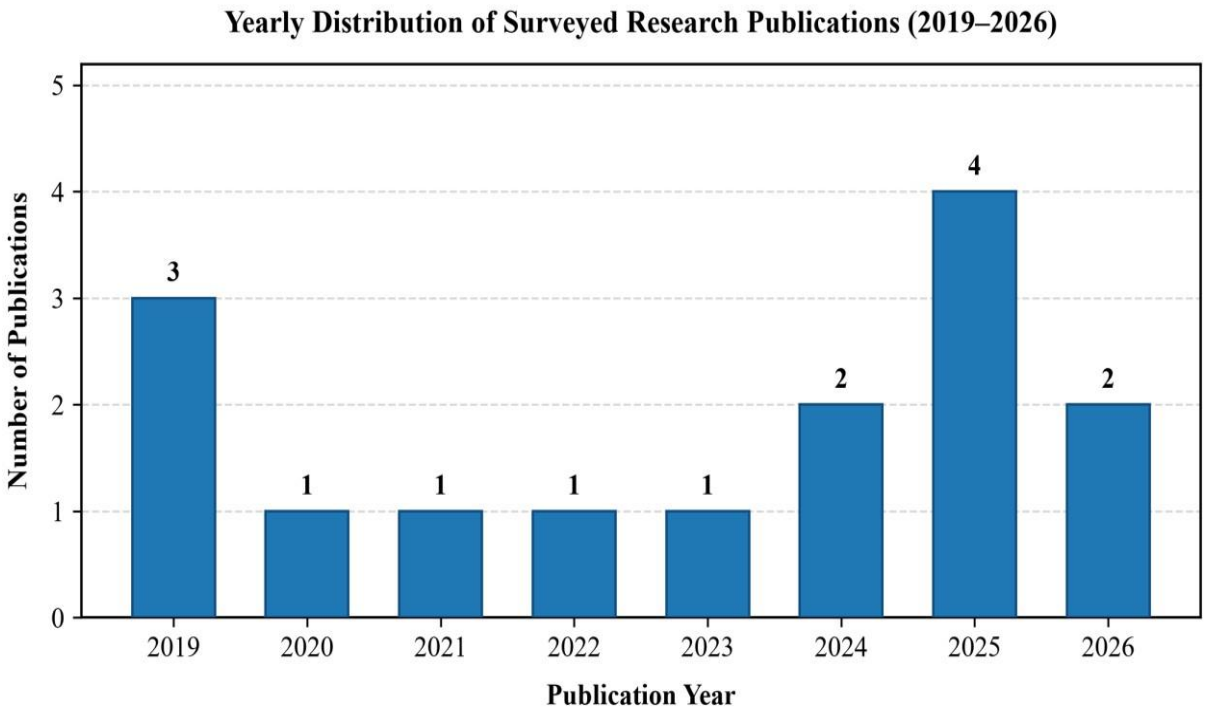


Figure 1: Yearly distribution of surveyed research literature on e-commerce and credit card fraud detection (2019– 2026).

The study does not claim to have collected or experimentally tested a new transaction dataset. Instead, the reviewed literature provides the basis for developing the proposed framework and identifying areas that require further investigation.

Stages in Methodology framework:

Stage 1 – Literature Synthesis

Existing research on Machine Learning-based fraud detection is reviewed to identify common techniques, important transaction features, and major challenges. Particular attention is given to feature engineering, ensemble models, hybrid approaches, and graph-based methods.

Stage 2 – Analysis of Detection Techniques

Different fraud detection approaches are analysed to understand how they identify suspicious transactions. Feature-based methods examine transaction characteristics, while graph-based methods consider relationships among users, accounts, devices, and transactions. Their potential benefits and limitations are compared.

Table 2: Comparative Analysis of Feature-Based vs. Graph-Based Fraud Detection Approaches.

Evaluation Criterion	Feature-Based Detection (Case Study 1)	Graph-Based GNN Detection (Case Study 2)
Core Architectural Paradigm	Tabular Feature Engineering + Tree Ensembles	Graph Neural Network Embeddings + ML Classifiers
Primary Feature Inputs	Structured financial, temporal, and device telemetry	Bipartite graph topology, entity nodes, and transaction edges
Representative ML Models	XGBoost, Random Forest, LightGBM, Logistic Regression	GraphSAGE GNN, Artificial Neural Networks, Random Forest
Targeted Fraud Signatures	Individual transaction anomalies, velocity spikes, card testing	Organized fraud syndicates, collusive merchant rings, shared devices
Class Imbalance Handling	SMOTE, Cost-Sensitive Loss Weighting, Focal Loss	SMOTE-ENN, Neighborhood Re-sampling, Graph Rewiring

Evaluation Criterion	Feature-Based Detection (Case Study 1)	Graph-Based GNN Detection (Case Study 2)
Computational Complexity	Low to Moderate (O(N · D) feature transformations)	High to Extreme (O(|V| + |E|) graph aggregations)
Inference Latency Profile	Ultra-Low (5 ms to 30 ms per transaction)	Moderate to High (120 ms to 800+ ms per query)
Real-Time Gateway Suitability	Extremely High (Optimal for synchronous preauthorization)	Limited for synchronous inline gating; optimal for near-line auditing

Stage 3 – Identification of Transaction Features

Important transaction attributes are identified for the proposed framework. These include transaction amount, transaction time, user location, device information, IP address, transaction frequency, and customer purchasing behaviour. These features can help distinguish normal activities from potentially suspicious patterns.

Table 3: Comprehensive Feature Engineering and Transaction Attribute Taxonomy.

Feature Category	Attributes and Telemetry	Detection Utility and Fraud Signal
Financial & Transaction	Amount, Currency, Merchant Category Code (MCC), Product SKU	Detects monetary anomalies, abnormal ticket sizes, and high-risk luxury purchases.
Temporal & Scheduling	Hour of Day, Day of Week, Order Time Delta, Holiday Indicator	Identifies abnormal purchase timing and rapid highvelocity transaction bursts.
Customer Behavioral	Velocity (5m, 1h, 24h), Spend Deviation from Historical Baseline	Measures deviation from established user behavior baselines; detects card testing.
Device Fingerprint	Canvas Hash, User-Agent, Operating System, Screen Concurrency	Unmasks device spoofing, headless browser automation, and account farming.
Network & Geospatial	IP Address, ASN, Proxy/VPN/Tor Flag, Distance Velocity	Detects anonymous routing/proxies and physically impossible travel velocities.
Derived Risk Indicators	Failed Login Attempts, Card-to-Device Ratio, Email Domain Risk	Flags credential stuffing, brute-force attempts, and synthetic identity takeovers.

Stage 4 – Evaluation Framework

Suitable evaluation measures are identified for comparing candidate Machine Learning algorithms.

Precision, recall, F1-score, and ROC-AUC are considered to assess detection performance.

Processing latency is also important because a real-time system must analyse transactions quickly.

Special attention is given to class imbalance and false-positive predictions.

Table 4: Evaluation Metrics and Operational Criteria for Real-Time Fraud Detection.

Evaluation Metric	Mathematical Formulation	Operational Purpose in Fraud Detection	Target Criteria / SLA
Precision	TP / (TP + FP)	Minimizes false positive declines, protecting merchant revenue and preventing customer friction.	High (≥ 85%–90%)
Recall (Sensitivity)	TP / (TP + FN)	Maximizes fraud interception, directly preventing catastrophic chargeback financial losses.	Critical (≥ 90%–95%)

Evaluation Metric	Mathematical Formulation	Operational Purpose in Fraud Detection	Target Criteria / SLA
F1-Score	2 · (Precision · Recall) / (Precision + Recall)	Harmonic mean providing a balanced operational measure under severe class imbalance (< 0.2% fraud).	High (≥ 88%–92%)
PR-AUC (Avg Precision)	∫ Precision(R) dR	Gold-standard metric for imbalanced data; evaluates trade-offs across all operating thresholds (avoids Accuracy Paradox).	Maximized (≥ 0.85)
ROC-AUC & FPR	AUC(TPR vs. FPR); FPR = FP / (FP + TN)	Assesses overall discriminative capability while strictly constraining false alarms on legitimate users.	ROC-AUC ≥ 0.95; FPR < 1.0%
Processing Latency	T_prep + T_infer + T_decide	Enforces strict payment gateway SLA compliance without introducing checkout abandonment friction.	Total SLA < 100 ms (Inference 10–30 ms)

Stage 5 – Development of the Proposed Framework

Based on the literature review, a conceptual framework is developed for real-time e-commerce fraud detection. The framework integrates transaction data collection, preprocessing, feature engineering, Machine Learning-based risk prediction, and risk-based decisions. It is intended to support transaction approval, additional verification, or further investigation according to the predicted risk.

The Proposed System Architecture

The proposed architecture is designed to identify suspicious e-commerce transactions before payment approval, where integration with the payment workflow permits. It consists of five major layers that work together to collect transaction information, process data, estimate fraud risk, and support appropriate decisions.

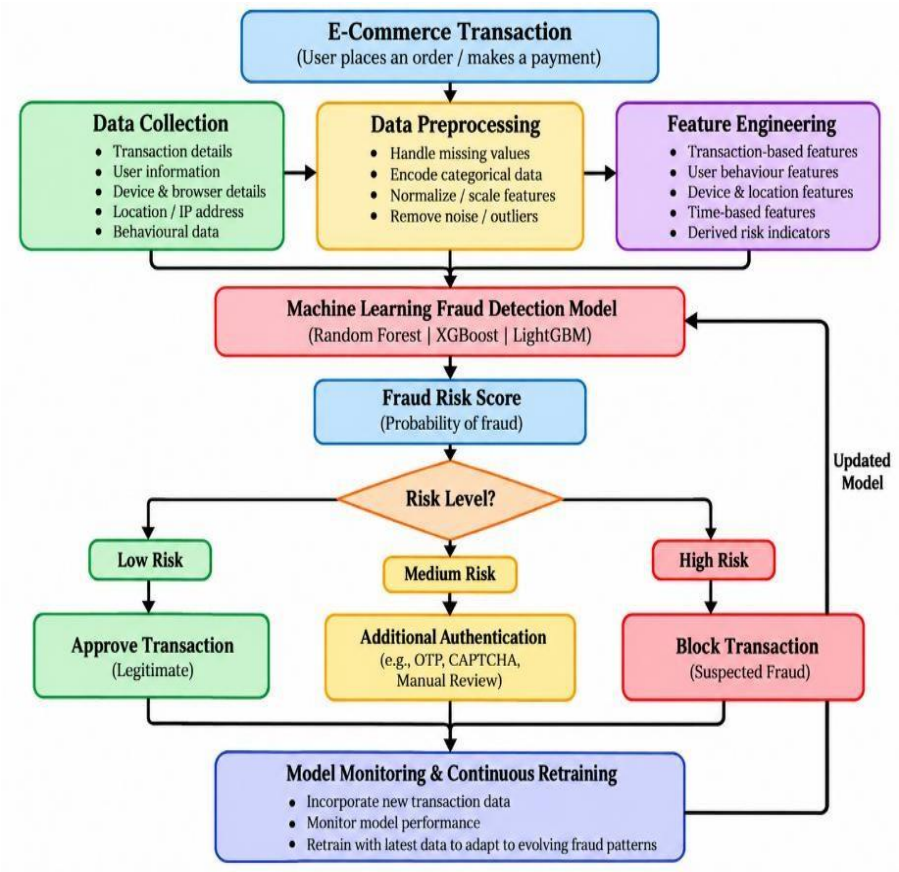


Figure 2: Proposed architecture and end-to-end decision framework for real-time fraud detection in e-commerce.

Architectural Overview

The proposed architecture for real-time fraud detection in e-commerce consists of five major layers, each responsible for a specific operation in the transaction monitoring and fraud prevention process (Figure 2):

1. Transaction Data Collection Layer

Function: Collects information related to online purchases and payment activities.

Components:

- Transaction amount and timestamp.
- Customer and account information.
- User location and IP address.
- Device and purchasing behaviour details.

Outcome: Provides transaction information for further analysis.

2. Data Preprocessing and Feature Engineering Layer

Function: Prepares raw transaction data for Machine Learning analysis.

Processes:

- Handling missing or inconsistent values.
- Encoding categorical variables.
- Scaling numerical features when required.
- Creating features such as transaction frequency and unusual spending patterns.

Outcome: Produces structured transaction features for fraud prediction.

3. Machine Learning Detection Layer

Function: Analyses transaction features to identify potentially fraudulent activities.

Candidate algorithms:

- Random Forest.
- XGBoost.
- LightGBM.

Processes: Model training, transaction classification, and fraud risk estimation.

Outcome: Generates a fraud prediction or risk score for each transaction.

4. Risk Assessment and Decision Layer

Function: Uses the predicted risk to support transaction decisions.

Decision options:

- Low-risk transactions: approve the transaction.
- Medium-risk transactions: request additional verification.
- High-risk transactions: block or hold the transaction for further review.

Outcome: Supports risk-based transaction handling. Actual thresholds must be selected and validated during implementation.

5. Monitoring and Model Improvement Layer

Function: Monitors detection performance and supports future model updates.

Components:

- Fraud alert and transaction monitoring.
- Model performance evaluation.

- Feedback from confirmed fraud cases.
- Periodic model retraining and validation.

Outcome: Helps the detection system adapt to changing fraud patterns over time.

Workflow of the Architecture

1. **Transaction Initiation:** A customer places an order and initiates an online payment.
2. **Data Collection:** The system collects available transaction, account, device, and behavioural information.
3. **Data Preprocessing:** The collected information is cleaned and transformed into a suitable format.
4. **Feature Extraction:** Relevant transaction features are generated for Machine Learning analysis.
5. **Fraud Risk Prediction:** The selected model estimates the likelihood that the transaction is fraudulent.
6. **Risk-Based Decision:** The system supports approval, additional verification, or blocking and review based on the predicted risk.
7. **Performance Monitoring:** Predictions and confirmed outcomes are used to evaluate detection performance.
8. **Model Updating:** The model can be retrained and validated using new labelled transaction data to address changing fraud patterns.

RESULTS:

The literature review highlights the potential of Machine Learning techniques for detecting fraudulent e-commerce transactions. The reviewed studies focus on feature engineering, ensemble learning, and graph-based approaches to identify suspicious transaction patterns. Based on these findings, a conceptual framework for real-time fraud detection is proposed.

The proposed framework consists of transaction data collection, data preprocessing, feature engineering, Machine Learning-based fraud prediction, risk assessment, and model monitoring. Random Forest, XGBoost, and LightGBM are considered candidate algorithms for future evaluation. The framework classifies transactions according to their estimated risk and supports transaction approval, additional authentication, or blocking for further investigation.

The proposed framework also incorporates model monitoring and periodic retraining to address changing fraud patterns. However, as this study is based on a literature review and conceptual framework, no experimental results or quantitative performance measurements are reported. The actual effectiveness of the proposed approach requires validation using an appropriate transaction dataset.

DISCUSSION:

The proposed framework illustrates how Machine Learning can support real-time fraud detection in ecommerce by analysing transaction amounts, timestamps, user locations, device information, IP addresses, and customer purchasing behaviour. These features can help identify suspicious activities and support faster transaction decisions compared with approaches that rely only on predefined rules.

Random Forest, XGBoost, and LightGBM provide alternative methods for detecting fraudulent transactions. Random Forest combines multiple decision trees, whereas XGBoost and LightGBM use gradient boosting techniques. Their performance depends on dataset characteristics, feature quality, model configuration, and computational requirements. Therefore, comparative evaluation is necessary to identify the most suitable algorithm for real-time fraud detection.

Table 5: Qualitative Comparison and Architectural Trade-Offs of Candidate Machine Learning Models.

Evaluation Dimension	Random Forest (RF)	XGBoost	LightGBM
Learning Paradigm	Bagging ensemble of unpruned parallel decision trees	Level-wise gradient boosting with 2nd-order Taylor expansion	Leaf-wise gradient boosting with GOSS sampling and EFB bundling
Training Latency & Load	Moderate; highly parallelizable across CPU cores	High; sequential tree growth requires careful tuning	Ultra-Low; histogram binning trains 5x–10x faster than XGBoost
Inference Latency Profile	Low (~20 ms to 45 ms per transaction)	Very Low (~15 ms to 30 ms per transaction)	Ultra-Low (~5 ms to 15 ms); optimal for sub-50ms gateway SLAs

Evaluation Dimension	Random Forest (RF)	XGBoost	LightGBM
High-Dimensional Sparsity	Good; robust via random feature sub-selection	Excellent; built-in sparsity-aware split finding	Outstanding; EFB natively bundles mutually exclusive features
Overfitting on Imbalanced Data	Very Low; bagging naturally reduces variance	Low; L1 and L2 regularization penalties constrain trees	Moderate; leaf-wise growth can overfit without max_depth limits
Model Interpretability	High; direct Gini impurity & permutation importance	Very High; native gain metrics & TreeSHAP support	High; split-gain metrics and accelerated TreeSHAP support
Production Gateway Suitability	High (Robust baseline for stable distributions)	Very High (Industry gold standard for tabular fraud)	Highest (Premier candidate for ultra-low latency streaming)

Several challenges must be considered, including imbalanced datasets, false-positive predictions, evolving fraud patterns, data privacy, and processing latency. Evaluation should consider precision, recall, F1-score, ROC-AUC, and processing latency to assess detection performance and operational suitability. Continuous monitoring and periodic model retraining may help the system adapt to new fraudulent behaviours.

Overall, the proposed framework provides a foundation for developing a Machine Learning-based fraud detection system for e-commerce platforms. Future work should focus on implementation, experimental evaluation, and comparison of candidate algorithms to determine their effectiveness in improving transaction security and reducing financial losses.

CONCLUSION

E-commerce fraud is a growing challenge due to the rapid increase in online transactions and the continuous evolution of fraudulent activities. Existing studies show that **machine learning techniques**, along with effective **data preprocessing, feature engineering, and class-imbalance handling**, can significantly improve fraud detection performance.

Based on the reviewed methodologies, the proposed approach combines **Random Forest, XGBoost, and LightGBM** to analyze transaction patterns and generate a **fraud probability/risk score**. This score can support decisions such as **approving low-risk transactions, requesting additional authentication for suspicious transactions, and blocking high-risk transactions**.

The system also incorporates **continuous monitoring and model retraining** to adapt to changing fraud patterns. Overall, the proposed methodology aims to provide **accurate, scalable, adaptive, and real-time e-commerce fraud detection** while reducing both missed fraud and unnecessary rejection of legitimate transactions.

REFERENCES:

1. M. Sánchez-Paniagua, E. Fidalgo, E. Alegre, and F. Jáñez-Martino, **"Fraud Detection in ECommerce: A Comparative Analysis of Features to Enhance Machine Learning Models,"** *Electronic Commerce Research*, vol. 26, pp. 2467–2502, 2026.
2. Sarwosri, B. Nuralamsyah, N. R. Kurniadi, A. R. Wahed, and S. Rochimah, **"E-Commerce Transaction Fraud Detection Using GNN-Based Feature Embedding and Machine Learning Methods,"** *IEEE Access*, vol. 14, pp. 84755–84771, 2026.
3. Gupta, S. Mishra, R. R. Kumar, S. Parija, and D. Muduli, **"A Machine Learning Approach for Credit Card Fraud Detection using Feature Engineering and Ensemble Models,"** *2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3)*, IEEE, 2025.
4. D. Jayalakshmi and N. Priya, **"Detection of Synthetic Fraud in E-Commerce Applications using Machine Learning Techniques – Survey,"** *Proceedings of the 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, 2025.
5. M. Vasant, S. Ganesan, and G. Kumar, **"Enhancing E-commerce Security: A Hybrid Machine Learning Approach to Fraud Detection,"** *FinTech and Sustainable Innovation*, vol. 1, Article A7, 2025.
6. B. Immanuel, M. Manikandan, P. Muthukumar, and A. Arikesh, **"E-Commerce Site Payment Fraud Detection using Machine Learning Technique,"** *2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT)*, IEEE, 2025.

7. A.Mutemi and F. Bação, "**E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review**," Big Data Mining and Analytics, vol. 7, no. 2, pp. 419–444, 2024.

8. G. Manoharan, S. D. N. H. Ali, M. Sathe, A. Karthik, A. Nagpal, and A. Sidana, **"Fraud Detection in E-Commerce Transactions: A Machine Learning Perspective,"** *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, IEEE, 2024.

9. R. Aggarwal, P. K. Sarangi, and A. K. Sahoo, **"Credit Card Fraud Detection: Analyzing the Performance of Four Machine Learning Models,"** *2023 International Conference on Disruptive Technologies (ICDT)*, IEEE, 2023.

10. Aditi, P. Garg, A. Dubey, and A. Mathur, **"Credit Card Fraud Detection Using Advanced Machine Learning Techniques,"** *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCiCT)*, IEEE, 2022.

11. A. K, M. M, A. K. Pani, and P. Kumar, **"An Approach for Detecting Frauds in E-Commerce Transactions using Machine Learning Techniques,"** *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, 2021.

12. N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, **"A Review of Credit Card Fraud Detection Using Machine Learning Techniques,"** *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, IEEE, 2020.

13. C. Chen, C. Liang, J. Lin, L. Wang, Z. Liu, X. Yang, J. Zhou, Y. Shuang, and Y. Qi, **"InfDetect: A Large Scale Graph-based Fraud Detection System for E-Commerce Insurance,"** *2019 IEEE International Conference on Big Data (Big Data)*, IEEE, 2019.

14. R. Jhangiani, D. Bein, and A. Verma, **"Machine Learning Pipeline for Fraud Detection and Prevention in E-Commerce Transactions,"** *2019 IEEE International Conference*, IEEE, 2019.

15. A. Saputra and Suharjito, **"Fraud Detection using Machine Learning in E-Commerce,"** *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 9, pp. 332–339, 2019.