Short communication

AI-Driven Fraud Detection: A Risk Scoring Model for Enhanced Security in Banking

***Abstract*—As technology makes advancements so does the risk of accessing it for wrong doings. In recent years as we moved from traditional banking systems to online banking and the volume of digital transactions has increased eccentric. This also comes up with increasing risk of fraudulent activities like accessing bank accounts, credit card frauds, account frauds, dormant account fraud, and many others. Detecting fraud activities is and crucial part of banking system.**

This research explores the application of artificial intelligence (AI) in detecting potentially fraudulent activities by generating a risk score to assess account behavior. A formula is developed to compute a score out of 100, which triggers automated security measures when exceeding a predefined threshold of 80. The formula evaluates four key activities commonly associated with fraud: new device logins, updates to contact number or email address, the addition of new payees or Zelle contacts, and transactions exceeding $1,000 in 48-hour time span.

Leveraging machine learning algorithms, this model incorporates behavioral patterns, historical data, and real-time anomaly detection to calculate the score. Accounts with scores above the threshold are temporarily locked, initiating further verification processes to ensure security while minimizing customer inconvenience. This research demonstrates the effectiveness of AI-driven fraud detection mechanisms and highlights the balance between security and user experience in modern banking systems.

Keywords*—*Artificial Intelligence, Machine learning, Customer Protection, Banking, Security, Fraud, Risk, Customer satisfaction, Business growth, Finance, Online banking, Account takeover

I. INTRODUCTION

Fraud is defined as a deliberate act of deception carried out with the intent to secure an unlawful advantage or gain. Fraud detection is a practice of recognizing a pattern which can potentially lead to a fraudulent activity.

In the last decade we have seen a significant transformation in Banking industry, especially with Online banking. Internet made Online banking easy and faster for everyone. This also made the financial system easily accessible to everyone, which made fraudulent activities more sophisticated. Cyber criminals take advantage of these systems and exploit the vulnerabilities in online banking. Over the years we have developed fraud detection techniques, but every technology has its time. Traditional rule-based systems are no longer compatible and need human assistance at some point. We need some sort of system which is real-time and modern to detect fraud detection patterns [1].

These techniques are traditional now and we need more advanced ways to detect fraud/risk in banking systems. AI-driven fraud detection systems utilize advanced machine learning (ML) techniques, encompassing supervised, unsupervised, and hybrid learning models, to detect anomalies and fraudulent activities in banking transactions [3]. Supervised learning methods, such as random forests, logistic regression, and neural networks, are commonly employed to classify transactions as fraudulent or legitimate based on historical, labeled datasets [5]. Conversely, unsupervised learning approaches, including clustering techniques and outlier detection algorithms, excel in uncovering novel fraudulent behaviors by analyzing patterns in unlabeled data [4]. Hybrid models, which integrate supervised and unsupervised methods, have gained prominence as they effectively address the shortcomings of single method approaches by enhancing accuracy and adaptability [6]. These advancements empower financial institutions to shift from traditional reactive fraud detection to a proactive approach, significantly improving their ability to mitigate risks in real-time.

This paper explores the transformative impact of AI-driven fraud detection systems on enhancing security measures and operational efficiency within the banking sector. The study provides a thorough analysis of the following key aspects:

1. The **evolution of fraud detection techniques**, emphasizing the transition from traditional rule-based systems to sophisticated AI-powered solutions.
2. A **comprehensive review of relevant literature**, showcasing recent advancements, challenges, and opportunities in leveraging AI for fraud prevention.
3. An in-depth explanation of the **research methodology** employed to evaluate the effectiveness of AI-based systems in minimizing fraudulent activities and ensuring robust customer protection.
4. The **design and implementation** of an AI-driven fraud detection framework, detailing its core components, scoring mechanism, and operational workflow.
5. **Ethical and practical considerations** associated with adopting AI for fraud detection, including privacy concerns, algorithmic transparency, and the need for sustainable practices.

By addressing these dimensions, this research aims to provide actionable recommendations for financial institutions to strengthen fraud prevention strategies, enhance customer trust, and strike a balance between security and user convenience.

II. LITERATURE REVIEW

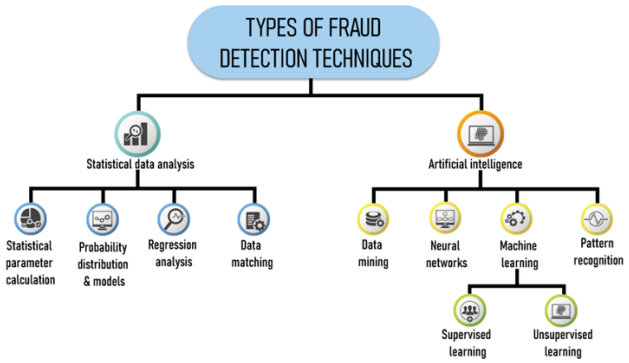

Fig. 1 Types of Fraud Detection Techniques [11]

The increasing sophistication of fraudulent activities in the banking sector has prompted the adoption of advanced technologies for fraud detection. Traditional rule-based systems, which rely on predefined patterns, have become less effective due to their inability to adapt to evolving fraud tactics. This limitation has led to higher false positive rates and necessitated significant manual oversight, highlighting the need for more intelligent and autonomous solutions.

Artificial intelligence and Machine Learning have emerged as pivotal technologies in enhancing fraud detection capabilities [10]. Supervised learning algorithms, such as decision trees, logistic regression, and neural networks, utilize labeled historical data to classify transactions as fraudulent or legitimate. These models have demonstrated effectiveness in identifying known fraud patterns, thereby improving detection accuracy.

Conversely, unsupervised learning methods, including clustering algorithms and anomaly detection techniques, do not require labeled datasets. These approaches are adept at uncovering new and emerging fraud patterns by identifying deviations from normal transaction behaviors. For instance, clustering methods can group similar transactions, enabling the detection of outliers that may indicate fraudulent activity.

Hybrid models that integrate both supervised and unsupervised learning have been developed to leverage the strengths of each approach. These models enhance adaptability and accuracy in fraud detection systems, addressing the limitations inherent in single-method frameworks. The combination of different ML techniques allows for a more comprehensive analysis of transaction data, leading to improved detection rates.

The application of deep learning, a subset of ML, has further advanced fraud detection efforts. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have been employed to capture complex patterns in transaction data. These models are capable of processing large volumes of data and identifying subtle indicators of fraudulent behavior, thereby enhancing the robustness of detection systems.

Despite these technological advancements, challenges remain in the implementation of AI-driven fraud detection systems. Issues such as data privacy concerns, the need for large, labeled datasets, and the potential for adversarial attacks pose significant hurdles. Moreover, the dynamic nature of fraudulent activities necessitates continuous updates and adaptations of detection models to maintain their effectiveness.

In summary, the integration of AI and ML into fraud detection systems has significantly enhanced the ability of financial institutions to identify and prevent fraudulent activities. The evolution from traditional rule-based systems to intelligent, adaptive models represents a critical advancement in safeguarding the integrity of financial transactions.

Below are a few models which are in place for fraud detection currently. We can clearly see the use cases and their strengths and weaknesses.

Models	Use Cases	Strengths	Weakness
Supervised Learning	Debit/Credit cards	High Accuracy	New patterns
Unsupervised Learning	Money laundering	Previously unknown types of fraud	False positive
Deep Learning	Real-time card transaction	complex patterns	Requires Large Datasets
Hybrid	Large-scale institutions	Faster and smarter	Increased Complexity
Rule-Based	Account based activity	Triggers instantly	New patterns
Graph-Based	Money laundering	Detects fraud with multiple connected entities	Computationally intensive
Natural Language Processing	Phishing attacks	Analyzing unstructured text data	Limited to text-based fraud scenarios

Table. 1 Popular AI Tools in Fraud Detecion [7]

AI-enabled software services are designed to detect and report to their surroundings in real time. They analyze the behavior, compare it with past, take appropriate actions, and predict potential threats.

II.I Traditional vs New Fraud Detection

There has been a vast change in fraud detection before and after digital era. As data got rich, and informational machine became smarter and efficient.

Below comparison highlights how AI revolutionized fraud detection, making it faster, smarter, & more customer centric.

	Before AI	After AI
Approach	Rule based	Machine learning based
Real Time Accuracy	Limited	Guarantee
Learning	Hardly	Innate
Transaction Volume	Limited Capacity	Unlimited Capacity
Proactive Measures	Slower	Faster
Impact	Medium	High
Adaptability	Static & Manual	Dynamic & machine based
Response	Reactive	Proactive

Table 2. Before AI and After AI comparison

The landscape of fraud detection and security has changed unparalleled since Machine Learning. With the ability to analyze data in split seconds, machines have become powerful and efficient and help in the interest of financial institutions. As you can clearly see, the impact of AI on Accuracy, Adaptability, Learning and responsiveness.

III. USE OF AI IN FRAUD DETECTION

The integration of Artificial Intelligence (AI) in fraud detection has transformed traditional approaches, enabling financial institutions to effectively combat the growing sophistication of fraudulent activities. AI-driven systems offer innovative tools and methodologies to detect and prevent fraud in real-time, leveraging the power of advanced algorithms and data analytics.

1. Real-Time Fraud Detection

AI enables real-time monitoring of transactions by analyzing vast amounts of data instantly. Machine learning models can detect anomalies and suspicious behaviors as they occur, allowing immediate action, such as freezing accounts or flagging transactions for review.

2. Machine Learning Techniques

AI employs various machine learning (ML) methods to detect fraud:

Supervised Learning: Models like logistic regression, random forests, and neural networks use historical labeled data to classify transactions as fraudulent or legitimate.

Unsupervised Learning: Techniques such as clustering and anomaly detection identify unusual patterns in data that do not conform to normal behavior, which could indicate potential fraud.

Hybrid Models: These combine supervised and unsupervised learning, offering a more robust solution to detect both known and novel fraud patterns.

3. Behavioral Analysis

AI systems analyze customer behavior, such as transaction frequency, location, device usage, and spending habits. Any deviation from a customer's typical behavior is flagged as potentially fraudulent, allowing for proactive fraud prevention.

4. Risk Scoring Models

AI-based fraud detection systems assign a risk score to every transaction based on multiple factors, including transaction amount, device details, and account activity. Transactions exceeding a defined threshold are flagged for further investigation. This research, for example, proposes a scoring mechanism that locks accounts temporarily if the score exceeds 80.

5. Automation and Efficiency

AI automates repetitive tasks, reducing the need for manual intervention in fraud detection. Automated systems process and analyze millions of transactions faster and more accurately than human teams.

6. Continuous Learning

AI models learn and evolve continuously by incorporating new data. This adaptability ensures that the system remains effective even as fraudsters develop new tactics.

7. Advantages of AI in Fraud Detection

Scalability: AI systems can handle a vast volume of transactions simultaneously, making them suitable for large-scale banking operations.

Enhanced Accuracy: By reducing false positives and negatives, AI minimizes disruptions to legitimate users.

Cost-Effectiveness: AI reduces operational costs by automating fraud detection processes and requiring less manual oversight.

8. Case Studies and Applications

Many financial institutions have successfully implemented AI to detect and prevent fraud. Examples include fraud detection in credit card transactions, detecting account takeover attempts, and identifying unauthorized access to online banking accounts.

By leveraging AI, banks can enhance their fraud detection systems, reduce financial losses, and improve customer trust. This chapter underscores the transformative role of AI in making fraud detection more proactive, efficient, and reliable.

IV. FRAMEWORK

1. Data Collection

- *Source of Data:*
  Transactional data from banking systems, including features such as transaction amount, login device information, frequency of payee additions, and updates to contact information.
- *Data Types:*
  Includes structured data such as transaction logs, account activity, and metadata IP addresses, device IDs, transaction location.
- *Historical Data:*
  Labeled datasets with past records of legitimate and fraudulent transactions are used for supervised learning.

2. Feature Selection and Engineering

- *Key Features Identified:*
  - Transaction Amount.
  - Frequency of high-value transactions.
  - Changes in contact details like email and contact number.
  - Number of new payees added in a specific timeframe.
  - Device-related anomalies aka new device login.
- *Feature Engineering:*
  Derived metrics such as transaction velocity (frequency of transactions in a short period) and geolocation mismatch.

3. Data Preprocessing

- *Handling Missing Value*s:

Imputed missing values for numerical features using median values and categorical features using mode.

- *Normalization:*

Applied feature scaling using StandardScaler to normalize transaction values.

- *Balancing the Dataset:*

Addressed class imbalance (fraud cases being fewer than legitimate cases) using techniques such as SMOTE (Synthetic Minority Oversampling Technique).

4. Model Development

- *Machine Learning Algorithms:*
  - *Supervised Models*: Logistic regression, decision trees, and random forests to classify transactions based on labeled data.
  - *Unsupervised Models*: Clustering algorithms (e.g., K-Means) and anomaly detection methods to identify unusual patterns.
  - *Hybrid Approach*: Combined supervised and unsupervised techniques to leverage the strengths of both.

- *Scoring Formula:*

Developed a custom risk-scoring formula to assign a fraud score (0–100) based on the model's output and feature weights.

Score=w1(New Device Login)+w2(Update Contact Info)+w3(New Payee Added)+w4(Transaction Amount)

5. Model Training and Validation

- *Training Data:*

Used 80% of the dataset for training and 20% for testing.

- *Cross-Validation:*

Applied K-fold cross-validation to evaluate model stability and reduce overfitting.

- *Evaluation Metrics:*
  - Precision, Recall, and F1-Score to measure model performance.
  - ROC-AUC Curve to assess the model's ability to distinguish between fraud and legitimate transactions.

6. Deployment Framework

- *Real-Time Detection:*
  Deployed the trained model in a production environment, integrating it with transaction monitoring systems.
- *Risk Thresholds:*
  Set a threshold score (e.g., 80 out of 100) for flagging transactions as potentially fraudulent. Transactions exceeding this score trigger automatic account locks and verification procedures.
- *Alert System:*
  Incorporated an alert system to notify customers and bank staff of flagged transactions.

7. Ethical and Security Considerations

- *Data Privacy:*
  Ensured compliance with data protection regulations, such as GDPR and CCPA.
- *Bias Mitigation:*
  Regularly monitored model for potential biases that could lead to unfair treatment of customers.
- *Transparency:*
  Made the decision-making process interpretable for users and regulators through explainable AI techniques.

This methodology provides a comprehensive framework for designing, training, and implementing an AI-based fraud detection system, ensuring both efficiency and reliability in banking operations.

V. FRAUD DETECTION SYSTEM

Components and Their Functions

1. **Customer**
   - Initiates transactions via online banking, mobile apps, or ATMs.
   - Provides data such as transaction amount, device information, and payee details.
2. **Banking System**
   - Core banking application that handles transaction processing and account management.
   - Sends transaction details to the Fraud Detection System for analysis.
3. **Fraud Detection System (FDS)**
   - *Data Preprocessing Unit*: Cleans and normalizes transaction data.
   - *Feature Extraction Module*: Identifies key fraud-related features such as transaction amount, new device login, etc.
   - *Machine Learning Model*: Predicts fraud likelihood based on processed data.
   - *Risk Scoring Module*: Calculates a fraud risk score for each transaction.
4. **Database**
   - Stores historical transaction data, fraud patterns, and model training data.
5. **Alert Management System**
   - Generates alerts for flagged transactions.
   - Notifies customers and bank staff for further action.
6. **Verification System**
   - Validates flagged transactions through customer authentication (e.g., OTP, phone call).
7. **Admin Dashboard**
   - Provides bank staff with insights into flagged transactions, fraud statistics, and system performance.

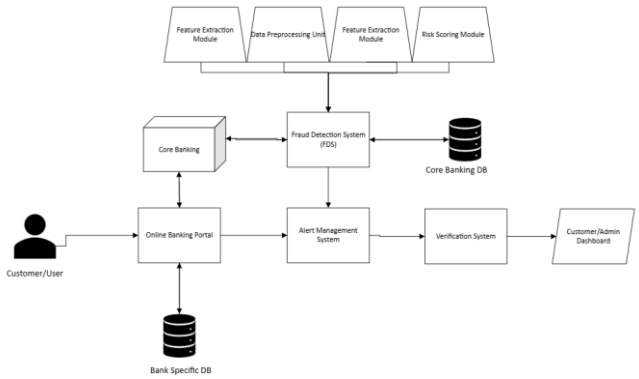

Fig. 2 Workflow diagram of Fraud Detection System [12]

VI. CODE SNIPPET

Below is an algorithm in Python for fraud detection in banking using AI/ML. It leverages a supervised machine learning approach with logistic regression as the classifier. This is a simplified version of a fraud detection system designed to work on structured transaction data.

```
# Import necessary libraries
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score

# Step 1: Load the dataset
# Assume a dataset with features such as 'TransactionAmount', 'NewDeviceLogin', 'UpdatedContactInfo', etc.
# 'is_fraud' is the target variable (1 for fraudulent, 0 for legitimate)
data = pd.read_csv('banking_transactions.csv')

# Step 2: Data preprocessing
# Separate features (X) and target variable (y)
X = data.drop(columns=['is_fraud'])  # Drop the target column from features
y = data['is_fraud']  # Define the target column

# Split the data into training and testing sets (80% training, 20% testing)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Standardize the feature values to normalize the data
scaler = StandardScaler()
X_train = scaler.fit_transform(X_train)
X_test = scaler.transform(X_test)

# Step 3: Train the machine learning model
# Use logistic regression as the classifier
model = LogisticRegression(random_state=42)
model.fit(X_train, y_train)

# Step 4: Make predictions
# Predict on the test set
y_pred = model.predict(X_test)

# Step 5: Evaluate the model
# Display the confusion matrix and classification report
conf_matrix = confusion_matrix(y_test, y_pred)
class_report = classification_report(y_test, y_pred)
accuracy = accuracy_score(y_test, y_pred)

# Output evaluation metrics
print("Confusion Matrix:\n", conf_matrix)
print("\nClassification Report:\n", class_report)
```

```
print("\nAccuracy Score:", accuracy)

# Step 6: Deploy the model for fraud detection (example use case)
# Define a function to predict fraud risk for a new transaction
def predict_fraud(transaction_data):
    """
    Predicts if a transaction is fraudulent.
    :param transaction_data: A dictionary containing transaction features.
    :return: Prediction (1 for fraud, 0 for legitimate)
    """
    # Convert the input dictionary into a dataframe
    transaction_df = pd.DataFrame([transaction_data])
    # Standardize the data using the fitted scaler
    transaction_scaled = scaler.transform(transaction_df)
    # Predict fraud risk
    prediction = model.predict(transaction_scaled)
    return prediction[0]

# Example transaction for prediction
new_transaction = {
    'TransactionAmount': 1500,
    'NewDeviceLogin': 1,
    'UpdatedContactInfo': 0,
    'NewPayeeAdded': 1,
    'TransactionFrequency': 5
}

# Predict and display the result
fraud_prediction = predict_fraud(new_transaction)
if fraud_prediction == 1:
    print("Transaction flagged as potentially fraudulent.")
else:
    print("Transaction appears legitimate.")
```

VII. CONCLUSION

The rapid digitization of the banking sector has brought about both unprecedented convenience and heightened risks of fraudulent activities. This research aimed to explore the transformative role of artificial intelligence (AI) in enhancing fraud detection mechanisms, providing a comprehensive framework for a proactive, real-time solution. The proposed system, which employs a risk-scoring mechanism based on activities such as new device logins, changes to contact details, addition of payees, and high-value transactions, demonstrates how AI can effectively identify suspicious behavior and mitigate risks.

By leveraging advanced machine learning techniques, the system combines supervised and unsupervised models to deliver accurate predictions and adaptable fraud detection capabilities. The integration of these technologies enables financial institutions to move beyond traditional rule-based methods, offering a more dynamic, scalable, and efficient approach. This shift not only enhances security but also fosters customer trust and satisfaction by minimizing disruptions caused by false alerts and manual verifications.

Moreover, the proposed methodology ensures compliance with ethical guidelines and data privacy regulations, addressing key concerns such as transparency, bias mitigation, and customer data protection. While the system shows great promise, it is important to acknowledge certain limitations, including its dependency on high-quality data, the risk of false positives or negatives, and the challenges of integrating AI into legacy banking infrastructure.

Future research could focus on incorporating advanced techniques like deep learning to further refine fraud detection capabilities, exploring cross-sector fraud patterns, and enhancing the interpretability of AI models. Such efforts will be crucial in staying ahead of evolving fraud tactics and ensuring the continued safety and reliability of banking systems.

In conclusion, this study highlights the critical role of AI in combating fraud in the financial sector, paving the way for more secure, efficient, and customer-centric banking solutions. By embracing AI-powered innovations, financial institutions can protect their assets and customers, fostering a safer digital economy for all.

REFERENCES

[1] S. N. John, C. Anele, O. O. Kennedy, F. Olajide and C. G. Kennedy, "Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp. 1186-1191, doi: 10.1109/CSCI.2016.0224

[2] Fang, W., Li, X., Zhou, P., Yan, J., Jiang, D., & Zhou, T. (2021). Deep Learning Anti-Fraud Model for Internet Loan: Where We Are Going. IEEE Access, 9(NA), 9777-9784. https://doi.org/10.1109/access.2021.3051079

[3] Hendri, N., & Sari, S. U. (2023). Sistematic Literature Review: The Strategy For Preventing Government Financial Report Fraud. JAK (Jurnal Akuntansi) Kajian Ilmiah Akuntansi, 10(2), 323-336. https://doi.org/10.30656/jak.v10i2.6599

[4] Chen, C., Liang, C., Lin, J., Wang, L., Liu, Z., Yang, X., Zhou, J., Shuang, Y., & Qi, Y. (2019). IEEE BigData - InfDetect: a Large Scale Graph-based Fraud Detection System for E-Commerce Insurance. 2019 IEEE International Conference on Big Data (Big Data), https://doi.org/10.1109/bigdata47090.2019.900 6115

[5] Bergh, C. M. M. R.-v. d., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 5-NA. https://doi.org/10.1186/s40163-018-0079-3

[6] Hu, X., Chen, H., Chen, H., Li, X., Zhang, J., & Liu, S. (2023). Mining Mobile Network Fraudsters with Augmented Graph Neural Networks. Entropy (Basel, Switzerland), 25(1), 150-150. https://doi.org/10.3390/e25010150

[7] Table 1 - Original table by Author Shubham Metha

[8] Găbudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Scheau, M. C. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks*, *9*(6), 104. https://doi.org/10.3390/risks9060104

[9] R. Rambola, P. Varshney and P. Vishwakarma, "Data Mining Techniques for Fraud Detection in Banking Sector," *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2018, pp. 1-5, doi: 10.1109/CCAA.2018.8777535

[10] S. K. Hashemi, S. L. Mirtaheri and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," in *IEEE Access*, vol. 11, pp. 3034-3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[11] https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

[12] Figure 2 - Original Image by Author Shubham Metha