International Journal of
Science, Architecture, Technology and Environment

The use of AI fraud detection tools in online payment prevention in real world.

Girish Babu B[1*], Syeda karishma akhtar Hashmi[2] , Vijetha Nayana[3], Dr.Kanchan G. Rajput[4]

[1,2,3]*PGDM, DSBS*

[4]*Dayananda Sagar Business School*

[*]*Corresponding author- : girishbabu293@gmail.com*

DOI: https://doi.org/10.63680/ijsate0426237.38

Abstract

The online payment fraud has gone up a lot because more people are using payment systems. This is a problem for banks and businesses everywhere in the world. The old ways of stopping fraud like using rules and checking things by hand are not very good at finding patterns of fraud. Artificial Intelligence is being used to make online payment systems safer and more reliable. This paper is going to show how Artificial Intelligence can be used in payments. It also talks about how Artificial Intelligence based fraud detection tools can stop payment fraud. Artificial Intelligence technologies, like machine learning and behavioral analytics help track transactions as they happen. They do this by looking at lots of data, such as what people have bought how they use their accounts and what device they use. These systems get better at finding activities over time. This means they can find activities more accurately and not bother people as much when it is a false alarm. Many companies have found that using Artificial Intelligence based fraud detection systems has reduced the amount of money they lose to fraud. They have also made it harder for people to launder money and have increased trust, with their customers in payment systems. The results show that using Artificial Intelligence to detect fraud not makes payments safer but also helps banks and businesses work better and make better decisions. As more people start using transactions it is very important to think about using Artificial Intelligence based fraud prevention tools. These tools can help reduce the risks of fraud and provide an online payment system for the online payment system. The online payment system will be safe when we use these tools to reduce the risks of fraud for the payment system.

Keywords: Machine learning, Cybersecurity, Artificial Intelligence, Fraud detection, Online payments, Digital transactions.

1. Introduction

Artificial intelligence (AI) has become an indispensable part of the digital world, and it is changing a lot of our everyday life. AI payment technologies apply sophisticated technologies to make the financial transactions easier and more efficient. These technologies comprise machine learning models and data

analytics, automation of work, precision, prevention of fraud, and better decision-making.

With the growing digitalization of the world, the risk of online payment fraud is growing at an alarming pace. This is a worrying scenario that shows that more improved means of fraud detection are urgently needed, and Artificial Intelligence (AI) is at the forefront. The outcomes of the application of AI fraud detectors by financial institutions are promising, and the application of AI in fraud prevention is increasingly adopted. The ability to identify patterns of fraud before they lead to a financial loss within seconds of processing the last 12 months of transactions of a user makes AI-driven fraud detection system an important tool in the prevention of online payment fraud.

The importance of AI fraud detection cannot be overestimated, and it is more accurate, fast, and reliable than the traditional rule-based systems. Real-time monitoring systems are significant in the process of early detection of fraud. They monitor user activities, device information, and transaction history to detect any suspicious activity, e.g. numerous transactions made at remote settings. In case an anomaly is observed, the system alerts businesses immediately. Quick action is due to quick detection which minimizes losses and enhances security.

Nonetheless, AI has weaknesses in terms of fraud detection. The greatest difficulty is that it requires vast and high quality data. The system will fail to detect fraud or have numerous false positives without them. The addition of AI to the current systems might also be complicated and costly. In addition, AI models are only constantly updated as new methods of fraud are developed, which will demand persistent investment and effort.

Review of Literature:

Antonis Papasavva, 2025 – Online Fraud Detection and Analysis with the help of AI-based

Models. This methodological literature review will discuss how Artificial Intelligence (AI) and Natural Language Processing (NLP) can be used to detect possible text fraud on the internet by analyzing text data. The research establishes 16 different types of fraud and also compares the different training resources and performance indicators. It finds that AI detects significantly, but the transition of scams and data constraints is a major challenge in model generalization.

Vulugundam Anitha, 2025 – Survey on the Online payment fraud detection methods based on machine learning algorithms. In this survey, the researcher will examine different supervised machine learning methods, including Support Vector Machines (SVM) and Logistic Regression, to detect fraudulent transactions. The study highlights a program of six steps of processing between data absorption to performance verification. The authors discover that classifier-specific systems such as C4.5 decision trees and SVMs are quite effective in binary classification problems in large financial data.

Mohammad Prince, 2025 – The creation of machine learning models to detect online transactions fraud in real-time. This paper suggests a big-scale real-time system of detection of fraud based on a multi-stage pipeline implemented on top of big data technologies, such as Apache Kafka and Spark. The system can identify suspicious patterns with minimum delay by analyzing their behavior with the Isolation Forest algorithm. On a dataset of more than 100 million transactions, simulation has resulted in a high recall rate of 97% and F1-score of 91%.

Mangal, Shubham, 2025 AI-Powered Fraud Detection in Digital Payments: A Machine Learning View. This paper will discuss how machine learning and neural networks can be used to defeat the drawback of conventional rule-based systems of detecting fraud. It underlines the use of AI in detecting sophisticated suspicious activities in real-time on e-commerce and mobile banking websites. Also, the paper covers such

essential secondary questions as data privacy, adversarial attacks, and the importance of explainability in AI-powered financial systems.

Haranadha Reddy Seshakagari, Deventhira HariramNathan, 2025 – AI-Augmented Fraud Detection and Cybersecurity Architecture of Digital Payments and E-Commerce Websites. The authors present an AI-enhanced cybersecurity model that is used to secure digital payment ecosystems based on behavioral analytics and anomaly detection. The study criticizes the inefficiencies in the application of the machine learning model and recommends the incorporation of deep learning and reinforcement learning. The purpose of the proposed framework is to be very accurate and resistant to situations of concept drift and imbalance of rare events.

Zong Ke, 2025 – AI Deepfake and Fraud detection in online payments with the help of GANbased models. The study examines how Generative Adversarial Networks (GANs), such as StyleGAN and DeepFake models, can be used to detect AI produced deepfakes in online payment systems. The paper suggests a new GAN-based defensive mechanism to detect the finer manipulations of faces in the images of payment. The model is tested to detect legitimate transactions and deepfakes, and the results obtained demonstrate that it has over 95 percent of detection rates.

Ganesh Khekare, Shivam Sunda, and Yash Bothra – 2025 – A Comprehensive Comparison of Traditional and Ensemble Machine Learning Models Performance in Online Fraud Detection. This paper will give a comparative study of the conventional machine learning models and ensemble models (Stacking and Voting Classifiers). Based on the highly skewed credit card fraud data, the researchers discovered that ensemble techniques are more precise with a better estimation of 0.99. Nevertheless, it was found that traditional models were more recallable, which led to a required trade-off among practitioners choosing a particular model to use in reallife fraud detection.

SI. NO	Area	Research gap
1.	Real-Time scalable and development efficiency	There is no empirical evidence on the development of such a system on scale in production environments under the peak period of transaction.
2.	Model explainability and reliability	Most AI detection systems are a black box in which it compels stakeholders to determine the reason why transactions are drawn and labeled.
3.	Relative performance of traditional vs ensemble models	This is to show a trade-off in falsepositive and false negative, which has not been completely addressed in the literature, particularly in the context of real transaction data, and multiple classes of imbalance.
4.	Hybrid and multi-techniques Frameworks	Whereas hybrid models are promising, most of the research tests in this framework are in experimental or synthetic conditions.

Research Methodology:

The present paper adopts a descriptive and analytical methodology to explore the application of Artificial Intelligence (AI)-based fraud detection systems in actual online payment systems. The primary aim of the research is to determine the effectiveness of these systems in stopping fraud in online payment systems.

Problem Statement.

The existing AI-based fraud detection technologies in online payments are currently challenged to attain the simultaneous balance of real-time scalability, development efficiency, model explainability, and robustness with the changing, imbalanced transaction data. Little empirical studies have been conducted on the development and implementation of real time systems capable of functioning at scale under peak rates of transaction. Most models are black boxes, which do not allow stakeholders to trust them and comply with regulations. The tradeoff between false positives and false negatives has not been completely addressed in the available literature, especially when a multi-class imbalance is present in the actual transaction data. The promising hybrid frameworks are mainly tested on an experimental or synthetic basis, not on an actual production environment.

Objectives:

1) Knowledge of the place of AI in digital payments.
2) AI fraud detecting applications with respect to preventing payment fraud.

Use of AI in online payments:

The way people do business has changed a lot over the years. Now it is more about doing business in a digital way. This journey is about finding payment methods that are faster and safer and more efficient. It is clear that businesses need to accept payments in a way that's efficient and safe and personal so they need to use Artificial Intelligence technology to stay competitive. The use of Artificial Intelligence will do more than just make payments it will also help us understand a lot of data. The future of payments depends on companies that use these ideas, which is why we need to learn more about how Artificial Intelligence is used in payments. We will see how it is changing the world. We already know that a time ago cash was the best way to pay for things but then debit and credit cards were introduced and they were more convenient and safer. Then point of sales technology made it even easier, for big transactions and a lot of people like that.

The way payments are made is closely linked to the way society and technology are changing. Since most of the world is using payments the issues of security and user experience and efficiency have become more complicated as digital transactions increase.

We have seen a lot of improvements. These new ideas have also created new problems and frustrations for users. People expect to be able to make payments like real time payments but most systems are not able to do that yet and delays can be very frustrating. Also we need to improve security than ever because cyber threats are getting worse and we need to make sure that peoples financial information is safe.

International trade needs payment systems that can adapt to markets and rules so we need to keep innovating to have powerful platforms that can handle the complexities of international transactions and follow the rules. So it is still very important to keep innovating even though we have already taken some steps. The payment landscape is always changing and companies need to stay that is why payment methods like Artificial Intelligence are so important and the use of Artificial Intelligence, in payments will continue to grow.

AI fraud detection in payment fraud prevention applications:

The use of AI solutions by financial institutions in new and existing workflows to enhance decision-making and fraud prepared by risk management is on the rise. The machine learning models that use AI to identify patterns can be trained on historical data and identify any potential fraudulent transactions before they are carried out. They can also demand human participation to undertake additional authentication procedures to determine a suspicious transaction. The predictive analytics applied in AI technology can also be used to forecast the kind of future purchases that one is likely to make, and it can be used to identify when a new form of purchase or transaction activity is suspicious.

In these aspects, AI Fintech can assist people to avoid having their money stolen through different forms of frauds, including, identity theft, payment fraud, credit card fraud and other forms of banking frauds.

How AI fraud is different from traditional fraud.?

Conventional methods of fraud detection are rooted in pre-defined rules based methods that are established and easy to implement. As an example, any new transactions above a specified range of averages on the basis of the spending patterns of a specific account. The human detection fraud analysts of the traditional type have a degree of domain experience, intuition, and expertise. In other cases, a human may be the only individual knowledgeable in conventional training who can confirm the validity of a certain transaction or identify a fraud attempt.

Nevertheless, the Traditional fraud detection systems are based on predetermined relationships (e.g., in case X, Y). Although this method can also be useful, it does not make use of the potential enormous and multifaceted interactions between a large number of data points. With the increase in size of transactions, the old system assembled and operated by human based fraud detection experts cannot keep up with increasing volume of data generated on the daily basis every minute. Making more employees is not only costly, but it might not be adequate too. The rule systems employed in the conventional fraud detection systems are usually highly inflexible and they are activated when a possible fraud signal is identified. This stiffness may result in high rate of false positives. As an illustration, say a particular account has never withdrawn above USD 100 so far and he/she comes to withdraw twice the amount, the system is likely to reject the transaction. However, as odd as this behaviour may be, it does not always mean fraud. The only thing that a customer might need to do in this case is to withdraw an out of the ordinary amount of money. Such false positives may initiate extra investigation and delay that result in less customer satisfaction.

AI systems have been very good at consuming large volumes of data to identify the complicated and hidden patterns. Through the broader perspective, AI systems are capable of detecting abnormal activity more efficiently. With AI systems, it is possible to observe large volumes of transactions that a human would never have the capacity to observe. AI-based fraud detection can enable real-time response and deliver a prompt answer to its counterparts in a shorter amount of time. After working out, AI algorithms do not cease learning. The more the AI systems work, the more they can learn, and they can understand new kinds of fraud and become more effective. AI models also need very massive data to train, learn and develop. This data has to be sourced or generated (synthetic data), but also maintained. The quality of the training data determines the accuracy of a given AI model. AI systems may not be easy to add to the existing systems. Although AI systems will save money over time, they might involve a high startup cost.

Proposed Solution.

This study will suggest the creation and experimental verification of a real-time, hybrid AI system, the combination of ensemble learning and explainable AI component, which is specifically aimed at scaling to production levels during peak transaction loads.

To achieve Scalability and Development Efficiency in Real Time: The frame work will use the stream processing and light weight and optimized ensemble models (ex: A combination of Isolation Forests and Gradient Boosting Machines) deployed on the edge computers to achieve low latency and high throughput in the production environment risk assessment to solve production environment scaling problem.

To satisfy Model Explainability and Trustworthiness: A dedicated XAI module (e.g., based on LIME values or SHAP values) will be used to give post-hoc explanations of flagged transactions, converting model decisions into explanations that can be understood by people, to establish trust in the model, to comply with regulators, and to allow human control.

In Comparative Performance (False Positives vs. False Negatives): The research will make a stringent comparison between the proposed hybrid ensemble model with the traditional and individual advanced models based on large, real-world, and imbalanced multi-class transactions datasets. The trade-off between false positives (reducing customer friction) and false negatives (minimizing financial losses) will be evaluated and optimized specifically by using performance metrics (e.g., F1-score, Precision-Recall AUC, and confusion matrices).

To validate Hybrid Framework: The suggested framework will be validated to work in a simulated production environment, simulating the optimal conditions of transaction and escaping the largely artificial or experimental background to present a solid empirical evidence of its efficiency and applicability on a

practical basis.

Sources of Data:

The poll because of the inability to get real data relies on secondary data in this study. The selected datasets will be used to estimate the real online payment transactions accessible on the web and containing Research papers, journals and fintech case studies among other sources like

- Publicly available datasets about online payment and credit card fraud.
- Reports on the industry that apply to AI-based fraud detection systems.
- Online articles, business journals, textbook and newspaper articles.

Scope of the study:

The objective of this paper is held by focusing on the application of Artificial Intelligence (AI) technologies, namely, machine learning and behavioral analytics in the digital payment ecosystem in real-life scenarios.

- It includes the description of the shift between the traditional models of fraud detection that is conducted by specific rules to more advanced and real-time monitoring systems that study the history of transactions, user behavior, and device data.
- The study looks at the efficiency of AI in detecting advanced and dynamic frauds like identity theft and credit card fraud and banking scams.
- The paper also discusses the problems of the future, such as GAN-based deepfakes and the need to introduce Explainable AI (XAI) to comply with regulations.
- It dwells upon the compromise between the efficiency of operations, real-time scalability and consumer trust ensured by safe and sustainable online payment infrastructure.

Limitations:

- The research is limited mainly by the fact that the secondary sources of data are used since the real-world data of financial transaction is very sensitive and is not always available because of privacy measures. Since the study is based on the existing literature and reports, the results are confined to the quality and scope of the original datasets and studies used.
- The fact that the AI technology is changing very fast implies that certain particular tools or fraud patterns that were discussed here can change within the very short period of time, which can potentially negatively impact the long-term relevance of the conclusions.
- The suggested hybrid framework is tested within the framework of a simulated environment, which might not be representative of all technical and human variables within the real production environment.
- The absence of variety in empirical data to be used in various geographic areas, fraud trends and digital payment platforms can differ incredibly across international markets.

Findings:

The old model of rules-based systems cannot work against the AI-enabled fraud of the future, 2026. Studies show that hybrid models, which involve the combination of Gradient Boosting Machines (GBM) and Isolation Forests, have an accuracy score of more than 91, which is much higher than a single classifier.

Deep learning is very accurate, but it is not transparent, which is a very important bottleneck.

Explainable AI is now a requirement by stakeholders and regulators. The use of Shapley Additive Explanations systems in which it is already demonstrated that 30% of the time spent by manual reviewers can be saved by providing clear justification of the flagged transactions.

Another change that will happen in 2026 is the emergence of GAN-based (Generative Adversarial Network) deepfakes and synthetic identities. These are problematic to conventional behavioural models, and a new tier of defensive AI will be required that is able to spot subtle facial or biometric manipulations in real-time.

Suggestions:

Banks need to start shifting towards open-box structures as opposed to black-box models. With the inclusion of Explainable AI within the Machine Learning Operations pipeline, all automated decisions are transparent and auditable. Apply friction strategies to the use of AI risk scores. Basic transactions must be frictionless and without complications, whereas highrisk abnormalities must receive additional authentication such as biometrics or mobile driver license (mDL) checks. Fraud trends change within weeks and not years. Have automated feedback loops in which frauds definitely confirmed get immediately reintroduced into the training set to combat concept drift. Federal the Federated Learning networks. This enables banks to distribute fraud “intelligence” but not sensitive “data” and have a collective defense against worldwide fraud syndicates.

Conclusion:

The history of digital payments has come to a point of gravity where the pace and the complexity of fake activities were faster than the ones conducted by human beings and legally governed methods. This study proves that Artificial Intelligence is the sole feasible infrastructure that can protect the contemporary financial ecosystem. Nonetheless, it is no longer accuracy that is the gold standard. To be effective in any real-life production setting, AI should strike a balance between scalability in real-time and transparency that can be understood by human beings. The proposed hybrid framework that involves adopting ensemble learning to achieve accuracy and XAI to establish trust that bridges the two key gaps in the literature, which are the critical gaps of Black-Box and Scalability.

Further in the future, the success with which fraud prevention can be achieved will be determined by how the industry will adopt a new strategy by aiding a proactive, explainable, and adaptive defense rather than a reactive one. Following the suggested hybrid solutions, financial organizations will be able not only to reduce financial loss but also to promote consumer trust that is the key to the further development of the digital economy.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

- Antonis, P. (2025). Application of AI-based models for online fraud detection and analysis. Journal of Financial Crime, 32(1), 45–62.
- Busireddy Seshakagari, H. R., & Hariram Nathan, D. (2025). AI-augmented fraud detection and cybersecurity framework for digital payments and e-commerce platforms. International Journal of Cybersecurity and Digital Trust, 6(2), 88–104.
- Khekare, G., Sunda, S., & Bothra, Y. (2025). A comprehensive performance comparison of traditional and ensemble machine learning models for online fraud detection. Journal of Big Data Analytics in Finance, 4(1), 21–38.
- Mangal, S. (2025). AI-powered fraud detection in digital payments: A machine learning perspective. Procedia Computer Science, 215, 312–320.
- Prince, M. (2025). Developing machine learning models for real-time fraud detection in online transactions. IEEE Access, 13, 45678–45689.
- Vulugundam, A. (2025). A survey on online payment fraud detection techniques using machine learning algorithms. International Journal of Advanced Computer Science and Applications, 16(3), 112–121.
- Zong, K. (2025). Detection of AI deepfake and fraud in online payments using GAN-based models. Expert Systems with Applications, 231, 120845.
- World Economic Forum. (2024). The future of financial services: AI-driven fraud prevention. World Economic Forum Publications.