INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1341-1346

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

# REAL-TIME FRAUD DETECTION IN ONLINE PAYMENTS: A COMPREHENSIVE REVIEW OF MACHINE LEARNING TECHNIQUES

**Navaneetha Talari[1], M. Geetha[2], Bellamkonda Nuthana[3], Remalli Rohan[4]**

[1]M. Sc-Data Science – PG Student, Department of Computer Science Telangana Social Welfare Residential Degree College for Women, Jagathgirigutta, Hyderabad, India.

[2,3]Degree Lecturer, Department of Computer Science Telangana Social Welfare Residential Degree College for Women, Jagathgirigutta, Hyderabad, India

[4]Researcher Computer Science Educator, Hyderabad, Telangana, India.

DOI: https://www.doi.org/10.58257/IJPREMS37828

## ABSTRACT

In the face of increasing cyberthreats, this report highlights the vital role that online payment fraud detection systems play in protecting digital transactions by providing a comprehensive analysis of current systems. The sophistication of fraud schemes targeting businesses and individuals is increasing along with the growth of online commerce. Focusing on cutting-edge techniques like machine learning, pattern recognition, and anomaly detection, the study examines the goals and tactics that facilitate efficient fraud detection. Analyzing transaction data in real time is essential for spotting fraud before it causes significant losses. These systems strengthen online transaction security, increase consumer trust, and safeguard financial assets by using sophisticated algorithms to examine large amounts of transaction data for anomalies that could point to fraud. The report tackles the need for robust solutions that change with new threats by highlighting flexible fraud detection systems. It lists the prerequisites for efficient systems and highlights how crucial they are to spotting, stopping, and reducing different types of online fraud, such as identity theft and illegal transactions, while promoting constant technological development to guarantee safe, reliable online trade.

**Keywords:** Online Payment Fraud, Machine Learning, Fraud Detection, Digital Payments, Cybersecurity.

## 1. INTRODUCTION

Digital payments are being adopted so quickly, particularly through the Unified Payments Interface (UPI), online payment fraud has significantly increased in India over the last five years. The percentage of fraudulent digital transactions in India has skyrocketed, rising from roughly 1.1% of all transactions in FY 2023 to 10.4% in FY 2024 as shown in figure 1. This spike is mostly the result of India's rapid digital transformation, which has increased financial inclusion but also created new fraud opportunities because of low financial literacy and frequently inadequate security measures by financial institutions that prioritized quick expansion. The Reserve Bank of India (RBI) has started public awareness efforts about safe digital payment methods in order to allay these worries. Combating the complexity of fraudsters who take advantage of digital financial growth is the goal of these activities. This line graph, which shows the percentage of online payment fraud reported in India during the last five fiscal years, shows a notable increase in the number of fraudulent transactions that were found. The data shows a notable rise, especially in the last several years, which is indicative of the escalating threat and improved detection capabilities.

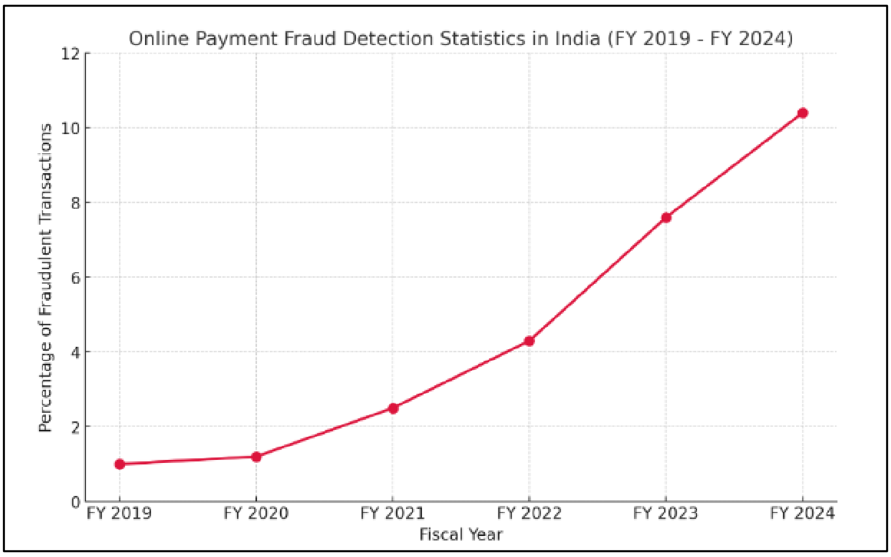

**Fig.1:** Online payment fraud detection statistics in India (FY 2019 - FY2023)

The swift growth of digital transactions has drastically changed the commercial landscape, providing consumers with unmatched ease while also increasing the risk of credit card fraud. Effective fraud detection strategies are desperately needed in light of this changing threat, especially when it comes to the use of machine learning (ML) techniques. 2019 was a turning point in this field as researchers showed how effective different machine learning algorithms are at spotting fraudulent activity. Most lately, studies in 2023 have kept looking into creative ways to identify fraud as shown in figure 2. To improve the dependability and effectiveness of fraud detection systems in real-time settings, researchers have been looking at the use of deep learning architectures, ensemble approaches, and innovative pre-processing techniques.

**Fig.2:** Online payment fraud

All things considered, this collection of work demonstrates a determined attempt to develop and improve fraud detection methods, utilizing a combination of cutting-edge neural networks and conventional machine learning algorithms to counteract increasingly complex fraudulent activity in financial transactions.

## 2. LITERATURE SURVEY

The literature review examines the latest developments in online payment fraud detection, with an emphasis on hybrid models, anomaly detection strategies, and machine learning approaches. Research highlights the efficiency of different algorithms and methods in accurately detecting fraudulent transactions. Understanding the changing field of fraud detection and the present difficulties in online payment security is made easier with the help of this overview in the table-1. Researchers are investigating a variety of machine learning (ML) techniques for fraud detection as a result of the growing concern over fraudulent activities, particularly in financial transactions. Niveditha et al. [1] used the Random Forest method to find anomalies in typical transaction patterns in order to detect credit card fraud. They obtained an amazing 98.6% detection accuracy using data balancing techniques like SMOTE, although some valid transactions were still incorrectly classified. Using ensemble learning, Gupta et al. [7] integrated many machine learning algorithms to improve fraud detection performance, highlighting the significance of resolving class imbalance for more trustworthy outcomes.

**Table.1:** Summary of methodologies

| Author | Data Set | Feature Extraction | Algorithms | Results |
|---|---|---|---|---|
| Justin M. et al. [5] | Medicare claims data | Addressed class imbalance | Neural networks, various sampling techniques | Improved detection rates, AUC 0.8505 to 0.8509 with ROS and ROS-RUS |
| Kumar et al. [7] | Transaction data with time and amount | Transaction time, amount, customer ID | Logistic Regression, Naive Bayes, Decision Tree, ANN | 98.69% accuracy (ANN) |
| Awhad et al. [10] | Facial image data for fraud verification | Convolutional Neural Network for facial features | Convolutional Neural Network (CNN), SVM | Effective in distinguishing real vs. fake images |

| | | | | |
|---|---|---|---|---|
| Alenzi and Aljehane et al. [11] | Noisy, imbalanced transaction data | Mean-based and clustering-based methods | Logistic Regression | Higher accuracy, sensitivity, and lower error rate |
| Yang et al. [6] | Proprietary transaction dataset | Statistical analysis of transaction features | Artificial Neural Network (ANN) | 98.69% |
| Gopinath et al. [13] | Kaggle dataset with 284,808 transactions | Historical transaction data | Random Forest, Logistic Regression, Decision Trees | Effective in identifying fraud; accuracy not explicitly stated, but strong performance noted. |
| Li et al. [15] | Real and synthetic datasets | Parameter optimization using cuckoo search | Optimized Support Vector Machine (CS-SVM) | Achieved accuracy of 98%; outperformed traditional methods. |
| Jianglin Xia [22] | Kaggle credit card transactions | AUC, F1-score metrics | Support Vector Machine (SVM) | Training AUC: 0.87, Testing AUC: 0.90 |
| Shalini Avinashbhai Naik et al. [24] | Unspecified dataset of credit card transactions | Parameter optimization | Decision Trees, Support Vector Machines, Logistic Regression | Training F-score: 0.305, Testing F-score: 0.260 |
| Choudhary, T. et al. [27] | PhishTank, UCI Dataset | URL features extraction | Random Forest, Decision Tree, Logistic Regression, SVM | RF: 98.80% (PhishTank), 97.87% (UCI) |
| Dai, M. [28] | Synthetic dataset | One-hot encoding | Support Vector Machine, Logistic Regression, Decision Tree | Decision Tree achieved best performance |
| Gaide, K. [29] | Data on online fraud cases from Latvian police. | General fraud detection techniques. | General fraud detection techniques. | Highlights lack of cyber hygiene as a major factor in fraud. |
| Kumar, V et al [31] | User-submitted credit card data | Analysis of transaction features | XG-Boost, Random Forest | Highest performance by XG-Boost and Random Forest |
| Viswanatha, V. et al. [32] | Historical transaction data | User behavior, transactions, financial data | Logistic Regression, Decision Trees, Random Forest | Effective in real-time fraud detection |
| Xiang, S. et al. [33] | Real-world transaction dataset | Temporal transaction graph | Gated Temporal Attention Network (GTAN) | Outperformed state-of-the-art baselines |

Several machine learning algorithms, such as logistic regression, support vector machines (SVM), decision trees, and neural networks, were compared by Shpyrko and Koval [2] in order to identify the best model for identifying fraudulent e-commerce transactions. Their study made clear how important it is to recognize problems quickly in real-time situations. Neural networks beat other models, showing their promise in managing the complexity of fraud detection, according to Saputra and Suharjito's [4] evaluation of algorithms such as decision trees, Naïve Bayes, Random Forest, and neural networks.

Using deep learning to detect fraud is another crucial field of research. Sharma et al. [8] investigated the application of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, finding that these models perform better than conventional techniques because of their capacity to extract complex patterns from huge datasets. Using neural networks to identify Medicare fraud, Johnson and Khoshgoftaar [5] discovered that addressing class imbalances was essential to increasing detection rates.

Research on fraud detection also heavily emphasizes anomaly detection techniques. In order to detect fraud while reducing false alarms, Maniraj [3] concentrated on employing strategies such as the Isolation Forest. Reinforcement learning was presented by Patel et al. [11] and offers a flexible solution for changing fraud patterns by enabling models to learn from prior fraud detection attempts over time. NLP was used by Rao et al. [9] to examine transaction descriptions and identify questionable activities. Jain et al. [12] highlighted the importance of big data in enhancing fraud detection systems by fusing big data technologies with machine learning, showing how fraud detection may be made more accurate and faster.

Additionally, promising are hybrid models that combine machine learning algorithms with rule-based systems. In order to detect credit card fraud, Verma et al. [10] developed a hybrid model that incorporated the advantages of both strategies and outperformed machine learning models alone. This combination may provide a more dependable way to combat fraud in different financial systems. Fraud detection has also seen notable advancements with Support Vector Machine (SVM) models. To increase classification accuracy, Li et al. [15] used a cuckoo search strategy to optimise SVM models. The quantum-enhanced SVM method put out by Kumar et al. [31] performed faster and more accurately than conventional techniques, particularly when handling extremely unbalanced datasets. Studies like those by Nikhil et al. [16] and Chhabra et al. [23] have concentrated on using machine learning to detect phishing websites as phishing and online fraud attempts become more complex. The increasing significance of machine learning in cybersecurity was demonstrated by their models' increased ability to identify fake websites by examining URL characteristics and other indicators.

Additionally, semi-supervised and graph-based learning methods have helped detect fraud. A semi-supervised graph neural network that builds transaction graphs to monitor the interactions between transactions over time was developed by Xiang et al. [33]. This approach is especially helpful in settings with little labelled data. This technology offers a more flexible way to detect fraudulent transactions in real-world applications, which could greatly enhance fraud detection. Last but not least, Zhang et al. [34] investigated the application of unsupervised learning strategies like low-rank recovery to detect fraud without significantly depending on labelled data. Their study showed how sophisticated algorithms like Outlier Pursuit may be used to overcome the problems caused by data imbalance, making it a useful tool for spotting fraud in a variety of financial settings.

In summary, machine learning is still essential for improving fraud detection in a variety of fields. The study examined here demonstrates that deep learning, hybrid techniques, and the use of Random Forest models are all essential for creating fraud detection systems that are more precise, flexible, and effective. These techniques will be crucial for safeguarding financial institutions and averting significant financial losses as internet fraud develops.

## 3. CONCLUSION AND FUTURE SCOPE

This study emphasizes how crucial it is to develop robust and adaptable systems in order to identify online payment fraud in the current digital environment. By integrating anomaly detection with cutting-edge machine learning methods, we demonstrate how sophisticated fraud detection systems can efficiently identify fraudulent activity while lowering false positives. Online transactions are safer and more dependable thanks to this strategy, which aids financial organizations in better risk management. Additionally, by precisely modeling and identifying variances in customer behavior, the use of huge, real-world datasets has improved the accuracy of algorithms used to detect fraud. Our study offers financial institutions a thorough approach and useful suggestions for defending against online dangers and protecting customer money.

This study emphasizes how crucial it is to have robust and adaptable systems in order to identify online payment fraud in the current digital environment. By integrating anomaly detection with cutting-edge machine learning methods, we demonstrate how sophisticated fraud detection systems can efficiently identify fraudulent activity while lowering false

positives. Online transactions are safer and more dependable thanks to this strategy, which aids financial organizations in better risk management. Large, real-world datasets have also been used to better simulate and identify changes in consumer behavior, which has increased the precision of fraud detection

## 4. REFERENCES

[1] Niveditha, G., Abarna, K., & Akshaya, G. V. Credit Card Fraud Detection Using Random Forest Algorithm. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol5(2), Pg.1-5, 2019

[2] Shpyrko, V., & Koval, B. Fraud detection models and payment transactions analysis using machine learning. Proceedings of the SHS Web of Conferences, Vol65, Pg.02002, 2019

[3] Maniraj, S. P. (2019). Credit Card Fraud Detection using Machine Learning and Data Science. International Journal of Engineering Research and Technology (IJERT), Vol6(10), 2019

[4] Saputra, A., &Suharjito. Fraud Detection Using Machine Learning in E-Commerce. International Journal of Advanced Computer Science and Applications, Vol10(9), 2019

[5] Johnson, J. M., & Khoshgoftaar, T. M. Medicare fraud detection using neural networks. Journal of Big Data, Vol6(1), Pg.63, 2019

[6] Yang, Y., Chen, R., Bai, X., & Chen, D. Finance fraud detection with neural network. E3S Web of Conferences, Vol214, Pg.03005, 2020

[7] Kumar, V. K. S., Kumar, V. G., Shankar, A., & Pratibha, K. Credit card fraud detection using machine learning algorithms. International Journal of Engineering Research & Technology (IJERT), Vol9(07), 2020

[8] Joshi, A. K., Shirol, V., Jogar, S., Naik, P., &Yaligar, A. Credit card fraud detection using machine learning techniques. Applied Mathematics, Vol 11, Pg. 1275-1291, 2020

[9] Zhang, D., Bhandari, B., & Black, D. Credit card fraud detection using weighted support vector machine. Applied Mathematics, Vol11, Pg.1275-1291, 2020

[10] Awhad, R., Jayswal, S., More, A., &Kundale, J. Fraud detection in credit cards using logistic regression. International Journal of Advanced Computer Science and Applications (IJACSA), Vol11(12), 2020

[11] Alenzi, H. Z., & Aljehane, N. O. Fraud detection using logistic regression. International Journal of Research, Vol7(02), 2020

[12] Tabassum, N. S., Venkat, &Charan. Detect financial fraud detection with anomaly feature detection. Geetanjali College of Engineering and Technology, 2020

[13] Gopinath, A. R., Sukruth, D. N., Sri Ajay, S., Varunraj, P. K., & Manohar, S. R. Credit Card Fraud Detection Using Machine Learning. JETIR, Vol8(6), 2021

[14] Kumar, G., Kumar, S., & Prakash, A. Credit Card Fraud Detection using Machine Learning. International Journal of Engineering and Advanced Technology (IJEAT), Vol10(4), 2021

[15] Li, C., Ding, N., Dong, H., &Zhai, Y. Application of Credit Card Fraud Detection Based on CS-SVM. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol7(4), 2021

[16] Nikhil, K., Rajesh, D. S., & Dhanush, R. Phishing Website Detection Using ML. Srinivas Institute of Technology, Vol7(4), Pg.194-198, 2021

[17] Rachitha, E., Rani, H. E., Prathiksha, &Swathi, B. V. Credit Card Fraud Detection. IJARIIE, Vol7(4), 2021

[18] Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., & Tan, K. H. An Intelligent Payment Card Fraud Detection System. Annals of Operations Research, 2021

[19] Sumant, C., Shaikh, I., Jadhav, A., & Agrawal, P. Find Transaction Fraud Using Face Detection and Hidden Keyboard. G H Raisoni College of Engineering and Technology, 2021

[20] Sai Kumar, D. S., Chowdary, T. S., Akshara, V., Akhil, N., Lukhman, S., &Parasuram, V. K. Fraud Detection in Online Market Transactions. International Journal of Advanced Research in Science, Communication and Technology, Vol2(1), 2022

[21] Wang, H., Wang, W., Liu, Y., & Alidaee, B. Integrating Machine Learning Algorithms with Quantum Annealing Solvers for Online Fraud Detection. IEEE Access, 2022

[22] Xia, J. Credit Card Fraud Detection Based on Support Vector Machine. EPRA International Journal of Research and Development, Vol7(4), 2022

[23] Chhabra, S., Gupta, V., Kumar, A., & Anand, A. Online Fraud Detection. Proceedings of the 2nd Indian International Conference on Industrial Engineering and Operations Management, 2022

[24] Naik, S. A., & Pise, N. Credit Card Fraud Detection Using Machine Learning. Academic Journal of Computing & Information Science, Vol5(13), Pg.55-61, 2022

[25] Li, P. (2022). Credit Card Fraud Detection Based on Random Forest Model. Journal of Computer Engineering and Intelligent Systems, Vol13(2), 2022

[26] Bourchouq, A., & Peiliang, W. Design of a Model in Machine Learning for Credit Card Fraud Detection. Highlights in Science, Engineering and Technology, Vol23, 2022

[27] Jiang, X. Unsupervised Financial Fraud Detection Using Low-rank Recovery. Various institutions in Canada.Choudhary, T., Mhapankar, S., Bhddha, R., Kharuk, A., & Patil, R. A Machine Learning Approach for Phishing Attack Detection. Terna Engineering College, India, 2023

[28] Dai, M. Multiple Machine Learning Models on Credit Card Fraud Detection. University of Toronto, Canada, 2023

[29] Gaide, K. Fraud Online. RēzeknesTehnoloģijuakadēmija, Latvia, 2023

[30] Haddab, D. M. Detecting Banking Frauds with Analytics and Machine Learning. Weizman Institute of Science, Israel, 2023

[31] Kumar, V., & Pahwa, R. Credit Card Fraud Detection Using Machine Learning. Dronacharya College of Engineering, India, 2023

[32] Viswanatha, V., Ramachandra, A.C., Deeksha, V., & Ranjitha, R. Online Fraud Detection Using Machine Learning Approach. NitteMeenakshi Institute of Technology, India, 2023

[33] Xiang, S., Zhu, M., Cheng, D., Li, E., Zhao, R., Ouyang, Y., Chen, L., & Zheng, Y. Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation. Various institutions in Australia, China, and Tencent Jarvis Laboratory, 2023

[34] Zhang, J. Credit Card Fraud Detection Using Predictive Model. University of California, Santa Barbara, USA, 2023