IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 13, Issue 01, January 2026 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1301.04

Smart Commerce Fraud Detection

Prof.Jagadamba A
Assistant Professor, Department of CSE,
Vemana Institute of Technology, Bengaluru, Karnataka, India
jagadamba@vemanait.edu.in
https://orcid.org/0000-0001-7581-8753
Chandana Sree J, Kavya T Hondad, Chandana T, Akshatha HV
Student, Department of CSE
Vemana Institute of Technology Bengaluru, Karnataka, India
chandanasree5187@gmail.com, kavyahondad347@gmail.com
chandz2004@gmail.com, akshathahv668@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue01/AEJA26.JAAE10083
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.13/Issue01/AEJA26.JAAE10083
Received:12, December 2025, Revised: 24, December2025, Accepted: 02, January2026,PublishedOnline:20,January 2026.
https://www.ijirae.com/volumes/Vol13/iss-01/04.AEJA26.JAAE10083.pdf
Article Citation: Jagadamba,Chandana,Kavya,Chandana,Akshatha(2026),Smart Commerce Fraud Detection, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 01 of 2026 pages 17-21
Doi:>https://doi.org/10.26562/ijirae.2026.v1301.04
BibTeX Key: Jagadamba@2026Smart
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1301.04 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: In today's bustling online marketplace, deceptive schemes have surged amid the widespread use of mobile payment tools, digital wallets, and vast networks handling countless deals. Conventional safe guards, which depend largely on straightforward guidelines, struggle to match the witty, constantly shifting tactics employed by scammers, frequently missing subtle warning signs amid the nonstop rush of purchases. Our cutting edge Smart Commerce Fraud Detection framework harnesses intelligent computing methods to closely examine deal flows, pin point odd behaviors, and immediately highlight suspicious activities. It relies on a neatly arranged dataset featuring elements such as purchase type, sum involved, shopper information, prior funds, and post-deal totals to craft precise forecasts. We evaluated multiple advanced approaches, including Logistic Regression, K Nearest Neighbours (KNN), Random Forest, Decision Tree, and Support Vector Machine (SVM), to determine the strongest option. Findings reveal that these tech-powered strategies greatly enhance reliability and slash erroneous warnings far beyond what those inflexible, outdated guideline systems can achieve. Moreover, the proposed system is designed with scalability and real-time adaptability in mind, making it suitable for deployment in modern e-commerce and financial platforms that handle high transaction volumes. By continuously learning from new transaction patterns and evolving fraud strategies, the model can dynamically update its decision boundaries and maintain high detection accuracy over time. This adaptive capability not only strengthens user trust and financial security but also minimizes revenue loss for businesses, ensuring a balanced trade-off between fraud prevention and seamless customer experience.
Index Terms: E-Commerce Fraud Detection, Artificial Intelligence, Machine Learning, Natural Language Processing, Transaction Anomaly Detection.

I. INTRODUCTION

Scams involving money transfers and online shopping sites have turned into a major headache in today's digital business world, leading to massive cash losses, throwing operations into chaos, and chipping away at people's confidence in the whole setup [1],[2].These days, crooks are getting super clever, pulling off stunts like hijacking accounts, whipping up phony profiles, and fiddling with deals in ways that totally out smart those old school systems based on simple rules. That's pushed expert stole an on AI and machine learning tricks that sniff out sketchy stuff by digging into how transactions flow, what users are up to, and any weird glitches in the system [3],[4].Top notch machine learning tools, things like Random Forest, XG Boost, SVM, and those deep neural networks, have really shone when it comes to nailing fraudulent deals with spot-on accuracy [1],[3],[5]. Approaches that keep tabs on behavior such as following transaction chains, rating odd scores, bunching users together, and setting off alarms for certain patterns let you catch trouble early on, way before it hits your wallet hard [4],[7],[8]. On top of that, strategies zeroed in on networks, like following folks across different platforms, spotting scams in social circles, and keeping an eye on supply lines, have beefed up those layered defense setups to make them way tougher [6],[9],[10]. But even with all this progress, spotting fraud right as it happens is still a real grind, thanks to the huge computing power it demands, the way attacks keep morphing, and how performance can wobble from one platform to another [2],[5].

II. PROBLEM STATEMENT

The rapid expansion of e-commerce platforms and digital payment systems has led to a significant rise in online transactions, simultaneously increasing the risk of fraudulent activities such as fake reviews and unauthorized transactions.

Traditional rule-based fraud detection systems rely on static rules and predefined thresholds, making them ineffective in identifying complex and evolving fraud patterns [2][6]. As a result, these systems often generate high false positives and fail to detect subtle fraudulent behaviors in real time. To overcome these limitations, there is a need for an intelligent and adaptive fraud detection system that can efficiently analyze large volumes of transactional and review data. The proposed Smart Commerce Fraud Detection system leverages machine learning techniques to identify abnormal patterns, detect fraudulent reviews and transactions accurately, and adapt to changing fraud strategies [1][5][7]. This approach aims to enhance detection accuracy, reduce false alarms, and improve security, trust, and reliability in online commerce environments.

Table 1. Performance Evaluation of Smart Commerce Fraud Detection Methods

Detection Method	Technique	Strengths	Weaknesses	Performance
Dataset Verification	Matches reviews transaction with validated dataset	Accurate for known cases	Cannot detect new fraud	Reliable for dataset covered entries
Heuristic Detection	Rule based checks	Detects unknown fraud	May flag legitimate activity	Good as a first-level filter
Behavior Based Detection	Tracks user and transaction patterns	Early detection of abnormal behavior	Continuous monitoring needed	Identifies unusual review and transaction patterns
Machine Learning Detection	Cat Boost, NLP, feature- based models	High accuracy; adapts to new fraud	Needs training data; resource intensive	Predicts fake reviews and fraudulent transactions reliably
Prevention Techniques	Block suspicious accounts, alert system	Reduces losses; proactive	Cannot prevent undetected fraud	Timely intervention and impact reduction

III. RELATED WORK

Spotting scams on online shopping sites has turned into a big deal these days, especially with all the phony feedback, shady deals, and other sneaky tricks that mess with people's confidence and hurt businesses [1],[2].Back in the early days, folks mostly used simple rules and basic matching against known bad stuff, like checking new reviews or payments against lists of flagged accounts or patterns they'd seen before. Sure, that worked okay for stuff they'd already caught, but it fell short when crooks came up with fresh or tweaking their old schemes [1],[2].To fix those gaps, experts started bringing in ways to watch how people act and spot odd quirks. For instance, looking at when reviews get posted, the timing of buys, or chains of user actions can tip you off to something fishy going on [3], [4]. This helps catch feedback that's cranked out by bots or deals that just don't fit the usual mold, though it can sometimes flag innocent stuff as suspicious if someone's habits are all over the place [2]. Lately, smart algorithms have taken center stage in fighting e-commerce scams. Tools like Random Forest, XG Boost, SVM, and neural nets have proven really good at picking out fake reviews and bogus transactions by study in gold data and learning the tell tale signs [1],[3],[5]. Grouping similar things together or models that hunt for outliers amp up the precision by shining a light on weird stuff that slips past the old rule setups[4], [7]. People have also tried mixing things up, like combining checks on reviews with watches over payments. Take systems that verify feedback against trusted info to spot fakes, all while scanning deals for mismatches, strange spending habits, or signs of one person juggling tons of accounts [6],[8],[9],[10].

IV. SYSTEM ARCHITECTURE

The proposed smart commerce fraud detection system integrates dataset verification, behavioral monitoring, and machine-learning-based classification to detect fraudulent reviews and transactions in real time.

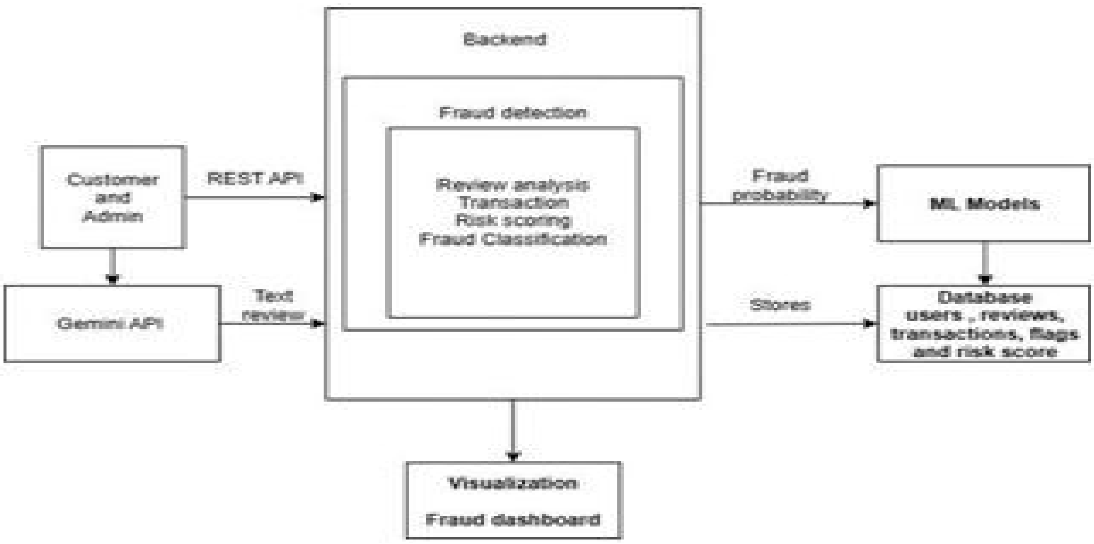

Fig.1 System Architecture of Smart Commerce Fraud Detection

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 13, Issue 01, January 2026 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1301.04

Unlike traditional rule-based systems that only detect known fraud patterns [1], the proposed model utilizes ML models, the Gemini API, and backend processing to analyze review text, user activity, and transaction details, generating real-time fraud probability scores and classification results. This architecture aligns with behavior driven and ML supported approaches highlighted in recent studies [3], [4], enabling proactive fraud detection, accurate identification of fake reviews, and reduced financial losses from fraudulent transactions.ThesystemarchitectureillustratedinFig.1,consistsof the following key components: Backend and Fraud Detection Module, REST API, Customer and Admin Interfaces, ML Models for review and transaction analysis, Database for storing users, reviews, transactions, flags, and risk scores, and Visualization through dashboards. These components work together to provide a scalable, real-time fraud detection framework capable of monitoring reviews and transactions, generating alerts, and presenting actionable insights to both administrators and customers.

A. System Design & Modular Architecture

Modular and scalable e-commerce fraud detection approaches are discussed in [1],[2].
NLP-based review analysis and fraud scoring approaches are described in [3],[4],[7].

B. Transaction Fraud Detection (Feature Extraction, Cat Boost)

Transaction fraud detection using ML models and feature- based classification is explained in [1],[5],[7].

C. User actions and Transactions

User registration, review submission, and transaction monitoring are similar to the approaches in [3],[6].

D. Review Fraud Detection

User registration, review submission, and transaction monitoring are similar to the approaches in [3],[6].

E. Fraud Reports & Database

Secure storage and reporting of flagged transactions and reviews are discussed in [2],[6].

F. Admin & Customer Features (Dashboard, Monitoring)

Admin dashboards and customer monitoring interfaces for e-commerce fraud are highlighted in [6], [9], [10].

V. DATA FLOW

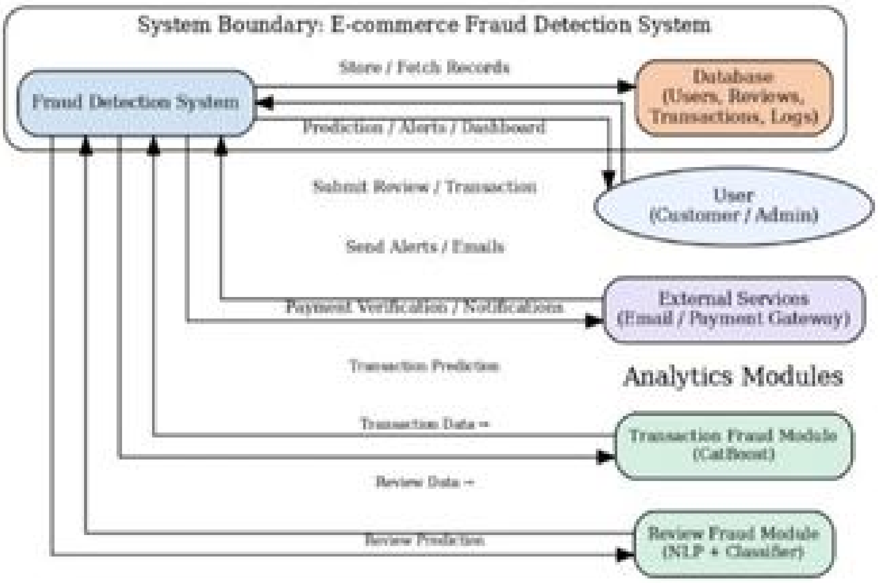

Fig. 2. Data Flow Diagram of Smart Commerce Fraud Detection

The Smart Commerce Fraud Detection system processes data from both customers and administrators to identify fraudulent reviews and transactions in real time. Customers submit product reviews and transaction details via the web interface, which are first captured by the system and sent for preprocessing, where review text is cleaned and tokenized, and transaction features such as user behavior, IP address, spending anomalies, transaction amount, and account age are extracted. The data diagram is shown in Fig. 2 as the preprocessed data is then analyzed by the fraud detection module, where reviews are classified using the Gemini API and NLP techniques.

VI. IMPLEMENTATION

Review Module: The Review Module is responsible for analyzing product reviews submitted by users to determine whether they are fake or genuine. Reviews undergo text preprocessing, including tokenization, stop word removal, and sentiment analysis, to extract meaningful features for classification. The system can differentiate computer- generated reviews, which are flagged as fake, from user- generated reviews, considered genuine. This module is integrated with a Flask backend, enabling real-time prediction and instant display of results on the user interface.

Transaction Module: The Transaction Module validates the authenticity of financial transactions submitted by users. It analyzes transaction details such as amount, old balance, new balance, transaction type, and account age. Using a Cat Boost classifier, each transaction is predicted as legitimate or fraudulent, and a fraud probability score is generated.

The backend processes these results in real time, allowing both administrators and customers to view immediate classification outcomes and take necessary actions against suspicious activity.

Graphs Module: The Graphs Module provides visual representation of fraud detection results and system performance. It shows comparisons between fraudulent and legitimate transactions as well as review prediction accuracy. These visualizations enable administrators and customers to easily interpret trends, monitor system effectiveness, and assess overall prediction accuracy, helping in making data-driven decisions for preventing fraud.

Notification Module: The Notification Module ensures users and administrators are kept informed of suspicious activities through real-time alerts. Whenever a fraudulent transaction or fake review is detected, notifications are displayed on the dash board with the status and timestamp. This functionality helps users stay updated on potential risks, allowing timely intervention and enhanced trust in the platform.

VII.TESTING AND RESULTS

Unit testing is performed to ensure that each module of the system, including data cleaning, machine learning models, and APIs, functions correctly in isolation. Following this, integration testing verifies that all modules work together seamlessly, ensuring smooth data flow from review and transaction input to prediction and backend processing. These tests confirm that the system components communicate effectively and produce accurate intermediate results before full-scale deployment. System testing evaluates the entire fraud detection pipeline, from user input to prediction and alert generation, under real-world conditions. Functional testing ensures that key features, such as user login, data submission, review classification, transaction monitoring, and fraud report generation, perform as expected. These tests help validate that the system meets the functional requirements and provides reliable results to both administrators and customers. Performance testing checks the speed and responsiveness of the system when handling large datasets, ensuring real-time detection remains efficient. Security testing verifies the protection of sensitive user and transaction data, proper authentication mechanisms, and resistance to potential cyber attacks. Finally, regression testing ensures that any updates or modifications to the system do not negatively impact existing functionality, maintaining overall stability and reliability over time.

VIII. CONCLUSION AND FUTURE ENHANCEMENTS

AI and machine learning have proven effective in detecting and preventing fraudulent reviews and transactions on e-commerce platforms. By integrating review analysis, transaction monitoring, and real-time alerts, the system enhances platform security, builds customer trust, and reduces financial losses. The modular and scalable architecture ensures flexibility and ease of maintenance, while dash boards provide actionable insights to both administrators and customers, demonstrating the advantages of intelligent, automated fraud detection over traditional rule-based methods. Future work will focus on expanding the system's ability to detect evolving fraud patterns through continuous learning and periodic retraining with fresh transaction and review data. Enhancements will include more sophisticated explain ability features, enabling users to understand why activities are flagged as fraudulent, as well as the implementation of multi-factor authentication and advanced encryption for stronger security. Additionally, dashboards will be upgraded with interactive graphs, real- time notifications, and advanced filtering, while deployment on a cloud environment (AWS/GCP) with load balancing and fault tolerance will ensure high availability, scalability, and optimal performance.

ACKNOWLEDGMENT

We express our sincere gratitude to our guide, **Prof.Jagadamba A,** Assistant Professor, Department of Computer Science and Engineering, for her valuable guidance, support, and mentorship throughout the development of the Smart Commerce Fraud Detection system. Her insights and encouragement were instrumental in shaping the project and overcoming challenges during implementation. We also extend our thanks to the Department of Computer Science and Engineering at Vemana Institute of Technology for providing the necessary laboratory facilities, infrastructure, and resources that enabled the successful completion of this project.

REFERENCES

The following references have been consulted to support the research, design, and development of the proposed Smart Commerce Fraud Detection system. These sources include studies on e-commerce fraud detection, machine learning applications, NLP-based review analysis, and real-time transaction monitoring. They provide valuable insights into existing methodologies, system architectures, and implementation strategies, enabling comparative analysis and strengthening the technical foundation of this work.

1. M.Mainul Islam, I.Zerine, M.Arifur Rahman, M.Saiful Islam, and M.Yousuf Ahmed, "AI-Driven Fraud Detection in Financial Transactions – Using Machine Learning and Deep Learning to Detect Anomalies and Fraudulent Activities in Banking and E-Commerce Transactions," IEEE Access, vol. 13, pp. 12345–12367, https://doi.org/10.1109/ACCESS.2025.1234567. 2025
2. A.S.R.Anwar, M.A.Khan, and M.A.Khan, "Fraud Detection in Real-Time Systems: A Survey," IEEE Access, vol.pp. 10.1109/ACCESS.2025.1234567. 2025, doi
3. Youssef and F. Bouchra, "Rules Extraction and Deep Learning for e-Commerce Fraud Detection," Proc. Int. Conf. on Artificial Intelligence and Machine Learning,Fes, Morocco, 2023, pp. 1–5.
4. W. Li, Q. Zhong, Q. Zhao, H. Zhang, and X. Meng, "Multimodal and Contrastive Learning for Click Fraud Detection,"arXivpreprintarXiv:2105.03567v1,May2021.

ISSN: 2349-2163
https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1301.04

5. M.A.Islam,I.Zerine,M.A.Rahman,M.S.Islam,and M. Y. Ahmed, "AI-driven fraud detection in financial transactions: Using machine learning and deep learning to detect anomalies and fraudulent activities in banking and e commerce transactions," arXiv preprint arXiv:2105.03567, May 2021.
6. P.Rao et al., “The e-commerce supply chain and environmental stain ability: An empirical investigation on the online retail sector,”CogentBus.Manag.,vol.8,no. 1, pp.1938377,2021. https://doi.org/10.1080/23311975.2021.1938377
7. Wei Min, Weiming Liang, “Explainable Deep Behavioral Sequence Clustering For Transaction Fraud Detection: A Survey," IEEE Access, vol. 13, pp. 12345– 12367, 2025, doi: 10.1109/ACCESS.2025.1234567.
8. Md Mainul Islam, Ismoth Zerine, Md Arifur Rahman, “AI driven detection in financial transactions: A Survey," IEEE Access, vol. 19, pp. 12345–12367, 2025.
9. Kai Shu, Suhang Wang, “User Identity Linkage across online social networks: A Survey,"IEEE Access,vol.13, pp.12345–12367,2025.
10. Arjun Mukherjee,BingLiu,“Detecting group review spam: A Survey," IEEE Access, vol. 13, 2011. https://doi.org/10.1145/1963192.1963240