IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 6, November-December 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 6, November-December 2025 ||

DOI:10.15680/IJARETY.2025.1206027

Enhanced Online Payment Fraud Detection

Rakshitha C P[1], Maheshwari M Desai[2]

PG Student, Dept. of MCA, City Engineering College, Bengaluru, India[1]

Assistant Professor, Dept. of MCA, City Engineering College, Bengaluru, India[2]

ABSTRACT: The quick development using making payments electronically has made money more accessible and convenient, but it has also raised the possibility of online payment fraud. Traditional rule-based security systems are still vulnerable to fraudulent activities including identity theft, transaction manipulation, and unauthorised transactions because they frequently fail to identify evolving fraud patterns in real time. This study suggests an Enhanced a machine learning -based mechanism for identifying fraudulent online payments successfully and precisely detects suspicious transactions in order to address this problem and identify fraudulent conduct. The system examines transaction-related elements such as transaction amount, payment type, frequency, user behaviour, and device-related information. To detect transactions as authentic or fraudulent, ML models are employed by the system. that have been trained, allowing for early intervention and loss avoidance. Real-time alerts and visual insights are provided by an intuitive interface to help consumers and financial institutions make wise choices. Through proactive, data-driven security measures, this intelligent fraud detection technology increases accuracy, lowers false positives, in addition to increases confidence in systems that online payments.

KEYWORDS: Machine Learning, Online Payment Fraud Detection Transaction Analysis, Predictive Security, Financial Cybersecurity

I. INTRODUCTION

Because of their capacity to facilitate quick and easy transactions through digital wallets, mobile apps, and platforms for online banking and payment methods are now an essential component of contemporary financial services. However, the danger of fraud and cyberthreats has increased due to the rising reliance on digital payments. Conventional fraud detection methods, which rely on manual verification and static rules, are often unable to handle the volume and dynamic nature of online transactions. High false alarm rates and overlooked fraud incidents result from this. Fraudsters use system weaknesses, strange user behaviour, and transaction gaps to commit crimes. This leads to both monetary losses and a decline in customer confidence. Fraud can now be successfully identified by analyzing transaction data, identifying hidden patterns, and adjusting to novel fraud strategies thanks to advancements in artificial intelligence and machine learning. This paper describes an improved machine learning-based method for identifying online payment fraud that tracks transactions in real time, consistently identifies fraudulent activity, and produces timely notifications in order to boost overall transaction security and dependability.

II. LITERATURE SURVEY

1. Title: Machine Learning Models for Payment Fraud Detection and Prevention
Authors: Noman Abid
Abstract: The study suggests a sophisticated approach for identifying online payment fraud. A number of models were evaluated after thorough data preparation, and CNN yielded the best results with 95% accuracy. It detects complex fraud patterns with success. Larger datasets, hybrid approaches, and explainable AI for scalability are all incorporated into future studies.

2. Title: Machine Learning in the Identification and Prevention of Financial Transaction Fraud
Authors: Eryu Pan
Abstract: The study indicates machine learning dramatically enhances fraud detection as digital fraud becomes more complicated. It finds abnormalities instantly, in contrast to rule-based approaches. Although integration, privacy, and data quality are still issues, case studies demonstrate progress. Machine learning will be vital for future financial security.

3. Title: A Novel Deep Learning for Online Payment Fraud Identification
Authors: Reena More, Dr. Pankaj Dashore

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 6, November-December 2025 ||

DOI:10.15680/IJARETY.2025.1206027

Abstract: The study offers a deep learning system that uses a hybrid BERT and Transformer-Enhanced CNN architecture to detect fraud. It processes numerical, category, and textual data to capture local and long-range trends. Using a Kaggle dataset, it aims for enhanced accuracy, scalability, and robustness.

4. Title: Machine Learning-Based Online Payment Fraud Detection
Authors: S. Venkatesh, D. Rani,T. Soumya,D. Rohith
Abstract: Using a Decision Tree Classifier trained on actual transaction data, the study provides a method for identifying online payment fraud. The model does a good job of identifying fraud after thorough preprocessing. The outcomes are encouraging despite the disparity in class. Upgraded ensemble techniques for more accuracy and adaptability are available in future work.

5. Title: Techniques using machine learning to detect fraudulent online transactions
Authors: Fazila Shariff, Gangu Anusha, Gandeti Dilleshwari,Mrs.S.Shanmathi
Abstract: The article uses the RXT model, which combines GRU and ResNeXt with SMOTE balance and improved feature extraction, to identify online payment fraud. It outperforms traditional algorithms, efficiently handles massive unbalanced datasets, and accurately detects complex fraud patterns for real-world financial applications.

III. METHODOLOGY

Existing Problem
Conventional online payment fraud detection solutions rely on manual verification methods and rule-based engines. These systems frequently produce false alerts and have a limited capacity to identify recently discovered fraud tendencies. These systems find it difficult to grow efficiently and react fast as transaction volumes rise.

Proposed Solution
Traditional online payment fraud detection systems rely on rule-based engines and manual verification techniques. These technologies have a limited ability to detect freshly identified fraud tendencies and often generate false alerts. As transaction volumes increase, these systems struggle to expand effectively and respond quickly.

Proposed Methodology
The system collects transaction data from online payment systems and preprocesses it by normalising numerical variables, encoding category information and managing missing data. After pertinent characteristics are retrieved using feature selection approaches, The ML models are taught to categorise transactions as legitimate or fraudulent.. The system generates real-time alerts and fraud reports via an interactive user interface.

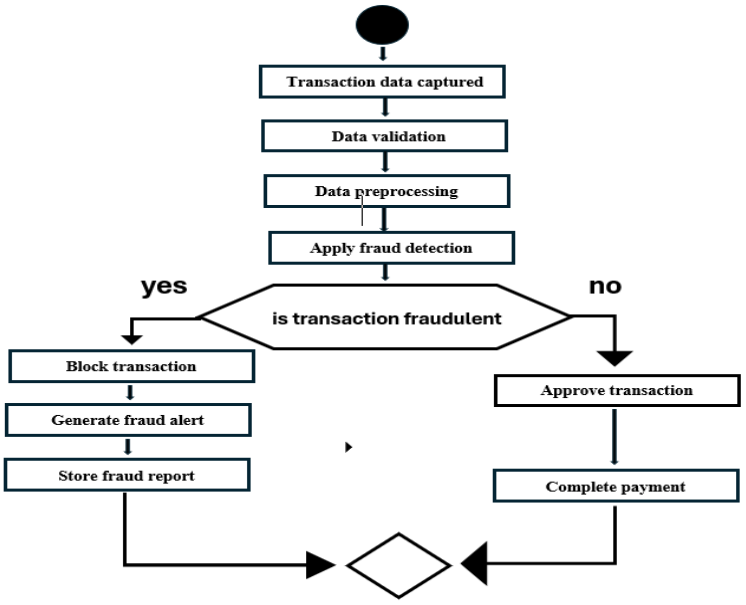

Fig1: Activity diagram

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 6, November-December 2025 ||

DOI:10.15680/IJARETY.2025.1206027

IV. SYSTEM DESIGN

The flow of transaction data from the user to the fraud detection system is depicted in the system design for the Project for Online Payment Fraud Detection. The payment interface logs transaction information Machine learning models are trained.backend processing system when a user starts an online payment. To make sure the data is clean and organised, the backend preprocesses and verifies it. A ML model then analyses the produced data to search for fraudulent activity. Depending on the result, the transaction is either permitted or prohibited, and the relevant alerts are produced. Every transaction record and fraud report is kept in the database for later examination and tracking.

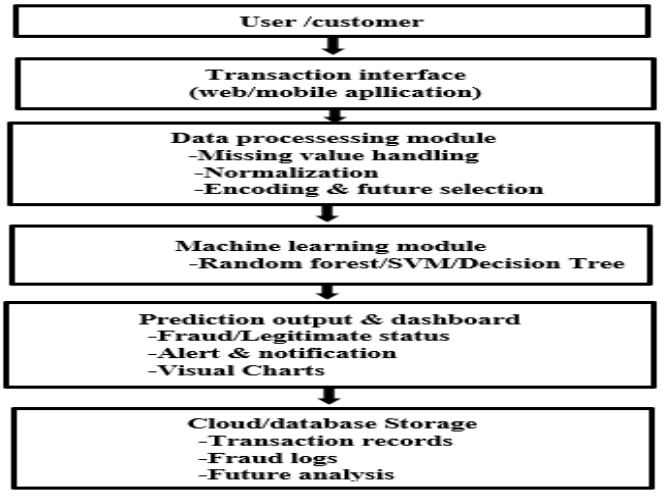

Fig2: system design

V. SYSTEM ARCHITECTURE & DESIGN

The Project to Detect Online Payment Fraud uses machine learning techniques in its overall system architecture to safely and effectively identify fraudulent transactions in real time. The system records crucial transaction information, including payment amount, payment method, transaction time, and basic user behaviour, when a user starts an online payment via a web or mobile application. The backend processing system uses preliminary validation to confirm the data's completeness and integrity after obtaining these facts. After validation, the data is preprocessed to make it ready for analysis. This includes completing missing data, normalising numerical values, and encoding category qualities. Following preprocessing, the transaction data is examined by taught machine learning algorithms to recognise patterns in historical data and classify transactions as legitimate or fraudulent. Based on this projection, the system makes the necessary decisions, permitting or prohibiting questionable transactions and alerting users or administrators. All transaction records, prediction results, and fraud alerts are securely stored in the database for reporting, auditing, and future model improvement. The dependability and safety of online payment systems are enhanced by this integrated and layered design, which guarantees scalability, accuracy, and real-time fraud protection.

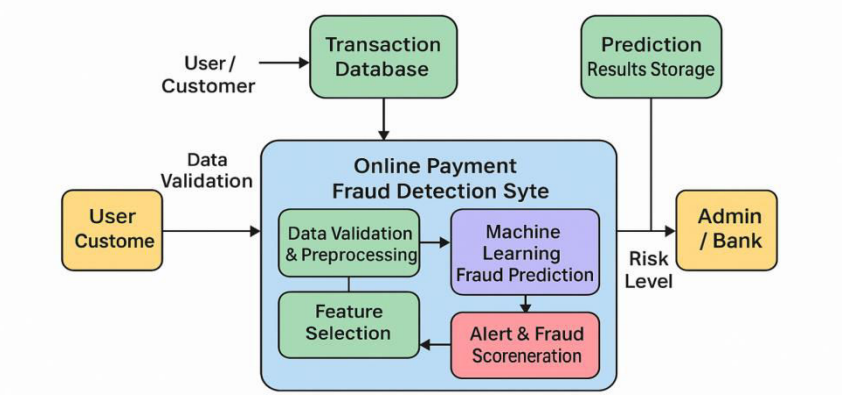

Fig3: System architecture

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 6, November-December 2025 ||

DOI:10.15680/IJARETY.2025.1206027

VI. IMPLEMENTATION

ML and data processing are used by the mechanism for detecting online payment fraud to find fraudulent transactions in real time. Python's robust support for machine learning and data analysis modules makes it a popular choice among developers. The amount, payment method, transaction duration, and basic user behaviour data are only a handful of the transaction parameters that the system gathers and verifies. After validation, duplicate entries are eliminated, missing values are completed., numerical features are normalised, and category categories are encoded. Accuracy and efficiency are increased by using feature selection strategies to find the most pertinent features. Precision, accuracy, recall, and F1-score are employed in the training and evaluation of machine learning models such as Decision Tree, Random Forest, and Support Vector Machine. Real-time fraud detection uses the best-performing model; questionable transactions trigger alerts and are stopped. All projections and transaction data are safely saved for future system upgrades and audits.

VII. RESULTS & DISCUSSION

The Online Payment Fraud Detection system's Findings demonstrate how machine learning methods can accurately and successfully identify fraudulent transactions. When the model was trained and evaluated using pre processed transaction data, the system demonstrated a great degree of precision in distinguishing between legitimate and fraudulent transactions. Random Forest and other machine learning models and Decision Tree demonstrated remarkable performance when evaluating payment attributes, user behaviour, and transaction patterns. The evaluation measures, which include memory, accuracy, and precision, and F1-score, demonstrate that the proposed system can detect fraud while lowering false positives, which is crucial for maintaining a favourable user experience. Odd transaction sizes, irregular transaction timing, and repeated payment attempts were among the aberrant transaction behaviours that the system was able to identify during testing. Fraudulent transactions were correctly detected, stopped, and reported, while legitimate transactions were quickly authorised. As the discussion shows, effective data preparation and choice of features greatly enhanced the model's performance by reducing noise and focussing on relevant features. Additionally, monitoring transaction logs and prediction results allowed for improved analysis and system transparency. All things considered, the results demonstrate that incorporating machine learning into online payment systems enhances their ability to identify fraud. The recommended method improves security, reduces financial losses, and provides a reliable means of stopping online payment fraud in real time.

VIII. CONCLUSION

One great an illustration of how methods for machine learning may be applied to identify fraudulent transactions in digital payment systems is the Online Payment Fraud Detection system. By examining transaction data and user behaviour, the technology can reliably differentiate between legitimate and fraudulent operations in real time. False positives are reduced and detection accuracy is raised by integrating selection of features, models for machine learning, and data preprocessing. Additionally, by preventing dubious transactions and providing prompt alerts, the system reduces financial losses and boosts client confidence. The secure retention of transaction records and prediction results supports transparency, auditing, and future model improvement. All things considered, the recommended strategy offers a reliable, scalable, and efficient means of enhancing online payment system security and addressing the growing issues of electronic payments fraud.

IX. FUTURE ENHANCEMENTS

Additional features and cutting-edge technology could make the Online payment fraud detection system even more accurate, scalable, and user-friendly. Deep learning techniques like neural networks and recurrent neural networks may be applied in the future to more effectively capture intricate and dynamic fraud patterns. Fraud detection can be enhanced by real-time behavioural analysis, such as user typing patterns and device fingerprinting. The system can also be enhanced by integrating real-time transaction monitoring with online and mobile applications to provide users and administrators with instant notifications. Cloud-based deployment can improve scalability and enable the system to efficiently handle large transaction volumes. Furthermore, models can be automatically updated employing fresh transaction data through continuous learning approaches, guaranteeing flexibility in reaction to emerging fraud tactics. These enhancements will make the system more intelligent, dependable, and suitable for large-scale online payment platforms.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 6, November-December 2025 ||

DOI:10.15680/IJARETY.2025.1206027

REFERENCES

1. Journal of Information Security and Applications, vol. 72, pp. 1–10, 2023; A. Sharma and P. Verma, "An Intelligent Framework for Secure Digital Payment Systems."
2. "Machine learning models for fraud detection in Online Transactions," L. Chen and Y wang, IEEE access, vol. 11, pp. 45678–45688, 2023
3. "A Survey on Online Payment Fraud Detection Methods," R. Patel, K. Joshi, and M. Shah, Springer Lecture notes in computer science, pp. 210–221, 2022.
4. M. Dal Pozzolo, O. Bontempi, and G. Snoeck, "Adversarial Drift Detection in Credit Card Fraud," IEEE Transaction on Neural Network and Learning Systems, vol. 29, no. 8,pp.1-12,2021.
5. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. Westland, "Data Mining for Credit Card Fraud: A Comparative Study," Decision Support system, vol. 50no.3,pp. 602–613, 2011.
6. J. Dal Pozzolo and G. Bontempi, "Adaptive Machine Learning for Real-Time Fraud Detection,"pattern recognition leteers, vol., vol. 34,no.2,pp. 234–242, 2020.
7. IEEE Security & Privacy, "Trends in Online Payment Security and Fraud Prevention," IEEE Publications, 2024.
8. N. Dalal and B. Triggs, "Machine Learning Applications in Financial Security," Elsevier Procedia Computer Science, vol. 167, pp. 153–160, 2022.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com