International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

AI-DRIVEN DETECTION OF MONEY LAUNDERING SOCIAL NETWORK TRANSACTION

[1]Megavath srinu, [2]Mrs E.Pavithra

[1]M. Tech Scholar in Department of CSE Sri Indu College of Engineering And Technology. Hyderabad
[2]Assistant. Professor in Department of CSE Sri Indu College of Engineering And Technology. Hyderabad

Abstract

The rapid advancement of digital financial technologies, online banking systems, peer-to-peer payment platforms, cryptocurrency transactions, and social networking applications has transformed the modern financial ecosystem. While these technologies provide convenience, accessibility, and speed in financial transactions, they have also created significant opportunities for cybercriminals and organized financial fraud networks to perform illegal monetary activities such as money laundering. Money laundering refers to the process of disguising illegally obtained funds and converting them into apparently legitimate assets by transferring money through multiple financial channels, accounts, institutions, or digital platforms. Traditional Anti-Money Laundering (AML) systems rely heavily on predefined rule-based mechanisms and manual investigation procedures that are often inefficient when dealing with modern large-scale digital transaction environments. These systems generate a high number of false-positive alerts and fail to identify sophisticated laundering strategies involving hidden relationships, layered transactions, shell accounts, and cross-border fund transfers. This research proposes **FinShield**, an Artificial Intelligence (AI) driven Anti-Money Laundering framework designed to identify suspicious financial activities in social network transactions using Machine Learning (ML), anomaly detection, behavioral analytics, and Social Network Analysis (SNA). The proposed system continuously monitors transaction flows, analyzes user behavior patterns, and constructs transaction relationship graphs where accounts are represented as nodes and financial transfers are represented as edges. FinShield employs supervised and unsupervised machine learning algorithms including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, Gradient Boosting, and Isolation Forest to classify transactions as legitimate or suspicious. The framework also identifies hidden fraud rings, suspicious clusters, circular transaction chains, and high-risk hub accounts through graph analytics.The proposed system significantly improves fraud detection accuracy while reducing false-positive rates compared to traditional AML systems. FinShield supports real-time monitoring and provides visualization dashboards that assist financial institutions and law enforcement agencies in detecting and preventing financial crimes efficiently.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Experimental evaluation demonstrates that AI-driven intelligent transaction analysis can effectively enhance financial security and strengthen modern AML operations.

Keywords

Artificial Intelligence, Machine Learning, Anti-Money Laundering, Financial Fraud Detection, Social Network Analysis, Random Forest, Behavioral Analytics, Transaction Monitoring, Digital Banking, Anomaly Detection, Fraud Analytics, Cyber Security.

1. INTRODUCTION

The digital transformation of financial systems has significantly changed the way financial transactions are performed across the world. Online banking systems, mobile wallets, cryptocurrency platforms, fintech applications, and peer-to-peer payment services have simplified financial operations by enabling instant fund transfers and cashless transactions. However, the same technological advancements have also increased the complexity of financial crimes such as money laundering, fraud, identity theft, and illegal transaction manipulation. Money laundering has become one of the most dangerous economic crimes because it enables criminals to conceal the origin of illegally obtained funds and integrate them into legitimate financial systems.

Money laundering generally involves three major stages known as placement, layering, and integration. In the placement stage, illegal funds are introduced into the financial system. During the layering stage, multiple complex transactions are performed to hide the origin of the money. Finally, the integration stage allows criminals to reintroduce the laundered money into the economy as apparently legal assets. Modern criminals utilize digital payment systems, shell companies, fake accounts, cryptocurrency wallets, and social networking platforms to create complicated transaction chains that are extremely difficult to track using traditional monitoring systems.

Traditional Anti-Money Laundering (AML) systems mainly rely on static rule-based approaches where transactions are flagged based on predefined thresholds such as transaction amount, frequency, geographical location, or suspicious account activity. Although these methods provide basic protection, they are insufficient in detecting modern financial crimes involving hidden transaction relationships, coordinated fraud rings, and dynamically evolving laundering techniques. In large

financial institutions processing millions of transactions daily, manual investigation of alerts becomes time-consuming and resource-intensive.

Artificial Intelligence and Machine Learning technologies have emerged as powerful solutions for intelligent fraud detection and transaction analysis. AI-driven systems can automatically learn transaction patterns from historical data and identify anomalies that indicate suspicious financial behavior. Machine Learning algorithms can recognize hidden patterns, detect behavioral deviations, and continuously adapt to changing fraud strategies without requiring constant manual rule updates. Social Network Analysis further strengthens fraud detection by examining relationships between accounts and identifying suspicious clusters, hubs, and circular transaction flows.

FinShield is proposed as an advanced AI-powered AML framework that combines machine learning techniques with social network intelligence to provide real-time detection of money laundering activities in digital finance ecosystems. The system analyzes transaction history, user behavior, account interactions, and financial relationships to identify potentially suspicious activities. By constructing transaction graphs and applying intelligent anomaly detection algorithms, FinShield improves fraud detection accuracy and reduces false-positive alerts.

Several researchers have explored AI-based financial fraud detection systems. Chen et al. proposed Graph Convolutional Networks (GCNs) for identifying hidden laundering patterns within transaction networks [1]. Weber et al. demonstrated the effectiveness of Random Forest algorithms for AML transaction classification using synthetic datasets [2]. Zhang et al. developed hybrid deep learning architectures integrating Dynamic Graph Convolutional Networks with Long Short-Term Memory (LSTM) models for temporal transaction analysis [3]. Pham et al. utilized Social Network Analysis techniques for detecting collaborative financial crimes among connected accounts [4]. These studies indicate the growing importance of AI and graph-based intelligence in modern Anti-Money Laundering systems.

2. LITERATURE SURVEY

Financial fraud detection and Anti-Money Laundering systems have evolved significantly over the last decade due to the increasing complexity of digital financial transactions. Earlier AML systems mainly focused on rule-based transaction monitoring mechanisms where transactions exceeding specific thresholds were automatically flagged for manual review. Although such systems were effective for detecting simple fraud patterns, they failed to

identify hidden and sophisticated laundering techniques.

Chen et al. [1] introduced Graph Convolutional Networks (GCNs) for analyzing transaction networks and identifying suspicious financial relationships. Their research demonstrated that graph-based transaction analysis can effectively detect hidden laundering rings and indirect account connections. However, the proposed approach faced scalability challenges when processing very large transaction datasets in real-time environments.

Weber et al. [2] applied Random Forest algorithms for AML transaction classification using synthetic financial datasets. Their work achieved high detection accuracy and demonstrated the effectiveness of supervised machine learning in identifying suspicious transactions. Nevertheless, the system primarily relied on tabular transaction features and lacked network-level relational intelligence.

Zhang et al. [3] proposed a hybrid framework combining Dynamic Graph Convolutional Networks with Long Short-Term Memory (LSTM) models to analyze both structural and temporal transaction behaviors. Their approach significantly improved fraud detection performance by capturing evolving transaction patterns over time. However, the framework required extensive labeled datasets and high computational resources for training.

Pham et al. [4] focused on Social Network Analysis for detecting collaborative money laundering operations. Their system examined account relationships, transaction chains, and interaction behaviors to identify coordinated fraud groups. Although highly effective in uncovering hidden fraud rings, the implementation complexity limited its practical deployment in real-time banking systems.

Alarab and Prakoonwit [5] investigated Graph Neural Networks (GNNs) for identifying illegal cryptocurrency transactions on blockchain networks. Their model successfully detected suspicious transaction patterns and fraudulent cryptocurrency activities. However, the system suffered from concept drift due to rapidly evolving transaction behaviors in cryptocurrency markets.

Boltaev and Rakhmatullaev [6] proposed a federated learning-based AML framework allowing financial institutions to collaboratively train machine learning models without sharing sensitive customer data. Their approach addressed privacy concerns and enabled inter-bank collaboration for fraud detection. Despite its advantages, practical implementation required significant infrastructure and coordination among institutions.

Recent studies have increasingly focused on explainable AI, anomaly detection, and hybrid machine learning architectures to improve AML

systems. Kumar and Singh [7] introduced hybrid AI-driven AML frameworks integrating rule-based systems with adaptive machine learning analytics to improve interpretability and fraud detection accuracy. Li and Zhao [8] explored Explainable Artificial Intelligence (XAI) methods to improve transparency and trust in machine learning-based financial fraud detection systems.

Overall, the literature demonstrates a clear transition from static rule-based AML systems toward intelligent AI-driven frameworks capable of analyzing transaction behavior, relational structures, and evolving fraud patterns. However, challenges such as scalability, false positives, explainability, data imbalance, and privacy-preserving collaboration remain active research areas.

3. EXISTING SYSTEM

Existing Anti-Money Laundering systems deployed in most financial institutions primarily depend on rule-based transaction monitoring approaches. These systems utilize predefined transaction thresholds and manually configured rules to identify suspicious financial activities. Transactions involving large monetary amounts, unusual transfer frequencies, international transfers, or transactions to high-risk regions are automatically flagged for further investigation.

Although traditional AML systems provide a basic level of financial security, they face multiple limitations in modern digital financial environments. One of the major problems is the generation of excessive false-positive alerts. Many legitimate transactions satisfy predefined rule conditions and are incorrectly identified as suspicious activities. This increases the workload on compliance officers and investigators, leading to inefficient resource utilization.

Another major limitation is the inability of traditional systems to detect sophisticated laundering strategies involving layered transactions, shell accounts, and hidden transaction relationships. Modern criminals divide large illegal funds into multiple smaller transactions and transfer them across interconnected accounts to avoid detection. Traditional systems analyze transactions individually rather than examining overall behavioral and relational patterns.

Manual investigation processes further slow down fraud detection and increase operational costs. Since financial institutions process millions of transactions daily, reviewing each flagged transaction manually becomes highly impractical. Existing systems also struggle to adapt to evolving criminal techniques because rule updates require continuous human intervention.

Therefore, there is a strong need for intelligent, adaptive, and automated Anti-Money Laundering systems capable of detecting hidden fraud patterns and analyzing complex financial relationships in real time.

4. PROBLEM STATEMENT

The rapid growth of digital banking, online payment platforms, social network transactions, and fintech applications has significantly increased the complexity and volume of financial transactions. Traditional Anti-Money Laundering systems are unable to efficiently monitor and analyze these large-scale digital transaction environments due to their dependence on static rules and manual investigation mechanisms.

Modern money laundering activities involve sophisticated techniques such as transaction layering, circular fund transfers, fake account generation, shell companies, and hidden social network interactions. Existing AML systems cannot effectively identify these complex fraud patterns because they lack behavioral intelligence, adaptive learning capabilities, and network-level analysis mechanisms.

Additionally, traditional systems generate large numbers of false-positive alerts, increasing operational workload and reducing investigation efficiency. Manual analysis of suspicious transactions consumes significant time and financial resources while still failing to detect advanced laundering operations.

Therefore, an intelligent AI-driven Anti-Money Laundering framework is required to perform real-time transaction monitoring, behavioral analysis, anomaly detection, and social network analysis to accurately identify suspicious financial activities and improve fraud prevention capabilities.

5. PROPOSED SYSTEM

The proposed system, FinShield, is an Artificial Intelligence driven Anti-Money Laundering framework developed to identify suspicious financial transactions in digital banking and social network payment environments. The system integrates Machine Learning algorithms, behavioral analytics, anomaly detection techniques, and Social Network Analysis to improve fraud detection accuracy and reduce false-positive alerts.

FinShield continuously monitors transaction flows and analyzes user behavior patterns based on historical transaction records. The system collects transaction attributes such as sender information, receiver details, transaction amount, transaction frequency, geographical location, and transaction timing. These features are processed using machine learning models trained to distinguish between legitimate and suspicious financial activities.

One of the major strengths of FinShield is its graph-based transaction analysis mechanism. The framework constructs transaction networks where accounts are represented as nodes and financial transfers are represented as edges. This graph representation enables the identification of hidden fraud rings, suspicious clusters, circular transaction flows, and central laundering hubs that are difficult to detect using traditional monitoring systems.

The proposed system also incorporates risk scoring mechanisms that assign fraud probability scores to individual transactions and accounts. Transactions with high-risk scores are automatically flagged for further investigation. Real-time monitoring dashboards and visualization tools help investigators analyze suspicious activities efficiently.

The system is scalable, adaptive, and capable of learning evolving fraud strategies through continuous model retraining and behavioral analysis.

6. METHODOLOGY

The FinShield framework follows a systematic methodology consisting of data collection, preprocessing, feature engineering, machine learning model training, social network analysis, fraud prediction, and result visualization.

Initially, transaction datasets are collected from banking systems, digital payment platforms, and social network transaction environments. The dataset includes transaction identifiers, sender and receiver account information, transaction amounts, timestamps, locations, and transaction categories.

During preprocessing, missing values, duplicate records, and inconsistent data entries are removed. Numerical features are normalized, and categorical variables are encoded to improve machine learning performance.

Feature engineering is performed to extract meaningful behavioral indicators such as transaction frequency, average transfer amount, velocity of transactions, night-time transaction activity, cross-border transfers, and round-amount transaction patterns. These features help machine learning models recognize suspicious behaviors effectively.

Multiple machine learning algorithms including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, Gradient Boosting, and Isolation Forest are trained using historical transaction data. Model performance is evaluated using metrics such as Accuracy, Precision, Recall, and F1-Score.

Social Network Analysis is then applied to construct transaction graphs and identify hidden relationships between accounts. Fraud prediction results are generated in real time and displayed through visualization dashboards.

7. IMPLEMENTATION

The FinShield system is implemented using Python and Flask for backend development and Scikit-learn for machine learning integration. Frontend technologies including HTML, CSS, JavaScript, Chart.js, and Vis.js are utilized to create interactive dashboards and transaction visualization interfaces.

The backend server processes transaction requests, applies trained machine learning models, calculates fraud risk scores, and generates alerts for suspicious activities. Transaction graphs are dynamically visualized using network analysis libraries to display account relationships and suspicious clusters.

SQLite database management systems are used to store transaction records, user information, fraud alerts, and historical analysis results. Machine learning models are saved and loaded using Joblib for efficient prediction handling.

The system supports real-time monitoring, fraud score visualization, alert notifications, transaction filtering, and performance analytics. Financial investigators can interact with the dashboard to analyze suspicious transaction chains and investigate potential money laundering activities effectively.

8. RESULTS

The FinShield framework was evaluated using multiple machine learning algorithms on financial transaction datasets. Experimental analysis demonstrated significant improvements in fraud detection accuracy compared to traditional rule-based AML systems.

Among all evaluated models, Random Forest and Gradient Boosting achieved the highest detection performance with improved Precision, Recall, and F1-Score values. The graph-based transaction analysis mechanism successfully identified suspicious account clusters, hidden laundering chains, and circular fund transfer patterns.

The proposed system reduced false-positive alerts considerably, thereby minimizing manual investigation workload and improving operational efficiency. Real-time monitoring and behavioral analysis enabled faster identification of suspicious financial activities.

The integration of Social Network Analysis further improved fraud detection capabilities by uncovering hidden relationships between accounts and identifying coordinated laundering activities.

9. CONCLUSION

FinShield demonstrates the effectiveness of Artificial Intelligence and Machine Learning

technologies in modern Anti-Money Laundering systems. Traditional rule-based AML mechanisms are no longer sufficient for detecting sophisticated financial crimes in highly interconnected digital financial ecosystems. The proposed framework integrates machine learning algorithms, behavioral analytics, anomaly detection, and social network intelligence to provide intelligent real-time fraud monitoring.

By analyzing transaction patterns, user behaviors, and account relationships, FinShield accurately identifies suspicious financial activities while significantly reducing false-positive alerts. The graph-based transaction analysis mechanism enables the detection of hidden laundering rings, circular transaction chains, and coordinated fraud networks.

The proposed system offers scalability, adaptability, and operational efficiency for financial institutions and regulatory agencies. Future enhancements may include blockchain transaction analysis, deep learning architectures such as Graph Neural Networks and LSTMs, federated learning integration, and real-time banking API connectivity.

REFERENCES

[1] Chen, C. et al., "Graph Convolutional Networks for Anti-Money Laundering Detection," IEEE, 2020.

[2] Weber, M. et al., "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks," ACM Transactions, 2021.

[3] Zhang, Y. et al., "Hybrid Deep Learning Framework for Financial Fraud Detection," Elsevier, 2022.

[4] Pham, T. et al., "Social Network Analysis for Financial Crime Detection," Springer, 2023.

[5] Alarab, I., and Prakoonwit, S., "Graph Neural Networks for Cryptocurrency Fraud Detection," IEEE Access, 2019.

[6] Boltaev, B., and Rakhmatullaev, H., "Federated Learning Framework for AML Systems," IEEE Access, 2021.

[7] Kumar, R., and Singh, A., "Hybrid AI Approaches for AML Systems," IEEE Access, 2024.

[8] Li, X., and Zhao, H., "Explainable Artificial Intelligence in Anti-Money Laundering," Springer, 2021.

[9] Torres, J. et al., "Unsupervised Anomaly Detection in Financial Systems," Data Mining and Knowledge Discovery, 2022.

[10] Hussain, K., and Zhao, Y., "Blockchain Analytics for Anti-Money Laundering Applications," IEEE Transactions, 2020.