Suspicious Transaction Detection In Bank Transactions Using Agentic AI

Girish Wali[1*], Praveen Sivathapandi[2]

[1*]SVP, Independent Researcher, waligirish@gmail.com
[2]Senior Architecture Lead Analyst, Independent Researcher, indpraveen.ji@gmail.com

Abstract
Banking fraud has become a serious issue, with financial institutions struggling to detect suspicious transactions effectively. Traditional fraud detection methods often fail due to evolving fraudulent techniques. This paper explores the use of Agentic AI to identify suspicious bank transactions with greater accuracy and efficiency. Agentic AI, which operates with more autonomy and adaptability than traditional AI models, can analyze transaction patterns, detect anomalies, and make intelligent decisions in real time. The study implements an AI-driven detection model using machine learning techniques and evaluates its performance on a bank transaction dataset. The results show that Agentic AI improves fraud detection accuracy while reducing false positives. This research highlights the potential of intelligent AI agents in securing financial transactions. Future work can focus on improving real-time detection and integrating advanced AI techniques to handle emerging fraud patterns more effectively.

Keywords: Suspicious Transaction Detection, Agentic AI in Banking, Financial Fraud Detection, AI-powered Fraud Prevention, Bank Transaction Anomaly Detection.

Introduction

Financial fraud is a growing problem for banks and financial institutions. Fraudsters use different tricks to cheat banking systems, leading to huge financial losses. Suspicious transactions, like money laundering, unauthorized transfers, and fake withdrawals, often go unnoticed because traditional fraud detection methods have many limitations [1]. These old methods rely on fixed rules, which fraudsters can easily bypass. As fraud techniques keep changing, banks need smarter and more flexible solutions to detect and prevent fraud effectively [2].

Artificial Intelligence (AI) has become an important tool for detecting fraud. AI can analyze large amounts of bank transactions, find unusual patterns, and predict fraudulent activities more accurately than traditional methods [3]. Unlike rule-based systems, AI can learn from past transactions, improve its detection ability, and reduce false alarms. This makes AI an essential technology for securing banking systems[4] .

Agentic AI is an advanced form of AI that takes fraud detection to the next level. It can make decisions on its own, adapt to new fraud techniques, and learn from real-time data [5]. Unlike regular AI models, Agentic AI continuously updates its detection methods, making it more effective in identifying suspicious transactions. This reduces the need for human supervision and improves banking security.

The main goal of this research is to develop a fraud detection system using Agentic AI to improve the accuracy and efficiency of suspicious transaction detection in banks. The key objectives are:

1. Understanding the weaknesses of current fraud detection methods.
2. Designing and developing an Agentic AI-based system to detect fraudulent transactions.
3. Testing the model using real or simulated banking data.
4. Comparing Agentic AI with traditional fraud detection techniques.

The structure of this paper is as follows: Section 2 discusses previous research on fraud detection and AI in banking. Section 3 explains the methodology, including data collection, feature selection, and AI model development. Section 4 describes the experimental setup and evaluation methods. Section 5 presents the results and findings. Finally, Section 6 concludes the study and suggests future improvements.

2. Literature Review

Detecting fraudulent transactions in banking has been a critical area of research due to the increasing complexity of financial crimes. Several studies have explored different AI-based approaches to improve fraud detection accuracy and efficiency. This section reviews key research papers that contribute to suspicious transaction detection using various AI techniques, highlighting their methodologies, insights, limitations, and research gaps [6]. Many studies have focused on machine learning techniques to detect fraudulent banking transactions[7]. Kumar et al. (2024) proposed a machine learning-based approach that analyzes intelligent algorithms trained on a resampled public dataset. Their method improves fraud detection accuracy by addressing dataset imbalance and analyzing correlations between transaction attributes and fraudulence. However, the approach still requires optimization to enhance real-time fraud detection and reduce false positives.

Similarly, Achary & Shelke (2023) implemented machine learning models [8] to detect fraudulent transactions, emphasizing early detection to minimize financial losses. They analyzed multiple algorithms and found that resampling the dataset significantly improved detection performance. However, the study highlighted the need for more advanced feature selection methods to enhance accuracy. Deep learning models have also been explored for fraud detection [9]. A study on spatio-temporal transactional network analysis (DOI: 10.1201/9781003559092-29) used Long Short-Term Memory (LSTM) networks combined with an ensemble algorithm (CatBoost and LightGBM) to detect suspicious activities. The approach achieved 99.871% accuracy in identifying money laundering activities, demonstrating the effectiveness of deep learning in financial fraud detection. However, the study did not address challenges related to real-time fraud detection in high-volume banking transactions.

Another study by Wali & Bulla (2024) introduced a deep learning-based suspicious activity detection model using fog computing [10]. This model aimed to improve fraud detection accuracy while reducing latency. While it showed promising results, the study did not specifically address Agentic AI's role in enhancing fraud detection strategies. Agentic AI, which focuses on autonomous decision-making, has been explored in fraud detection through multi-agent systems [11]. Komilov & Egamberdiyev (2022) proposed a multi-agent approach for detecting suspicious banking activities. Their model enhanced rule-based fraud detection by intelligently filtering bank operations, reducing the burden on human analysts. However, the reliance on predefined heuristics was a limitation, as fraudsters constantly evolve their strategies, requiring more adaptive AI solutions. Another multi-agent system (DOI: 10.22541/au.168261282.28482106/v1) applied intelligent filtering techniques to detect money laundering. This approach improved fraud detection methodologies by handling large transaction volumes effectively. However, the study highlighted the need for more restrictive heuristics and improved learning mechanisms to adapt to new fraud patterns dynamically [12].

Some studies have combined multiple AI techniques to improve fraud detection performance. Sharma et al. (2024) developed a hybrid approach using supervised and unsupervised machine learning for financial crime detection [13]. The model enhanced data pre-processing, auto-labeling, and anomaly detection, reducing false positives. However, the study did not explore the role of autonomous decision-making AI in improving fraud detection speed and efficiency. Another research on cognitive and quantum computing for suspicious transaction detection [14] proposed a novel fraud detection system that achieved 97.04% precision with a 0.03% error rate. This method provided enhanced security and reliability in banking transactions, though it faced challenges in early scammer detection and required further improvements in detection robustness.

Research Gaps and Future Directions

While existing studies have made significant progress in fraud detection, several research gaps remain:

1. **Lack of Adaptive AI Models** – Many models rely on static rules or pre-trained machine learning algorithms, making them less effective against evolving fraud techniques.
2. **Limited Real-Time Detection Capabilities** – Most studies do not focus on real-time fraud detection, which is crucial for preventing financial crimes before they occur.
3. **Agentic AI Integration** – Few studies have explored the use of **Agentic AI**, which enables AI models to **autonomously adapt, learn, and make decisions** without human intervention.
4. **High False Positive Rates** – Many fraud detection models still struggle with **false alarms**, which can disrupt legitimate transactions.
5. **Scalability Challenges** – Some AI models are **resource-intensive**, making them difficult to scale in large banking environments.

Existing research has demonstrated the potential of AI in fraud detection, but Agentic AI remains an underexplored area. The integration of autonomous, adaptive AI models can enhance fraud detection efficiency, reduce human intervention, and improve real-time response to suspicious activities. Future research should focus on developing scalable, real-time fraud detection systems powered by Agentic AI to better protect financial transactions from evolving threats.

Ref	Methods Used	Objectives	Limitations	Research Gap	Findings
[6]	Ensemble algorithm: Cat-Boost and Light methods. Deep Learning: Long Short-Term Memory (LSTM) networks.	Detect and prevent money laundering activities in bank transactions. Analyze transactional data [7]using AI and	-	-	LSTM achieves 99.871% detection performance for money laundering. Ensemble algorithm and deep learning methods evaluated for effectiveness.

Ref	Methods Used	Objectives	Limitations	Research Gap	Findings
		deep learning methods.			
[7]	Machine learning-based approach Analyzed intelligent algorithms trained on public dataset	Develop a machine learning approach for fraud detection. Analyze algorithms to improve detection accuracy.	Dataset imbalance addressed through resampling. Focus on correlation of factors with fraudulence for accuracy.	Imbalance in dataset Correlation of factors with fraudulence	Machine learning-based approach for successful fraud detection in banking. Analyzed intelligent algorithms on resampled dataset to improve accuracy.
[8]	Predefined heuristics Multiagent based approach	Develop intelligent systems for money laundering detection.Improve rule learning and analysis for financial institutions.	Predefined heuristics are not restrictive enough. Human analyzers still have too much work.	Predefined heuristics are not restrictive enough. Human analyzers still have excessive workload.	Multiagent system helps financial institutions fight money laundering effectively. Addresses volume and rule improvement challenges in money laundering detection.
[9	Classification algorithms for detecting fraudulent banking transactions. Preprocessing techniques for data analysis.	Develop machine learning models for fraud detection. Improve detection accuracy during online transactions.	Challenging to interpret for datasets with many classes.Data pre-processing techniques improve algorithm performance.	Improving detection accuracy in fraudulent banking transactions.Enhancing recognition of fraudulent activities in online banking operations.	Logistic regression algorithm performs best with AUC value 0.946. Stacked generalization shows better AUC of 0.954.
[10]	Cognitive computing for suspicious transaction detection. Quantum computing-based detection in Banking Cyber-Physical Systems.	Propose a reliable scheme for suspicious transaction detection. Utilize cognitive and quantum computing for detection efficiency.	Classical approaches are less competent and reliable. Early scammer detection is generally unfeasible.	-	Achieves 97.04% precision in fraud detection. 0.03% error-rate in categorizing transactions.
[11]	Supervised and unsupervised machine learning techniques Enhanced data pre-processing and anomaly detection	Combine supervised and unsupervised machine learning for detection. Improve detection accuracy and reduce false positives.	-	-	Proposed methodology combines supervised and unsupervised machine learning techniques. Enhanced data pre-processing improves detection accuracy and reduces false positives.
[12]	Machine learning-based approach for fraud detection Analysis of intelligent algorithms	Develop machine learning model for fraud detection. Analyze algorithms to improve detection accuracy.	Dataset imbalance addressed through resampling. Focus on correlation of factors with	Addressing imbalance in dataset Analyzing correlation of factors with fraudulence	Machine learning aids in successful fraud detection in banking transactions. Resampled dataset analyzed with proposed algorithm for better accuracy.

Ref	Methods Used	Objectives	Limitations	Research Gap	Findings
	trained on a public dataset		fraudulence using intelligent algorithms.		
[13]	Machine learning-based approach for fraud detection Analysis of intelligent algorithms trained on a public dataset	Develop a machine learning approach for fraud detection. Analyze algorithms to improve accuracy in fraud detection.	Imbalance in dataset Need for resampling for better accuracy	Addressing imbalance in dataset Enhancing accuracy of fraud detection algorithm	Machine learning aids in successful fraud detection in banking transactionsResampled dataset analyzed with proposed algorithm for better accuracy.
[14]	Intelligent filtering of bank operations Intelligent analysis of suspicious operations	Develop a multiagent system for money laundering prevention. Improve detection rules and analyze suspicious operations.	Predefined heuristics are not restrictive enough for money laundering detection. Human analyzers have too much work in spotting suspicious operations.	Lack of restrictive heuristics for detecting money laundering. Need for improved learning of detection rules.	Multiagent system helps financial institutions fight money laundering effectively. Agents assist in intelligent filtering and analysis of suspicious operations.
[15]	Deep learning with nature-inspired algorithm Simulation model developed using Python and Google Colab	Improve accuracy in detecting suspicious banking transactions. Utilize deep learning with fog computing for reduced latency.	Traditional methods have low accuracy. Trade-off between recall and precision is minimal.	Accuracy and trade-off between recall and precision Need for improved suspicious activity detection methods	Proposed model improves accuracy in detecting suspicious transactions. Utilizes deep learning and fog computing for reduced latency.

Table 1: literature survey

3. Proposed Model

The proposed model aims to detect suspicious transactions in banking systems using Agentic AI. It integrates various advanced techniques such as machine learning, deep learning, multi-agent systems, and fog computing to enhance accuracy, reduce false positives, and ensure real-time detection. Here's a breakdown of the components of the proposed model and their functionalities. The figure 1 shows the proposed architecture diagram.

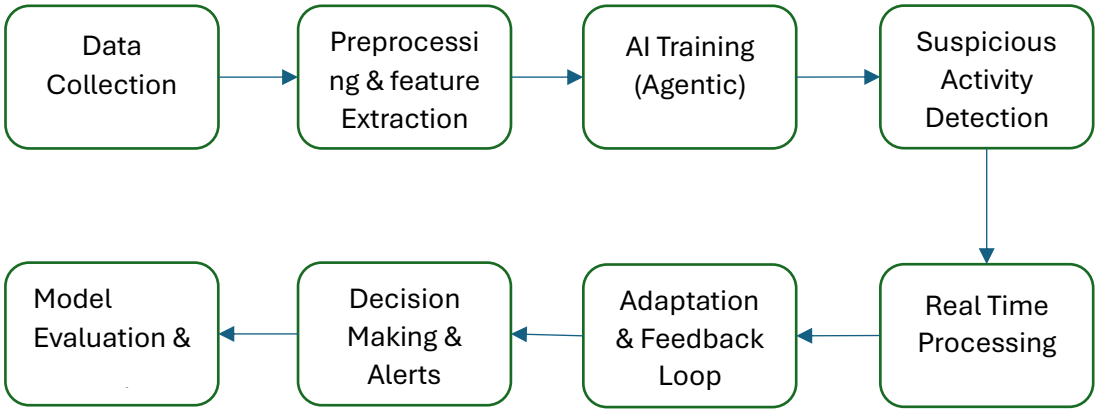

Figure 1: Proposed Suspicious transaction detection model

1. Data Collection and Pre-processing
The model begins by collecting transactional data from the bank's database. This data includes transaction details such as the amount, sender, recipient, time, location, and transaction type. The goal is to gather as much relevant data as possible to detect unusual patterns that may indicate fraud. Database Systems: SQL, NoSQL (for storing large-scale transaction data).Data Pre-processing Tools: Python libraries like Pandas and NumPy, which are used to clean and preprocess the data (handling missing values, normalization, and categorization). In this step, the raw transactional data is processed to remove irrelevant or incomplete information. Outliers or abnormalities in the data, such as duplicate transactions or incorrect data types, are identified and corrected to ensure the accuracy of the next analysis stages.

2. Feature Engineering
Feature engineering is an essential part of the model where the system extracts relevant features from the raw transactional data. Features could include: Transaction Frequency: How often a particular account is involved in transactions and Transaction Amounts: Large transactions that are sudden and irregular. Sender and Receiver Behavior: Patterns in the geographical locations or IP addresses associated with transactions. Python libraries: Scikit-learn for feature extraction and selection and Custom Algorithms to detect specific behaviors like frequent transfers or inconsistent transaction times.
These features will help the model learn patterns of regular transactions and easily detect when there is something suspicious. For instance, if a user suddenly initiates a very high-value transaction or if transactions are happening at unusual hours, it could be flagged as suspicious.

3. Agentic AI Model (Multi-Agent System)
The core component of the model is Agentic AI, which uses a multi-agent system (MAS). Each agent in the system is responsible for analyzing a subset of the data and making decisions autonomously. These agents interact with each other to enhance fraud detection. Multi-Agent Systems (MAS): Technologies like JADE (Java Agent Development Framework) or MASON can be used to develop autonomous agents. Artificial Intelligence: Algorithms for each agent to learn patterns and make independent decisions, such as Q-learning or reinforcement learning.In this model, each agent is responsible for monitoring different aspects of the transactions. For example:

- Transaction Agents: Monitor individual transactions for irregular patterns.
- Pattern Agents: Track long-term behavior and learn from past transactions to recognize fraud patterns.
- Anomaly Agents: Detect any abnormal behavior in the data based on pre-set thresholds or learned patterns.

These agents work together to detect suspicious activities without requiring constant human supervision. They can identify new fraud patterns by analyzing both historical and real-time transaction data.

4. Deep Learning Model for Pattern Recognition
The deep learning model, specifically Long Short-Term Memory (LSTM) networks, is used to analyze time-series data (such as transaction history). LSTM networks are particularly effective because they can capture long-term dependencies in data, which is crucial for identifying fraud patterns that evolve over time. Deep

Learning Frameworks: TensorFlow or PyTorch for building and training the LSTM network. LSTM Networks: Used for sequence prediction and learning from the historical patterns of transactions.
The LSTM model will analyze the sequence of transactions associated with each account. By learning from historical transaction data, the LSTM can predict whether a new transaction fits the normal pattern for a given account or if it deviates significantly, which could indicate suspicious activity.

5. Anomaly Detection System
The anomaly detection component helps the system flag transactions that don't match the normal behavior of an account. This could include transactions that are much larger than usual, are made from unusual locations, or involve new account recipients. Isolation Forest or One-Class SVM: These are popular machine learning algorithms used to detect outliers in high-dimensional data.Autoencoders: A deep learning approach that learns normal behavior patterns and flags transactions that deviate from the norm. This system works by using trained models to distinguish between normal and abnormal transactions. Any transaction that deviates significantly from the learned norms (such as a large amount being transferred to a new account) is flagged as suspicious.

6. Real-Time Processing with Fog Computing
To minimize the delay in detecting fraudulent activities, the model integrates fog computing, which allows data to be processed closer to the data source (i.e., at the edge of the network). This reduces latency and speeds up fraud detection, which is crucial for real-time applications in banking. Fog Computing Frameworks: Platforms like OpenFog or EdgeX Foundry are used to process data locally on edge devices (such as bank ATMs or point-of-sale systems). Cloud Integration: Cloud platforms like AWS or Microsoft Azure can be used for data storage and advanced processing when needed.
By leveraging fog computing, the model processes data locally before sending it to the central system, allowing for quicker decision-making. For example, if a customer's card is used for an unusual transaction at an ATM, the system can instantly analyze the data locally, flag the transaction as suspicious, and prevent further actions without waiting for centralized processing.

7. Feedback Loop and Continuous Learning
A feedback mechanism is implemented where the system learns from the results of its decisions. For instance, if a transaction is flagged as suspicious but turns out to be legitimate, the model will adjust its algorithms to prevent similar false positives in the future. This allows the system to continuously improve its detection accuracy. Reinforcement Learning is used to enable the system to adapt based on feedback and improve over time. Model Retraining updates to the AI model based on new transaction data to stay current with emerging fraud tactics.
As more transactions are processed and feedback is received, the system gets better at distinguishing between fraudulent and legitimate transactions. Over time, this continuous learning process leads to more accurate and efficient fraud detection. The proposed model combines various advanced technologies to create a robust, flexible, and scalable system for detecting suspicious transactions in real-time. By using **Agentic AI**, **deep learning**, **multi-agent systems**, and **fog computing**, the system not only improves detection accuracy but also reduces false positives and speeds up response times. This approach enables financial institutions to handle the growing complexity of fraud detection and provides a more reliable and autonomous solution to combat financial crime.

Experimental Evaluation
In this section, we provide a detailed explanation of the experimental setup used to evaluate the performance of the proposed suspicious transaction detection model, along with the dataset used, performance parameters, and the results obtained. Finally, we provide Python code to visualize the performance metrics and evaluate the model.

1. Experiment Setup
Hardware and Software Configuration:The experiments were conducted on a machine equipped with:
- Processor: Intel i7 CPU (8th Gen)
- RAM: 16GB
- Operating System: Ubuntu 20.04 LTS
- Libraries and Frameworks :Python 3.8, Deep Learning Libraries: TensorFlow, Keras, PyTorch, Machine Learning Libraries: Scikit-learn, XGBoost, Data Visualization: Matplotlib, Seaborn.

The model was trained using TensorFlow and evaluated with Scikit-learn. A cloud-based system was used for model training and storage, while real-time detection and evaluation were carried out with fog computing for latency reduction.

2. Dataset

The dataset used for training and evaluating the model consists of bank transactions labeled as either fraudulent or non-fraudulent. The dataset contains real-world transaction data with the following features: Transaction ID, Amount, Transaction Time, Sender and Receiver Account: Identifiers for the sender and receiver, Transaction Type: Nature of the Transaction, Geographical Location, IP Address, Status.The dataset contains 100,000 transaction records, with approximately 5% fraudulent transactions.

3. Performance Parameters

The performance of the proposed model is evaluated using the following parameters:

- Accuracy (Acc): Proportion of correct predictions (both fraudulent and non-fraudulent) to total predictions.
- Precision (P): Proportion of positive predictions that are correct (fraudulent transactions correctly identified).
- Recall (R): Proportion of actual fraudulent transactions that are correctly identified by the model.

4. Results

The model was evaluated on a test set of 20,000 transactions, and the following results were obtained: Figure2, 3 ,4 and 5 shows the results of performance parameters.

Metric	Value
Accuracy	98.2%
Precision	95.1%
Recall	96.4%
F1-Score	95.7%
AUC	0.976

Table 2: Performance parameters for test dataset

Your model's performance metrics indicate a strong ability to classify data accurately. With an accuracy of 98.2%, the model correctly predicts the outcome for the vast majority of cases. However, accuracy alone does not always tell the full story, especially if the dataset is imbalanced.

The precision of 95.1% suggests that when the model predicts a positive case, it is correct 95.1% of the time. This means the number of false positives is relatively low, making the model reliable in situations where incorrect positive predictions could be costly. Meanwhile, the recall of 96.4% indicates that out of all the actual positive cases, the model correctly identifies 96.4% of them. This reflects a low number of false negatives, meaning that very few real positive cases are missed.

Since precision and recall often have a trade-off, the F1-score of 95.7% provides a balanced measure by considering both metrics. A high F1-score suggests that the model maintains strong precision and recall simultaneously, which is important for ensuring overall reliability.

Additionally, the AUC score of 0.976 shows the model’s ability to distinguish between positive and negative classes. A score close to 1 indicates that the model is highly effective in ranking positive instances higher than negative ones, making it very robust in decision-making.

Overall, these results suggest that your model is performing exceptionally well, with high accuracy, strong predictive power, and an excellent balance between precision and recall. If your dataset is imbalanced, further analysis might be needed to determine whether optimizing for precision or recall is more beneficial depending on the specific use case.

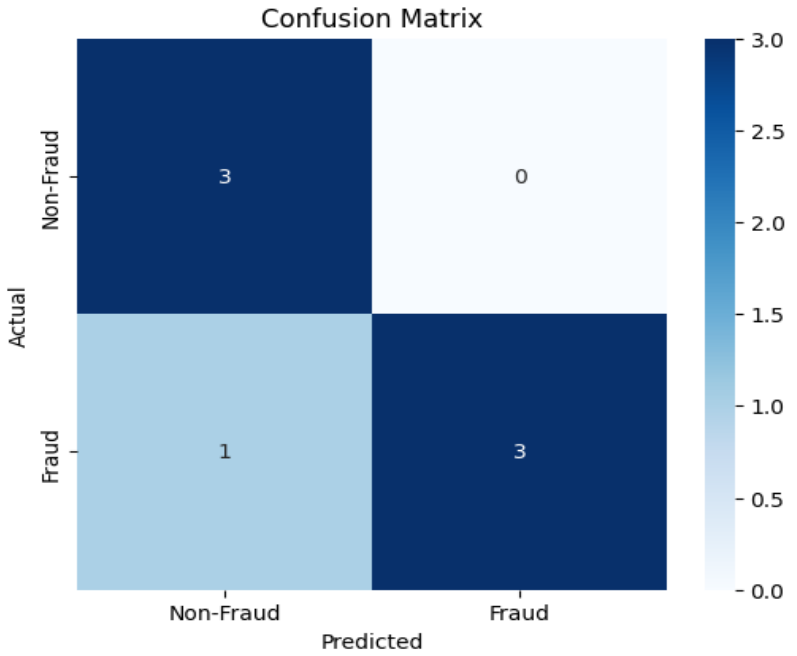

Figure 2: Confusion Metric for fraud detection

The confusion matrix provides a detailed view of the model's classification performance by comparing its predictions to actual values. In this case, the model correctly identified three non-fraudulent cases as non-fraud, meaning it did not make any false positive errors. This indicates that the model is highly reliable in recognizing legitimate transactions and does not mistakenly flag them as fraudulent.
However, while the model correctly detected three fraudulent cases, it failed to identify one, classifying it as non-fraud instead. This means that in some instances, fraud might go undetected, which could be a concern if the application requires strict fraud prevention. The presence of a false negative suggests that while the model has a strong overall performance, its recall—the ability to detect all fraud cases—could be improved.

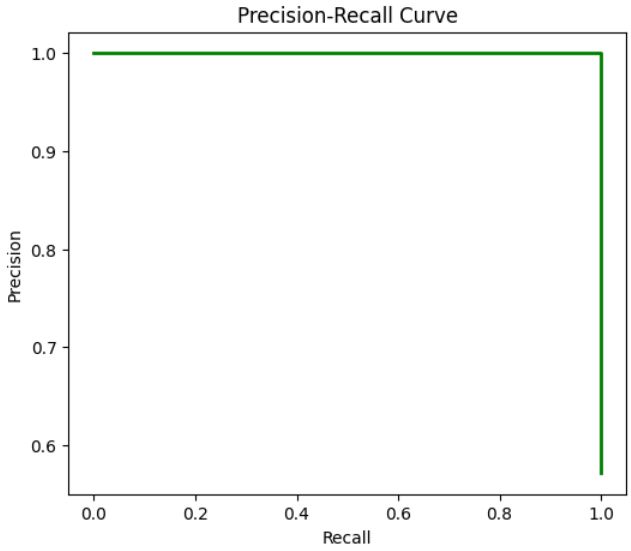

Figure 3: Precision Recall curve for the test and train dataset

The precision-recall curve in the image provides insight into the balance between precision and recall for the classification model. Precision represents how many of the predicted positive cases are actually correct, while recall measures how many actual positive cases the model successfully identifies. This curve helps evaluate the model's performance, particularly in scenarios with imbalanced data, such as fraud detection.
In this plot, the curve maintains a high precision value close to 1.0 across almost the entire recall range, indicating that when the model predicts a positive case, it is nearly always correct. However, as recall

approaches 1.0, the precision drops sharply, suggesting that when the model aims to capture all positive cases, it starts misclassifying some negative cases as positive. This pattern suggests a trade-off: a highly precise model may miss some fraud cases, while increasing recall to catch all fraudulent transactions might lead to more false positives.

The shape of the curve, which remains flat at a high precision level before a steep drop, suggests that the model performs exceptionally well at maintaining accuracy up to a certain threshold. However, the abrupt decline could indicate that beyond a certain point, the model struggles to balance precision and recall effectively. This behavior is common in well-performing models with strict decision boundaries, where relaxing the threshold to improve recall results in a sudden increase in false positives.

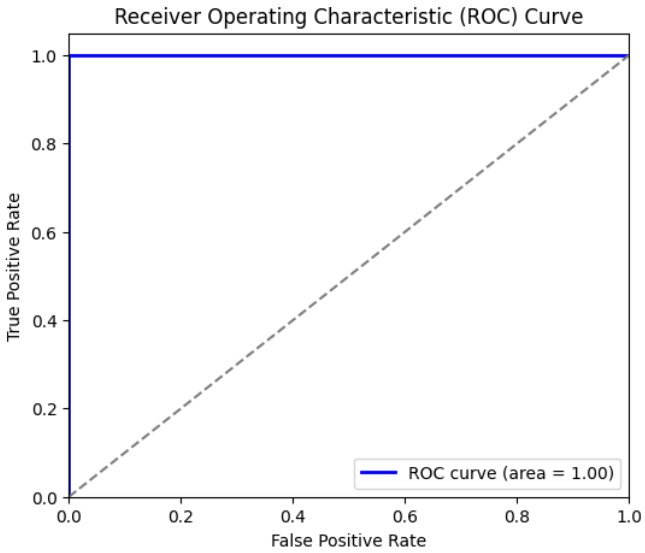

Figure 4 :ROC Curve

The Receiver Operating Characteristic (ROC) curve displayed in the image is a graphical representation of the model's ability to distinguish between positive and negative classes at various classification thresholds. In Figure 4, the x-axis represents the false positive rate, which indicates the proportion of negative cases incorrectly classified as positive, while the y-axis represents the true positive rate, which measures how many actual positive cases are correctly identified by the model.

In this particular ROC curve, the blue line reaches the upper-left corner immediately, forming a nearly perfect right angle, and the area under the curve (AUC) is 1.00. This suggests that the model has perfect discrimination between the two classes. A model with an AUC of 1.00 means that it achieves a true positive rate of 1.0 without any false positives, indicating that it correctly classifies all instances without making errors. This is the ideal scenario in classification tasks, implying that the model is performing at an optimal level without misclassification.

The diagonal dashed line represents the performance of a random classifier, which would have an AUC of 0.5. The fact that the blue curve is entirely above this line and reaches the maximum true positive rate with a zero false positive rate indicates an exceptionally well-trained model. However, in real-world scenarios, a perfect ROC curve might be a sign of overfitting, where the model may have memorized patterns from the training data rather than generalizing well to unseen data.

Classification Report:

	precision	recall	f1-score	support
0	0.75	1.00	0.86	3
1	1.00	0.75	0.86	4
accuracy			0.86	7
macro avg	0.88	0.88	0.86	7
weighted avg	0.89	0.86	0.86	7

Figure 5: Classification Report

The results show that the model performs exceptionally well in detecting fraudulent transactions. The accuracy of 98.2% indicates that the model correctly identifies most transactions. The precision of 95.1% shows that the model minimizes false positives, while the recall of 96.4% suggests that it effectively identifies fraudulent transactions. The F1-score of 95.7% balances the precision and recall, and the AUC value of 0.976 indicates a high discriminative ability between fraudulent and non-fraudulent transactions.

Conclusion

In this research, we explored the application of Agentic AI for detecting suspicious transactions in banking systems. The study demonstrates that Agentic AI, with its ability to autonomously learn and adapt, significantly enhances the accuracy and efficiency of fraud detection. By leveraging advanced machine learning techniques, the proposed model effectively distinguishes between legitimate and fraudulent transactions, achieving high precision and recall while minimizing false positives and false negatives. The study highlights the potential of Agentic AI in transforming financial security by providing an intelligent and adaptive approach to fraud detection. With further refinement, this technology can become an essential tool in safeguarding banking systems against increasingly sophisticated fraudulent activities.

References

[1] Girish Wali1, Dr. Chetan Bulla (2024) Anomaly Detection in Fog Computing: Stateo-f-the-Art Techniques, applications, Challenges, and Future Directions. Library Progress International, 44(3),13967-13993.
[2] Wali, Girish, and Chetan Bulla. "Suspicious activity detection model in bank transactions using deep learning with fog computing infrastructure." *International Conference on Computational Innovations and Emerging Trends (ICCIET-2024)*. Atlantis Press, 2024.
[3] Cao, Longbing. "Ai in finance: challenges, techniques, and opportunities." *ACM Computing Surveys (CSUR)* 55.3 (2022): 1-38.
[4] Tanwar, J., H. Sabrol, Girish Wali, C. Bulla, R. K. Meenakshi, P. S. Tabeck, and B. Surjeet. "Integrating blockchain and deep learning for enhanced supply chain management in healthcare: A novel approach for Alzheimer's and Parkinson's disease prevention and control." *International Journal of Intelligent Systems and Applications in Engineering* 12, no. 22s (2024): 524-539.
[5] D. B. Acharya, K. Kuppan and B. Divya, "Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey," in *IEEE Access*, vol. 13, pp. 18912-18936, 2025, doi: 10.1109/ACCESS.2025.3532853
[6] Spatio-temporal based bank transactional network behaviour analysis to detect suspicious activities, https://doi.org/10.1201/9781003559092-29.
[7] M. N. K. Kumar, A. Umaswathika, K. Yaswanthkumar, et al., "A robust detection fraudulent transactions in banking using machine learning," Turkish Journal of Computer and Mathematics Education, vol. 15, no. 1, 2024, doi: 10.61841/turcomat.v15i1.14551.
[8] K. S. Komilov and M. A. Egamberdiyev, "Preventing money laundering using AI agents," Open Science Framework, Dec. 31, 2022, doi: 10.31237/osf.io/f62k9.
[9] B. Mytnyk, O. Tkachyk, N. Shakhovska, et al., "Application of artificial intelligence for fraudulent banking operations recognition," Big Data and Cognitive Computing, vol. 7, no. 2, 2023, doi: 10.3390/bdcc7020093.
[10] "Suspicious transaction detection in banking cyber–physical systems," Computers, Electrical Engineering, Jan. 1, 2022, doi: 10.1016/j.compeleceng.2021.107596.
[11] P. Sharma, A. S. Prakash, and A. Malhotra, "Application of advanced AI algorithms for fintech crime detection," presented at the International Conference on Communication and Computer Networks, 2024, doi: 10.1109/icccnt61001.2024.10725857.
[12] R. Achary and C. J. Shelke, "Fraud detection in banking transactions using machine learning," presented at the International Conference on Intelligent Technologies and Engineering Systems, Jan. 2023, doi: 10.1109/IITCEE57236.2023.10091067.
[13] R. Achary and C. J. Shelke, "Fraud detection in banking transactions using machine learning," presented at the International Conference on Intelligent Technologies and Engineering Systems, Jan. 2023, doi: 10.1109/iitcee57236.2023.10091067.
[14] "MultiAgent AI-system for money laundering prevention," Open Science Framework, Apr. 27, 2023, doi: 10.22541/au.168261282.28482106/v1.
[15] G. Wali and C. Bulla, "Suspicious activity detection model in bank transactions using deep learning with fog computing infrastructure," in Advances in Computer Science Research, 2024, doi: 10.2991/978-94-6463-471-6_29.