International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2343-2352
Journal homepage: http://iieta.org/journals/ijsse

An Accurate Fraud Source Path Identification Using Integration of Graphical Neural Networks, Long-Short Term Memories, and XGBoost

Allamudi Anil Kumar, S. Hrushikesava Raju*

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522302, India

Corresponding Author Email: hkesavaraju@gmail.com

https://doi.org/10.18280/ijsse.151114

Received: 23 October 2025
Revised: 24 November 2025
Accepted: 27 November 2025
Available online: 30 November 2025

Keywords:
multi-layered method, graph-based networks, long-short term memories, XGBoost meta classifier, fraud source detection, accuracy

ABSTRACT

With the increase in web usage in terms of e-commerce and financial transactions, cybercriminals would attempt fraud for the benefit of money, and exploit vulnerabilities through multiple channels, in which identifying the true source path is a challenge. The traditional and existing approaches had high false positives and delayed investigation of static forensic behavior tracings. To detect the source path, a multi-layered hybrid model is required that consists of data preprocessing, extraction of behavior features, and an integrated set of graphical neural networks (GNNs), long-short term memories (LSTMs), and XGBoost approaches for real-time identification. In this, reconstruction of paths using GNNs, making temporal analysis using LSTMs, and applying a meta-classifier using XGBoost. For enhanced interpretability, the Explainable AI technique Shapley Additive exPlanations (XAI SHAP) is applied. The models were evaluated based on publicly available transaction datasets, anonymized cross-platform logs, and institutional support. The effectiveness of the proposed model against methods observed to be better in terms of accuracy, reduced false positives, and faster source path tracing, using evaluation measures such as accuracy and area under the curves (AUCs). The source path identification depends on the device used, network forensics, and behavioral biometrics as practices adapted in the proposed model as key stimuli.

1. INTRODUCTION

The tracing of the fraud source path requires advanced technology approaches to identify the path accurately, using basic practices, as well as a hybrid mechanism. This section decomposes into three divisions: problem statement, research gaps, and objectives.

1.1 Problem statement

The usage of e-commerce platforms, online banking, and mobile payment systems has significantly increased, resulting in making awareness of fraudulent activities, causing financial loss to normal users. Fraudsters exploit digital advertising mechanisms by presenting misleading offers, exaggerated discounts, or deceptive links that users will share sensitive information for complete payments for the products that are never delivered. In many cases, users are redirected through unauthorized pages that are similar to the legitimate shopping portals, where transactions are completed using card details or online banking applications, but order tracking and delivery confirmation remain unavailable. Such fraudulent workflows are designed to obscure the origin of the transaction, making it difficult to trace an individual, organization, or coordinated network. Traditional investigation and tracking mechanisms are typically time-consuming and reactive, allowing additional attacks to be done before the source is identified. Hence, a robust and proactive approach is needed that can rapidly detect fraudulent behavior, accurately trace the source path of malicious entities, and minimize further financial losses in social commerce ecosystems. The source path identification involves multiple entities exploiting vulnerabilities across different networks, such as compromised accounts, synthetic means, and identity theft.

1.2 Research gaps

The methods considered for fraud detection, such as rule-based, single machine learning (ML) method, GNNs, Legacy systems, semi-supervised learning (SSL), and XAI. The payments are done through mobile applications and online banking systems, but tracking the source point of the organization or person by traditional methods may consume more time and may result in losses. Hence, a novel approach that guarantees the detection of the source. It is difficult to identify the source, which is a complex challenge. According to the FTC analysis in 2023 and 2024, every year the fraud rate increases due to an increase in the usage of e-commerce and financial transactions. The appropriate actions, such as blocking access, banning the origin sources, and restricting further transactions, would reduce user exposure and limit damage when fraudulent activities are detected. The technical indicators such as device identifiers, server logs, IP addresses, and geographical patterns to establish traceability, are tracked when suspicious activity is involved. As a consequence, traditional and existing models are unable to function, which

can result in delayed responses, continued exploitation, and security breaches. This limitation focuses on the need for continuous monitoring and rapid source identification while maintaining low false alarm rates. Such a framework should adopt a multi-layered design with data preprocessing, discriminative feature extraction, and a hybrid ML strategy to accurately isolate fraudulent sources. The specific fraud source detection techniques, along with their shortfalls, are mentioned in Table 1 to emphasize the research gaps addressed.

The various traditional and standalone methods used are rule-based systems won't support evolving patterns, single-layer ML methods may ignore cross channel relationships, Supervised models focus on labelled history, and frequent retraining, Legacy models suffer with inefficient real-time processing due to high latency, Graph Neural Networks are expensive in hierarchical organization, Self-Supervised methods possess bias, an unable to detect synthetic patterns, and XAI models incur additional burden when involved in complex systems. The existing fraud detection approaches have several limitations that reduce their effectiveness in dynamic digital transactions. The approaches are rigid in design and fail to adapt to evolving fraud patterns, resulting in high false-positive rates and may miss detection. The absence of cross-channel correlation limits their ability to capture coordinated activities across multiple platforms. Supervised learning models are particularly vulnerable to novel attack strategies, as they depend heavily on labeled data and require frequent retraining whenever novel fraud behaviors arise. Traditional rule-based and legacy systems also struggle with real-time source tracing due to fragmented and siloed data patterns. Graph-based models, although effective in representing relationships, incur computational costs as the scale and complexity increase. Similarly, self-supervised techniques may introduce imbalanced synthetic samples, which can distort learning, while overall system performance may degrade when it involves processing overhead.

1.3 Objectives

These gaps, addressed in Table 1, would demand a multi-layered deep learning model. Hence, a hybrid model is required that accurately identifies the fraud source path in the e-commerce and financial transactions environment. This method should make use of cross-channel tracing using a multilayered approach, such as GNN, LSTM, XGBoost, and SHAP, for enhancing detection rates, along with reliability. Several objectives are ensured, such as (i) forming a multi-layered approach that makes use of behavioral patterns, device IDs, network attributes, and transactional metadata. (ii) ensure accurate fraud source path by reconstructing among entities such as accounts, users, and IP addresses. (iii) Captures temporal and dynamic dependencies of fraud patterns using LSTM. (iv) Performs fusion in making a decision using a meta classifier to reduce false positives. (v) Integrating with explainable AI as SHAP for auditing fraud source path and ensuring transparency and interpretability. Hence, LSTM, GNN, and XGBoost would be combined to form a fusion that would enhance accuracy and ensure robustness using SHAP.

2. LITERATURE REVIEW

There exist many studies on fraud identification over social platforms as well as on e-commerce sites. When fraud occurs, it means loss or identity theft of a person or user. Tracking the location of the fraud place, as well as the exact address, is quite challenging. Hence, firstly, we will demonstrate the studies on how the location of the fraud or the source needs to be known, so that action can be initiated. Kumar et al. [1] demonstrate that unwanted portions in e-commerce sites or fraudulent e-commerce sites created by hackers can cause damage to the individual's income. To identify these false sites, a proper stage approach that includes data preprocessing, feature selection, and model training is required. The models used combinedly, such as Ant Lion Optimizer (ALO) and Extreme Learning Machine (ELM), would reduce noise, increase accuracy, and avoid mutual inference. Kumar et al. [1] and Ali et al. [2], attempted a discussion on forensic techniques such as a multistage process, which includes data collection, interviews, forensic auditing, and analytics on irregular transactions.

A set of strategies is demonstrated with their benefits and shortfalls, highlighting effectiveness and flexibility, and ensuring the risks are addressed. Kumar et al. [3] made a discussion on the usage of a deep learning model CNN against others like LSTM, GAN, and RNN in analyzing the accounts, especially in terms of cash deposits, withdrawals, and unusual balances. The significant factor involved is efficiency, which increases the effectiveness of the model in fraud detection in accounts. Vishnu et al. [4] had a discussion on the usage of nonfiscal token (NFT) for the transactions made in e-commerce sites and retail stores. The blockchain-based system NFT makes the transaction more secure and transparent. Hence, warranties are maintained safely by both customers and companies.

From Korchenko et al. [5], a discussion was made on solutions to cyber threats in terms of setting up criteria such as openness, behavior, DDos attacks detection, device identification on which fraud is exposed, speed, content delivery, bot detection, integration environment, confidentiality assurance, cloud or local deployment, and use of AI technology. The strategies used are analyzed with benefits, drawbacks, and accuracy of identification over cyberthreats. Mohan et al. [6] had a demonstration on websites that trick people and commit fraud. The various machine models include decision trees, support vector machines, logistic regressions, and an ensemble of hybrid models using soft voting, grid search, and canopy feature selection. The effectiveness is measured in terms of accuracy, precision, recall, and F1-score. Aljabri and Mohammad [7] had a demonstration on click fraud on the portions of an app/website where advertisements attract users who may lose amounts unnecessarily. This phishing is to be eliminated or minimized using a machine learning model, Random Forest, which produces better accuracy than others in the domain.

Abdul Samad et al. [8] had a discussion on various machine learning models on two datasets for phishing user privacy. The accuracy of Gradient Boosting and Random Forest over Dataset-1 is a little less than that of Extreme Gradient Boosting over Dataset-2. The hyper factors considered are data balancing, feature selection, and hyperparameter tuning. Hafidi and Mahnane [9] had a discussion on providing the website as input, and using a machine learning model to produce output as a fraud site or a genuine site. Before machine learning models, hackers would steal the privacy of an individual and cause damage in terms of identity and money. Zhang et al. [10] had a discussion on fraudulent

behavior in e-commerce sites, motivating biometric authentication since biometrics is a unique validation method. To provide faster performance and prevent losses, a method called the multi-modal behavioral transformer is used. This method records every activity using the mouse trajectory, analyzes both the inner details of the page and the inter-page.

Reddy et al. [11] had a discussion on reducing fraud using machine learning and AI approaches. This study recommends practices that proactively enhance the prevention efforts against fraud by identifying anomalies. The conventional practices and proposed system are compared for detailed analysis. From Rao et al. [12], it is demonstrated that systems shift from rule-based to ML, then to DL. The human efforts in the shifts shown are also based on three aspects, such as multi-modal engineering support, scalability addressing, and newer methods such as adversarial ML, federated learning, reinforcement learning, LLMs, and their suitability over e-commerce sites for fraud identification. Hernandez et al. [13] had a discussion on fraud detection, such as credit card fraud. The methods PRISMA, Kichenham, and specific machine learning models are applied for the detection of credit card load fraud from different countries. The studies over a period of users, and specific articles were analyzed for drafting the review. From Zenzerović and Šajrih [14], it is demonstrated that the work of Bao et al. includes objectives such as the usage of new tools to detect fraud and prevent it by combining best practices as a novel detection model. The other studies are compared against the specific study, which would reveal challenges and prevention practices. According to Beemamol [15], a discussion was held on various approaches used in different problem domains since 1989. The methods used to enhance the detection of fraud are taken from interdisciplinary environments. To improve the detection rate, integrate interdisciplinary approaches.

Alrasheed [16] conducted a discussion on the misuse of cryptocurrencies in financial fraud, the challenges that traditional methods experience, such as technological complexity, complexity in user identification, and weakness in legal regulatory aspects. To enhance security and privacy, AI is to be integrated into legal, regulatory, and reinforcement systems. Liu et al. [17] demonstrated browser biometrics in accessing internet applications. Nowadays, sites are accessed with ads, which may cause damage to individuals' income. When fraud occurred through advertisements, the biometric validation feature would track the user and report the location of fraud. Additional details of the user are revealed if browser biometrics are set up. This study tracks HTTP traffic, user interactions, and targets.

From Padmapriya et al. [18], to avoid threats over the usage of web cameras for transmission of surveillance data over the cloud, the encryption and decryption take place using the integration of mechanisms such as DWT, Huffman compression, and ECC. The proposed model supports detecting abnormal events like vulnerabilities or third-party access during the transmission of data over the cloud. The benefits achieved are reduced costs, increased storage space, and tracking of data. Guan and Chen [19] demonstrated that a virtual identity alignment algorithm would identify real identities based on virtual accounts used in multiple sources. Based on functionalities, and behavior such as data collection, management, task management, identity alignment, and suspicious user evaluation, applies automatic strong lawful initiatives over crimes done by users. Hilal et al. [20] had a discussion of machine learning models such as supervised learning, semi-supervised learning, and unsupervised learning models. The fraud occurs in many domains, like insurance, money laundering, commodities, etc. The criminals' acts may not be completely prevented; hence, anomaly detection techniques are required to detect the fraud. Baesens et al. [21] demonstrated machine learning and analytical models for detecting fraud in financial transactions (or money loss transactions. Many data engineering techniques are applied and analyzed to improve the interpretability. The performance is enhanced by dividing the analytical model into feature and instance steps. Based on Dey and Sangaraju [22], the discussion on load balancing is initiated by ensuring features such as global and local stability, improved performance, eliminating the delay and latency, and optimizing the resources. In regard to Dey and Sangaraju [23], it demonstrates hybrid load balancing in a novel performance evaluation that involves multiple balancing approaches based on the category of activity over task load distribution, and enhances measures such as throughput and execution time. In view of Kumar and Raju [24], a hybrid model that detects fraud in financial transactions, with accuracy and security, along with real-time monitoring.

Table 1. Listed methods with their identified gaps

Method Involved	Purpose	Gaps
Rule-based systems	The rules of attributes focused on high amounts, and unusual locations may be violated.	Uses static rules, contains high FPR, and may miss novel fraud patterns.
Single-layer machine learning (ML) models	One data source, like the transaction amounts, detects anomalies.	Chance of lower accuracy, and ignoring cross-channel features.
Supervised models	Uses labeled historical data for fraud classification.	Poor generalization on new frauds, and retraining is needed.
Legacy systems	The transactional data in batches is processed.	Observes more latency, path tracing is not always genuine, and fails in device behavior.
Graph neural network (GNN) variants	The factors, such as accounts, devices, and IPs, are modeled to detect fraud and trace flows.	Expensive, and struggles with the cold start problem for new samples.
Self-supervised semi-supervised learning (SSL)	The labeled data by learning from unlabeled transaction patterns is reduced.	Observes not identifying fraud with synthetic data, and more biases in unlabeled data.
Explainable AI (XAI)	For fraud source attribution, it requires auditable trails.	Observations such as explainability drops and overhead due to complex ensembles.

Sha et al. [25] demonstrated diversified graphical networks on transactions that involve users, financial organizations, and nodes using attention mechanisms and temporal patterns in capturing complex scenarios. This study struggles in

processing large heterogeneous networks, resulting in false positives. Raju et al. [26] demonstrated exploring the fault detection, such as weak conditions are identified by a hybrid model, especially on flyovers/bridges, using DL approaches, Transfer learning, R-CNN, and LSTM for ensuring better effectiveness.

Table 2 demonstrates the gaps involved in significant studies and recommendations to overcome such gaps.

Table 2. Significant studies and identified gaps

Ref.	Methodology	Key Gap
Kumar et al. [1]	Ant Lion Optimization + Extreme Learning Machine for feature selection, removal of noise.	Sometimes fails against evolving phishing tactics, using static feature selection.
Kumar et al. [3]	CNN vs. LSTM/GAN for transaction analysis to identify fraud.	Support of Limited to structured data (unstructured behavioral logs were ignored).
Vishnu et al. [4]	NFT-based blockchain for secure transactions.	Blockchain scalability requires high latency/NFT gas fees.
Aljabri et al. [7]	For click-fraud detection uses Random Forest.	No real-time adaptation (static model vs. adaptive bots).
Zhang et al. [10]	Multi-modal behavioral transformers with mouse tracking enabled.	Privacy-invasive biometrics reports continuous monitoring risks.
Rule-based fraud systems [13, 14, 20]	Uses static rule engines for abnormality checks.	Manual screening for threshold violations.
Single-layer machine learning (ML) models [6-9, 11, 13, 20]	Uses SVM, Decision Trees, Random Forest, etc, for click Fraud, and transaction fraud.	Restricted to single baseline models.
Deep learing (DL) approaches [3, 10-12]	Uses temporal and contextual features for enhancing detection capability.	Involves complexity.

3. METHODOLOGY

In this, the tracking of the fraud source is demonstrated in Figure 1 for module interaction, Figure 2 for the flow of activities involved to identify the source accurately, and PS1 demonstrates the pseudo procedure that dictates achieving efficient detection of the source that initiated the fraud. The modules involved are Data collection as the Input layer, data preprocessing, a multi-layered approach, a Deep learning ensemble, XAI explainability, cross-layer correlation, and Evaluation of effectiveness in the Output layer. The correlation GNN → LSTM → XGBoost → SHAP is significant due to capturing structural first, later temporal patterns for meta-fusion, to enhance predictions. A parallel pipeline is not recommended due to intermediate predictions, and ensures fault-tolerant routing of XGBoost, which would ensure performance.

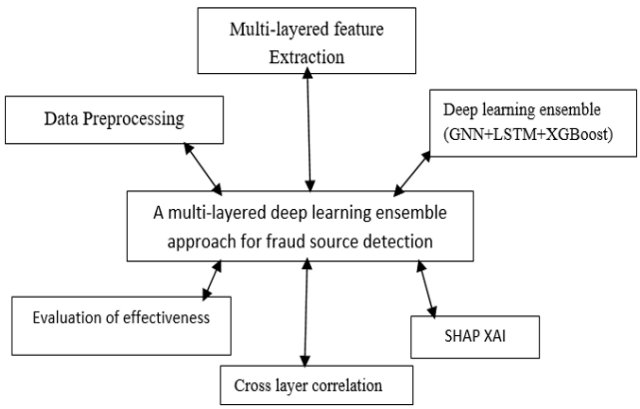

Figure 1. Significant modules of a multi-layered system for fraud source path detection

This methodology involves Figure 1, which shows significant modules, such as data preprocessing for quality assurance over input data, extraction of features for fusion, an integrated module for combining GNN, LSTM, and XGBoost, integration of SHAP for interpretation, and reducing false positives, and evaluation of measures such as accuracy, AUC, and error rates. Figure 2 denotes a flowchart of identifying the true source fraud path, and PS1 as a stepwise pseudo-code, justification of the ensemble components (GNN, LSTM, XGBoost), SHAP-based explainability for enhancing interpretability, and the cross-layer correlation mechanism for increasing accuracy.

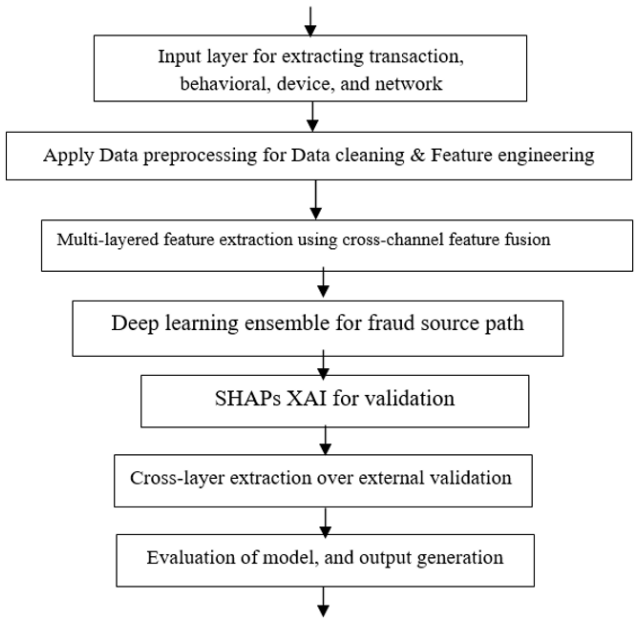

Figure 2. Flowchart of the proposed model for fraud source detection

From Figure 2, the model starts from an input layer that extracts raw information from transaction logs, behavioral patterns, device fingerprints, and network metadata. The data taken from the input source for preprocessing and evaluation

is publicly available in the IEEE-CIS Fraud Detection Dataset, Kaggle 2023, https://www.kaggle.com/competitions/ieee-fraud-detection/data. Then, data preprocessing is applied for making quality data by applying normalization on transaction amounts, then a multilayered approach is applied for layer-wise fraud detection, then a deep learning ensemble is applied for processing the data using GNN, LSTM, and XGBoost meta classifier, then XAI explainability SHAP is applied for making decisions, then cross-layer correlation is applied to fuse the features from external entities such as dark web, geolocation mismatches, and application logs verification. Then, finally, display the output such as Fraud type, source path, and validation status.

PS1: Pseudo_Procedure Fraudsource_detection_ using_multilayered_Deeplearnig_ensemble(raw_data):
Input: Raw data for transaction logs, behavioral biometrics, Device Fingerprints, and Network Metadata
Output: Fraud Source path

Step 1: Addressing the Input layer for extracting raw and unstructured data from multiple channels initially.
- 1.1 For anomalies, analyze transaction logs for abnormal monetary amounts and time stamps.
- 1.2 For impersonation detection, user interaction patterns like keystrokes and mouse movements are considered.
- 1.3 Apply device fingerprints using hardware/software configurations.
- 1.4 Apply Network metadata over connections to detect snooping/VPN Usage.

Step 2: Apply data preprocessing for converting raw data into an analysis-ready format.
- 2.1 Apply missing value handling to prevent errors from incomplete data, using median and mode imputation.
- 2.2 Apply z-score normalization for fair comparison using scaling, which avoids high-value transactions.
- 2.3 Apply Device hashing, called one-way hashing, for privacy-preserving device identification.
- 2.4 Behavioral encoding for raw biometrics into a time-series sequence (temporal windows).

Step 3: Apply multilayer feature extraction for interconnected representations.
- 3.1 Transaction graphs are used for relationships between entities using Graph neural networks.
- 3.2 Temporal sequences are used for capturing behavior using LSTM.
- 3.3. Network features are observed for connection suspiciousness.

Step4: Apply Deep Learning Ensemble using specialized models for analyzing different fraud aspects, then combine insights.
- 4.1 Detect attacks across accounts using GNN, and explore fraud ring/path propagation learning from device edges.
- 4.2 Detect subtle behavior (behavioral dynamics) over time using LSTM
- 4.3 Considers all evidence for the final prediction using XGBoost meta-classifier (fusion risks)

Step5: Apply SHAP XAI for black box decisions interpretable for investigators (reduce false positives).
- 5.1 Use SHAP for features that most influence
- 5.2 Observe counterfactuals for knowing changes that affect output

Step6: Apply cross-layer correlation for predictions against external entities, which reduces false positives.
- 6.1 Observe the dark web if the credentials are leaked
- 6.2 Observe geolocation for verification of location consistency.
- 6.3 Observe application logs to know supporting evidence from brute force attempts.

Step7: Address the output layer for the results evaluation for different stakeholders
- 7.1 Fraud type that categorizes the fraud
- 7.2 Propagation path shows attack progression
- 7.3 Confidence score shows certainty level
- 7.4 Display validation status verified/rejected

Step8: Analyze the effectiveness of the model using accuracy and performance

(1) Fraud score = $(\sum_1^n wi. \prod Layeri\ Fraud) / \sum wi$ (1)
where, wi denotes the weight of layer i, $\prod$ denotes the indicator function that uses 1 for fraud confirmation at layer, otherwise 0. If the score is above 0.7, it means a high fraud score.

(2) Latency computation by
$T_{PL} = T_{GNN} + T_{LSTM} + T_{XGBoost} + T_{XAI}$ (2)
where, T denotes Processed time for Predictive Learning, GNN, LSTM, XGBoost, and XAI.

(3) AUC = $\int$TPR(FPR)d(FPR) (3)
where, AUC is defined as the area under the ROC curve by integrating the True Positive Rate (TPR) over the False Positive Rate (FPR)

(4) Complexity = O(E×d) + O(N×T×h2) + O(K×F) + O(F×Nshap) (4)
where, each term is complexity involved in stages such as GNN, LSTM, XGBoost, and SHAP in which E is no. of edges, d is dimension, N is no. of transactions, T is the temporal length, h is hidden dimension, K is no. of boosting rounds, F is no. of fused features, and Nshap denotes no. of samples needed for SHAP value computation.

The PS1 is started by extracting initial context from transaction logs, behavioral biometrics, device fingerprints, and network metadata. Among these, detection of anomalies over transactions, impersonation over behavioral, snooping over Device fingerprints, and attacks over VPN network usage. Later, data cleaning and normalization are applied to handle missing values, scale the amounts for normalization, Device hashing for privacy preservation, and behavior sequence encoding. Then, a multi-layered approach is applied in which a transaction graph is constructed by making

relationships between entities, temporal sequences for behavioral trends using LSTM, and network forensic features. Then, GNNs are applied for detecting coordinated fraud rings, LSTMs for slow behavioral drifts, and XGBoost Meta Classifier for weighing all evidence and making a final prediction. Then, SHAP XAI is used for making decisions by investigators, and cross-layer correlation for leaks in the dark web, location mismatches in geolocation validation, and checking anomalies in the application logs. Then, the output layer displays the fraud source path of fraud progression, confidence score of fraud, and validation status.

The metrics are evaluated in terms of fraud score, latency, and AUCs. In this, ensured the strictly serial dependency of inference modules (GNN → LSTM → XGBoost → SHAP), then, computation of end-to-end decision latency is the sum of stage latencies $T_{PL} = T_{GNN} + T_{LSTM} + T_{XGBoost} + T_{XAI}$. The complexity is computed based on the sum of the overheads of LSTM, GNN, XGBoost, and SHAP. The implementation environment used is Python. The setup involved consists of data preprocessing, splitting the dataset into training, testing, and validation (70, 15, 15), and the hyperparameters used are embedding dimension in GNN, Hidden units, sequence window in LSTM, number of trees, and max. depth in XGBoost, and hardware to be used based on NVIDIA and CUDA machines. In the implementation of the hybrid model, and to ensure performance, the terms considered are E ≈ 3.1M edges, d = 128 embedding dimension, T = 20 temporal window, h = 64 hidden units, F = 220 fused features, N = 590K transactions (IEEE-CIS) for large systems. These terms achieve scalability on a variety of types, such as GPU, GNN, pruning, and SHAP.

4. RESULTS AND DISCUSSION

4.1 Dataset description

The dataset used is the IEEE-CIS Fraud Detection Dataset, which is publicly available for financial fraud analysis. The composition involves a total number of transactions of 590,000, in which 96.5% are legitimate transactions, and 3.5% are highly imbalanced. The features of it are classified into 4 categories: identity features, transaction features, network features, and behavioral features. Among these, the first category describes IDs of devices, browser information, and IP attributes, the second category includes amount, time delta, payment type, and product, the third category describes IP-geo mismatch and indicators of Proxy, and the fourth category includes temporal patterns and frequency of transactions. The dataset is split into 70% train, 15% validation, and 15% test. The data preprocessing is initiated over the dataset, in which missing numerical values are handled by median imputation, while categorical features are handled by mode imputation, resulting in bias to be avoided, which was caused by skewed transaction distributions. The standardization of transaction amounts and time intervals using z-score normalization to avoid data leakage. The high cardinalities of card and device identifiers are transformed using one-way hashing to preserve privacy, while low cardinalities are handled by label encoding. LSTM is used to capture temporal dynamics such as transactions and user interactions. The heterogeneous transaction relations are traced using a GNN model among entities such as IP addresses, Devices, accounts, etc.

4.2 Experimental setup observations of measures

The effectiveness of the model is assessed using the fraud score, given in PS1, to assess weighted cross-layer processing of fraud confirmation. If the fraud score > 0.7, it denotes high confidence in fraud activity. The performance is evaluated based on the latency consumed by the specialized models used, such as GNN, LSTM, XGBoost, and XAI SHAP processing time. From this, the multi-layered deep learning model is considered an end-to-end model, and its performance is better than that of traditional models. The proposed model enhances accuracy by a significant extent and lowers false positive generation. The key aspects that made this happen are cross-channel correlation, adaptation to detect novel frauds, and delivery of verified results.

Table 3. Measures assessment over considered models

Method	Accuracy	Precision	Performance	Robustness	Cost-Effectiveness
Rule-based systems	Low	Low	High	Very Low	High
Single-layer machine learning (ML) models	Medium	Medium	High	Low	Medium
Supervised models	Medium	Medium	Medium	Medium	Medium
Legacy systems	Low	Low	Low	Very Low	High
Graph neural network (GNN)	High	High	Low	High	Low
Self-supervised semi-supervised learning (SSL)	Medium	Medium	Medium	High	Medium
Explainable AI (XAI)	Medium	High	Low	Medium	Low
Multilayered deep learing (DL) Ensemble	High	High	Above Medium	High	Medium

Based on Table 3, the methodologies were interpreted in the comparison of intensities based on measures such as accuracy, precision, performance, robustness, and cost-effectiveness. From Table 3, the performance is very good for rule-based systems and single-layer ML models. The accuracy is very good for GNNs, and our proposed multi-layered deep learning ensemble approach. The precision is high for models such as GNNs, XAI models, and a multi-layered deep learning ensemble approach. For new fraud detection, the models such as GNNs, SSLs, and a Multilayered deep learning ensemble are high. Nowadays, cost is not an issue due to safety assurance is given as the top priority.

Table 4 demonstrates operational advantages gained from cross-layer learning using GNN, LSTM, and SHAP correlation, resulting in a stronger performance on the proposed model. From Table 4, the only model, a multi-layered deep learning ensemble, is very good at accuracy, precision, and robustness. The proposed model is also good in

performance and cost aspects. Compared to traditional and considered individual models, the proposed model is best in its features and layer-wise validation. The performance of the proposed model is superior due to cross-channel fusion from device transaction metadata, behavior analytics, and network forensics, due to graph intelligence in which each entity is independent, suspicious activities over time as temporal patterns are detected by LSTM, combines embeddings of GNN and LSTM by a meta fusion mechanism XGBoost, and increases confidence by SHAP. The benchmark, like a baseline, is a setter for these models, which is a faster execution of the models. In addition to metrics to be evaluated, paired t-test, and McMenar's test were conducted over 10 folds, and classification per instance, over the same set of instances, for performance assessment.

Table 4. Evaluated scores against the considered models

Method	Accuracy (%)	Precision (%)	Performance (%)	Failure rate (%)	Cost-Effectiveness (%)
Rule-based systems	65	70	< 100 ms	> 60	95
Single-layer machine learning (ML) models	80	85	/, 300 ms	45	85
Supervised models	85	88	1 sec	40	88
Legacy systems	70	75	2 sec	70	90
Graph neural network (GNN)	93	95	2 sec	15	60
Self-supervised semi-supervised learning (SSL)	87	89	1.5 sec	20	75
Explainable AI (XAI)	88	96	5 sec	35	70
Multilayered deep learning (DL) ensemble	98.5	98.8	200 ms	8	84

Figure 3, which is derived from Table 4, shows that the proposed model is best in robustness, accuracy, and precision. For any model, accuracy denotes the number of correctly identified fraud sources such as True positives and True negatives, out of all predictions, Precision denotes the number of correctly flagged fraud cases out of true positives and true negatives, and robustness denotes withstanding and successful validation of novel frauds as well as adversarial attacks, are good means that the model is the best and effective model when compared against other models.

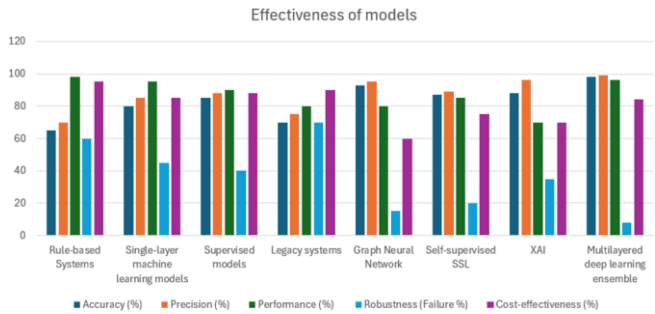

Figure 3. Effectiveness of the models in specific terms

Table 5. Evaluated area under the curves (AUCs) over specified methods in fraud source path detection

Method	AUC Score
Rule-based systems	0.72
Single-layer machine learning (ML) Models	0.86
Supervised traditional models	0.89
Graph neural network (GNN)	0.94
Proposed multi-layered deep learing (DL) ensemble	0.983

Based on Table 5, the evaluated AUCs of specific models involving the proposed model of CNN, LSTM, XGBoost, and XAI are superior, ensuring no leakage of information. The visual drawing of the AUCs of the models would also demonstrate the effectiveness of the models in Figure 4.

4.3 Example case study

Example case study demonstration based on synthetic dataset, would involve stages such as initial compromised clicked source, correlating device used, IP with Geo mismatch detection reveals external threat intelligence, suspicious detection over time (deviation) by LSTM, Fraud entity linkage involves account and device by GNN, meta fusion by XGBoost, and SHAP feature validation (depicts importance of each feature and layer to ensure transparency) for interpretability.

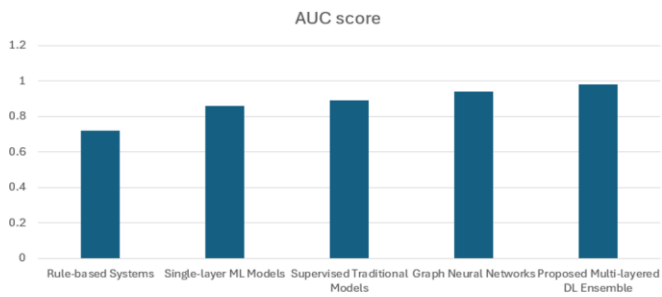

Figure 4. Area under the curves (AUCs) of specific models against the proposed model

Table 6. Confusion matrix for the considered dataset

Risk Type	Predicted Low	Predicted High
Low	116 (TN)	4 (FP)
High	2 (FN)	78 (TP)

For the confusion matrix shown in Table 6, justification demonstrates Table 7 on the model's job during a fraud event scenario, in which GNN is used for device and account tracing, LSTM for suspicious behavior, and XGBoost for fusing the confidences of all models, and identifying external threats by dark web and geolocation. For unseen, realistic data, the data is divided into training 70%-validation 15%, and testing 15%. The performance on the test set is demonstrated in the

confusion matrix, which is defined in Table 6.

As per Table 6 and the dataset, FPR is observed at 3.3%, which denotes a very low risk flagged wrongly, and FNR is observed as 2.5%, which denotes a few missed dangerous cases.

The SHAP global feature plot set demonstrates that the top contributing factors in fraud detection are Dark web exposure, transaction velocity, Device fingerprint anomaly, Behaviour drift, Account linkage, and IP Geo-mismatch. Global SHAP uses almost 20 contributing factors for fraud detection, whereas Local SHAP denotes a misclassified fraud attempt. SHAP identifies a faster, traceable route and ensures better usability.

4.4 Significance tests

By enforcing a unified dataset, mechanisms such as standardized preprocessing, consistent evaluation metrics, and formal statistical testing were observed, and then the comparative experiments were conducted in a rigorous and unbiased manner. The inclusion of paired statistical tests and misclassification analysis reports the performance gains of the proposed framework are both quantitatively very good and statistically validated. The identical preprocessing was used for all baseline models. The other baseline models, such as combined models, required support network behavior correlation. The statistical tests p-tests and McNemar's test are preferred for confirming significant improvements. The notable tests p-tests for model performance, and McNemar's test for difference in misclassification, provide the effectiveness of the model, and the disagreement. The p-values obtained from the paired t-test and McNemar's test over 10-fold validation are mentioned in Table 8, which ensures the proposed model has better performance than other models (low performance).

Table 7. Illustration of an example case study a fraud event using the proposed model

Entity Tracked	Model Layer Contribution	Evidence Collected
Device_ID: DF-78A	Graph neural network (GNN)	Collects device details from the browser used using IP address. Abnormal browser fingerprint detected, linked to flagged user cluster
IP: 172.xx.xx.xx	LSTM + XGBoost	IP–Geo behavioral mismatch from the user baseline profile
Account A → Account B	GNN	Suspicious fund transfer chain identifies fraudulent peer node
Temporal behavior drift	Long-short term memorie (LSTM)	Demonstrates Deviations in login timing and transaction frequency
Dark web record match	External Entity Check	Credential presence validated in leaked DB

Table 8. P-test and McNemars test on models used

Method	Accuracy	CI	Paired Test	McNemars Test
Rule based	65	0.61-0.68	<.001	<.001
Single layer machine learning (ML) method	80	0.77-0.83	<.001	<.001
Supervised ML	85	0.82-0.88	<.001	<.001
Graph neural network (GNN)	93	0.90-0.95	.003	0.005

Hence, the proposed framework's benefits lie not only in merging multiple models but in strategically aligning their strengths to ensure relational structure by GNN, temporal evolution by LSTM, and nonlinear feature interactions in a unified manner, by XGBoost. To ensure accuracy, robustness, and interpretability, this integrated combination is required. Especially in the feature interactions aspect, the models used would be useful for capturing higher-order relational dependencies, such as fraud rings, shared device misuse, and coordinated transaction flows using GNN, learning temporal patterns from ordered transaction and interaction sequences, as well as behavioral drift denotes, such as gradual changes in transaction timing, frequency, or interaction style by LSTM. The mechanism for learning feature importance weights and interaction effects between structural embeddings, temporal signals, and engineered risk indicators by XGBoost, to reduce false positives. The usage of global SHAP reveals dominant contributors such as device fingerprint anomalies, transaction velocity, and graph connectivity scores, while local SHAP highlights instance-specific evidence.

5. CONCLUSIONS

Existing fraud detection techniques suffer from high false alarm rates, static rules, limited source traceability, and weak adaptability to evolving fraud behaviors. Addressing these requires a layered deep learning framework that merges multiple analytical perspectives to achieve accurate detection. The complementarity of the proposed model would overcome the pitfalls of the methods demonstrated in Table 1. In this, how challenges are overcome means that transaction relationships are modeled as graphs for complex interaction patterns through GNNs, while temporal behavioral sequences over time are used to identify deviations and evolving attacks by LSTM and XGBoost. Explainable learning would highlight influential features and provide transparent reasoning, allowing for easily informed and timely decisions. The cross-layer correlation with external intelligence sources, including geolocation inconsistencies, application logs, and illicit activity indicators, is used to assess the confidence in detected anomalies. Analysis of device fingerprints, behavioral drift, and coordinated network activity allows the ensemble framework to deliver better accuracy against previously unseen and adversarial fraud attempts and improved operational trust. The strategic transition from reactive fraud response to proactive fraud prevention, envisioned through federated learning, privacy-preserving computation, and advanced adversarial defense as future scenarios, for large-scale digital commerce ecosystems.

ACKNOWLEDGMENT

I convey my gratitude to my organization Koneru Lakshmaiah Education Foundation, for using computing facilities, resources, and continuous support. I extend my thanks to the co-authors whose efforts made the article significantly.

REFERENCES

[1] Kumar, S., Vyas, T., Gautam, S., Shaji, B., Naidu, D.S., Bhatnagar, V. (2024). An innovative approach to detecting fraud in e-commerce applications based on anomaly intrusion detection systems using ALO-ELM approach. In 2024 Asian Conference on Intelligent Technologies (ACOIT), Kolar, India, pp. 1-6. https://doi.org/10.1109/ACOIT62457.2024.10939503

[2] Ali, A.M., Khinger, I.K., Subhe, A., Al-Orfali, A.K. (2024). Forensic accounting techniques in detecting frauds. Journal of Ecohumanism, 3(5): 543-558. https://doi.org/10.62754/joe.v3i5.3922

[3] Kumar, P.R., Wakade, A., Kumar, J., Swain, S.R., Kumar, J., Kumar, A. (2025). On detecting frauds in retail transactions for enhanced security with deep learning model. Procedia Computer Science, 260: 468-475. https://doi.org/10.1016/j.procs.2025.03.224

[4] Vishnu, G., Kumar, D., Singh, K. (2023). Blockchain-based ecommerce warranty system using NFTs. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, pp. 337-343. https://doi.org/10.1109/IC3I59117.2023.10397739

[5] Korchenko, O., Korchenko, A., Azarov, I. (2024). Analysis of modern solutions for the identification of anonymous users. In International Conference on Applied Innovations in IT, pp. 284-319. https://doi.org/10.1007/978-3-031-89296-7_15

[6] Mohan, D., Amritha, R., Raj, C.C. (2024). URL based phishing detection system using ensemble of LSD model. In 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India, pp. 68-73. https://doi.org/10.1109/ICDICI62993.2024.10810953

[7] Aljabri, M., Mohammad, R.M.A. (2023). Click fraud detection for online advertising using machine learning. Egyptian Informatics Journal, 24(2): 341-350. https://doi.org/10.1016/j.eij.2023.05.006

[8] Abdul Samad, S.R., Balasubaramanian, S., Al-Kaabi, A.S., Sharma, B., et al. (2023). Analysis of the performance impact of fine-tuned machine learning model for phishing URL detection. Electronics, 12(7): 1642. https://doi.org/10.3390/electronics12071642

[9] Hafidi, M., Mahnane, L. (2022). A hybrid model to detect phishing-websites. International Journal of Internet Technology and Secured Transactions, 12(6): 483-502. https://doi.org/10.1504/IJITST.2022.126472

[10] Zhang, Z., Yin, H., Rao, S.X., Yan, X., et al. (2025). Identifying e-commerce fraud through user behavior data: Observations and insights. Data Science and Engineering, 10(1): 24-39. https://doi.org/10.1007/s41019-024-00275-6

[11] Reddy, S.R.B., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P.V., Polireddi, N.S.A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. Measurement: Sensors, 33: 101138. https://doi.org/10.1016/j.measen.2024.101138

[12] Rao, S.X., Jiang, J., Han, Z., Yin, H. (2025). Fraud detection in e-commerce: A systematic review of transaction risk prevention. https://doi.org/10.5772/intechopen.1009640

[13] Hernandez Aros, L., Bustamante Molano, L.X., Gutierrez-Portela, F., Moreno Hernandez, J.J., Rodríguez Barrero, M.S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11(1): 1-22. https://doi.org/10.1057/s41599-024-03606-0

[14] Zenzerović, R., Šajrih, J. (2023). Financial statements fraud identifiers. Economic Research-Ekonomska Istraživanja, 36(3): 2218916. https://doi.org/10.1080/1331677X.2023.2218916

[15] Beemamol, M. (2024). Mapping the trends of financial statement fraud detection research from the historical roots and seminal work. Journal of Economic Criminology, 6: 100096. https://doi.org/10.1016/j.jeconc.2024.100096

[16] Alrasheed, R.A.R. (2025). Building public trust in bahrain: Leveraging artificial intelligence to combat financial fraud and terrorist financing through cryptocurrency tracking. Social Sciences, 14(5): 308. https://doi.org/10.3390/socsci14050308

[17] Liu, Z., Dani, J., Cao, Y., Wu, S., Saxena, N.(2025). The first early evidence of the use of browser fingerprinting for online tracking. In Proceedings of the ACM on Web Conference 2025, New York, pp. 4980-4995. https://doi.org/10.1145/3696410.3714548

[18] Padmapriya, V.M., Thenmozhi, K., Hemalatha, M., Thanikaiselvan, V., Lakshmi, C., Chidambaram, N., Rengarajan, A. (2025). Secured IIoT against trust deficit-A flexi cryptic approach. Multimedia Tools and Applications, 84(9): 5625-5652. https://doi.org/10.1007/s11042-024-18962-x

[19] Guan, L., Chen, S. (2024). Virtual identity alignment system based on multi-source intelligence. In Proceedings of the 2024 2nd International Conference on Advances in Artificial Intelligence and Applications, New York, pp. 157-161. https://doi.org/10.1145/3712623.3712626

[20] Hilal, W., Gadsden, S.A., Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications, 193: 116429. https://doi.org/10.1016/j.eswa.2021.116429

[21] Baesens, B., Höppner, S., Verdonck, T. (2021). Data engineering for fraud detection. Decision Support Systems, 150: 113492. https://doi.org/10.1016/j.dss.2021.113492

[22] Dey, N.S., Sangaraju, H.K.R. (2024). A particle swarm optimization inspired global and local stability driven predictive load balancing strategy. Indonesian Journal of Electrical Engineering and Computer Science, 35(3): 1688-1701. https://doi.org/10.11591/ijeecs.v35.i3.pp1688-1701

[23] Dey, N.S., Sangaraju, H.K.R. (2023). Hybrid load balancing strategy for cloud data centers with novel performance evaluation strategy. International Journal of Intelligent Systems and Applications in Engineering,

11(3): 883-908.
[24] Kumar, A.A., Raju, S.H. (2025). Hybrid machine learning for fraud detection: Balancing accuracy and security in digital transactions. International Journal of Safety & Security Engineering, 15(2): 331-337. https://doi.org/10.18280/ijsse.150214
[25] Sha, Q., Tang, T., Du, X., Liu, J., Wang, Y., Sheng, Y. (2025). Detecting credit card fraud via heterogeneous graph neural networks with graph attention. arXiv preprint arXiv:2504.08183. https://doi.org/10.48550/arXiv.2504.08183
[26] Raju, S.H., Adinarayna, S., Jadala, V.C., Rao, K.Y., Sesadri, U., Sreeraman, Y. (2025). An optimized approach for defect detection in the flyovers using faster R-CNN, LSTM, and Transfer Learning. Mathematical Modelling of Engineering Problems, 12(8): 2874-2882. https://doi.org/10.18280/mmep.120828