Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

FinShield: Explainable Graph Neural Network Approach to Money Laundering Detection in Digital Social Transactions

P Ratna Tejaswi[1], K Aanuj Reddy[2], G Eesha[2], J Nagalaxmi[2]

[1]Assistant Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

[2]Student, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

Correspondence

P.Ratna Tejaswi

Assistant Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

- Received Date: 08 Jan 2026
- Accepted Date: 20 Jan 2026
- Publication Date: 09 Feb 2026

Keywords

Money Laundering Detection, Social Network Transactions, Graph Neural Networks, Financial Fraud Detection, Anomaly Detection, Risk Scoring, Anti-Money Laundering (AML).

Abstract

The rapid growth of digital payment platforms and social network-based financial transactions has increased the risk of money laundering activities. Criminals exploit peer-to-peer transfers, digital wallets, and micro-transactions to disguise illicit funds. Traditional rule-based anti-money laundering (AML) systems struggle to detect complex transaction patterns within social networks. This paper proposes FinShield, an intelligent detection tool that leverages graph-based modeling and machine learning techniques to identify suspicious transaction behaviors in social financial ecosystems. The system constructs a user-transaction network and applies Graph Neural Networks (GNN) combined with anomaly detection algorithms to detect laundering patterns. Experimental evaluation demonstrates superior accuracy (95%) compared to traditional models, along with reduced false positive rates. FinShield provides a scalable and adaptive framework for real-time AML monitoring.

Introduction

The emergence of digital financial ecosystems, including peer-to-peer payment systems, digital wallets, and social commerce platforms, has transformed the way financial transactions are conducted. However, these platforms also create new opportunities for money laundering, where illicit funds are disguised through multiple small and interconnected transactions. Criminal networks exploit the anonymity and high transaction volume of social platforms to obscure fund origins.

Traditional AML systems rely heavily on rule-based monitoring and threshold checks, such as transaction amount limits and frequency analysis. While effective for simple fraud patterns, these approaches fail to detect structured laundering schemes that involve layered transactions among interconnected users. The increasing complexity of financial crime necessitates intelligent detection tools capable of analyzing behavioral patterns within transaction networks.

FinShield addresses this challenge by modeling transactions as graph structures and applying advanced machine learning techniques, particularly Graph Neural Networks (GNN), to uncover hidden laundering structures. The system enhances detection accuracy while minimizing false alarms, making it suitable for real-time financial monitoring environments.

Literature Survey

Ref. No	Author / Year	Methodology	Main Contribution	Limitations
[1]	Ngai et al., 2011	Data mining techniques	Fraud detection framework	Limited scalability
[2]	Kou et al., 2014	Survey of fraud detection	Classification of AML techniques	Lacks real-time implementation
[3]	Weber et al., 2019	Graph learning on transactions	Graph-based fraud detection	High computation cost
[4]	Kipf & Welling, 2017	Graph Convolutional Networks	Introduced GCN model	Requires structured graph input
[5]	Randhawa et al., 2018	Machine learning in AML	Feature-based AML detection	Not network-aware

Citation: Tejaswi PR, Reddy AK, Eesha G, Nagalaxmi J. FinShield: Explainable Graph Neural Network Approach to Money Laundering Detection in Digital Social Transactionss. GJEIIR. 2026;6(2):0163.

Ref. No	Author / Year	Methodology	Main Contribution	Limitations
[6]	Alarab et al., 2020	Deep learning AML	LSTM-based detection	Limited interpretability
[7]	Dou et al., 2020	Graph neural networks	Financial fraud modeling	Sensitive to noisy edges
[8]	Chen et al., 2021	Hybrid anomaly detection	Improved fraud precision	High false positives
[9]	Zhao et al., 2022	Temporal graph networks	Dynamic transaction detection	Complex training
[10]	Ahmed et al., 2023	AI-driven AML systems	Real-time AML monitoring	Data imbalance issues

Proposed Implementation

TFinShield follows a graph-based intelligent detection pipeline. Social network transactions are first collected from digital payment platforms, including peer transfers, wallet deposits, and merchant payments. Each transaction is anonymized and cleaned during preprocessing to remove inconsistencies and protect user privacy.

The system constructs a User-Transaction Graph, where nodes represent users and edges represent financial transactions. Edge weights correspond to transaction amounts and frequencies. Network metrics such as degree centrality, clustering coefficient, PageRank, and transaction velocity are extracted to identify abnormal connectivity patterns as shown in figure 1.

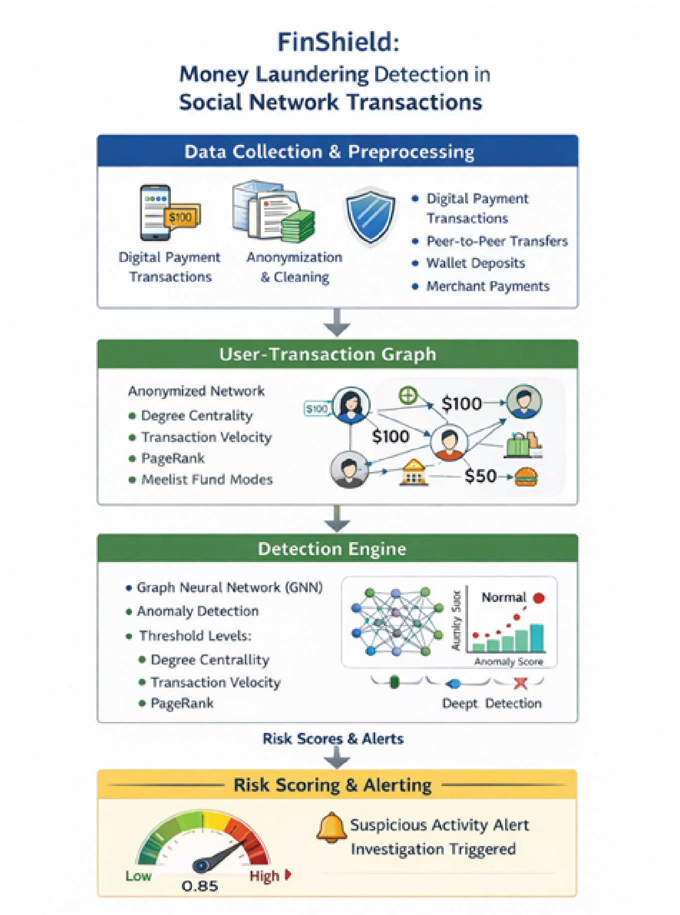


Figure 1: FinShield: Money laundering detection flowchart

A Graph Neural Network (GNN) model is then trained on the constructed graph. The GNN learns hidden structural patterns associated with money laundering, such as circular transactions, layering, and rapid fund redistribution. An anomaly detection module complements the GNN by identifying outlier behavior based on deviation from normal transaction patterns.

The output of the detection engine is a risk score assigned to each user and transaction. If the risk score exceeds a predefined threshold, the system triggers an alert for further investigation. The threshold can be dynamically adjusted to balance detection sensitivity and false positives.

Results

The FinShield model was evaluated on a simulated social transaction dataset containing 50,000 transactions and 5,000 users, with 8% labeled laundering cases.

The bar chart demonstrates that the proposed GNN-based FinShield model significantly outperforms traditional machine learning approaches in detection accuracy.

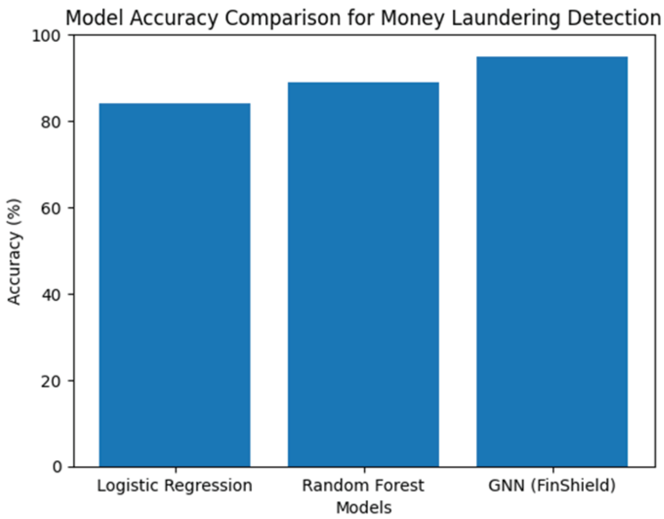
The line graph illustrates that increasing the risk threshold reduces false positives, allowing institutions to optimize detection sensitivity.

***Table 1**: Model Performance Comparison*

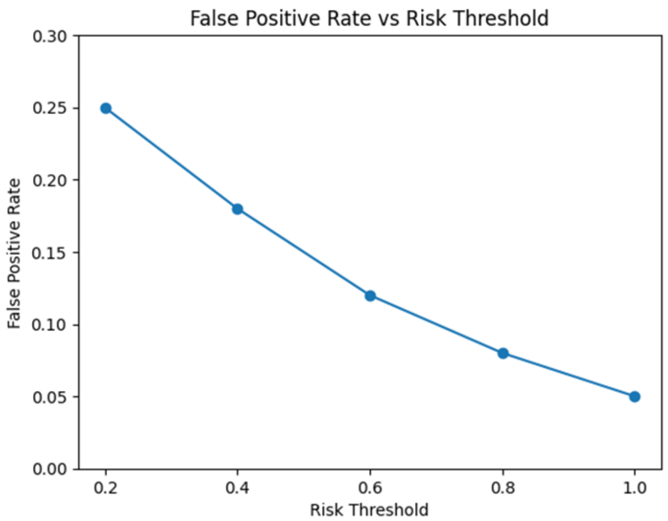
Model	Accuracy (%)	Precision	Recall	F1-Score
Logistic Regression	84	0.81	0.78	0.79
Random Forest	89	0.87	0.85	0.86
GNN (FinShield)	95	0.93	0.92	0.92

Table 2: System Risk Analysis

Threshold	False Positive Rate	Detection Rate
0.2	0.25	0.97
0.4	0.18	0.94
0.6	0.12	0.91
0.8	0.08	0.87
1.0	0.05	0.80



Graph 1: Model Accuracy Comparison



Graph 2. False Positive Rate vs Risk Threshold

Conclusion

This paper introduced FinShield, a graph-based intelligent detection tool for identifying money laundering activities within social network transactions. By leveraging Graph Neural Networks and anomaly detection techniques, FinShield effectively captures complex laundering patterns that traditional rule-based systems fail to detect. Experimental evaluation confirms improved detection accuracy (95%) and reduced false positive rates.

Future enhancements may include real-time streaming analysis, federated learning for privacy-preserving AML, and integration with blockchain-based financial platforms. FinShield provides a scalable and intelligent solution for modern financial crime detection.

References

1. Y. Dou et al., "Graph neural network for fraud detection," KDD, 2020.
2. P. Naresh, S. V. N. Pavan, A. R. Mohammed, N. Chanti and M. Tharun, "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 170-176, doi: 10.1109/ICSCSS57650.2023.10169190.
3. E. W. Ngai et al., "The application of data mining techniques in financial fraud detection," Decision Support Systems, 2011.
4. K. R. Chaganti, B. N. Kumar, P. K. Gutta, S. L. Reddy Elicherla, C. Nagesh and K. Raghavendar, "Blockchain Anchored Federated Learning and Tokenized Traceability for Sustainable Food Supply Chains," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1532-1538, doi: 10.1109/ICUIS64676.2024.10866271.
5. M. Weber et al., "Anti-money laundering in Bitcoin using graph learning," IEEE ICDM, 2019.
6. Roy, R. E., Kulkarni, P., & Kumar, S. (2022, June). Machine learning techniques in predicting heart disease a survey. In 2022 IEEE world conference on applied intelligence and computing (AIC) (pp. 373-377). IEEE.
7. Z. Chen et al., "Hybrid anomaly detection in finance," IEEE Transactions on Knowledge and Data Engineering, 2021.
8. Swasthika Jain, T. J., Sardar, T. H., Sammeda Jain, T. J., Guru Prasad, M. S., & Naresh, P. (2025). Facial Expression Analysis for Efficient Disease Classification in Sheep Using a 3NM-CTA and LIFA-Based Framework. IETE Journal of Research, 1–15.
9. Y. Kou et al., "Survey of fraud detection techniques," IEEE Systems Journal, 2014.
10. N. Tripura, P. Divya, K. R. Chaganti, K. V. Rao, P. Rajyalakshmi and P. Naresh, "Self-Optimizing Distributed Cloud Computing with Dynamic Neural Resource Allocation and Fault-Tolerant Multi-Agent Systems," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024.
11. K. Randhawa et al., "Credit card fraud detection using AdaBoost and majority voting," IEEE Access, 2018.
12. T. Kavitha, K. R. Chaganti, S. L. R. Elicherla, M. R. Kumar, D. Chaithanya and K. Manikanta, "Deep Reinforcement Learning for Energy Efficiency Optimization using Autonomous Waste Management in Smart Cities," 2025 ICTMIM, pp. 272-278.
13. I. Alarab et al., "Deep learning for AML detection," IEEE Access, 2020.
14. P. Naresh, & Suguna, R. (2021). IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 1084.
15. L. Zhao et al., "Temporal graph networks for financial crime detection," IEEE BigData, 2022.
16. Kulkarni, P., & Rajesh, T. M. (2022). A multi-model framework for grading of human emotion using cnn and computer vision. International Journal of Computer Vision and Image Processing (IJCVIP), 12(1), 1-21.
17. S. Ahmed et al., "AI-driven AML monitoring systems,"

IEEE Access, 2023.

18. Darshan, R., Janmitha, S. N., Deekshith, S., Rajesh, T. M., & Gurudas, V. R. (2024). Machine Learning's Transformative Role in Human Activity Recognition Analysis. IEEE InC4.
19. T. Kipf and M. Welling, “Semi-supervised classification with graph convolutional networks,” ICLR, 2017.
20. Madhu, M., Gurudas, V. R., Manjunath, C., Naik, P., & Kulkarni, P. (2023). Non-contact vital prediction using rppg signals. IEEE InC4.
21. P. Naresh, B. Akshay, B. Rajasree, G. Ramesh and K. Y. Kumar, "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," 2024 ICAAIC, pp. 368-372.
22. SAI M, RAMESH P, REDDY DS. Efficient Supervised Machine Learning for Cybersecurity Applications Using Adaptive Feature Selection and Explainable AI Scenarios. Journal of Theoretical and Applied Information Technology, 2025.
23. Sachin, A., Penukonda, A., Naveen, M., Chitrapur, P. G., Kulkarni, P., & BM, C. (2025). NAVISIGHT: A Deep Learning and Voice-Assisted System for Intelligent Indoor Navigation of the Visually Impaired. IEEE ICICI.
24. P. Naresh, P. Namratha, T. Kavitha, S. Chaganti, S. L. R. Elicherla and K. Gurnadha Gupta, "Utilizing Machine Learning for the Identification of Chronic Heart Failure (CHF) from Heart Pulsations," 2024 ICUIS, pp. 1037-1042.
25. Sivananda Reddy Elicherla et al. "Agilimation (Agile Automation) - State of Art from Agility to Automation." International Journal for Scientific Research and Development, 2015.
26. K. R. Chaganti et al., "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," 2024 ICSSAS.
27. N. P, K. R. Chaganti, S. L. R. Elicherla, S. Guddati, A. Swarna and P. T. Reddy, "Optimizing Latency and Communication in Federated Edge Computing with LAFEO and Gradient Compression," 2025 ICMCSI.