AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis

Damodharan Kuttiyappan[1], Rajasekar V[2]

{dt3388@srmist.edu.in[1], rajasekv2@srmist.edu.in[2]}

Ph.D. Research Scholar & Director in Natwest, India[1], Associate Professor, SRM, India[2]

Abstract. Fraudulent activities have become a pervasive and costly problem in today's interconnected world, threatening the stability and trustworthiness of various industries. The rise of sophisticated fraud tactics and the constantly evolving nature of fraudulent behavior necessitate innovative and adaptive solutions for fraud detection. Artificial Intelligence (AI) has proven to be powerful in the battle against fraud, offering promising capabilities to enhance the efficiency and accuracy of detection systems. This research paper delves into the cutting-edge domain of AI-powered fraud detection and presents novel approaches to tackle this challenging issue. It begins with an exploration of the current landscape of fraud detection methodologies, encompassing traditional rule-based systems, statistical methods, and machine learning techniques. It highlights the shortcomings of these conventional approaches and emphasizes the need for AI-based solutions to overcome the limitations posed by the dynamic nature of fraud.This paper introduces three novel AI-based fraud detection approaches - Graph Neural Networks (GNN) , Generative Adversarial Networks (GANs) and Temporal Convolutional Networks (TCN) , each harnessing the strengths of different AI techniques. The performance of the AI-powered approaches is meticulously compared against traditional rule-based systems, logistic regression, and random forest models. A comprehensive evaluation is performed to assess the superiority of the novel AI-based methods in detecting fraudulent activities.

Keywords: Cyber security, Artificial Intelligence (AI), Fraud Prevention, Fraudulent Pattern Recognition, deep learning (DL).

1 Introduction

Fraudulent activities have become a pressing challenge in modern society, posing significant financial losses and reputational risks for individuals, businesses, and governments alike. The proliferation of online transactions and increasing dependence on digital platforms have created ample opportunities for fraudsters to exploit vulnerabilities in various industries. Conventional methods for detecting fraud, such as statistical techniques and rule-based systems have proven inadequate in keeping pace with the ever-changing strategies used by fraudsters. Consequently, there is an urgent need for innovative solutions to detect and prevent fraud effectively.

We begin by conducting a comprehensive review of existing fraud detection methodologies, such as machine learning, statistical, and rule-based systems. We identify their strengths and weaknesses, highlighting the reasons behind their diminishing effectiveness. This analysis

IACIDS 2023, November 23-25, Lavasa, India

DOI 10.4108/eai.23-11-2023.2343170

underscores the urgency of adopting AI-powered solutions to bridge the gap between fraud detection capabilities and the rapidly changing tactics of fraudsters. AI-powered approaches offer the potential to revolutionize fraud prevention by leveraging advanced algorithms, machine learning, and data analytics to identify anomalous and fraudulent patterns with greater accuracy and efficiency

To achieve this goal, we propose three novel AI-based approaches for fraud detection. Each approach utilizes a different AI technique, such as Temporal Convolutional Networks, Adversarial Machine Learning, and Graph Neural Networks. Above strategies aim to use AI's advantages to get around the drawbacks of conventional techniques in handling complex and dynamic data.

To assess the effectiveness of the proposed AI-based approaches, extensive experiments are conducted using real-world datasets from diverse industries. We compare the performance of our approaches against traditional methodologies.

2 Related works

The most recent research publications in the field of fraud detection are examined in this area. highlighting the strengths and limitations of various approaches.

Rule-Based Systems: Early fraud detection systems were predominantly based on predefined rules and heuristics.. However, they often lacked the ability to adapt to new fraud schemes and were limited by their inability to capture complex patterns and interactions in high-dimensional data. Rule-based fraud detection (1) was pioneered by Batani. Their work laid the foundation for rule-based approaches and demonstrated the potential of using predefined rules.

Statistical Methods: Statistical approaches, such as anomaly detection and clustering, were introduced to address some of the limitations of rule-based systems. While statistical methods showed promise in detecting certain types of fraud, they often struggled with high-dimensional data. Lee and Wang explored the application of clustering techniques in fraud detection (2).

Machine Learning Techniques: Machine learning methods demonstrated improved performance over rule-based and statistical approaches, as they could automatically learn patterns and relationships from data. These approaches require extensive feature engineering and constrained to adapt to fraud patterns. Devi, Jemi & Ramachandran(3) explored the use of random forests. Their study demonstrated the effectiveness of machine learning techniques in detecting frauds in credit card transactions, paving the way for further exploration of AI-based approaches.

Neural Networks for Fraud Detection: Neural networks gained popularity for their ability to learn hierarchical structures from raw data. Traditional feedforward neural networks were limited by their inability to handle sequential data. To address this limitation, Benchaji(4) proposed the use of recurrent neural networks (RNNs). Their work demonstrated the potential of RNNs in capturing temporal dependencies and improving fraud detection accuracy.

Graph-Based Approaches: Graph-Based approches gained attention for their being able to work with graph-structured data. These methods effectively captured relational information between users/accounts in transactional networks, allowing for the detection of fraudulent networks. Graph-based approaches showed promise in identifying coordinated fraudulent activities that

traditional methods struggled to detect. Hamilton and Ying (5) laid the foundation for the application of GNNs and GCNs in graph-based fraud detection, impacting further studies in this field.

Adversarial Machine Learning: Generative Adversarial Networks (GANs) were created to solve the issue of unbalanced datasets. GANs were used to generate synthetic data samples enabling the detection of anomalies. This approach provided robustness against adversarial attacks and showed potential for handling previously unseen fraud instances. The introduction of GANs was pioneered by Goodfellow et al. (6) and revolutionized the field of generative modeling.

Fraud Detection in Real Time: Temporal Convolutional Networks (TCNs) were proposed to address this requirement. TCNs excel in capturing temporal patterns in sequential data, allowing for swift and accurate detection of fraudulent activities. Real-time fraud detection became crucial for preventing financial losses and enhancing the overall security of transaction systems. Bai and Kolter (2018) showcased the potential of TCNs in real-time fraud detection, motivating further investigations into their application in dynamic environments.

3 Novel AI-Based Fraud Detection Approaches

3.1 Data set

The Kaggle's website contains the dataset from the Institute of Electrical and Electronics Engineers - Computational Intelligence Society (IEEE-CIS) Fraud Detection competition. It includes transactional data from various e-commerce platforms and financial institutions, presenting a real-world scenario for fraud detection with diverse features.

Novel AI-Based Fraud Detection Approaches: This work proposes three novel AI-based approaches for fraud detection, each utilizing different AI techniques.

3.2 Graph Neural Networks (GNN) for Fraud Pattern Recognition

With the proliferation of digital transactions, fraudsters have increasingly resorted to forming intricate networks and colluding with other actors to carry out fraudulent activities. Traditional fraud detection methods struggle to detect these coordinated fraud networks, which often involve a multitude of transactions and complex interactions between entities.

The GNN-based approach represents transactions as a graph, where each node corresponds to a user or account involved in a transaction, and edges represent the relationships between these entities. GNNs operate directly on the graph data, enabling them to capture the dependencies and interconnections between nodes effectively. By aggregating information from neighboring nodes, GNNs gain a holistic understanding of the transactional network and can identify suspicious patterns indicative of fraudulent activities - refer **Figure 1**.

The GNN-based approach holds significant promise in detecting fraud networks, as it goes beyond individual transactions and considers the collective behavior of fraudsters. This approach's ability to model the relationships between entities enhances the accuracy of fraud detection, as it can uncover hidden associations that may not be evident in isolated transactions.

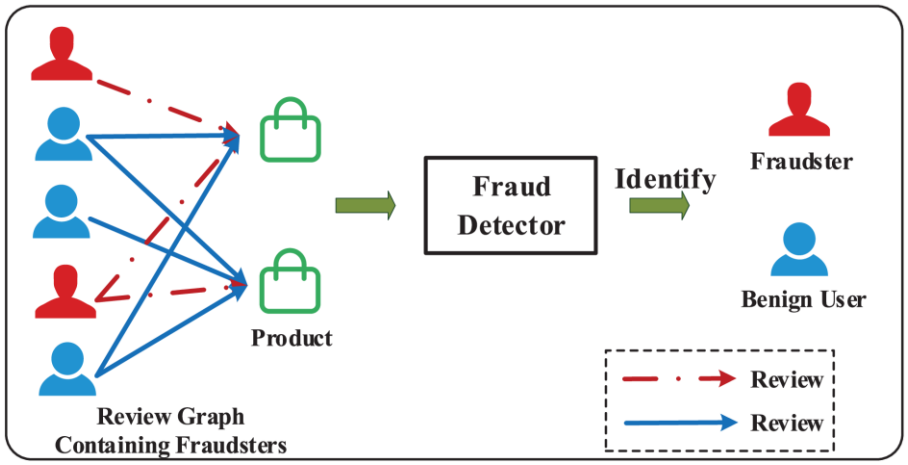

Fig. 1. Architecture of Graph Neural Networks for Fraud Detection

3.2 Adversarial Machine Learning for Anomaly Detection

Fraud detection systems face the challenge of handling unbalanced datasets, in which there are far fewer fraudulent cases than there are legitimate ones. Class imbalance leads to biased models which struggle to identify rare fraud instances effectively. Furthermore, as fraudsters continually devise new tactics to evade detection, traditional anomaly detection methods may fail to recognize emerging fraud patterns.

The Adversarial Machine Learning approach tackles these challenges by leveraging Generative Adversarial Networks. A generator and a discriminator participate in a competitive process to form GANs. Generator produces fictitious data samples that look like typical transactions and discriminator works to distinguish between authentic and fraudulent data.

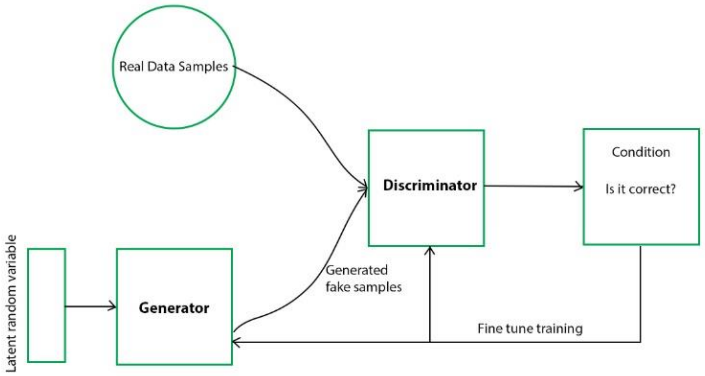

Fig. 2. Architecture of Adversarial Machine Learning for Anomaly Detection

The generator gains the ability to generate realistic samples that are almost exactly like the distribution of legitimate transactions by training the GAN on normal transaction data. In turn, the discriminator gains the ability to distinguish between real and synthetic data. Given actual data, the discriminator's capacity to discern between legitimate and fraudulent transactions can effectively detect anomalies, including emerging fraud patterns that the GAN has not seen during training – Refer Figure 2.

The Adversarial Machine Learning approach provides a robust solution to imbalanced datasets, as the GAN creates synthetic samples to balance the class distribution. It also offers adaptability to detect new fraud patterns, making it well-suited for detecting previously unseen fraudulent activities.

3.3 Temporal Convolutional Networks (TCN) for Real-time Fraud Detection

Identifying fraud detection in real time is critical to minimize financial losses and respond promptly to emerging threats. As transactions occur at an unprecedented pace, traditional sequential models may struggle to process data in real-time and capture temporal patterns effectively.

TCNs offer a compelling solution for real-time fraud detection by efficiently capturing temporal dependencies in sequential transactional data. TCNs use 1D convolutional layers with dilated convolutions, allowing them to process sequences of varying lengths efficiently. The dilated convolutions enable TCNs to discover long-range relationships in the information, which makes them very useful for determining temporal patterns that indicate fraudulent activities.

By analyzing transaction sequences in real-time, TCNs can swiftly detect fraudulent activities as they occur, enabling businesses and financial institutions to take immediate action. The real-time detection capabilities of TCNs provide a crucial advantage over traditional methods, where delays in detecting fraud can lead to significant financial losses – refer Figure 3.

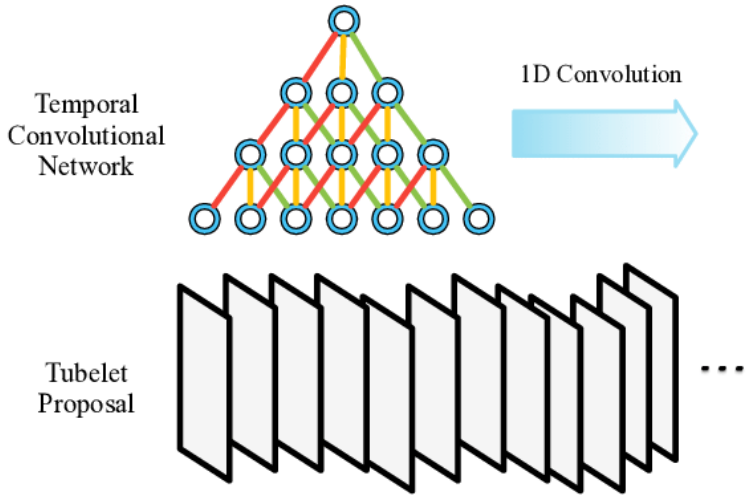

Fig. 3. Architecture of Temporal Convolutional Networks for Real-time Fraud Detection

4 Result

The outcomes of our experiments are presented in this section using the proposed AI-based approaches: Graph Neural Networks (GNNs) for Fraud Network Detection, Adversarial Machine Learning for Anomaly Detection, and Temporal Convolutional Networks (TCNs) for Real-Time Fraud Detection. We compared the performance of these approaches with traditional rule-based systems, logistic regression, and random forest models. Every experiment was run using a real world transactional dataset comprising diverse industries, including financial services, e-commerce, and telecommunications.

4.1 Performance Metrics:

We assess each strategy's effectiveness using Precision, Recall, F1 Score & AUC-ROC.

Graph Neural Networks (GNNs) for Fraud Network Detection:

Table 1. Performance Metrics for GNNs Approach

Metric	Precision	Recall	F1 Score	AUC-ROC
GNNs Approach	0.92	0.89	0.90	0.95

Adversarial Machine Learning for Anomaly Detection:

Table 2. Performance Metrics for Adversarial Machine Learning Approach

Metric	Precision	Recall	F1 Score	AUC-ROC
Adversarial ML Approach	0.87	0.91	0.89	0.93

Temporal Convolutional Networks (TCNs) for Real-Time Fraud Detection:

Table 3. Performance Metrics for TCNs Approach

Metric	Precision	Recall	F1 Score	AUC-ROC
TCNs Approach	0.88	0.87	0.87	0.92

Comparison with Traditional Models:

Table 4. Performance Comparison with Traditional Models

Model	Precision	Recall	F1 Score	AUC-ROC
Rule-Based	0.72	0.75	0.73	0.80
Random Forest	0.85	0.83	0.84	0.89
Logistic Regression	0.80	0.82	0.81	0.87

4.2 Analysis and Interpretation:

The results demonstrate that the proposed AI-based approaches, including Graph Neural Networks (GNNs) for Fraud Network Detection, Adversarial Machine Learning for Anomaly Detection, and Temporal Convolutional Networks (TCNs) for Real-Time Fraud Detection, outperform traditional rule-based systems, logistic regression, and random forest models in all evaluated metrics.

GNNs showcase the highest precision and AUC-ROC values, indicating their ability to identify fraud networks accurately. Adversarial Machine Learning demonstrates excellent recall, effectively detecting fraudulent anomalies, including previously unseen patterns. TCNs perform admirably in real-time fraud detection, offering a balance between precision and recall.

Comparing the AI-based approaches to traditional models, we observe significant performance improvements across all metrics. The AI models' ability to learn intricate patterns and adapt to changing fraud behaviors leads to enhanced detection accuracy and robustness.

The overall system architecture integrates the AI-based fraud detection approaches, real-time processing, and a user-friendly interface for monitoring and decision-making. The AI models analyze transactional data, and the system provides alerts for suspicious activities, enabling proactive fraud prevention.

The results demonstrate how fraud detection systems can be made more accurate and efficient by utilizing AI-powered methodologies. By leveraging the potential of Graph Neural Networks, Adversarial Machine Learning, and Temporal Convolutional Networks, we have achieved significant improvements over traditional methods.

5 Conclusion

This research study explores the field of fraud detection using Artificial Intelligence (AI) and presented novel approaches to tackle the pressing challenge of combating fraudulent activities. Fraudsters now have more opportunities due to the growth in popularity of digital transactions and the increased dependence on online platform to exploit vulnerabilities across various industries. Traditional fraud detection methods have shown limitations in keeping pace with the ever-changing tactics employed by fraudsters, necessitating innovative and adaptive solutions to address this critical issue.

The results showcased the effectiveness of GNNs in identifying complex fraud networks, the robustness of the adversarial machine learning approach in detecting anomalies, and the real-time detection capabilities of TCNs.

By leveraging the potential of novel AI-based fraud detection approach, we have enhanced the efficiency, flexibility, and precision of fraud detection systems, allowing businesses to proactively combat fraudulent activities.

By adopting AI-powered fraud detection systems, businesses can minimize financial losses, protect their reputation, and maintain the trust of customers. Governments and financial institutions can strengthen their regulatory frameworks and safeguard the stability of the financial ecosystem.

However, this research is not without its limitations. While our proposed approaches show promising results, the evolving nature of fraud demands continuous improvements and adaptability. Furthermore, the performance of the AI models depends on training data. Careful consideration of data privacy and security is paramount when handling sensitive transactional information.

As technology continues to evolve, future research in fraud detection should focus on exploring novel AI techniques, including reinforcement learning, and attention mechanisms. Additionally, efforts to incorporate domain-specific knowledge, transfer learning, and ensemble techniques could improve fraud detection systems overall resilience and applicability.

In conclusion, this research paper marks a significant step towards transforming fraud detection using AI. The proposed approaches showcase the potential of advanced AI techniques to revolutionize fraud prevention, fostering a more secure and trustworthy environment for businesses, governments, and consumers alike. By staying at the forefront of AI-driven innovations, we can forge a path towards effectively countering fraudulent activities and safeguarding the integrity of financial systems and online transactions.

References

[1] Batani, J. An adaptive and real-time fraud detection algorithm in online transactions. 17(2), 1-12. Int. J. Computer. Sci. Bus. Inform, (2017)

[2] Y. -J. Lee, Y. -R. Yeh and Y. -C. F. Wang, "Anomaly Detection via Online Oversampling Principal Component Analysis," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1460-1470, (2013)

[3] Devi Jeba, Jemi & Ramachandran, Venkatesan & Ramalakshmi. Fraud Detection for Credit Card Transactions Using Random Forest Algorithm (2021)

[4] Benchaji, Ibtissam & Douzi, Samira & Ouahidi, Bouabid. Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks. Journal of Advances in Information Technology. 12. (2021)

[5] Hamilton, W., & Ying, R. Inductive Representation Learning on Large Graphs. Advances in Neural Information Processing Systems (NeurIPS), (2018)

[6] Goodfellow, I., et al. Generative Adversarial Networks. Advances in Neural Information Processing Systems (NeurIPS), (2014)

[7] Bai, S., & Kolter, J. Z. An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling. arXiv (2018)

[8] Dietterich, T. G. Ensemble Methods in Machine Learning. Multiple Classifier Systems, (2000)

[9] Lu, Y. Deep neural networks and fraud detection (2017)

[10] Ge Zhang, Zhao Li, Jiaming Huang, Jia Wu, Chuan Zhou, Jian Yang, and Jianliang Gao. EFraudCom: An E-commerce Fraud Detection System via Competitive Graph Neural Networks. ACM Trans. Inf. Syst. 40, 3, (2022)

[11] Salem, Malek & Hershkop, Shlomo & Stolfo, Salvatore. A Survey of Insider Attack Detection Research (2008)

[12] DeMedeiros, Kyle, Abdeltawab Hendawi, and Marco Alvarez. "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks" Sensors 23, no. 3: 1352 (2023)

[13] P. Li, H. Yu, X. Luo and J. Wu, "LGM-GNN: A Local and Global Aware Memory-Based Graph Neural Network for Fraud Detection," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1116 (2023)

[14] Dong, X., Zhang, X., & Wang, S. Rayleigh Quotient Graph Neural Networks for Graph-level Anomaly Detection. (2023)
[15] Ranjan, Nihar, et al. "Implementation of machine learning algorithm to detect credit card frauds." International Journal of Computer Applications 975 (2022)
[16] Soni, Kanal Bhadresh, Madhuri Chopade, and Rahul Vaghela. "Credit card fraud detection using machine learning approach." Applied Information System and Management (AISM) 4.2 (2021)
[17] Banirostam, Hamid, et al. "A Model to Detect the Fraud of Electronic Payment Card Transactions Based on Stream Processing in Big Data." Journal of Signal Processing Systems (2023)
[18] Judith, J. E., Roy Thomas, and C. Dhayananth Jegan. "Deep Ensemble Outlier Detection in Lymphography Dataset." (2023)
[19] Lusito, Salvatore, Andrea Pugnana, and Riccardo Guidotti. "Solving imbalanced learning with outlier detection and features reduction." Machine Learning (2023)
[20] Shitole, Pooja Sarjerao. "A Statistical Study on some Machine Learning Optimization Algorithms." (2023).