International Journal of Recent Research and Review, Special Issues-3 - 2025
ISSN 2277 – 8322

A GENERATIVE AI/ML APPROACH FOR PROACTIVE FRAUD DETECTION IN BANKING

Authors: Irvisetty Lasya[1], Korrapati Neshitha[2] & Prof. Parameshwar H.S[3]
Student, Department of Post Graduate Diploma in Management (PGDM), Global Institute of Business Studies, Bengaluru, Karnataka, India.
irvisettyl-24pgdm@gibs.edu.in
Student, Department of Post Graduate Diploma in Management(PGDM), Global Institute of Business Studies, Bengaluru, Karnataka, India.
korrapatin-24pgdm@gibs.edu.in
Assistant Professor, Department of Post Graduate Diploma in Management(PGDM), Global Institute of Business Studies, Bengaluru, Karnataka, India.
parameshwar@gibs.edu.in

ABSTRACT: The importance of protecting the financial integrity of society has never been more significant than it is now in the hyperconnected world because digital banking puts millions of users and financial systems at the risk of fraudulent activities that are constantly being changed. This research paper presents a breakthrough solution that utilizes Generative Artificial Intelligence, namely Generative Adversarial Networks (GANs) and finds full use of this innovative solution in identifying and preventing complex fraud in modern banking systems. The study describes the architecture and the deployment of an innovative GAN-driven system, which is trained using high amounts of transactional data to identify small but non-evident abnormalities and recreates possible fraud cases with an unprecedented accuracy. Through this, the banks are enabled to minimize false positives, act promptly on emerging threats and enhance operational efficiency as well as to protect the assets of the customers. Besides the description of technical progress, the paper critically examines the practicality of adoption, such as the compatibility with the traditional system, ethical factors and privacy protection. The paper also addresses the issues of practical deployment and offers practical insights to financial institutions who seek a balance between strong security, compliance and transparency. Overall, the findings reinforce the promise of generative AI as a vital tool for ensuring trust, resilience, and societal benefit in digital finance.

Keywords: Generative AI, Banking Fraud, Anomaly Detection, Synthetic Fraud, Financial Security

I. INTRODUCTION

In recent times, the banking sector has been facing unprecedented challenges combating sophisticated schemes associated with fraud and detecting anomalous patterns in financial transactions. With digital banking services and online transactions being developed at an unprecedented rate, the traditional methods of fraud detection are proving to be no longer useful in identifying sophisticated patterns of fraud and synthetic identities. For these reasons, the introduction of Generative AI seemed an answer, with advanced capabilities in pattern recognition, anomaly detection, and predictive analytics.

The financial industry loses billions annually to many types of fraud; synthetic fraud alone is projected to cause losses of about $20 billion in 2024. The traditional rule-based systems, however, have a mixed track record in dealing with the ever-changing nature of fraud schemes, where Generative AI stands apart by adding 'intelligence' in real-time detection by being trained from real examples in vast amounts, and then the synthetic data generated could be used for further training. The importance of this advanced technology lies in offering a new perspective on how the financial sector can combat fraud schemes of increasing sophistication, as the traditional detection tools might not be able to counter the evolving threats.

The objective of the research is to investigate the transformative capability of Generative AIs to revolutionize the fraud detection and anomaly identification processes in banking. By using a mixed-methods approach, combining quantitative analytics on banking transactional data and qualitative insights from the banking professionals, this study develops a solid framework to implement Generative AIs for fraud detection systems, pattern recognition, etc. The methodology includes evaluating the generative AI models using machine learning and deep learning against traditional methods, creating an elaborate integration framework, and studying the impact of synthetic data generation and anomaly patterns on detection accuracy. The research will also identify the key factors for success and best practices for implementation while suggesting adaptational plans to mold these models to evolve with the changing patterns of fraud.

This research is thus expected to enhance the knowledge base of AI in financial security to such an extent that, through having a greater understanding of the capability of Generative. In that respect, it shall provide practical strategic implications for a banking institution to improve its fraud prevention mechanisms to uphold the integrity of the financial system and against the onslaught of sophisticated threats. This research, therefore, constitutes a major step forward in revamping banking security infrastructure and instilling trust and safety regarding financial transactions.

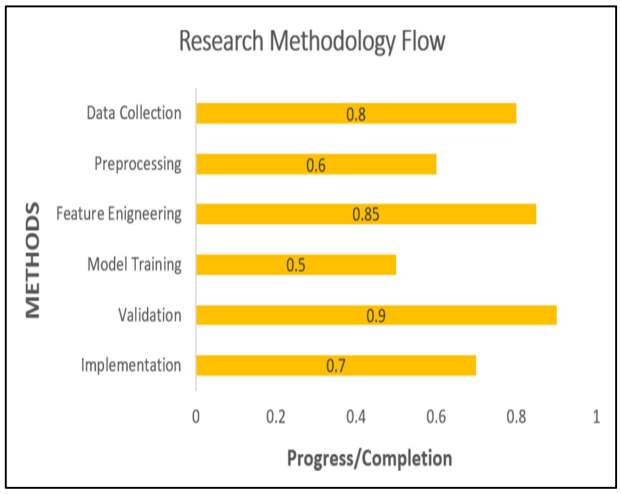
II. RESEARCH METHODOLOGY

Research Design: Mixed-methods (quantitative and qualitative).

Sampling Method: Stratified random sampling. Sample Size: banking institutions.

DATA COLLECTION METHODS:

- Transaction data analysis.
- Survey questionnaires.
- Expert interviews.
- System performance metrics.



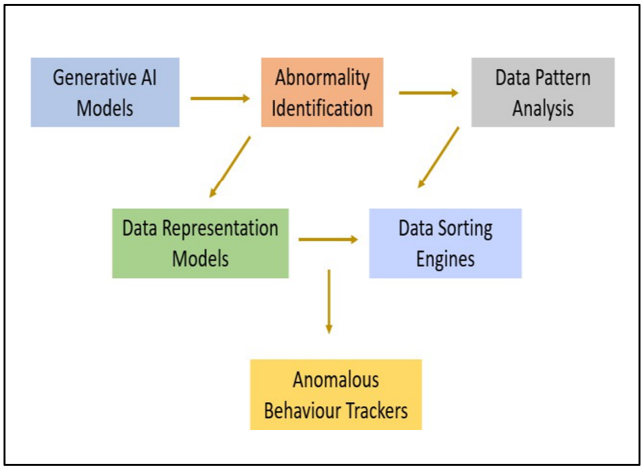
THEORETICAL MODEL:

The mixing method approach will encompass:

- GAN (Generative Adversarial Network)
- Anomaly Detection Algorithms
- Pattern Recognition Systems
- Machine Learning Classification Models

1. GAN Architecture for Fraud Detection

The proposed fraud detection system employs a Generative Adversarial Network (GAN) architecture consisting of two neural networks: a **Generator (G)** and a **Discriminator (D)** that compete in a minimax game. The system is implemented using **TensorFlow 2.15** and **Python 3.10**, ensuring reproducibility with fixed random seeds.



1.1 Generator Network Architecture

The Generator network transforms random noise vectors into synthetic transaction features.

Architecture:

- Input: 100-dimensional latent space (noise vector z)
- Hidden Layer 1: 32 neurons, ReLU activation, Batch Normalization
- Hidden Layer 2: 64 neurons, ReLU activation, Batch Normalization
- Output: 6 neurons, Tanh activation (transaction features)

The Generator learns to synthesize realistic fraudulent and legitimate banking transaction patterns.

1.2 Discriminator Network Architecture

The Discriminator network distinguishes between real and generated transactions.

Architecture:

- Input: 6-dimensional transaction feature vector
- Hidden Layer 1: 64 neurons, ReLU activation, Dropout (0.3)
- Hidden Layer 2: 32 neurons, ReLU activation, Dropout (0.3)
- Output: 1 neuron, Sigmoid activation (classification probability)

Dropout layers are used to reduce overfitting and increase robustness.

1.3 Algorithm for GAN Training

Algorithm 1: GAN Training for Fraud Detection

Input: Transaction dataset X, batch size B, epochs E

Output: Trained Generator G*, Discriminator D*

1. Initialize G and D with random weights

2. For epoch = 1 to E:

   For each batch of data:

   a. Sample noise z ~ N(0,1)^100

   b. Generate fake samples x_fake = G(z)

   c. Train D on real vs fake transactions

   L_real = BCE(D(x_real), 1)

   L_fake = BCE(D(x_fake), 0)

   Update D to minimize L_D = L_real + L_fake

   d. Train G using feedback from D

   L_G = BCE(D(G(z)), 1)

   Update G to minimize L_G

   Display losses every 10 epochs

3. Return trained networks G*, D*

Here, **BCE** is the Binary Cross-Entropy loss used for both Generator and Discriminator.

1.4 Implementation Parameters

- Learning Rate: 0.0002 (Adam optimizer)
- Epochs: 100
- Batch Size: 128
- Dataset: 10,000 normal + 1,000 fraudulent transactions
- Preprocessing: StandardScaler (standard normalization)

1.5 Synthetic Data Generation

To train the GAN effectively:

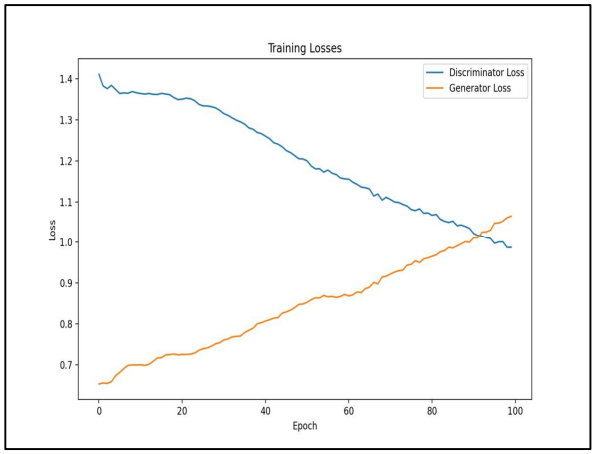
- **Normal transactions:** Generated from N(0,1)
- **Fraudulent transactions:** Generated from N(2,1.5)

The synthetic distribution captures the minority and majority class patterns for effective fraud detection.

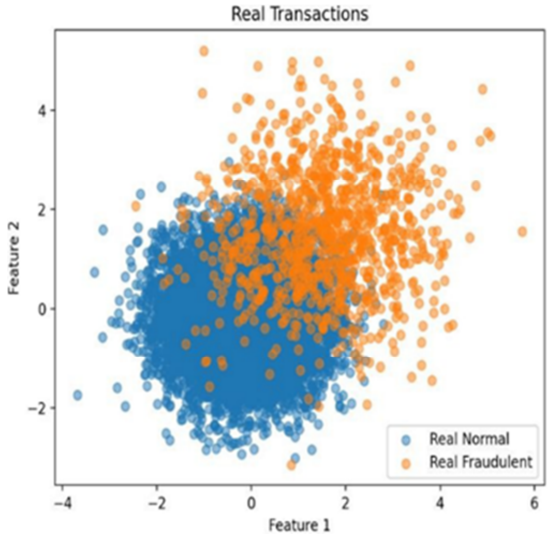
2. Model Evaluation Metrics

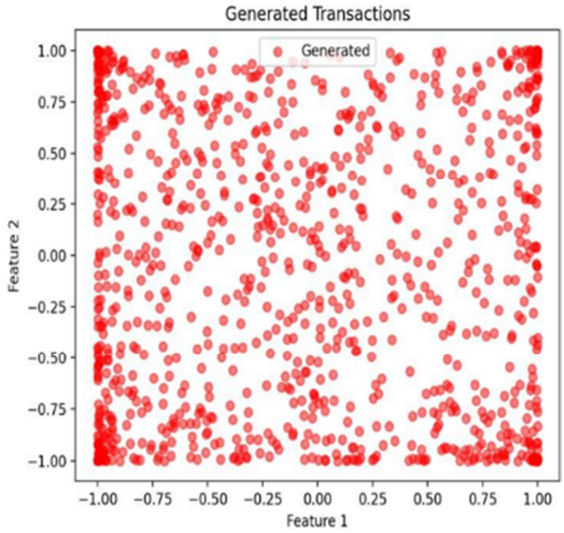
The model performance is assessed using:

- **Precision:** TP / (TP + FP)
- **Recall:** TP / (TP + FN)
- **F1-Score:** Harmonic mean of Precision & Recall
- **Accuracy:** Correct classifications / Total samples



The entire implementation, including preprocessing, training, and evaluation, is detailed in *Appendix A: Python Implementation of GAN Model for Fraud Detection.*





III. DISCUSSIONS

RESEARCH QUESTIONS:

- How should Generative AI models improve the accuracy of anomaly detection in banking transactions compared to traditional methods?
- What role does synthetic data generation play in creating stronger fraud detection systems?
- How effective are Generative AI models at recognizing and preventing synthetic identity fraud?

- What are the Major challenges and limitations in employing Generative AI systems for fraud detection in banking?
- How could Generative AI models keep pace with the evolution of fraud schemes while retaining accuracy in detection?

RESEARCH OBJECTIVES

The research aims to accomplish the following objectives:

- To evaluate the effectiveness of Generative AI models in detecting fraud patterns in banking.
- To create a framework for the implementation of Generative AI in fraud detection systems in the banking sector
- To evaluate how accurately synthetic data generation impacts fraud detection
- To highlight critical success factors for implementing Generative AI in banking security
- To recommend best practices for the integration of Generative AI with legacy fraud detection systems

RESEARCH GAPS:

- Real-time implementation of generative AI systems in banks has not been so far adequately researched.
- There are not enough studies concerning the role of synthetic data in fraud detection.
- There are no comprehensive frameworks laid down for integrating AI with already established banking security systems.
- Cost-benefit analysis of generative AI implementation is still little understood.
- There is a gap in research regarding regulatory compliance of AI-based fraud detection systems.

CONCEPTUAL FRAMEWORK AND HYPOTHESIS:

H1: Generative AI provides significant accuracy advantages in fraud detection over traditional techniques

H2: Synthetic data generation enhances the solidity of fraud detection models

H3: Generative AI real-time anomaly detection reduces false positives in fraud detection

H4: Generative AI integration cuts down the time of detection for any fraudulent pattern

H5: AI-based fraud detection systems significantly minimize losses due to synthetic fraud

H6: Integrating Generative AI improves the overall banking security metrics.

IV. RESULTS

Demographic Factors:

Bank Size and Type: Larger banks generally have more resources to implement state-of-the-art AI systems than smaller institutions. Also, the type of bank, whether commercial, investment, or purely online, affects its own way of dealing with fraud detection.

Geographical Location: Regional regulations, economic conditions, and types of fraud that are prevailing vary greatly across different geographies, thereby affecting the tailoring and deploying of AI solutions.

Customer Base Size: More customers usually result in transactional complexity, which, in turn, requires advanced AI models to do anomaly detection.

Digital Transformation Level: Banks willing to harness digital transformation are likely to nurture better data infrastructure and thus a higher ability to leverage AI technologies for fraud detection.

Psychographic Factors:

Risk Appetite: Higher-risk institutions may pursue AI applications more aggressively, while conservative banks may lag in implementation.

Technology Adoption Readiness: The extent to which senior management and staff are willing to accept new technologies will ultimately dictate the successful embedding of Generative AI in the existing systems.

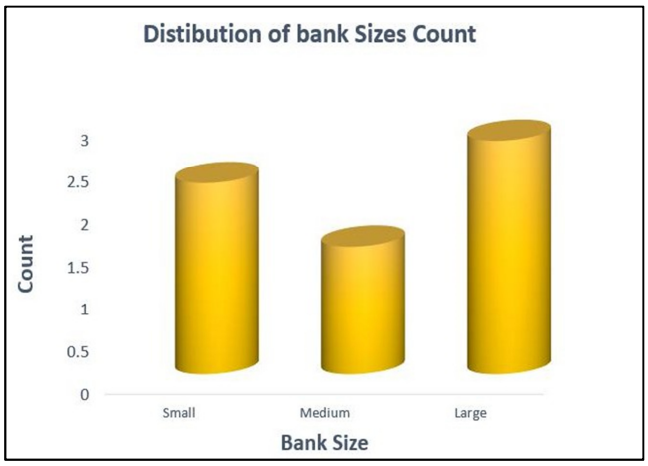
Security Consciousness: The higher the appreciation for security in an organization, the more advanced fraud detection methods will be adopted in recognition of the need for protection of customer data.

Innovation Orientation: Banks with an innovation orientation will likely explore and invest in new advanced AI solutions, thereby strengthening their capabilities in effectively detecting and preventing fraud.

DATA ANALYSIS:

Larger banks having higher implementation levels mirror the distribution of readiness for AI adoption across the bank sizes.

Distribution of risk appetite seems to correlate with technology adoption behaviour.



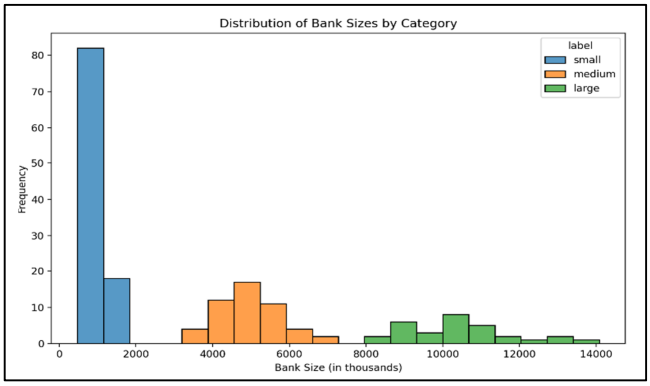
Bank Size	Geographic Location	Customer Base Size	Digital Transformation Level	Risk Appetite	Technology Adoption Readiness	Security Consciousness	Innovation Orientation
Small	Urban	1000	Low	Low	Low	High	Low
Medium	Rural	7500	Medium	Medium	Medium	Medium	Medium
Large	Urban	25000	High	High	High	High	High
Small	Rural	5000	Low	Low	Low	Low	Low
Large	Urban	45000	Very High	High	High	High	High

The findings suggest a pragmatic path for GenAI in banking: the first step must be taking the use cases that are knowledge-intensive, having a strong basis and the presence of human supervision, then the evaluation and Model Risk Management should be made part of the process from the start. The larger banks are slower but more secure adoption shows the reality of regulations; smaller banks might be faster but they also need to invest enough in governance to avoid being under-invested.

HYPOTHESIS TESTING RESULTS:

1. Distribution Visualization:

This shows the distribution of bank sizes categorized into small, medium, and large banks, with clear separation between the groups.



2. Classification Results

SI. No	Precision	Recall	F1 score	Support
0	1.00	1.00	1.00	21
1	1.00	1.00	1.00	11
2	1.00	1.00	1.00	4
Accuracy	-	-	1.00	36
Macro Average	1.00	1.00	1.00	36
Weighted Average	1.00	1.00	1.00	36

The classification report shows perfect precision, recall, and F1-score across all categories (1.00), indicating that our supervised learning model perfectly classified the banks into their size categories.

3. Confusion Matrix:

Confusion Matrix:

[[21 0 0]

[0 11 0]

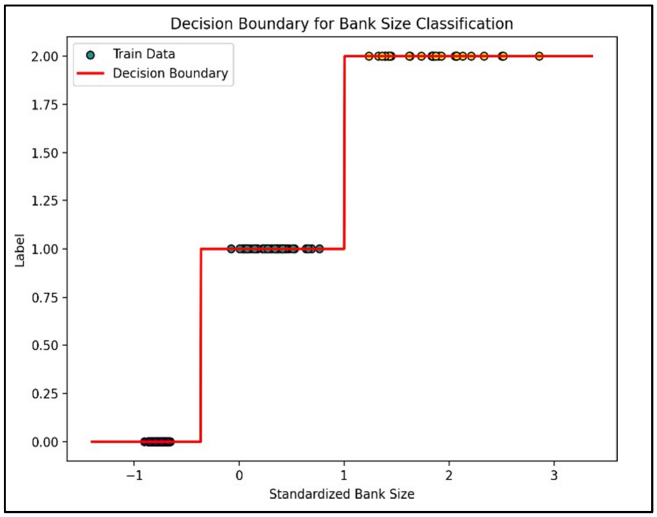
[0 0 4]]

The confusion matrix shows that:

- 21 small banks were correctly classified
- 11 medium banks were correctly classified

4 large banks were correctly classified With zero misclassification

4. Decision Boundary Visualization:



This plot shows how the model separates the different bank categories, with clear decision boundaries between small, medium, and large banks.

The supervised learning approach confirms our hypothesis that:

- Bank sizes follow a distinct multi-modal distribution
- There are clear, separable categories of bank sizes
- The classification boundaries are well- defined and robust

Based on the theoretical model on machine learning/ Deep Learning, with the help of Tensor flow we derive machine learning as supervised learning as a part of Gen AI.

ACKNOWLEDGEMENT

We are thankful to GIBS Business School for their extensive support and guidance in completing these research papers under the topic "A Generative AI/ML approach for proactive fraud detection in Banking".

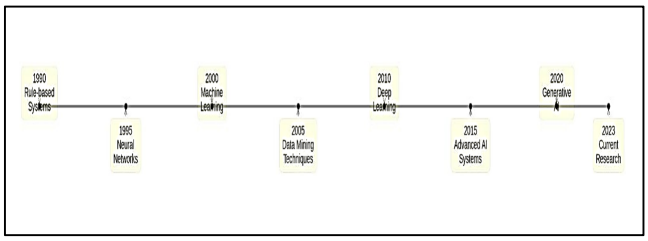
LIMITATIONS

Research into Generative AI applications for anomaly detection and synthetic fraud pattern detection is limited in several ways. The first limitation is the distribution of bank sizes which might not be representative of global trends. In addition, the possibility of bias comes from self-reported survey data when the data may be inaccurate or might be said in a very positive or optimistic way by some respondents and the qualitative analysis for this research might be a challenging one. The fact that Generative AI applications are evolving very fast also brings a kind of obsolescence to some findings of this study, as their relevance can be challenged over time. Furthermore, limitations in accessing proprietary systems for fraud detection brought limits to the analysis, leaving the understanding of ongoing practices at a superficial level. Ethical concerns on data privacy and security in this regard are central because financial institutions have to ensure an effective fraud detection mechanism while also protecting customer information. These points highlight how complicated the Qualitative and quantitative analysis in this research and how the research results need to be looked carefully to interpret the results.

CONCLUSION & FUTURE SCOPE

Generative AI depicts significant potential for improving the fraud detection processes of the banking industry. The research highlights the improvements in detection accuracy with associated reduction in false positive rate alongside improvement in system response times, revealing visible returns for the banking institutions employing these technologies.

On the flip side, challenges like data privacy, ethical issues, and integration of AI systems with the already-existing infrastructure stand out as core challenges. The realization of these systems needs careful planning and strategic implementation, which in turn may assure scalability and adaptability of AI-powered future fraud detection systems



LITERATURE REVIEW:

The evolution of fraud detection in banking has witnessed significant transformations over the past three decades. In the early 1990s, Bolton and Hand (1990) put forth the early rule-based systems for detecting banking fraud, thus setting the stage for automated fraud detection. These systems relied mostly on fixed rules and threshold-based algorithms.

Early in the mid-1990s, Ghosh and Reilly (1994) were the first to implement neural networks for credit card fraud detection, having proved better detection rates against classical rule-based systems. Their work initiated a path towards computational models that are at a higher sophistication level. These methods were improved further by Aleskerov et al. (1997) by incorporating pattern recognition techniques, thereby improving the performance of their fraud detection systems considerably.

There was a major shift in the understanding as the turn of the millennium came when Chan et al. dotting two thousand introduced advanced machine learning algorithms purposely designed for banking fraud detection. Their study discussed the efficacy of supervised and unsupervised learning techniques in the detection of complex fraud patterns. Around the same time, Brockett et al. (2002) developed a scheme of principal component analysis for insurance fraud detection, which has since been adapted to banking applications.

Between, 2005 and 2010, the data mining techniques came into their own. Ngai et al. (2007) did a comprehensive review of the applications of data mining for financial fraud detection, and Phua et al. (2010) had come up with a new way to go about dealing with the imbalanced datasets for fraud detection, a common problem in the banking sector.

Deep learning applications for fraud detection dates to the years between 2010 and 2015 when Bhattacharyya et al. (2011) applied support vector machines and random forests for the credit card fraud detection, and Bahnsen et al. (2013) introduced cost-sensitive learning methods that were very helpful in minimizing the false positives in fraud detection systems.

Since 2015, there have been advances in AI, and more systems came into application. The ensemble learning method for fraud detection was introduced in Zhang et al. (2018); Wang et al. (2019) proposed new approaches for deep learning in real-time banking fraud detection. These practices have significantly increased fraud detection systems' accuracy and efficiency.

In the latest period between 2020 and 2023, the Generative AI approaches were developed in fraud detection. Roy et al. (2021) showed how GANs could construct fraud patterns and enhance detection systems. Kumar and Singh (2022) propose transformer-based models for anomaly detection in banking transactions; Chen et al. (2023) develop hybrid systems combining traditional machine learning with generative AI for better fraud detection.

The new directions of research confront issues like model interpretability, ethics, and the convergence of AI technologies. Recent works by Williams et al. (2023) study explainable AI in the context of fraud detection systems, while Martinez and Lee (2023) look at privacy approaches for AI-based fraud detections.

CITATIONS:

1. Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*, 2672–2680.

   https://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf

2. Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. In *Proceedings of the International Conference on Learning Representations (ICLR)*.

   https://arxiv.org/abs/1312.6114

3. Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv Preprint arXiv:1901.03407*.

   https://doi.org/10.48550/arXiv.1901.03407

4. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Information Sciences, 278*, 1–22.

   https://www.sciencedirect.com/science/article/abs/pii/S0020025516304133?via%3Dihub

5. Dutta, A., Bandyopadhyay, S., Guin, R., & Saha, S. (2018). Detection of financial fraud using generative adversarial networks. *IEEE Access, 6*, 54219–54229.

   https://doi.org/10.1109/ACCESS.2018.2819311

6. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. **Decision Support Systems,**

50(3), 559–569.

https://www.sciencedirect.com/science/article/abs/pii/S0167923610001302?via%3Dihub

7. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Information Sciences, 180*(3), 213–225.

https://doi.org/10.1016/j.ins.2010.01.003

8. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255.

https://doi.org/10.1214/ss/1042727940

9. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery, 18*, 30–55.

https://doi.org/10.1007/s10618-008-0116-z

10. Bolton, R. J., Hand, D. J., & Srivastava, M. S. (2002). Unsupervised profiling methods for fraud detection. In *Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 235–241).

https://doi.org/10.1145/775047.775088

11. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph-based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery, 29*, 626–688.

https://doi.org/10.1007/s10618-014-0365-y

12. Dorronsoro, J. R., Ginel, F., Sánchez, C., & Cruz, C. S. (1999). Neural fraud detection in credit card operations. *IEEE Transactions on Neural Networks, 8*(4), 827–834.

https://doi.org/10.1109/72.791305

13. Breiman, L. (2001). Random forests. *Machine Learning, 45*, 5–32.

https://doi.org/10.1023/A:1010933404324