iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77419

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

AI-Driven Approaches to Improve Cybersecurity in Financial Transactions

Sneha B. Sahane
Assistant Professor, Master of Computer Application, Dr. Moonje Institute of Management & Computer Studies, Nashik,422005.

Abstract: ***The rapid digitalization of financial services has significantly increased exposure to cyber threats targeting financial transactions. Traditional rule-based cybersecurity mechanisms are insufficient against evolving attack strategies such as fraud, identity theft, adversarial manipulation, and advanced persistent threats. Artificial Intelligence (AI) and Machine Learning (ML) provide adaptive, scalable, and real-time solutions for detecting and mitigating financial cyber risks. This paper presents a comprehensive study of AI-driven approaches for improving cybersecurity in financial transactions. It analyzes supervised, unsupervised, deep learning, graph-based, and reinforcement learning techniques, along with their applications in fraud detection, anti-money laundering (AML), identity verification, and threat intelligence. Implementation frameworks, challenges, ethical implications, and future research directions are also discussed. The results indicate that AI significantly enhances detection accuracy and response efficiency while introducing challenges related to explain ability, privacy, fairness, and adversarial robustness.***

Keywords: Artificial Intelligence, Cybersecurity, Financial Transactions, Fraud Detection, Deep Learning, Graph Neural Networks, Federated Learning, Anti-Money Laundering, Explainable AI.

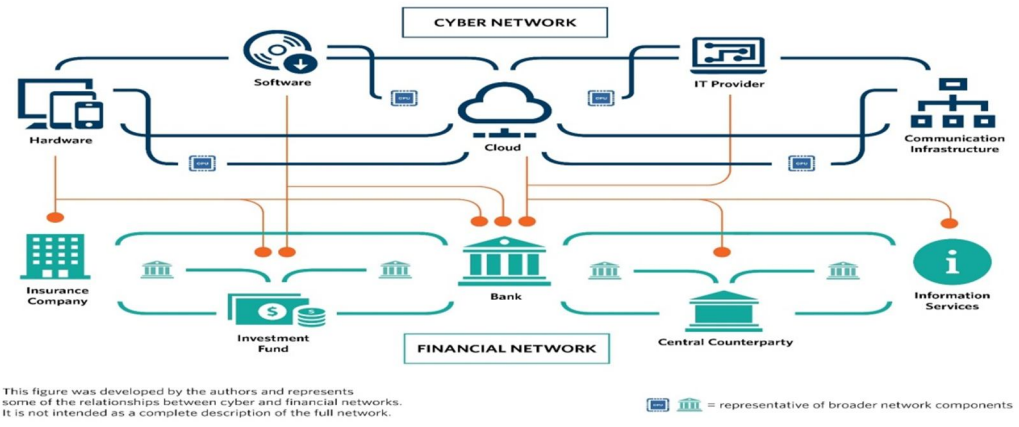
I. INTRODUCTION

The global financial ecosystem has transitioned toward digital platforms including online banking, mobile payments, e-wallets, and cryptocurrency systems. While digital transformation enhances operational efficiency and accessibility, it also increases vulnerability to cyber threats. Financial institutions face attacks such as phishing, account takeover, malware injection, insider threats, and sophisticated fraud schemes. Traditional cybersecurity systems rely on rule-based filters and static signatures. However, modern cyber threats evolve dynamically, rendering static defenses ineffective. AI-driven approaches provide adaptive learning mechanisms capable of detecting anomalies and predicting threats in real time. Recent research emphasizes the growing importance of intelligent fraud detection systems [2], [6]. Anomaly detection techniques [3] and deep learning models [4] have significantly improved predictive capabilities. This paper provides a detailed exploration of AI-driven financial cybersecurity systems.

II. ARCHITECTURE OF AI-DRIVEN FINANCIAL CYBERSECURITY SYSTEMS

AI-based financial cybersecurity systems typically follow a multi-layered architecture integrating data ingestion, feature engineering, model training, and real-time inference.

FIGURE 1
Interaction Between Cyber and Financial Networks (Schematic Diagram)



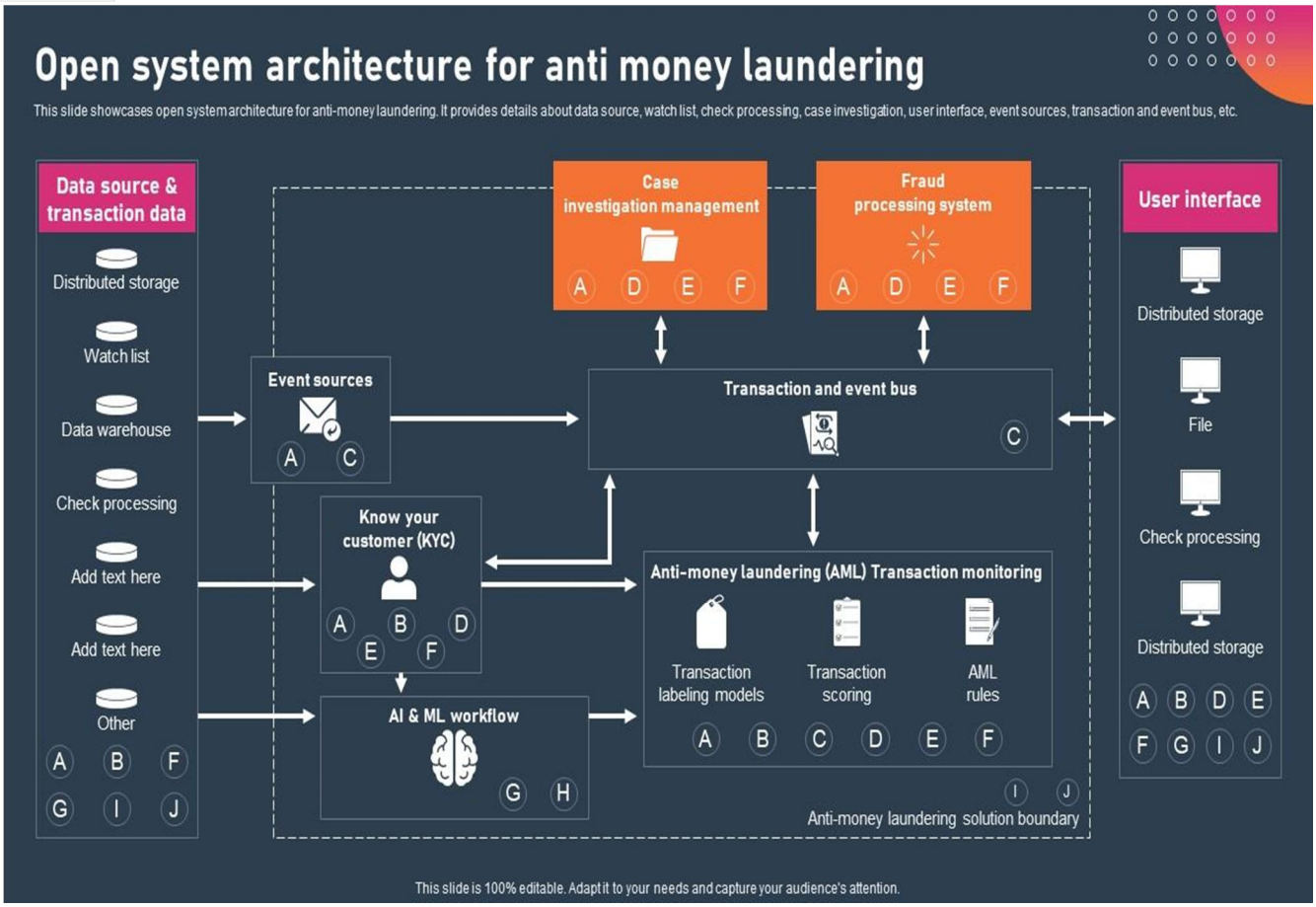


Fig. 1. General architecture of an AI-driven cybersecurity system for financial transactions.

The architecture consists of:

1) Data Acquisition Layer (transaction logs, user behavior, network data)
2) Preprocessing & Feature Engineering
3) AI Model Layer (ML/DL algorithms)
4) Real-Time Decision Engine
5) Monitoring & Feedback Loop

III. AI TECHNIQUES FOR FINANCIAL CYBERSECURITY

A. Supervised Learning

Supervised learning models use labeled transaction datasets to classify transactions as legitimate or fraudulent. Common models include Logistic Regression, Random Forest, and Support Vector Machines (SVM). Ensemble models improve classification performance in imbalanced datasets [6].

B. Unsupervised Learning and Anomaly Detection

Unsupervised techniques detect deviations from established behavioral patterns. These methods are particularly useful when fraud labels are limited [3].

Examples include:

1) K-means clustering
2) Principal Component Analysis (PCA)
3) Autoencoders

C. *Deep Learning Approaches*

Deep learning enables automated high-dimensional feature extraction [4].

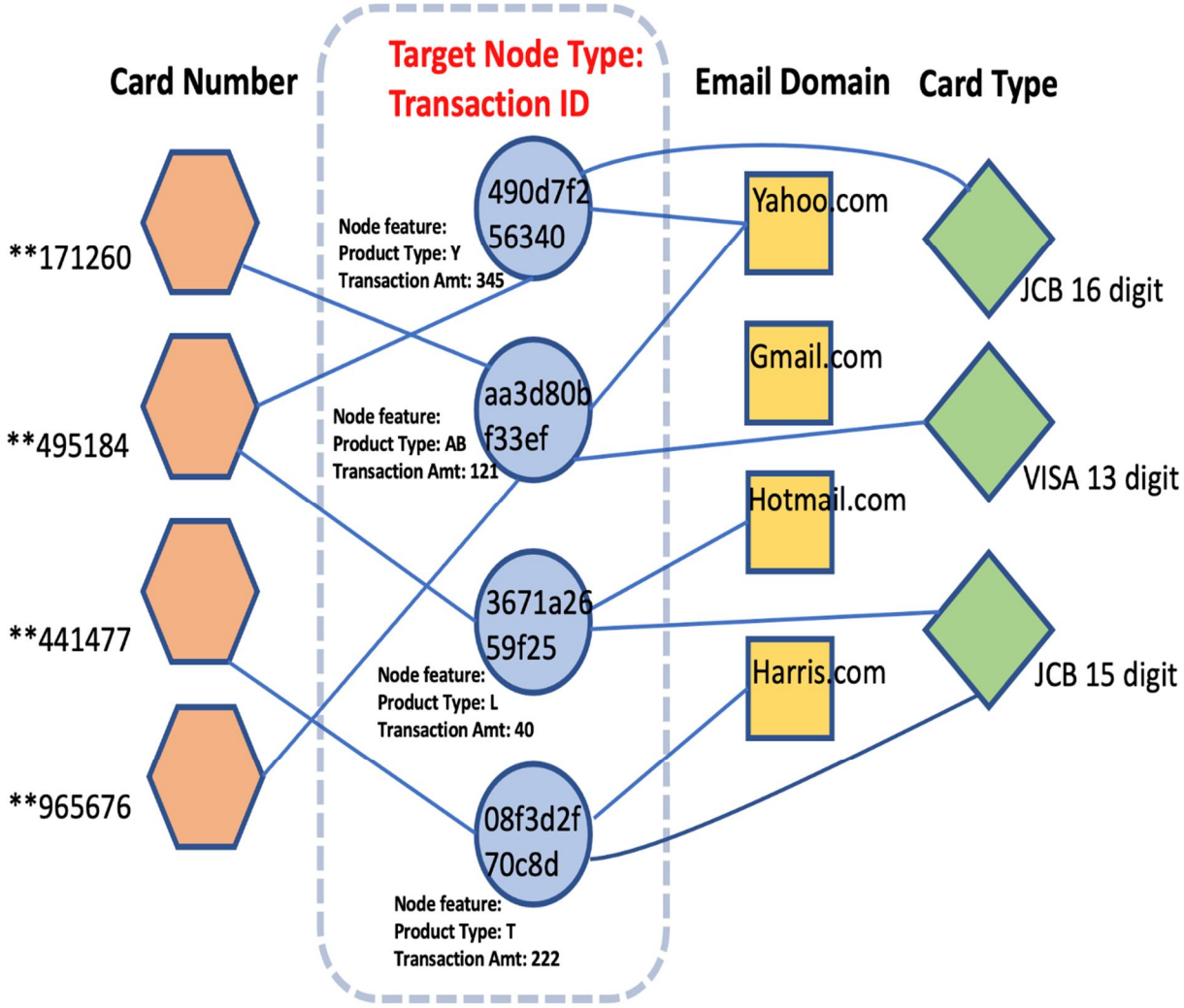


Fig. 2. Deep learning models applied in financial fraud detection.

1) Recurrent Neural Networks (RNNs): Suitable for sequential transaction analysis.
2) Convolutional Neural Networks (CNNs): Effective for behavioral and spatial pattern extraction.
3) Graph Neural Networks (GNNs): Detect complex fraud networks and AML-related transaction graphs [7].

D. *Reinforcement Learnin*

Reinforcement learning optimizes adaptive authentication systems. It dynamically adjusts security policies based on risk scores, inspired by sequential decision-making frameworks [11].

IV. APPLICATIONS IN FINANCIAL TRANSACTIONS

A. *Fraud Detection*

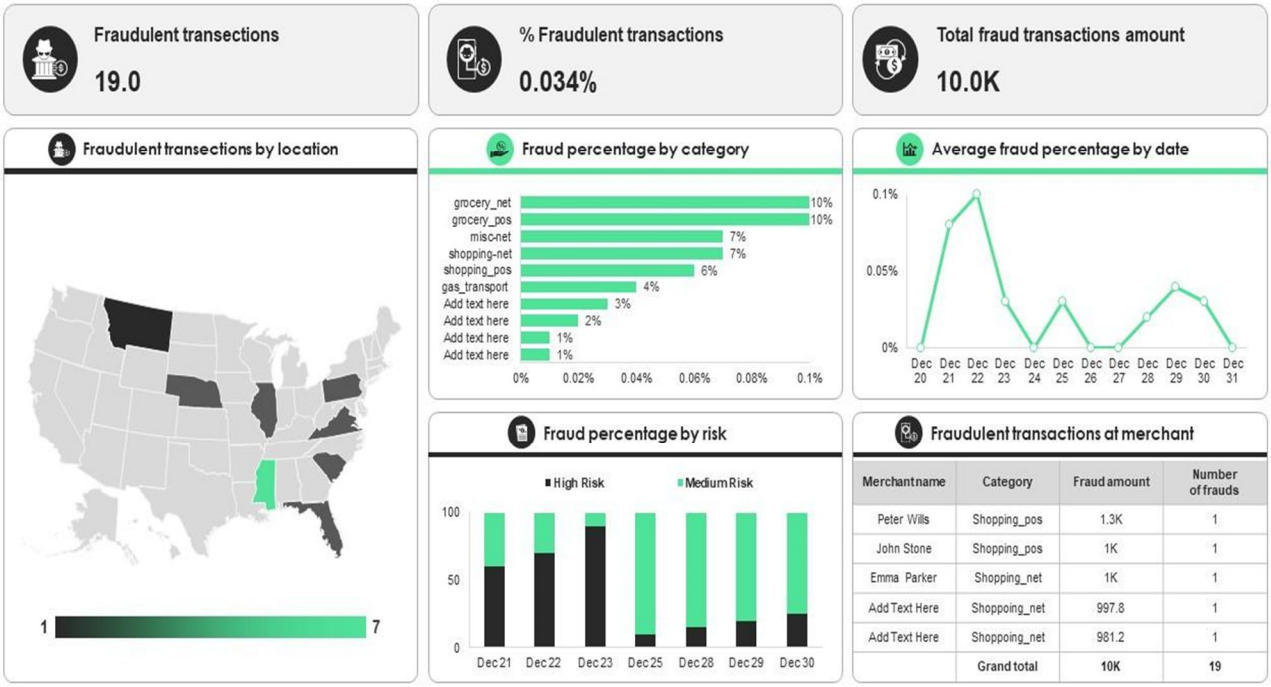
Fraud detection systems analyze transaction parameters such as:

1) Transaction amount
2) Frequency
3) Geolocation
4) Device fingerprint
5) Behavioral biometrics

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Dashboard for real time credit card fraud detection

This slide represents dashboard that assist banking companies to detect and prevent credit card frauds effectively. It includes various components such as fraud transections by category, location, date, merchants, etc.



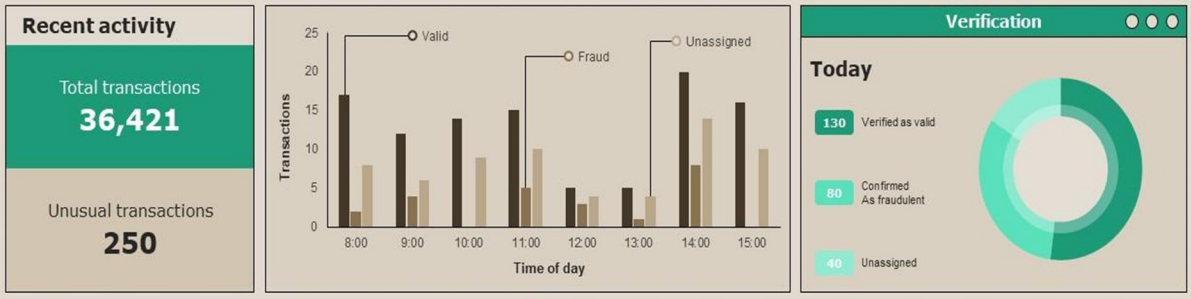
Fraudulent transactions at merchant

Merchant name	Category	Fraud amount	Number of frauds
Peter Wills	Shopping_pos	1.3K	1
John Stone	Shopping_pos	1K	1
Emma Parker	Shopping_net	1K	1
Add Text Here	Shoppoing_net	997.8	1
Add Text Here	Shoppoing_net	981.2	1
	Grand total	10K	19

This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

Dashboard for monitoring fraud and money laundering transactions

This slide showcases dashboard for monitoring fraudulent and money laundering transactions. It provides information about legitimacy, total transaction, unusual transactions, bank, client, investigation, in peer review, etc.



Unusual transaction alerts

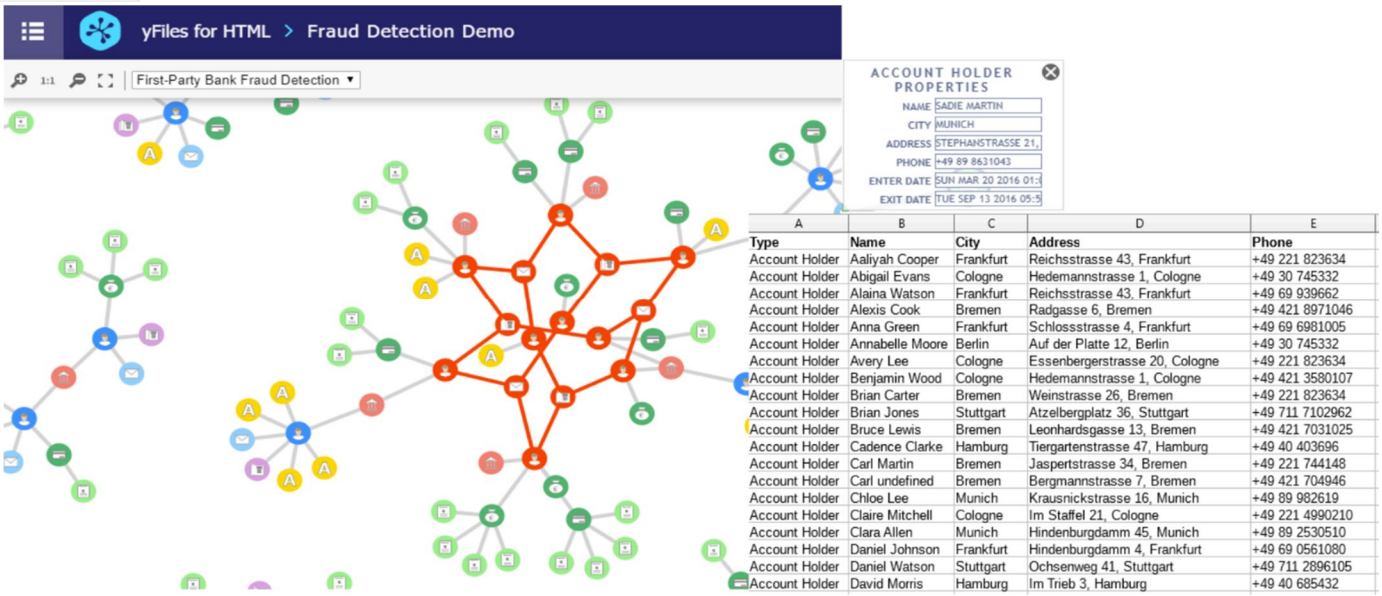
- Client johnson did more than 10 transactions at same time a day totaling $550,000
- Client martha did more than 25 transactions in same month totaling $2,550,000
- Add text here
- Add text here

Ongoing investigation

Bank	Client	Assigned to	Progress
Federal bank USA	Johnson	Agent smith	Investigation opened
Add text here	Martha	Agent smith	In peer review
Add text here	Add text here	Agent smith	Complete
Add text here	Add text here	Agent smith	Confirmed as unusual

This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



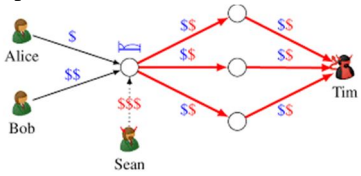
A	B	C	D	E
Type	Name	City	Address	Phone
Account Holder	Aaliyah Cooper	Frankfurt	Reichsstrasse 43, Frankfurt	+49 221 823634
Account Holder	Abigail Evans	Cologne	Hedemannstrasse 1, Cologne	+49 30 745332
Account Holder	Alaina Watson	Frankfurt	Reichsstrasse 43, Frankfurt	+49 69 939662
Account Holder	Alexis Cook	Bremen	Radgasse 6, Bremen	+49 421 8971046
Account Holder	Anna Green	Frankfurt	Schlossstrasse 4, Frankfurt	+49 69 6981005
Account Holder	Annabelle Moore	Berlin	Auf der Platte 12, Berlin	+49 30 745332
Account Holder	Avery Lee	Cologne	Essenbergerstrasse 20, Cologne	+49 221 823634
Account Holder	Benjamin Wood	Cologne	Hedemannstrasse 1, Cologne	+49 421 3580107
Account Holder	Brian Carter	Bremen	Weinstrasse 26, Bremen	+49 221 823634
Account Holder	Brian Jones	Stuttgart	Atzelbergplatz 36, Stuttgart	+49 711 7102962
Account Holder	Bruce Lewis	Bremen	Leonhardsgasse 13, Bremen	+49 421 7031025
Account Holder	Cadence Clarke	Hamburg	Tiergartenstrasse 47, Hamburg	+49 40 403696
Account Holder	Carl Martin	Bremen	Jaspertstrasse 34, Bremen	+49 221 744148
Account Holder	Carl undefined	Bremen	Bergmannstrasse 7, Bremen	+49 421 704946
Account Holder	Chloe Lee	Munich	Krausnickstrasse 16, Munich	+49 89 982619
Account Holder	Claire Mitchell	Cologne	Im Staffel 21, Cologne	+49 221 4990210
Account Holder	Clara Allen	Munich	Hindenburgdamm 45, Munich	+49 89 2530510
Account Holder	Daniel Johnson	Frankfurt	Hindenburgdamm 4, Frankfurt	+49 69 0561080
Account Holder	Daniel Watson	Stuttgart	Ochsenweg 41, Stuttgart	+49 711 2896105
Account Holder	David Morris	Hamburg	Im Trieb 3, Hamburg	+49 40 685432

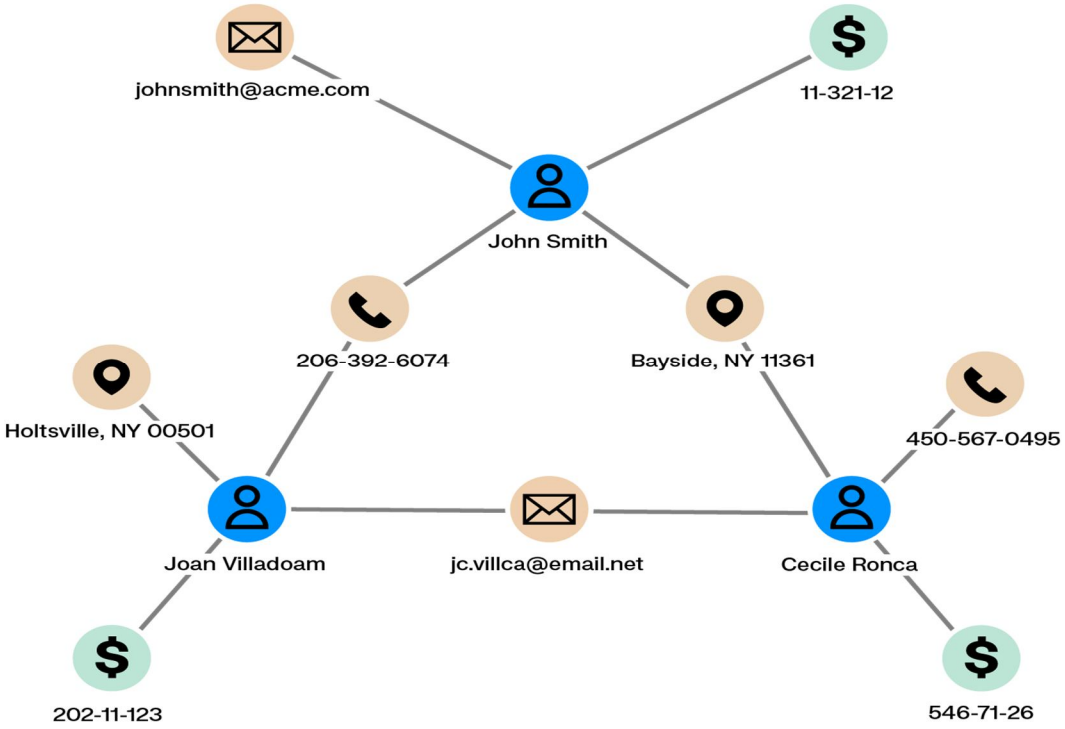
Fig. 3. Real-time fraud detection dashboards using AI analytics.

Streaming active learning improves detection in dynamic environments [12].

B. Anti-Money Laundering (AML)

AI models analyze transaction graphs to detect suspicious financial networks.





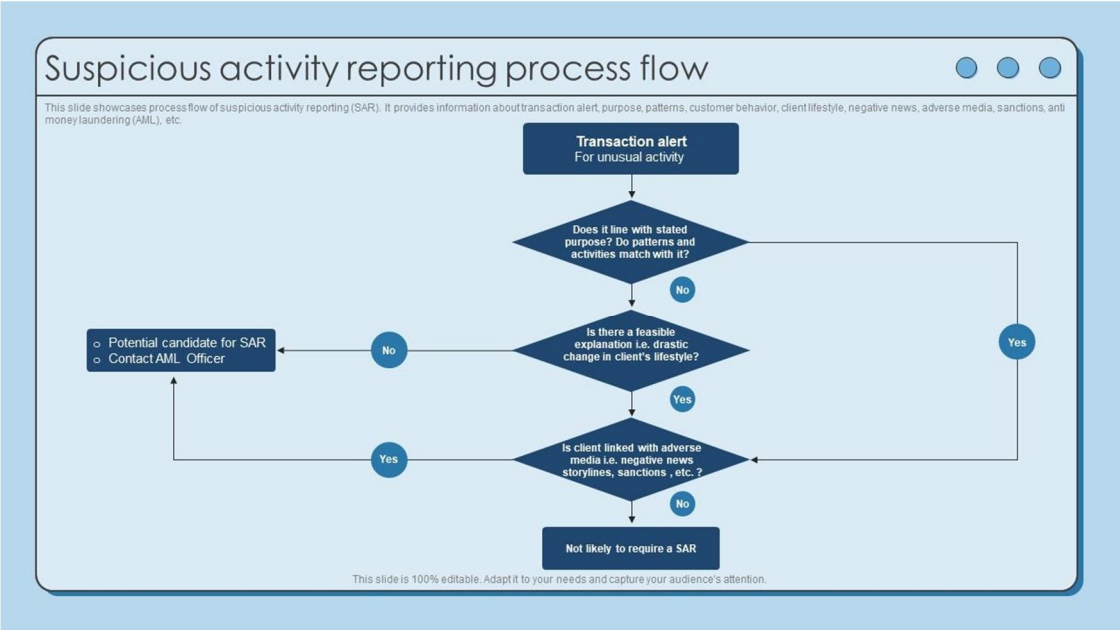


Fig. 4. Graph-based AML detection identifying suspicious transaction networks.

Graph Neural Networks enable multi-hop relationship analysis for hidden illicit patterns [7].

C. Identity Verification and Behavioral Biometrics

AI enhances authentication through:

1) Facial recognition
2) Voice recognition
3) Keystroke dynamics
4) Mouse movement analysis

These techniques prevent account takeover and identity theft.

V. IMPLEMENTATION FRAMEWORK

AI-driven financial cybersecurity implementation includes:

A. Data Collection and Preprocessing

1) Transaction logs
2) User behavior profiles
3) Network telemetry
4) External threat intelligence

Feature engineering and normalization are critical.

B. Model Training and Evaluation

Evaluation metrics include:

1) Accuracy
2) Precision
3) Recall
4) F1-score
5) ROC-AUC

Cost-sensitive modeling improves fraud detection performance under class imbalance [1].

C. Deployment and Continuous Monitoring

Systems require:

1) Low-latency inference
2) Model drift detection
3) Continuous retraining
4) Regulatory auditing compliance

VI. CHALLENGES AND LIMITATIONS

1) Data Privacy and Regulatory Compliance: Financial institutions must comply with global standards such as NIST cybersecurity frameworks [16]. Federated learning enables decentralized training without sharing raw data [14].
2) Adversarial Attacks: Deep learning models are vulnerable to adversarial manipulation [9]. Robust model training and adversarial defenses are essential.
3) Bias and Fairness: Explainable AI tools such as LIME improve interpretability and fairness [10].
4) Scalability and Infrastructure Costs: Large-scale AI systems require high computational resources and optimized deployment pipelines.

VII. ETHICAL AND REGULATORY CONSIDERATIONS

AI systems in financial cybersecurity must adhere to:

1) Transparency
2) Accountability
3) Fairness
4) Privacy preservation

Regulatory bodies increasingly demand interpretable AI decisions.

VIII. FUTURE RESEARCH DIRECTIONS

1) Federated Learning in Multi-Bank Ecosystems [14]
2) Blockchain-AI Integration for Immutable Transaction Tracking
3) Adversarially Robust AI Models
4) Quantum AI for Advanced Cryptographic Analysis

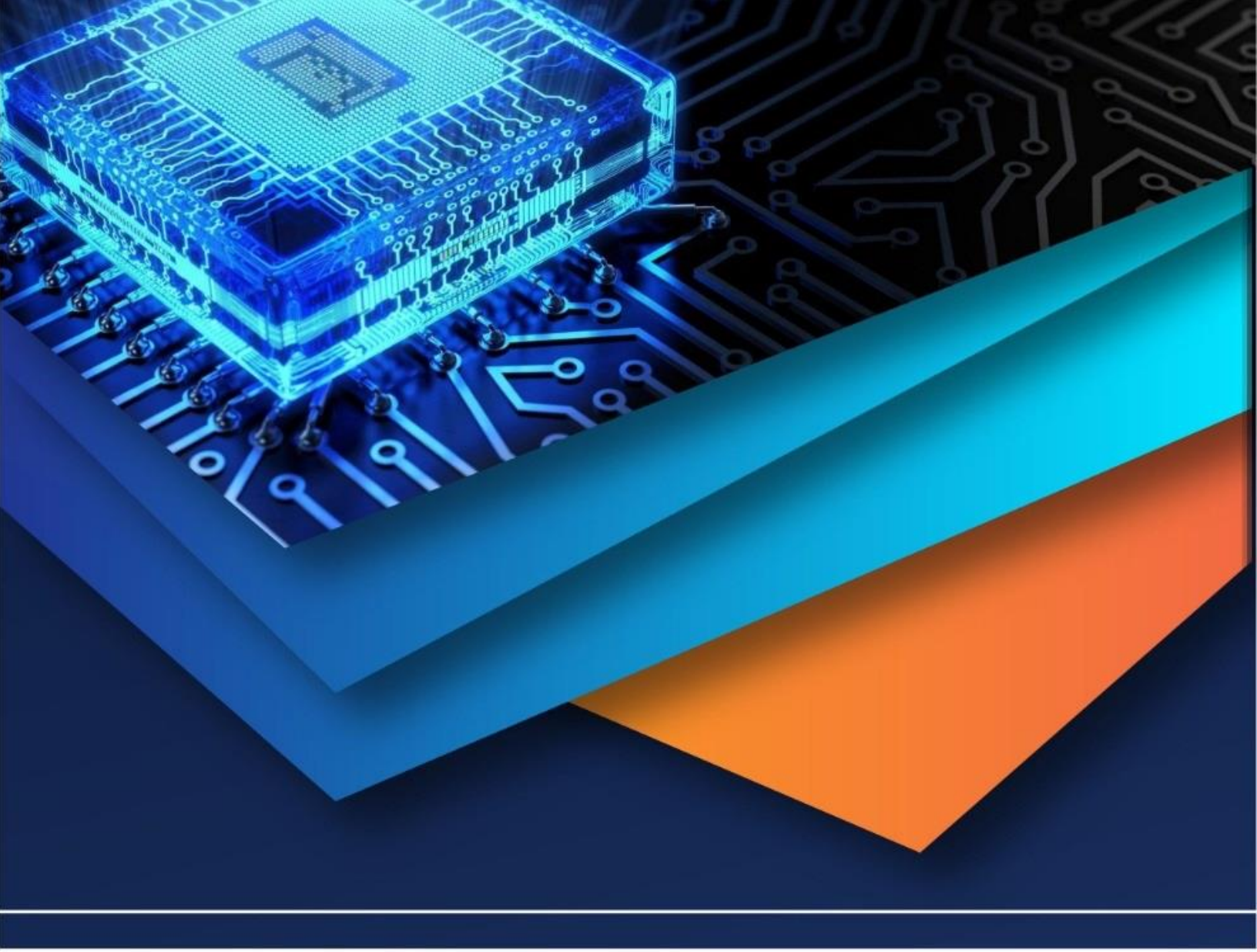
IX. CONCLUSION

AI-driven approaches substantially enhance cybersecurity in financial transactions by enabling adaptive, real-time threat detection. Machine learning, deep learning, graph analytics, and reinforcement learning collectively strengthen fraud detection, AML compliance, and identity verification. Despite these advancements, challenges related to privacy, explainability, bias, and adversarial robustness remain significant. Future research should focus on privacy-preserving AI, regulatory compliance, and resilient AI architectures to ensure secure and trustworthy financial ecosystems.

REFERENCES

[1] S. J. Stolfo et al., “Cost-based modeling for fraud and intrusion detection,” Proc. DARPA DISCEX, 2000.
[2] A. Ngai et al., “Data mining techniques in financial fraud detection,” Decision Support Systems, 2011.
[3] V. Chandola et al., “Anomaly detection: A survey,” ACM Computing Surveys, 2009.
[4] I. Goodfellow et al., *Deep Learning*. MIT Press, 2016.
[5] J. West and M. Bhattacharya, “Intelligent financial fraud detection,” Computers & Security, 2016.
[6] S. Bhattacharyya et al., “Credit card fraud detection,” Decision Support Systems, 2011.
[7] T. Kipf and M. Welling, “Graph convolutional networks,” ICLR, 2017.
[8] M. Egele et al., “Dynamic malware-analysis techniques,” ACM CSUR, 2012.
[9] N. Papernot et al., “Adversarial deep learning limitations,” IEEE EuroS&P, 2016.
[10] B. Ribeiro et al., “Explaining classifier predictions,” KDD, 2016.
[11] D. Silver et al., “Mastering the game of Go,” Nature, 2016.
[12] F. Carcillo et al., “Streaming active learning for fraud detection,” 2020.
[13] M. Conti et al., “IoT security and forensics,” 2018.
[14] P. Kairouz et al., “Federated learning advances,” 2021.
[15] European Central Bank, “Card fraud statistics,” 2023.
[16] NIST, *Cybersecurity Framework*, 2018

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)