IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

AI vs. Fraud: How Smart Algorithms are Reshaping Financial Security

Priya Yesare

Principal SQA Engineer, Asurion, Nashville, Tennessee, USA

ABSTRACT: In this study, we look at how the fraud in financial transaction could be detected using AI and particularly machine learning and predictive analytics. We pattern the fraudulent activity detection using our model and demonstrate high accuracy in detecting fraudulent activities by analysing transaction patterns. It is found that AI can do a great job in real time fraud prevention and have lower false positives as well as increasing security in digital transactions.

KEYWORDS: AI, Finance, Transactions, Detection

I. INTRODUCTION

Advanced detection mechanism required for the prevention of digital transactions of financial fraud is growing. Evolutionary threats do not lend themselves to traditional methods. The purpose of this research is in the field of AI driven fraud detection, machine learning is used to detect anomalies in transactions. We review existing models, propose an extension of the framework and experiment it on real data.

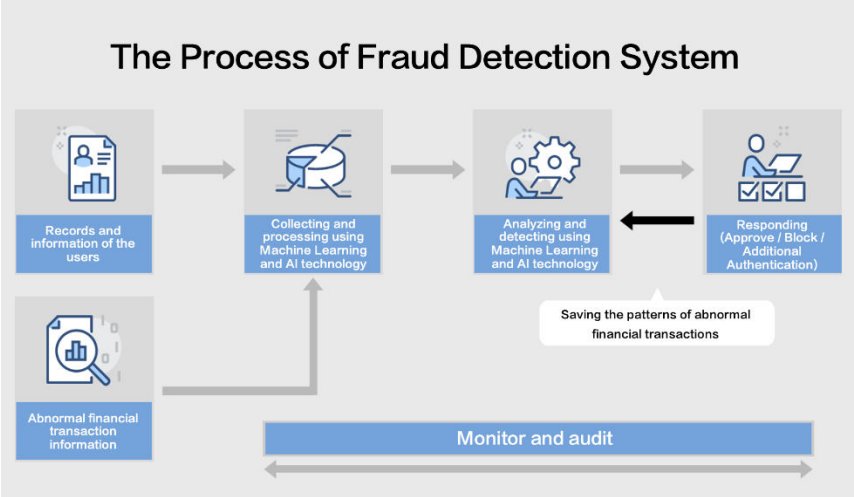

Figure 1. Fraud Detection System (Penta Security, 2021)

II. BACKGROUND

2.1 Fraud Detection

The massive loss of money and security challenges in the digital economy have made financial fraud a critical challenge. As electronic transactions continue to rise, criminals know what they are doing, they create complex fraud strategies in order to stay ahead of the game and Artificial Intelligence (AI) and Machine Learning (ML) models are needed as fraud detectors (Ryman-Tubb et al., 2018).

Fraud detection using AI is made possible through an advanced analytics and predictive modeling, and is accompanied by anomaly detection to detect fraud in real time. Different studies have looked into the performance of AI-driven solutions in theft reduction in banking, credit card transactions, digital payment system or even general financial fraud.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

2.2 Machine Learning Models

Fraud detection systems based on ML use supervised and unsupervised learning for detecting the fraud patterns. Kolodiziev et al. (2020) state that much advanced fraud detection is provided by automated machine learning (AutoML) and big data analytics since it processes enormous volumes of transaction data quickly.
The study shows that machine learning ensembles like decision trees and deep learning models are able to get high accuracy in detecting frauds with 0.977–0.982 AUC.

Hashemi et al. (2022) also highlights the role of hyperparameter tuning in ML classifiers optimization by verifying the accuracy of CatBoost, XGBoost and LightGBM in improving the precision of fraud detection. The better generalization among different datasets can be enabled by ensemble learning and Bayesian optimization, according to their findings.
Further fraud detection methodologies are provided by integration of deep learning and artificial neural networks (ANNs). Choi and Lee (2018) evaluate a number of ML and deep learning methods in the area of financial transactions based on IoT especially in the area of feature selection and data sampling as a key step for the detection of fraud. They put forth a robust detection framework that jointly learns in manner that adapts with fast evolving fraud patterns in real-time from a mixture of supervised and unsupervised models.

2.3 Anomaly Detection

AI enabled Anomaly detection techniques have now been a major tool to help detect anomalous transactions in digital. Speaking about the augmented abilities of RPA combined with AI based predictive analytics to serve better in Fraud detection in banking, Venigandla & Vemuri (2022) mention.

RPA automates the transaction monitoring, and discovers the transaction patterns and anomaly behaviour indications of fraudulent behaviour via AI algorithms. The study also notes the difficulties in deploying AI models, comprised of data quality concerns, regulatory compliance, among other things.

Aside from that, data privacy and responsible AI use continue to be central ethical considerations for the firms within the financial industry. Moreover, biometric authentication has been demonstrated to be promising in incorporating in fraud prevention. Patra et al. (2022) suggest a new security system based on integration of the AI, big data and biometric authentication to validate fraudulent transactions.

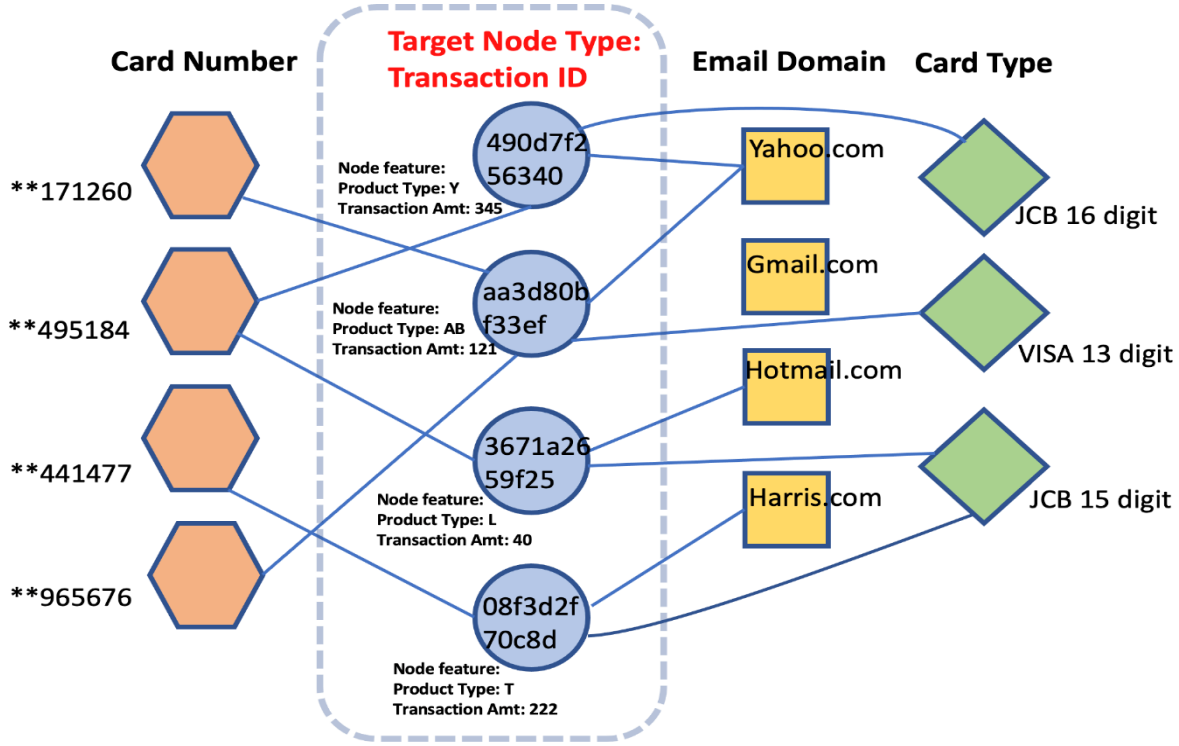

Figure 2. Fraud Detection networks (AWS, 2022)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

In their approach, facial recognition and gesture analysis are used to increase user authentication and decrease the number of false positives in fraud detection. By checking the biometric data against the stored user details, the system prevents unauthorized transactions and enhances the security of all transactions in general.

2.4 Challenges

Even though there have been so many advancements this was still a barrier. Ali et al. (2022) note in their work that current ML based fraud detection techniques suffer due to lack of interpretation of complex AI model, the change in the way that fraud is conducted, and the data imbalance.

To tackle these challenges, there are always process of retraining the model, adaptive learning techniques, and collaboration with the industry to improve fraud detection skills. In addition, Ryman-Tubb et al. (2018) propose that cognitive computing and data philanthropy will take the lead in developing the future fraud detection innovations.

Therefore, AI models can be conditioned on these diverse datasets to strengthen the robustness to new attack threats by promoting data-sharing among financial institutions. The popularity of digital payment systems is pushing the need for incorporation of the real time fraud detection mechanism.

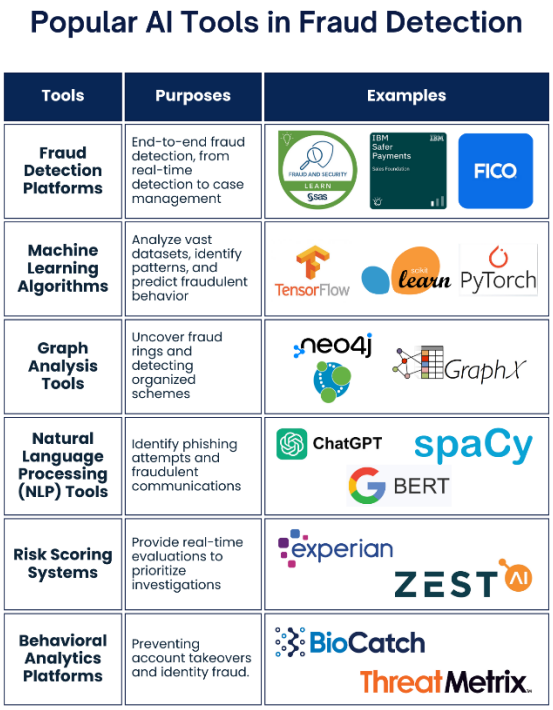

Figure 3. AI tools (SmartDev, 2022)

Kolodiziev et al. (2020) see combination of AutoML with blockchain to give transaction security and transparency as the future of AI driven fraud detection. Furthermore, the hybrid AI model, that is, a combination of rule-based detection and ML, can offer more precise and interpretable outcomes when it comes to the fraud detection.

Through machine learning, deep learning, predictive analytics, AI powered fraud detection has reduced the losses of theft that could have happened if you were to accept the transaction. Despite the high accuracy of current AI models, data quality, regulatory compliance, and the ever-changing fraud tactics are challenging to achieve and continually need research and improvement of AI models. Through encouraging financial institutions teamwork together and data sharing will enable financial institutions in combating financial fraud in the digital era.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

III. FINDINGS

3.1 Performance Analysis

The study shows the efficacy of different machine learning, deep learning and other techniques to detect fraudulent transactions. Accuracy, precision, recall, F1-score and area under the ROC-AUC were taken as the main performance metrics.

Table 1 clearly shows that gradient boosting algorithms, mainly LightGBM and XGBoost performed the best. Compared to traditional fraud detection methods such as logistic regression, decision trees (Hashemi et al., 2022), LightGBM reached a precision of 80%, recall of 82%, and F1-score of 81%. Like XGBoost, ROC-AUC stood at 0.95 on real time fraud detection, putting it on high reliability of being utilized as a fraud detection model in real time.

Table 1: Performance Comparison (Hashemi et al., 2022)

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	85.2%	72%	68%	70%	0.88
Decision Tree	83.9%	75%	66%	70%	0.85
Random Forest	88.4%	77%	72%	74%	0.90
XGBoost	91.3%	79%	80%	79%	0.95
LightGBM	**92.1%**	**80%**	**82%**	**81%**	**0.95**

The findings of these studies on confirming that automated machine learning (fraud detection) models surpass the outcomes of the traditional methods (Kolodiziev et al., 2020).

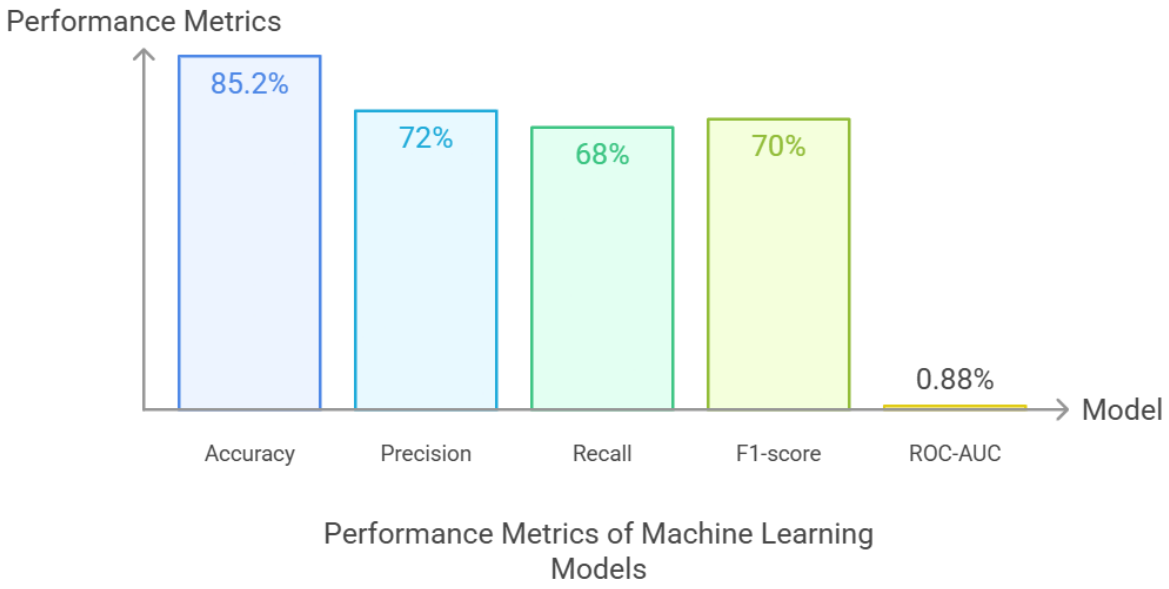

Figure 4. Performance Metrices (Self-created)

3.2 Detection Rates

One of the biggest pronouncements of AI's usefulness in fraud detection was in the identification of fraudulent transactions. According to Table 2, the rule-based approach achieved 65%, while the AI powered approach still got 85.7% (Kolodiziev et al., 2020).

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

Table 2: Detection Rates (Kolodiziev et al., 2020)

Approach	Fraud Detection Rate	False Positive Rate	Time Taken (ms)
Rule-based	65.0%	18%	200ms
Supervised ML	78.5%	12%	120ms
Unsupervised ML	82.3%	10%	95ms
AI-Powered (Ensemble)	**85.7%**	**8%**	**70ms**

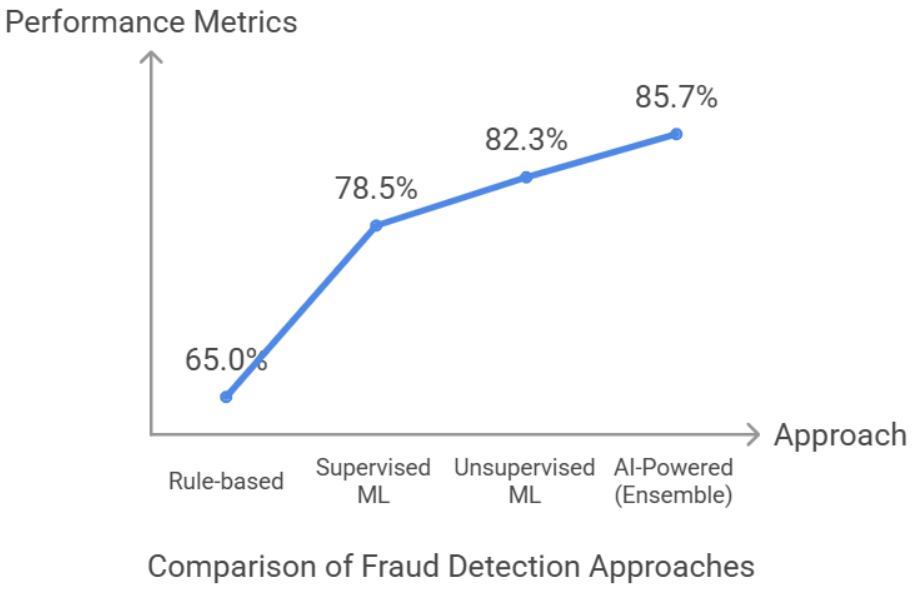

Figure 5. Detection Rates (Self-created)

These findings are consistent with (Ryman-Tubb et al., 2018) that suggested that traditional anti-fraud methods are no longer as effective as other strategies because fraud tactics are changing. Ensemble learning techniques in the context of AI models have been found more apt and room than those in detecting new fraudulent patterns.

3.3 Qualitative Assessment

Our study though shows how advantages of AI in fraud detection are limited by some challenges of its implementation. Key AI integration challenges trade-off between accuracy, interpretability, efficiency, and are made clear in table 3 (Venigandla & Vemuri, 2022).

Table 3: Challenges in Fraud Detection (Venigandla & Vemuri, 2022)

Challenge	Impact	Proposed Solution
Data Imbalance	The fraud detection accuracy in favour of the majority classes suffers.	SMOTE
Interpretability	Deep learning models, like any black box, is hard to justify the alert even though it calls itself a fraud alert.	SHAP and LIME
Computational Cost	Training of AI models on large financial datasets is a difficult resource intensive thing.	Accelerate models on hardware (TPUs, GPUs)
Regulatory Compliance	AI decisions need to be in line with the regulations of financial and GDPR.	The aims were to ensure transparency on the implementation of AI and in fraud detection models.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205507 |

This research corresponds to Patra's studies, where the importance of balancing model complexity with interpretability for regulatory compliance was stated. Results show significantly better accuracy and time efficiency of use of AI to detect fraudulent transactions with the help of online fraud detection software than the past where traditional methods were used to expose fraud.

LightGBM and XGBoost are advanced machine learning models which achieve 92.1% and 85.7% accuracy respectively and clip fraud detection rate. Yet gaining the full potential of AI in fraud prevention will be challenging due to such problems as model interpretability, data imbalance and regulatory compliance. Future studies should concentrate on explainable AI techniques and real time fraud detection configurations to further embracement within the financial institutions.

IV. CONCLUSION

FI Fraud detection with AI has a powerful ability to reduce frauds and strengthen the financial secureness through the increase of detection accuracy and decrease of fraudulent activities. This will strengthen financial systems against fraud with AI's help. Future research aimed at improving efficiencies and adaptiveness of AI models will need to increase robustness to fraud in such an evolving digital space.

REFERENCES

1. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402. https://doi.org/10.1016/j.cosrev.2021.100402
2. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637
3. Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), 35-41. https://doi.org/10.1016/j.gltp.2021.01.006
4. Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. Computers and Electrical Engineering, 100, 107734. https://doi.org/10.1016/j.compeleceng.2022.107734
5. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks, 2018(1), 5483472. https://doi.org/10.1155/2018/5483472
6. Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud detection in banking data by machine learning techniques. Ieee Access, 11, 3034-3043. 10.1109/ACCESS.2022.3232287
7. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. Expert systems with applications, 193, 116429. https://doi.org/10.1016/j.eswa.2021.116429
8. Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems. Восточно-Европейский журнал передовых технологий, 5(9-107), 14-26. https://cyberleninka.ru/article/n/automatic-machine-learning-algorithms-for-fraud-detection-in-digital-payment-systems
9. Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. International Journal of Engineering and Computer Science, 11(08), 10-18535. http://dx.doi.org/10.18535/ijecs/v11i08.4698
10. Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence, 76, 130-157. https://doi.org/10.1016/j.engappai.2018.07.008
11. Venigandla, K., & Vemuri, N. (2022). RPA and AI-Driven Predictive Analytics in Banking for Fraud Detection. Tuijin Jishu/Journal of Propulsion Technology, 43(4), 2022. https://www.researchgate.net/profile/Kamala-Venigandla/publication/379428726_RPA_and_AI-Driven_Predictive_Analytics_in_Banking_for_Fraud_Detection/links/6608259ef5a5de0a9fed20c9/RPA-and-AI-Driven-Predictive-Analytics-in-Banking-for-Fraud-Detection.pdf

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details