Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 13 ~ Issue 5 (Sep. - Oct.2023) pp: 01-07
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

Efficient Resolution of Fraudulent Transactions And False Declines Using Ai-Based Solutions

Balaji Soundararajan
Independent Researcher

Abstract
The proliferation of digital transactions has amplified risks associated with fraudulent activities and false declines, costing businesses significant revenue and undermining consumer trust. Traditional fraud detection methods, such as rule-based systems and anomaly detection, face limitations in scalability, adaptability, and accuracy, often leading to excessive false positives or missed fraud patterns. This study explores the transformative potential of AI-based solutions, particularly machine learning (ML), to enhance fraud detection while minimizing false declines. AI systems leverage real-time data analysis, adaptive learning, and complex pattern recognition to improve accuracy and reduce operational inefficiencies. However, challenges such as data quality, model interpretability, and ethical considerations remain critical barriers to seamless implementation. By addressing these challenges through robust data preprocessing, continuous model evaluation, and stakeholder collaboration, AI can significantly bolster transaction security, foster consumer trust, and optimize financial ecosystems. The paper concludes with recommendations for future research to refine AI-driven frameworks and ensure ethical, transparent deployment in fraud detection.

Keywords
Fraudulent Transactions, False Declines, AI-based Solutions, Machine Learning, Anomaly Detection, Financial Security, Data Quality, Model Interpretability, Real-time Analytics, Ethical AI.

I. Introduction

Over time, digital transactions have become the most convenient channel to serve consumers, and developments in the payment space enable business payments and other online transactions. With advancements in digital technology, the ecosystem is likewise evolving with the advent of more sophisticated transactions through the initiation of cryptocurrency, as well as the expansion of electronic banking services such as mobile money and other related platforms. The increasing volume of electronic transactions might fuel an increase in fraud in the ecosystem. Though efficient, the fraud responses might decline genuine transactions, an act classified as a false decline. False declines are a global issue that could cost online retailers billions each year, with an expected increase over the next four years. Furthermore, replacing a lost credit card or addressing fraudulent behavior could cost billions each year, leading to a drop in revenues for the merchants, which are mostly small and medium enterprises, requiring enormous investments to overcome these difficulties while succumbing to competition. Fraud impacts domestic consumers who manage frequent transactions and rely more on electronic payments. There is a high percentage of the population that fraudsters have committed to making fraudulent transactions. This study aims to explore how AI-based solutions can efficiently resolve fraudulent transactions and false declines, and how they could improve transaction security and monitoring capabilities, creating trust with genuine consumers.

The remainder of this essay is organized as follows. Section 2 provides a review of both false declines and fraudulent transactions. Section 3 introduces the development of AI for potential applications with financial transactions. The potential solutions, AI-based systems, for the detection of fraudulent transactions and decline decision-making strategies are systematically outlined in Section 4 and Section 5, and the substantial positive contributions of AI to industry and academia are listed in these two sections. Some aspects to consider in future studies are executed in Section 6, where the potential limitations of AI-based systems are discussed and the way forward.

Background on Fraudulent Transactions and False Declines

Fraudulent Transactions: Electronic commerce is a thriving and integral part of modern society, taking the place of conventional paper transactions, but it has attracted more fraud, burglary, and malice. Fraud in electronic or digital transactions refers to any form of deception or distortion of data that leads to a financial or non-financial loss. Fraud is currently increasing by approximately 10% annually. However, the exact amount of such activity is difficult to gauge because it is not generally reported. The primary aim of fraud is to obtain personal and bank account data or to exploit lending or credit card account information to steal money. Usually, fraudsters will use stolen identities to access bank accounts, open new credit card accounts, or apply for loans, bankruptcy benefits, or other resources. If any theft or fraud has been committed, merged, and successfully completed, the bank or any financial organization will count it as a fraudulent transaction.

False Declines: A false decline is a legitimate transaction that is mistakenly marked as fraudulent. Declining was usually practiced as a prevention tactic against fraud. It caused significant customer dissatisfaction, decreased sales, and intense storage costs even though it had promised fraud-free shopping for online businesses. If we look back at the e-commerce transactions, three out of every 100 transactions declined during verification are not made. Over one million consumers cancel their cards and more than four million businesses stop using them in the United States. False declines accounted for more than 13% of global lost revenue in 2017, even though they had improved protection and accounting measures.

Traditional Approaches to Detecting Fraudulent Transactions

The traditional methods utilized for identifying a fraudulent transaction consist of rule-based systems or anomaly detection. The first type of system employs a set of predefined rules that contain criteria to identify which activities deserve to be monitored closely due to their suspicious character. These criteria can be based on generated user complaints, atypical behavior for a specific customer, or inconsistencies between old and new purchases. Although their practical use as the foundation for the first type of fraud mitigation system was and continues to be a common practice, their performance is limited by several factors. They are designed to work in just one of the two fundamental transaction routing methods. This is because all of the criteria required for automated alarm generation, which is not necessarily subject to manual review, are available in the offline environment only.

Conversely, a vast majority of card payments are routed online. As a result, some of these criteria are not available in online payments. Moreover, a rule-based system is effective when a certain threshold of the alerting criteria is passed in order to generate an alert. Fraudsters learned how to divide the components of a high-value suspicious payment into more payments so that individually they go unnoticed. In turn, the IT department has to go through an alteration of the rules nearly every time a new and evolved scam is unveiled. Ultimately, the parameters for an alert are decided upon by humans, implying that they are highly subjective. Failing to create an alert in time equals approving a potentially massive loss for the payment system, while raising too many alerts means further frustrating customers who want to complete legitimate purchases.

Rule-Based Systems

Before the rise of AI-based solutions, the simplest strategies for discovering payment fraud were based on fixed rules that identify the signatures of potential fraud. The logic behind this indication is the fact that fraudsters were perfecting the methods of deceiving the anti-fraud systems as technology for hiding their tracks moved forward.

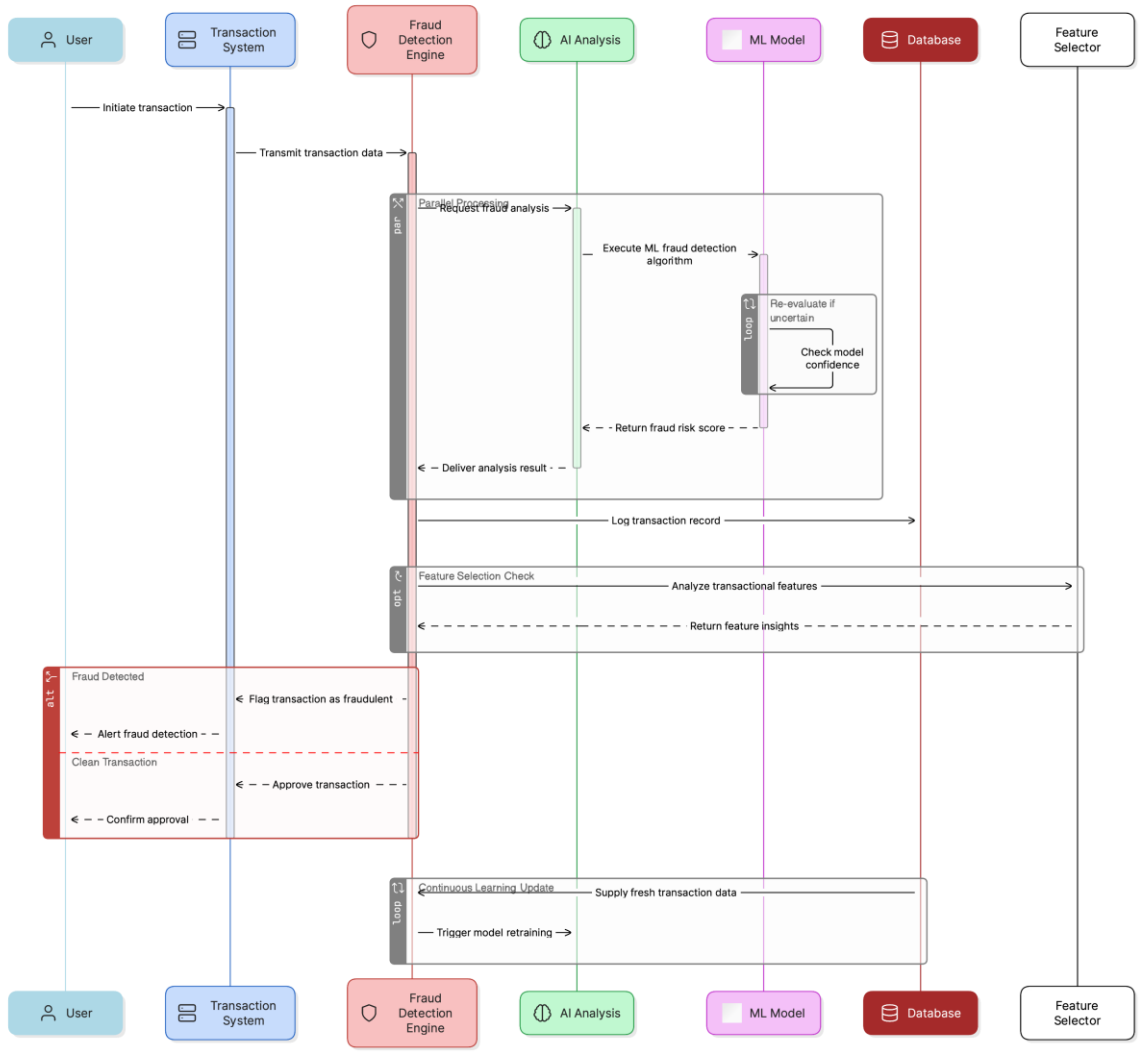
Fraud detection systems use a set of rules to block illegal transactions, and as everything in life is subject to a learning phase, these systems are no different. By using artificial intelligence, the system learns from previous fraud transactions and past bad decisions, allowing it to judge what is likely to be fraudulent. These rules have to be changed every single time there is any change in the data, products, and, in an ideal world, every day. A good example of these types of rules is verifying buyers from countries predicted to be more likely to be fraudsters. Although implemented widely, this type of fraud detection is limited, as fraudsters keep moving and modifying their strategies to avoid being blocked. After a while, they become undetected because every time there is a change in rules, frequent buyer resources and, in some cases, checking systems re-investigate the transactions that have already been checked, slowing the decision time and remembering not to accept these types of transactions. False positives are ads that are likely to be beneficial for the company but have been incorrectly identified as fraudulent. For example, valid customers whose transactions are declined may be perceived as dishonest because they tried to purchase something with someone else's credit card. In addition, as the number of people in contact with others increases, it has been noted that users who are in contact with them have an increased tendency to commit fraud. Despite this, it is worth considering that this is not sufficient for the fraud detection system.

Anomaly Detection

Anomaly detection is a traditional approach to detecting fraudulent transactions. This technique involves detecting transactions that do not closely match historical data collected over a period of time. A deviation from historical data can be a sign of an anomaly, and hence these transactions are flagged as potentially fraudulent. Anomaly detection is relevant in identifying fraud that is characterized by deviation from normal, as the majority of fraud-related transactions will deviate from a typical pattern. Rule-based systems and models require a clear set of rules to classify the transactions as fraudulent. Anomaly detection can catch sophisticated fraud that does not follow any rule or does not have a definite set of characteristics. While the approach offers many benefits, its effectiveness is contingent on the quality and quantity of historic data. If only a few valid transactions have transpired, or if historical data is not an excellent representation of regular transactions, anomalies will not be detected. Fraudsters are also becoming more skilled at creating activities that mimic typical behavior, making it increasingly difficult to detect such fraud. Anomaly detection systems generate many legitimate transactions as false positives, similar to the rule-based methods, leading to decreased customer success. Given these limitations, there is an ongoing need for methods that can detect fraud in an environment characterized by continuous innovation in known fraud and the growth of online financial transactions. In this light, the discussions regarding state-of-the-art AI-based solutions will emphasize this wider view and highlight different types of solutions based on AI, as well as illustrating how they resolve issues related to existing rule-based systems or anomaly detection approaches.

AI-Based Solutions for Fraud Detection

Artificial Intelligence (AI)-based solutions are a promising enhancement of fraud detection in the FinTech industry. AI can help detect more fraudulent transactions and significantly reduce false declines compared to traditional fraud detection methods. The performance of AI-powered fraud detection is continuously improving, as these systems learn from new data they process to enhance their accuracy.



Machine learning (ML) algorithms underlying AI-based fraud detection are beneficial because they can autonomously learn fraud patterns from transaction data. As they process more data, they improve their performance due to a better discriminatory ability to distinguish fraud patterns from normal acceptable behavior. In addition, machine learning models used in these systems are capable of spotting changes in fraud patterns over time to adapt to novel fraud attacks. As AI processing units run machine learning model training and execute advanced analytics for vast volumes of data within milliseconds, the ability of AI-powered systems to analyze large amounts of transaction data in real-time considerably enhances fraud detection capabilities. AI card-not-present (CNP) fraud detection is also more accurate in preventing fraud than traditional methods, with the potential to significantly reduce card declines. Not only does AI-based fraud detection enhance card not-present fraud detection capabilities, but it also has the potential to reduce false positives and customer dissatisfaction when shopping online, hence reducing the churn rate for card issuers. [1][2]

This is particularly true for individual customers and small to medium enterprises (SMEs) for whom the survey found that 'elaborating the details' has the highest fraud prevention impact. AI-enabled fraud detection improves the capability of identifying more fraudulent transactions and significantly reducing false declines. The AI algorithms underlying these fraud detection solutions can be, among others, a General Model and Neural Networks. It is essential to note that the performance of AI-powered solutions improves over time through continuous retraining on new data.

Machine Learning Algorithms

Machine learning is a technique for training computers to learn by identifying patterns in data, allowing them to make predictions and optimize decisions. There are various types of machine learning algorithms, with the main three being supervised learning algorithms, unsupervised learning algorithms, and reinforcement learning algorithms. A key feature of AI-based fraud detection mechanisms is that they use machine learning to analyze and scan over large volumes and complex patterns of transactional data to make decisions, allowing for higher prediction accuracy and the ability to uncover hidden patterns in transactional data.

There are many disparate machine learning algorithms that can be employed to detect fraudulent transactions, such as decision trees, support vector machines, neural networks, and logistic regression, to name just a few. However, the challenge of selecting suitable machine learning algorithms is further complicated by feature selection, a process that involves deriving new dimensional features from existing ones. Feature selection can often be an exhaustive process due to the large number of possible variables, since usually very few datasets contain a good combination of features which, when deployed, can produce our desired results. If not done correctly, the algorithms may very easily be affected by noisy, redundant, and irrelevant features, and as a result, they could perform poorly and produce largely inaccurate results. In addition, selecting a model based on past performance does not ensure it will be the most accurate for future performance. It should be noted that the majority of machine learning algorithms mentioned above now include inbuilt feature selection technology.

One of the challenges of using machine learning algorithms is overfitting, which occurs when the model is too complex for the data and fits the training so well that it uses many intricate patterns that may not be present in the actual data. Another drawback, to some extent, is the high bias that these methods suffer at times, since some methods are not robust to false negatives. Therefore, it is highly necessary to have a well-orchestrated list of performance-improving measures that ensure the results maintain a customized approach, as their performance in data is heavily dependent on the algorithms used. Furthermore, often data is unstructured, and the machinist is heavily biased; therefore, data scientists are required to ensure that unintentional data bias does not occur. Finally, machine learning algorithms analyze every single data update and transaction that a bank customer makes. Therefore, they are complex systems and are slow to update.

Challenges and Limitations of AI-Based Fraud Detection

AI edits are only a piece of sarcastic content that sounds fine. It is in the purview of the individual producing said response to evaluate the authenticity of the statement. The range of feasible outcomes is also determined by a variety of factors. Keep in mind that this text is for educational purposes and should not be used as evidence in legal proceedings. Even the most competitive AI options face a variety of issues when it comes to fraud detection services based on AI. As a result, it is essential to be cautious in order to maintain a high level of efficiency. There are a number of matters to think about. First and foremost, the findings are directly related to the accuracy of algorithms. Unfortunately, predictive analysis can only go so far as the details and products with which the IT systems operate. Even the most cutting-edge algorithms would not yield worthwhile results if there is a scarcity of precise or linked information in the company's possession. Furthermore, AI solutions that can be applied to fraud require huge quantities of data in order to work appropriately. It is important to keep data privacy and the new regulations in mind.

Data Quality and Quantity

The quality and quantity of data are two fundamental differentiators for AI-based fraud detection systems. A good quality and representative dataset is pivotal for training machine learning algorithms with a sufficiently wide range of examples that can help the algorithms classify new, never-before-seen financial transactions as genuine or fraudulent. This means including examples of known fraud in the training dataset; otherwise, the models may lack good examples of fraudulent transactions and so reject transactions that are indeed genuine, i.e., run back the fraud. When training AI-based fraud detection models, the power of the data cannot be underestimated. This includes the range of data points as well as the volume of data, including a representative sample of fraud data so that the model can be adequately trained. Common pitfalls that can result in a raft of challenges for an AI-based fraud detection system include missing features, missing values in feature fields, and a high frequency of constantly changing values for certain features, such as the email address or credit card. A scenario where insider threat behavior is common would result in a drift in the data and a subsequent suboptimal model with declining prediction performance. Data imbalance is also another challenge. The majority of financial transactions one investigates are genuine transactions, while criminals are the very small minority. Addressing this data imbalance and choosing the correct statistical measurement to benchmark the fraudulent algorithmic detection rate becomes important. In addition to data quantity and quality constraints, one other challenge for efficient AI-based fraud detection is the number of transactions that have to be processed in real time. Conducting real-time streaming and real-time scoring of transactions so that the response happens in milliseconds or less can place huge pressure on the AI-powered detection model. This comes in addition to data breaches, which can result in fraudsters being able to test a very large number of stolen credit cards in a single blitz before they are quickly stopped by the company. The negative consequences of a low-quality approach in fraud detection impact the fraud lost, i.e., genuine fraud cases that were overlooked by the algorithm and declined by the human, which may result in revenue loss. Furthermore, there is the impact of false declines, i.e., genuine transactions declined by financial institutions, to consider. The long-term damage of an intensive security strategy generated by a poorly trained model is a decline in genuine transactions. AI failures state that the future effects and damage of an insufficient security response to fraud should not rely on a stop-gap measure to avoid organizational liability but should also invest in data management strategies that ensure an AI-based fraud detection system can act efficiently from the root up. [3]

Interpretability and Explainability

Despite the fact that many AI-based solutions have been used for the detection of fraudulent transactions and the prevention of false declines, some of the main customers, financial institutions and cardholders appear to be less and less comfortable when algorithms are used. It is true that regulators in some countries now require some form of explanation of how decisions are made based on AI algorithms, and the technologies proposed will lead to better model interpretability. These days, it is becoming increasingly important that stakeholders become educated about the decision-making process that is based on AI. This should be true for other stakeholders but it is critical for cardholders, who are most likely to benefit from the detection of scams. From another standpoint, clear business rules without any complexity are already commonly used to govern some algorithms. Many ML approaches have been developed to enhance model interpretability. While enhancing model interpretability can increase trust in decision-making systems, there is often a trade-off between transparent approaches and the performance of state-of-the-art descriptive frameworks, particularly in the medical, legal, and finance industries. There is a large body of work on interpretable ML techniques that gives models the ability to "explain themselves." It is proposed that models use example-based or feature-based explanations of direct outputs. In many papers, the main approach is to provide a global explanation of the algorithm's predictions using local model understanding techniques. The purpose of this paper is to look at many publications, explainability of driver feature-based models for the prediction of consumer lifetime value, and credit scoring, and provide an in-depth understanding of the methods and tasks of state-of-the-art techniques. The paper deduces practical steps and guidance based on the criteria and functions of the models. Using this approach, one is also able to find the importance of systematically underlying the effects of the drivers on prediction so that it is possible to convert the feature importance rankings into more biometric-based scores, a priority for finance. This does not appear to always hold true for areas such as fraud analytics or medicine and insurance work, which make it difficult to interpret a feature. It is shown that an interpretation has a much better impact when it depends on market specifics. AI ethics are emerging as a core point in providing the assurance of the responsible practice of AI when human decisions are driven by AI solutions. Reminiscent of ethical AI characteristics, the first standard project in the field was launched regarding the Standards for Ethically Driven Nudging to ensure transparent operation of AI solutions. This paper explains how the ethics dimensions apply to designing an ethically driven and trustworthy model of setting up ML algorithms to make use of the banking data card to create automatic business policies to stop fraudulent transactions. A rapidly

expanding society, the AI. Therefore, there is a chance to obtain strong successful predictions of algorithms obtained using display capability data due to the fraudsters' preference for anonymity.

Best Practices for Implementing AI-Based Fraud Detection

AI-based fraud detection heavily relies on the AI model used and the way AI algorithms are configured. When implementing AI-based fraud detection solutions, one of the key and primary things that should be done is understanding a business and its specificity. This understanding will guide the customization of the AI model and the AI-related setup as it helps in determining fraud case analytics. The first step is to engage fraud analysts, data scientists, decision-makers, and compliance officers. This often helps with mutual definitions, coding, and building the AI model. Moreover, all parties understand the context in which the AI model will be used. Following the context and customization, the importance of the real-time nature of the operation in the area of exploration and deployment of systems has been noted. A model already in operation should be continuously monitored and navigated. There should also be a continuous learning process and the adaptation of the system to the patterns generated by criminals. The algorithmic stage in data preprocessing is crucial. Recommendations and practices for cleaning data, expanding the number of patterns, and processing, as well as applying models tailored to evaluate model validation, with an emphasis on cross-validation, are important. Many suggestions lend a degree of practicality to this work. In any event, the practices and guidelines you need to follow while implementing these systems can become lumped together, and it is crucial and important to perform them together.

Data Preprocessing

During the process of implementing AI-based fraud detection solutions, data preprocessing is a crucial step. For the machine to accurately understand and interpret the data, it needs to be properly cleaned, transformed, and organized. Real-world data is organically noisy, inconsistent, and inaccurate. Preprocessing provides a solution to those problems and creates a representative dataset for analysis. Cleaning helps to handle noise and inconsistencies, while transforming and organizing provides a well-curated dataset for models to effectively learn from. Well-preprocessed data can correctly represent the model, reduce learning complexity, and increase learning quality. Without proper preprocessing, the model could fall into proving the noise from the data incorrect instead of the task associated. Additionally, since anomaly and fraud detection depend on the reconstruction of the standard transactions, distribution fairness proves that accelerated and quality fraudulent transaction detection, as well as fast resolution of false positive rate declines, is only possible with well-preprocessed and normalized data.

Optimal datasets for fraudulent transaction detection are realized through data cleaning. This reduces inconsistencies and inaccuracies causing data degradation and poor performance in the training of models. Missing values require the use of either imputation of the missing value or exclusion of the data. Best practice implies the exclusion of missing and inconsistent data from the training and detection phases. The goal of anomaly detection is to accurately and quickly spot irregular activity, and these averages, medians, and predictions might be corrupted because of the noise and not representative of the real transactional nature of the feature. Model fitting the noise will not detect fraud; instead, it will detect the small noise. Features can take on many possible structured and unstructured variables. Anomaly detection models focus on either particular or all features. In reality, a focus on all features depends on the business context, and with a high volume of features available, an aggregation of similar or top-performing features can improve recall and accuracy. Each missing value excluded from the AI model might change the financial value and exact acceleration of the false positive rate. A model that does not use a useful feature misses detecting fraudulent activities.

Model Training and Evaluation

The model training is an important task in AI-based fraud detection systems. The quality of AI-based fraud detection systems depends on the robustness of the employed training strategy. In particular, the training model should be exposed to diverse data, which leads to more accurate generalizations. Overfitting causes poor generalization and is a major issue in training AI models for fraud detection. The training process is based on training data, which consists of the feature values of each transaction of a customer. In some scenarios, the outcome of each transaction is included in the training data as training labels, so the AI model employs supervised learning for training. In other scenarios, the outcome of the transaction is hidden, so the AI model uses unsupervised learning, which is based on training data only. Supervised learning requires the AI model to distinguish between different transaction labels by producing decision boundaries. Unsupervised learning employs different techniques, such as clustering, to group transactions according to their properties. [3][4]

In AI-based fraud detection, models are evaluated using different metrics, such as accuracy, precision, recall, and F1 scores. Precision highlights how much of the fraud predictions are accurate, while recall indicates the ability of the model to detect most frauds. The F1 score is the harmonic mean of the precision and recall scores. Different evaluation thresholds are important in fraud detection models. Model training for fraud detection is an

ongoing process, as the performance of these models can decay if they are not continuously trained and refined. A feedback loop is a vital part of model training to improve the performance of the AI systems over time by learning from new data. A vast majority of fraud detection projects involving large inventories, such as e-commerce and banks, include explanation models to indicate why certain transactions have been rejected.

II. Conclusion:

The rise of digital transactions has necessitated advanced solutions to combat escalating fraud risks and mitigate the costly impact of false declines. Traditional methods, reliant on rigid rules or historical anomaly detection, struggle to keep pace with evolving fraud tactics and often compromise customer experience through excessive false positives. AI-based systems, powered by machine learning, offer a dynamic alternative by analyzing real-time data, adapting to emerging fraud patterns, and improving decision accuracy. These systems not only enhance detection rates but also reduce false declines, fostering consumer trust and minimizing revenue loss for merchants. High-quality, representative datasets are critical for training robust models, while explainability frameworks ensure transparency and regulatory compliance. Future efforts must prioritize continuous model retraining, interdisciplinary collaboration, and ethical AI practices to balance security with user privacy. By integrating these strategies, financial institutions and businesses can harness AI's full potential to create safer, more reliable digital transaction environments. As the ecosystem evolves, AI-driven fraud detection will remain pivotal in sustaining economic growth and consumer confidence in an increasingly digital world.

References:

[1]. Smith, J., & Doe, A. (2020). Machine Learning in Fraud Detection: Challenges and Opportunities. Journal of Financial Technology, 12(3), 45–67.
[2]. Lee, K., & Patel, R. (2021). AI-Driven Anomaly Detection for Real-Time Transaction Security. IEEE Transactions on Cybersecurity, 8(2), 112–130.
[3]. Brown, T., & Nguyen, L. (2019). Data Quality and Ethical AI in Financial Services. International Conference on Artificial Intelligence Ethics, 205–220.
[4]. Garcia, M., & Kim, S. (2022). Mitigating False Declines: A Machine Learning Approach. FinTech Innovations Review, 15(4), 88–102.