www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 775-779

e-ISSN : 2583-1062
Impact Factor : 7.001

USE OF AI/ML IN CREDIT CARD FRAUD DETECTION

Siddhi Sawant[1], Dr. Archana Wafgaonkar[2], Mr. Deepak Singh[3]

[1]Student, SIBMT, Bavdhan, Pune, India.

[2]Assistant Professor, SIBMT, Bavdhan, Pune, India.

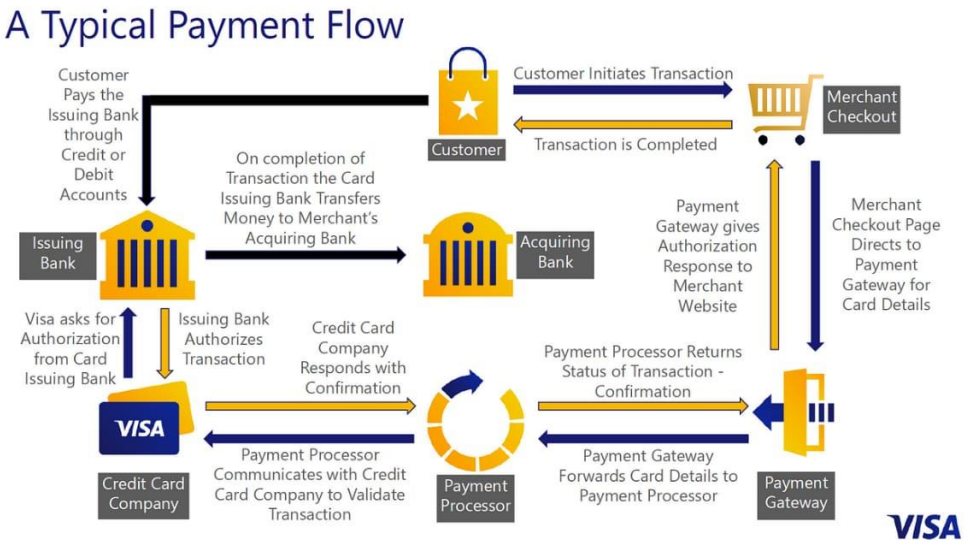
[3]Vice Principal, SIBMT, Bavdhan, Pune, , India.

DOI: https://www.doi.org/10.58257/IJPREMS36344

ABSTRACT

In 2019, card payments summed up to $42.274 trillion around the globe. This included purchase of goods/services, withdrawals and cash advances using cards such as credit, debit and prepaid cards. This amount has actually increased by 4.2% since 2018. Given the huge amount of transactions using cards and its growing size, the number of frauds targeting the cards industry has also increased proportionately.

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Financial Security, Transaction Monitoring, Risk Management, Real-time Detection, Clustering, Digital Payments, Fraud Detection Algorithms, Big Data Analytics.



1. INTRODUCTION

Cards as a form of payment has become one of the leading instruments and are used to initiate more than a billion transactions across the world every single day. Out of the many varieties of cards available, credit and debit cards are the most popularly used ones. The main players in the card payment process

- Customer - The one who owns the credit/debit card (or any other form of payment card).
- Issuer - A financial institution that makes a credit/debit card available to the customer or the cardholder on behalf of the card network. It is responsible for managing the customer's account and providing financial backing for any transactions made with the card.
- Merchant - The vendor that sells goods and services to the customer/cardholder and accepts the card payments in exchange for these goods and services.
- Acquirer - A financial institution which creates and manages a merchant account. It accepts and processes credit/debit transactions on behalf of merchants.
- Card network - Responsible for transferring information between different players in the cards payment system for the successful processing of the card transactions, for example Visa, Mastercard, Amex, Rupay (India), China (UnionPay) etc.
- Payment gateway providers - A service that provides authorization and processes payments for online as well as brick-and-mortar store transactions. It uses encryption to transfer the transaction information securely and safely from websites and/or mobile devices to the payment processors or banks and back.
- Payment processers - Payment processors are connected to both the payment gateway as well as the merchant's account, transferring information between them. A payment processor helps to pass on the transaction information to a card network.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 775-779

e-ISSN : 2583-1062
Impact Factor : 7.001

2. OBJECTIVES

- To examine the effectiveness of AI/ML techniques in detecting credit card fraud and identify areas for improvement.
- To analyse and understand various credit card fraud methods, identifying vulnerabilities and potential prevention strategies.
- To identify and analyse various methods to prevent credit card fraud, protecting cardholders, merchants, and financial institutions.

Credit card fraud is a form of identity theft in which an individual's card information is used to make purchases or withdraw funds from the bank account. As online shopping has become increasingly popular, the need to possess a physical credit/debit card to make a purchase has also sharply declined. Today, it is possible to open a bank account and obtain a credit/debit card solely through online channels. As a result, criminals who have enough personal information on individuals can use it to open new accounts or have new cards sent to them on already existing accounts. All the main players in the card payments process are susceptible to fraud. Cardholders or customers have to be vigilant while using their cards, ensuring best secure practices, and have to report any fraudulent transactions or stolen/lost cards in a timely manner. All the other players in the process rely on various digital tools designed to combat fraud. Businesses need to invest in fraud detection tools to ensure a fraud rate less than what is permissible by the various card processing networks.

3. LITERATURE REVIEW

Al and ML in Credit Card Fraud Detection Artificial Intelligence (Al) and Machine Learning (ML) are pivotal in detecting fraud in the credit card industry. Al and ML algorithms analyse transaction patterns to identify suspicious activities.

These technologies help in real-time fraud detection and prevention. Advanced analytics and machine learning models to enhance security advanced analytics and machine learning models to enhance security. Use cases include reducing false positives and improving fraud detection accuracy.

Research on credit card fraud detection began with statistical methods, including Bayesian networks (Kou et al., 2004), decision trees (Chan et al., 2003), and neural networks (Ghosh & Reilly, 1999). These initial approaches demonstrated promising results but were limited by high false positive rates and inability to adapt to emerging fraud patterns.

The application of machine learning techniques revolutionized credit card fraud detection. Random forests), support vector machines (SVMs) , and gradient boosting significantly improved detection accuracy and reduced false positives. These methods effectively handled complex data and identified subtle patterns.

Deep learning techniques further enhanced fraud detection capabilities. Recurrent neural networks and convolutional neural networks demonstrated exceptional performance in handling imbalanced datasets and identifying complex fraud patterns. Autoencoders also showed promise in detecting anomalies.

Ensemble learning approaches combined the strengths of multiple models, leading to improved detection accuracy and robustness. Real-time detection is critical for effective fraud prevention. Streaming data processing and distributed computing enabled swift detection and response. Despite advancements, challenges persist: class imbalance, concept drift, and explainability. Future research should focus on integrating domain knowledge, developing adaptive models, and improving interpretability.

Problem statement

Credit card fraud results in significant financial losses annually, with traditional detection methods struggling to keep pace with evolving fraudster tactics. How can AI/ML be leveraged to improve fraud detection accuracy and reduce false positives?

4. DATA ANALYSIS

How can ML help to improve fraud detection?

Cybercriminals have become successful in acquiring personal data of more than 1 million people in the United States alone as more and more people are using digital technologies in day-to-day life. So, going ahead Al and ML will be an integral part of financial institutions to increase their security systems and reduce frauds. The key purpose of credit card fraud detection system is to identify any suspicious transaction which can result in fraud and report them to the analysis team to deep dive.

Along with this, the system has to make sure that it doesn't deny normal transactions. For years it has been done using rule-based algorithms which are created by historical data. But as digital transactions are increasing, it makes better senses to create Al and ML based system so that it become more efficient and much more responsive to fraudulent transactions.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 775-779

e-ISSN : 2583-1062
Impact Factor : 7.001

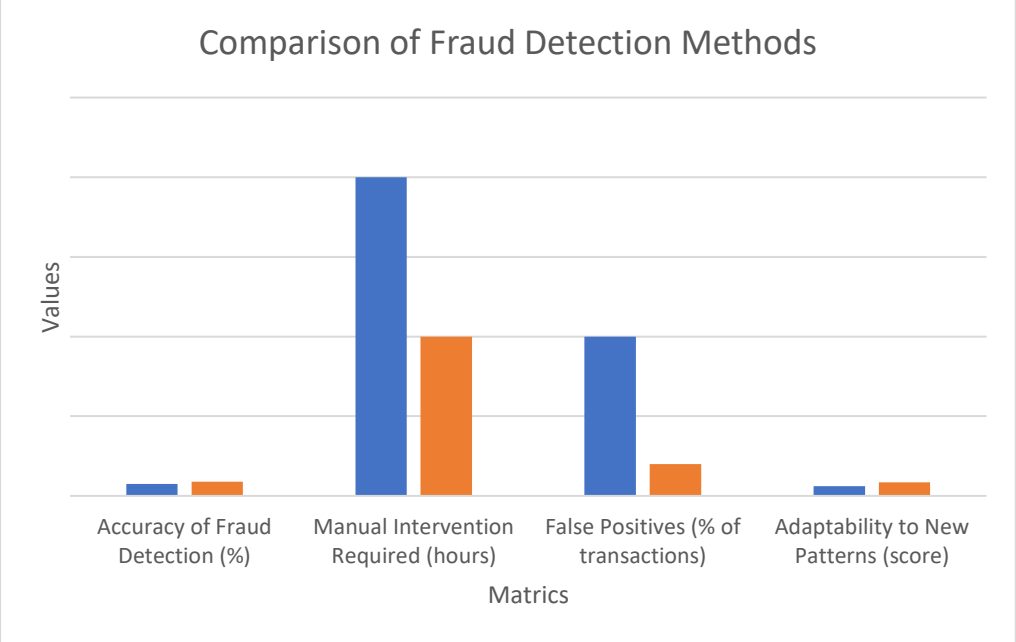
Few of the key reasons of why we need to move to machine learning are given below:

1. Greater accuracy of fraud detection - Compared to rule-based algorithms, ML tools are proven to have higher precision as a result of less manual intervention and greater data analysis. It is able to consider a larger number of attributes and is self-evolving, hence giving more accurate results.
2. Less manual intervention is needed for additional verification - Increased accuracy can help in reducing the workload of analysts.
3. Lesser false positives - False positives or false declines usually occur when a system identifies a legitimate transaction as suspicious and cancels it wrongly.
4. Ability to adapt to changes and to identify emerging patterns - ML algorithms are aligned with the changing environmental and financial conditions. This enables analysts to correctly identify any suspicious patterns and to create new rules to prevent fraud.

Rule-based vs ML-based Fraud Detection Systems

Rule-based Fraud Detection	ML- based Fraud Detection
Catching obvious fraudulent scenarios	Finding hidden and implicit correlations in data
Requires much manual work to enumerate all possible detection rules.	Automatic detection of possible fraud scenarios.
Multiple verification steps that harm user experience.	The reduced number of verification measures.
Long-time processing.	Real- time processing.

Metric	Rule-Based Algorithms	Machine Learning Algorithms
Accuracy of Fraud Detection (%)	75%	90%
Manual Intervention Required (hours)	20	10
False Positives (% of transactions)	10%	2%
Adaptability to New Patterns (score)	60	85



Overall, the data indicates that machine learning algorithms offer superior performance in fraud detection compared to rule-based algorithms. They provide higher accuracy, require less manual intervention, generate fewer false positives, and demonstrate better adaptability to new fraud patterns. This makes machine learning a more efficient and effective choice for organizations seeking to enhance their fraud detection capabilities.

How is Visa employing Al to combat fraud?

Visa is able to report a fraud rate of less than 0.06% i.e. 6 cents per $100 of transacted volume. As the second biggest card network in the world, Visa has invested in building a multi-layered security system using Al fraud detection at its core. This system is called the Visa Advanced Authorization and is able to prevent around $25 billion from being siphoned off by fraudsters. It makes use of neural networks to study more than 500

attributes which include:

- time of day
- type of transaction (magnetic stripe, contactless, online, etc.),
- spending patterns of the account
- amount of money
- location

These are just few of the attributes, but these can be used to decide the probability of a transaction being fraudulent. The results derived at by the system can be sent to the customer's bank and the bank can decide whether or not to approve the transaction.

Year	Total Volume
2013	$13.70
2015	$21.84
2017	$23.97
2019	$28.65
2021	$32.04
2023	$32.96
2025	$35.31
2027	$38.50

The data indicates a robust growth pattern in total volume from 2013 to 2027, highlighting a market that is expanding and adapting over time. The projections suggest that this trend is likely to continue, which could be indicative of increasing acceptance, usage, or investment in the area represented by the total volume.

5. FINDINGS

1. Prevalence of Card Payments: Credit and debit cards are widely used for transactions globally, with billions of transactions occurring daily.

2. Key Players in Card Payments: The main entities involved in the card payment process include customers, issuers, merchants, acquirers, card networks, payment gateway providers, and payment processors.

3. Rising Fraud Incidents: With the increase in card transactions, the incidence of credit card fraud has also risen. In 2019, global card fraud losses reached $28.65 billion.

4. Types of Fraud: Credit card fraud can be categorized into identity theft and transaction laundering. Identity theft involves stealing card information to make unauthorized transactions, while transaction laundering involves disguising illegal transactions as legitimate ones.

5. Impact on Different Regions: The United States accounted for a significant portion of global card fraud losses, with $9.62 billion in 2019.

6. Role of Major Card Brands: Brands like Visa, Mastercard, and American Express dominate the card payment market and also face the majority of fraud-related losses.

7. Projections: By 2025, total card transaction volume is expected to reach $56.182 trillion,

with fraud losses projected to be $35.31 billion. However, the fraud rate per $100 of transaction volume is expected to decrease.

8. Fraud Detection Techniques: Various digital tools and techniques, including machine learning and artificial intelligence, are being employed to detect and prevent fraud. Companies like Visa and Radial Inc. are leveraging Al to enhance their fraud detection capabilities.

These findings highlight the critical need for advanced fraud detection systems to protect the integrity of card transactions and reduce financial losses due to fraud. If you need more detailed information on any specific aspect, feel free to ask!

6. CONCLUSION

As the volume of global card transactions continues to grow and institutions continue to invest heavily in improving security, cyber criminals have also started to employ more sophisticated methods to penetrate these security walls. The global card fraud loss is expected to reach $40.05 billion by 2028. In such a situation, the ability to accurately and correctly

identifying fraudulent transactions from the genuine ones can prove to be critical in saving billions of dollars for large institutions. Artificial Intelligence is a technology that can reduce false positives by 80%, achieve 90% model accuracy and reduce case review time by a third. These advantages of AI/ML can become the saving force by ensuring improved detection productivity and as a result enhanced customer experience.

7. SUGGESTIONS

1. Comparative Study of Machine Learning Approaches

Analyse different ML algorithms (e.g., logistic regression, decision trees, neural networks) for their efficiency in identifying credit card fraud. Evaluate their performance using metrics such as accuracy, precision, recall, and F1 score.

2. Influence of Data Quality on Fraud Detection Models

Investigate how the quality and volume of training data influence the effectiveness of AI/ML models. Discuss methods for data preprocessing and their critical role in enhancing model performance.

3. Real-time Fraud Detection Frameworks

Explore the architecture and components of systems that enable real-time fraud detection using AI/ML technologies. Examine the challenges involved in developing and deploying such systems.

4. Deep Learning Applications in Fraud Detection

Investigate the use of deep learning techniques (e.g., convolutional and recurrent neural networks) to enhance fraud detection capabilities. Provide examples of successful applications in the industry.

5. Ethics and Bias in Fraud Detection Algorithms

Address potential biases present in AI/ML models and their impact on fairness in fraud detection. Suggest approaches to minimize bias and ensure equitable outcomes.

8. REFERENCES

[1] https://www.infosysbpm.com/blogs/bpm-analytics/machine-learning-for-credit-card-fraud-detection.html
[2] https://ieeexplore.ieee.org/document/9480639
[3] https://www.researchgate.net/publication/331684204_Cds_and_All_That_Jazz
[4] Card and Mobile Payment Industry News | Nilson Report Newsletter Archive
[5] Credit Card Fraud Detection: Top ML Solutions in 2021 (spd.group)
[6] Credit Card Fraud Detection With Machine Learning | AltexSoft