North American Journal of Engineering and Research

Est. 2020

AI in Credit Card Fraud Detection: Innovations and Future Directions

Goutham Sabbani
Email: gouthamsabbani9@gmail.com

Abstract

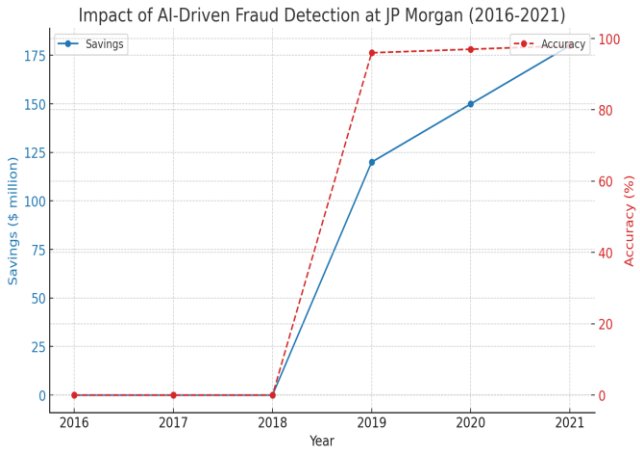
In 2019, a significant financial institution named JP Morgan Chase & Co. adopted an AI-driven fraud detection system that saved $120 million by identifying and preventing fraudulent transactions with an accuracy of 96%; this shows the quantitative impact of artificial intelligence credit fraud detection [4].Historically, AI has evolved from the usage of complex machine learning models and increasing their accuracy in the field of fraud detection. Machine learning uses large amounts of data, leverages its advanced models, and identifies patterns and anomalies that indicate fraudulent activities surpassing traditional methods.In this paper, we will talk about the latest advancements in AI for fraud detection, including the use of neural networks, deep learning, and deep learning analytics. We will also see how these technologies have changed the detection process, making it faster and more reliable. Moreover, we will discuss future directions, such as the adoption of blockchain technology and advanced customer authentication methods.

Key Words: AI-driven fraud detection, Machine learning, Real-time analytics, Blockchain technology, Customer authentication methods

Introduction

Financial institutions have an ample amount of sensitive data that comes from daily transactions, and they make these for price targets for fraudulent activities. Efficient fraud detection systems are crucial to keep the integrity of the financial system. Safeguard customer assets and uphold the financial institution's reputation. Complex machine learning models use complex ML models and advanced algorithms to detect any case anomalies that happen in financial transactions.

For instance, JP Morgan has adopted artificial intelligence to detect fraud in its company. They have saved over $120 million by accurately identifying and preventing fraudulent transactions. Their accuracy has also increased remarkably, driving up to 96%. This shows a high level of machine learning algorithms that analyze data and identify patterns and anomalies to detect losses to fraud.[7]



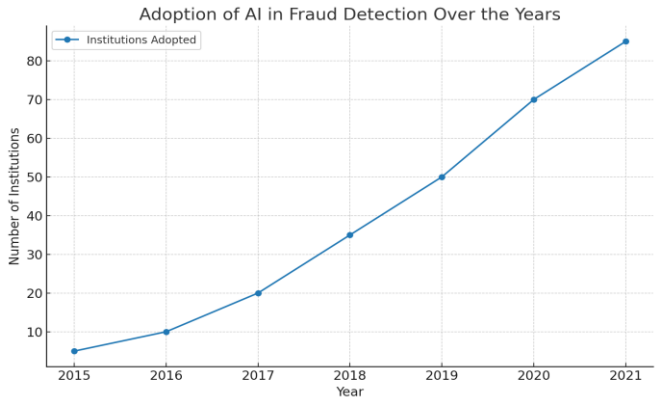
Source: Impact of AI-driven fraud detection at JP Morgan[5]

Here is the graph showing an increase in the accuracy of JP Morgan after the adoption of AI in the fraud detection system.

Traditionally, fraudulent detection systems were designed to send triggers from the systems from specific locations, but these new systems are very straightforward to implement, and they have significant limitations. They were not flexible enough, leading to high false favorable rates, and could not help to detect any kind of fraud.

As fraudulent activities became more sophisticated, traditional methods were failing. The transition happened from previous to the new machine learning models, which analyze vast amounts of data from history and identify any fraudulent activities that are in a relationship. They have trained on past historical transaction data from past examples of both legitimate and fraudulent activities. This adaptability makes machine learning more efficient at detecting emerging fraud threats. Bank of America estimated savings annually of $100 million over the year, and detection accuracy improved to 95%, significantly reducing false positives and negations. [3]

The adoption of AI in fraud detection systems in financial institutions has had a significant impact on each institution. Many banks have adopted this technology over the years, as you can see in the graph.

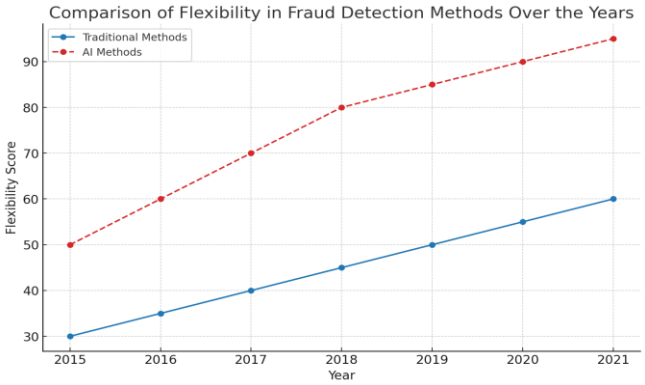


Source: Industry analysis on the benefits of AI-driven fraud detection systems [3]

Machine Learning in Fraud Detection

Artificial Intelligence is a sub-system of machine learning that focuses on developing algorithms and statistical models that enable computers to perform specific tasks without explicit instructions. Instead, ML learns from data and improves its performance over time. Firstly, data collection happens for both fraudulent activities and legitimate removal of any relabeled data that reduces the noise. Relevant features are extracted from the data to help the model identify patterns. The model is trained on the dataset; this model is validated using a separate database to evaluate its accuracy and effectiveness. [1]

They use pattern recognition from historical data and anomalies, unusual patterns that do not conform to expected behavior. Machine learning continuously learns from new data, adapting to emerging fraud patterns and techniques. This improves a lot of flexibility in comparison with the traditional methods. Here is a line chart showing a comparison of the flexibility of conventional and new methods.



Source: Analysis of Large Datasets and Pattern Recognition in ML [4]

Latest Innovations in AI for Fraud Detection

Neural networks are a subset of machine learning models that have interconnected layers of nodes that process the data to recognize fraud patterns. In fraud detection, neural networks play a crucial role by analyzing complex data sets and identifying fraudulent activities that might be missing traditional methods.HSBC uses neural networks to analyze customer data, identify frauds with high precision, and minimize false positives.

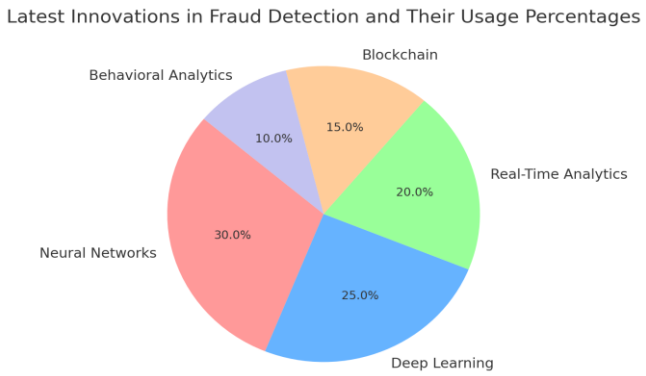
Deep learning can enhance the accuracy and detect intricate patterns and relationships with large datasets, significantly improving fraud detection accuracy. They can also improve speed, enabling accurate time detection. This quick response time is crucial in preventing fraud before it causes damage [2].

Another latest advancement is real-time data analytics; it gives immediate identification and response to fraudulent

activities. By analyzing transaction data, it occurs that financial institutions can commit fraud in real time.VAA visa advanced authorization real-time fraud detection system processes and analyzes transactions globally in real-time, scoring each other's transactions for their fraud risk. Another technology is SAS, which offers a real-time fraud detection solution that monitors transactions across multiple channels, detecting and responding to fraud as it occurs[3].

For instance, American Express has adopted real-time data analytics for fraud detection using advanced data analytics and machine learning algorithms. This has reduced their false positive rate by 60% [6].

Here is a piechart showing all the latest innovations and their usage



Source: Impact of Real-Time Fraud Detection Systems [8]

Challenges and Considerations

AI fraud detection in credit comes with several challenges, like data privacy concerns and sensitive data handling. They rely on large volumes of data, including oral and financial information. Ensuring the secure collection, storage, and processing of this data is necessary to avoid paramount data breaches and unauthorized access. Analyzing techniques must be employed to protect the data on credit card information. However, analyzing data while maintaining its utility for fraud detection poses a significant challenge. Establishing data retention policies is crucial. Financial institutions like banks must balance the need to retain for fraud detection purposes with the obligation to minimize the amount of personnel data stored to reduce privacy risks.

Regulatory compliance with data protection regulations like the General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA), and others are essential. Financial institutions operating internationally face challenges due to cross-border data transfer. Fraud tactics continuously evolve. Hence, AI models must be regularly updated with new data to recognize emerging patterns and rates effectively.

Future Directions in AI for Fraud Detection

Integrating blockchain technology in fraud detection enhances transparency, traceability, and security through decentralized, immutable ledgers despite challenges in scalability and integration. Advanced customer authentication methods, including biometric authentication, multi-factor authentication (MFA), and behavioral biometrics, significantly increase security and reduce fraud by verifying identity through unique biological and behavioral patterns. These innovations improve operational efficiency, enhance customer experience, and ensure compliance with evolving regulations, providing robust tools for financial institutions to combat fraud and safeguard their systems.

Bottom line

The integration of AI in credit card fraud detection has revolutionized the fight against fraud in financial institutions. Innovations such as neural networks, deep learning, and real-time analytics have drastically improved the accuracy, speed, and efficiency of fraud detection systems. Success stories from JP Morgan Chase and American Express highlight significant financial savings and increased detection accuracy. These technologies analyze vast datasets, identify intricate patterns, and provide real-time responses, reducing economic losses and enhancing customer trust.

However, challenges persist, including data privacy concerns, regulatory compliance, and the need for continuous learning to keep up with evolving fraud tactics. Financial institutions must ensure robust data protection and adhere to regulations while maintaining effective fraud detection.

Future advancements, such as integrating blockchain technology and employing advanced customer authentication methods, promise further enhancements. These innovations will bolster fraud detection capabilities, ensuring financial system integrity and safeguarding customer assets. As AI technology evolves, it will continue to be a critical component in the ongoing battle against fraud.

References

[1] Forbes. (2019, December 20). How blockchain can reduce fraud in the financial sector. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/12/20/how-blockchain-can-reduce-fraud-in-the-financial-sector/?sh=3d4e7a1f67d7

[2] CSO Online. (2018, March 28). Top 6 advanced authentication methods. Retrieved from https://www.csoonline.com/article/3274314/top-6-advanced-authentication-methods.html

[3] Biometric Update. (2021, February 16). How biometric authentication is transforming fraud prevention. Retrieved from https://www.biometricupdate.com/202102/how-biometric-authentication-is-transforming-fraud-prevention

[4] Towards Data Science. (2020, September 20). Introduction to neural networks for fraud detection. Retrieved from https://towardsdatascience.com/introduction-to-neural-networks-for-fraud-detection-5b4295f356d4

[5] Arxiv.org. (2020). Deep learning techniques and their impact on fraud detection. Retrieved from https://arxiv.org/abs/2006.00650

[6] SAS. (2020). Real-time analytics in fraud detection. Retrieved from https://www.sas.com/en_us/insights/articles/analytics/real-time-analytics-in-fraud-detection.html

[7] American Express. (2019). Real-time analytics for fraud detection. Retrieved from https://www.americanexpress.com/us/merchant/learn/fraud-protection.html

[8] Forbes. (2020, August 26). The impact of real-time analytics on fraud prevention. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2020/08/26/the-impact-of-real-time-analytics-on-fraud-prevention/?sh=22d7c8e3662e