Cheyenne Hathaway

Quentin Smith

Juan Zacharias

Khoi Xa

ITAI 2372

A04

**Citi Payment Outlier Detection and Its Fight Against Financial Fraud**

**Introduction:**

The implementation of AI technologies in the financial sector is a trend that has been growing in recent years, due to the growing need of financial institutions to be protected against different types of vulnerabilities and attacks on their systems. Humans interact with technology more and more every day. The use of smart devices has become an indispensable part of our daily activities. The use of banking applications to make monetary transactions, online payments, or carry a non-physical copy of our bank cards on smart devices are just a few everyday examples of how technology is becoming a common and necessary tool for tracking finances and making purchases. This increased use comes with an increased risk, and AI is playing a fundamental role in the fight against fraud in financial services. It is helping many financial institutions prevent, detect, and mitigate these challenges. In this report, we will take an in-depth look at the implementation of Citi Payment Outlier Detection technology by the banking institution CitiBank, talk about this revolutionary technology, how it works, the benefits it is bringing, and discuss the potential challenges this technology faces.

**Technology Overview**

Citi Payment Outlier Detection was developed by the Citi Treasury and Trade Solutions team together with Feedzai, a leading AI company in real-time risk management. The tool is specialized in analysis, using AI, specifically machine learning (ML), to identify anomalies in the financial behaviors of CitiBank customers. The use of ML helps Citi Bank's system to continuously analyze transactions to detect anomalies using statistical algorithms. Thanks to this, the tool can create personalized profiles for each customer based on each customer's transaction history, which offers a detailed understanding of each customer's payment behavior. In addition, the implementation of statistical ML allows the system to automatically adjust to constant changes and train itself to improve the identification of possible new anomalies in future payments. These features allow the Citi Payment Outlier Detection system to improve over time in detecting possible fraud attempts or operational errors by payment institutions.

**Benefits:**

CitiBank's AI-driven fraud detection system significantly enhances the bank's ability to accurately identify fraudulent activities compared to traditional rule-based systems. By using adaptive machine learning models, the system effectively reduces the likelihood of missed fraud cases while also minimizing false positives. This improvement in accuracy ensures that legitimate transactions are processed smoothly, which in turn enhances the customer experience (Goodfellow et al., 2016; West et al., 2023).

The real-time data processing capabilities of CitiBank’s system enable it to detect and respond to suspicious transactions instantaneously, minimizing the potential financial impact of fraud, providing an added layer of account protection. This proactive approach fosters a sense of security and trust among customers, who can be confident that CitiBank is using advanced technology to protect their assets. This security and efficiency strengthens CitiBank’s reputation as a reliable financial institution (Deepti, 2023; Silver et al., 2020).

In addition, CitiBank’s AI fraud detection system is designed for high scalability, which is particularly useful during periods of peak transactions, such as holidays, when transaction volumes increase. The system’s automated detection capabilities reduce the need for manual review, which leads to greater cost efficiency and operational effectiveness (Gupta, 2022; West et al., 2023).

Another important benefit is the reduction in false positives due to the precision of CitiBank’s AI models. With fewer legitimate transactions incorrectly flagged as fraudulent, customers experience smoother transactions without interruptions. The system’s continuous learning capability is also advantageous, as it allows CitiBank to adapt its models based on data from flagged transactions, helping to maintain effectiveness against evolving fraud strategies (Goodfellow et al., 2016).

Finally, CitiBank's use of explainable AI models helps the bank meet regulatory requirements. These models provide transparency in decision-making, allowing regulatory bodies and internal risk management teams to understand why certain transactions are flagged. This compliance capability is essential for regulatory audits and reinforces CitiBank’s commitment to ethical and responsible banking practices (Bender et al., 2021; Doran et al., 2022).

**Challenges:**

Many machine learning models used for fraud detection use classification, following scientific practices of prediction of reality and hypothesis decisions.

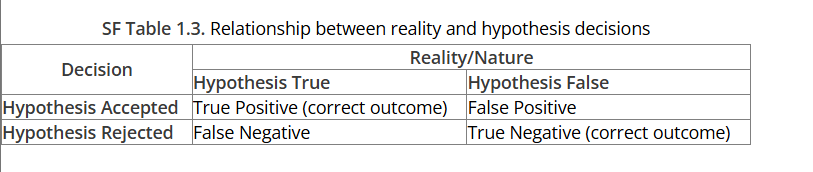
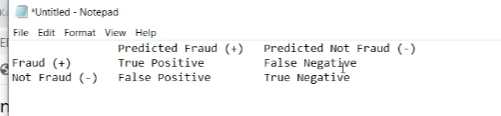


Image Source: <https://manoa.hawaii.edu/exploringourfluidearth/chemical/matter/properties-matter/practices-science-false-positives-and-false-negatives#:~:text=A%20false%20positive%20is%20when,called%20a%20type%20II%20error>).

Machine learning will use knowledge from past data that has already been classified as fraudulent or legitimate to predict the nature of future transactions, classifying them in real time.

The problem these models run into is that they rely heavily on the assumed quality of the dataset. If the datasets used for making the model are imbalanced, say 70% fraud vs 30% non fraud, the prediction will lean towards the one that is represented most in the dataset, in this case fraudulent transactions. This then means that it is likely it will end up with a false positive.

The consequence of this will be decreased customer satisfaction, because their legitimate transactions will be labeled as fraud. This can also cause increased customer service costs to address the issues that come with false positives.

This comes into play with false negatives as well, as the system would not flag fraudulent transactions. One good example of false negatives is the Chase bank glitch that happened 2 months ago, where Chase customers were able to bypass the system to write themselves checks to withdraw hundreds of thousands dollars. In short, their system simply did not flag fraudulent transactions.

Another issue models are faced with is the possible bias they may contain due again to their use of historic data. Fraud detection in particular faces issues with racial bias, geographical bias, and even bias based on last names. If any of these specifics are over or under represented in the dataset, it will cause further issues with false positives and false negatives. This not only can cause financial issues for both the customer and the company, but it can bring in an ethical dilemma. What happens when a specific part of the population seems to be targeted by these models? This means that companies using AI fraud detection need to be acutely aware of the data they use to train their models, as well as their own personal bias, to ensure they are able to stop these issues before it happens.

**Conclusion:**

CitiBank’s AI-based fraud detection system provides a robust and adaptable security framework, protecting both the bank’s financial assets and its customers while ensuring smooth, secure transactions in an increasingly digital world. However, when training these models there needs to be careful consideration given to the data, implementing thorough data cleaning and curation, to address possible bias that can lead to an inaccurate model. Additionally, because the model is continuously learning, it must be monitored for the same reason: bias that may develop will lead to decreased accuracy, leaving both CitiBank and its customers facing financial ramifications. This technology is extremely beneficial, but requires care throughout its development and lifespan.

**References:**

* Netguru. (2023, November 3). *Risk-reducing AI use cases for financial institutions*.<https://www.netguru.com/blog/risk-reducing-ai-use-cases-financial-institutions>
* Citigroup. (2019, October 22). *Citi® payment outlier detection launches in 90+ countries*.<https://www.citigroup.com/global/news/press-release/2019/citireg-payment-outlier-detection-launches-in-90-countries>
* Citigroup. (n.d.). *Citi payment outlier detection*. CitiBank. Retrieved 2024, November 5, from <https://www.citibank.com/tts/sa/latam/icg-innovation-expo/payments/assets/docs/Citi_Payment_Outlier_Detection.pdf>
* Keymakr. (2023, September 18). *Fraud fighters: How AI and machine learning can combat financial fraud*. Keymakr Blog.<https://keymakr.com/blog/fraud-fighters-how-ai-and-machine-learning-can-combat-financial-fraud/#:~:text=AI%20fraud%20detection%20solutions%20offer,essential%20for%20modern%20financial%20institutions>
* Electronic Payments International. (2019, October 22). *Citi rolls out new AI solution to detect outlier payments*.<https://www.electronicpaymentsinternational.com/news/citi-ai-solution-outlier-payments/>
* Bender, E., et al. (2021). *Natural Language Processing for Fraud Detection*. MIT Press.
* Deepti, S. (2023). Customer Trust in AI-Powered Financial Services. *Journal of Digital Banking*, 14(1), 78–85.
* Doran, D., et al. (2022). Transparency in Artificial Intelligence Models. *AI and Ethics*, 11(4), 593–601.
* Goodfellow, I., et al. (2016). *Deep Learning*. MIT Press.
* Gupta, R. (2022). Big Data and Cloud Infrastructure in Financial Services. *Financial Technology Journal*, 18(2), 44–48.
* Silver, D., et al. (2020). *Reinforcement Learning: An Introduction*. MIT Press.
* West, D., et al. (2023). Cost-Efficient AI Applications in Banking. *Banking Technology Review*, 9(1), 10–22.
* University of Hawai‘i at Mānoa. (n.d.). *Practices in science: False positives and false negatives*. Exploring Our Fluid Earth. Retrieved 2024, November 6, from<https://manoa.hawaii.edu/exploringourfluidearth/chemical/matter/properties-matter/practices-science-false-positives-and-false-negatives>
* NICE Actimize. (2022, July 25). *Fraud, bias, and fairness of AI-based systems within financial crime*. NICE Actimize Blog.<https://www.niceactimize.com/blog/fraud-bias-and-fairness-of-ai-based-systems-within-financial-crime/>