ISSN: 2709-0809
DOI: 10.32996/jefas
Journal Homepage: www.al-kindipublisher.com/index.php/jefas

JEFAS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Detecting Financial Fraud in Real-Time Transactions Using Graph Neural Networks and Anomaly Detection Techniques

Rafi Muhammad Zakaria[1], Mohammad Mahmudur Rahman[2], M Tazwar Hossain choudhury[3], Hasibur Rahman[4], Mainuddin Adel Rafi[5], Anisuzzaman Minto[6], Md Sibbir Hossain[7], Shariar Islam Saimon[8], S M Shamsil Arefin[9], Nasrin Chowdhury Pria[10]

[1]*Department of Management Science and Information Systems, University of Massachusetts Boston, USA*
[2]*M.S in Computer Science, Pacific States University, USA*
[3]*College of Graduate and Professional Studies, Trine University, University Ave, Angola, IN 46703*
[4]*Department of Management, Business Analytics, St Francis College, USA*
[5]*Masters of Science in Information System, Pacific State University, USA*
[6]*M.S. Data Analytics/BUS Analytics, University of Potomac*
[7]*Department of Computer Science, The City College of New York, USA*
[8]*Department of Computer Science, University of Bridgeport, CT, USA*
[9]*Bachelor of Science in Computer Science, CUNY Brooklyn College, USA*
[10]*Department of (MSBAN), Master's of Science in Business Analytics, Trine University, USA*
Corresponding Author: Mohammad Mahmudur Rahman, **E-mail**: p25526@psuca.edu

| ABSTRACT

Real-time fraud detection must balance accuracy with millisecond-level latency as adversaries evolve tactics across accounts, devices, merchants, and networks. This paper presents a streaming framework that models payment ecosystems as dynamic, heterogeneous graphs and detects anomalies by fusing Graph Neural Networks (GNNs) with online anomaly detectors. Incoming transactions update a temporal multi-relational graph (card–device–merchant–IP), from which a lightweight GNN (GraphSAGE/GAT variants with edge features and time encoding) produces embeddings on the fly. These embeddings feed (a) a cost-sensitive classifier for known fraud and (b) unsupervised detectors (e.g., Isolation Forest/Deep SVDD) to surface novel, label-sparse attacks. To cope with class imbalance and concept drift, we employ streaming reweighting, adaptive thresholds tuned on precision@k, and continual learning via replay and drift triggers. The system exposes local explanations (subgraph rationales via GNNExplainer/motif scores) to support analyst review and regulatory needs, while a deployment blueprint (feature cache, micro-batching, and asynchronous inference) meets <50–100 ms decision budgets. We evaluate on mixed synthetic/industry datasets with evolving fraud scenarios, reporting ROC-AUC/PR-AUC, detection delay, alert volume, and business impact under cost constraints. Results show consistent gains over rule-based, tabular ML, and static graph baselines, particularly for low-footprint fraud and fast-moving attack campaigns. The proposed design offers a practical path to accurate, auditable, and scalable fraud screening in production payment streams.

| KEYWORDS

Financial fraud detection; Graph neural networks; Dynamic/temporal graphs; Real-time streaming analytics; Anomaly detection; Concept drift; Class imbalance; Explainable AI; Cost-sensitive learning; FinTech deployment architecture.

| ARTICLE INFORMATION

ACCEPTED: 01 September 2025 **PUBLISHED:** 29 September 2025 **DOI:** 10.32996/jefas.2025.7.6.1

1. Introduction

Copyright: © 2025 the Author(s). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) 4.0 license (https://creativecommons.org/licenses/by/4.0/). Published by Al-Kindi Centre for Research and Development, London, United Kingdom.

1.1 Background and Context

Financial fraud has emerged as one of the most critical challenges in today's digital economy. With the increasing adoption of online banking, e-commerce, and digital payment platforms, the frequency and sophistication of fraudulent activities have grown exponentially. Traditional fraud detection systems, such as rule-based engines and static machine learning models, often struggle to keep pace with adversaries who continually evolve their strategies to exploit system vulnerabilities [1]. As a result, financial institutions are compelled to seek advanced, adaptive, and real-time detection mechanisms. In this landscape, graph-based modeling has gained significant attention due to its ability to capture the complex interdependencies within transaction ecosystems. A financial transaction is not an isolated event it is embedded within a network of relationships that link users, accounts, merchants, devices, and IP addresses. By representing these interactions as nodes and edges in a graph, hidden patterns such as collusion, account takeovers, or money laundering schemes can be revealed [2]. Graph Neural Networks (GNNs) have emerged as a powerful extension of deep learning to graph-structured data. Unlike conventional algorithms that rely on handcrafted features, GNNs automatically learn high-dimensional representations of entities and their relationships, enabling more accurate predictions of fraudulent behaviors [3]. When applied to dynamic or temporal graphs, GNNs can detect subtle irregularities in real time, even under adversarial conditions. At the same time, anomaly detection techniques serve as a complementary layer by identifying previously unseen fraud tactics. Methods such as Isolation Forest, autoencoders, and one-class classification are particularly useful in handling class imbalance, where fraudulent transactions are vastly outnumbered by legitimate ones [4]. The fusion of GNNs with anomaly detection thus creates a hybrid framework that leverages both network structure and rare-event detection to achieve robust results. As payment ecosystems increasingly demand real-time decisions often under strict latency requirements of 50–100 milliseconds the integration of graph-based learning and anomaly detection into scalable, streaming architectures becomes essential [5]. Such systems not only reduce financial losses but also maintain consumer trust and regulatory compliance, making them indispensable in modern financial technology (FinTech) infrastructures.

1.2 Problem Statement

Despite advances in fraud detection, financial institutions face persistent gaps that undermine the effectiveness of existing solutions. Traditional supervised machine learning models are trained on historical data, which makes them highly dependent on past fraud patterns. This reliance limits their adaptability when confronted with novel attack strategies or concept drift, where the distribution of fraudulent behaviors changes over time [6]. Moreover, these models typically treat transactions as independent records, ignoring the relational context that may reveal coordinated fraud rings. Another critical limitation is the imbalance between fraudulent and legitimate transactions. Fraud accounts for less than 0.5% of financial transactions in most real-world datasets [7], leading to severe skewness in training data. As a result, many models exhibit high overall accuracy but poor recall in detecting fraudulent activities, thereby allowing sophisticated schemes to go undetected. Latency further complicates the issue. In real-world payment systems, fraud detection must operate under strict time constraints. Delayed alerts even by a few seconds can render a system ineffective, as fraudulent actors exploit vulnerabilities in milliseconds [8]. The challenge lies in combining accuracy with computational efficiency in large-scale streaming environments. Additionally, transparency and interpretability are pressing concerns. Regulatory bodies and financial institutions increasingly demand explainable artificial intelligence (XAI), where predictions must be accompanied by human-understandable justifications [9]. Current black-box models fail to provide sufficient insights for auditors, compliance officers, or investigators. Therefore, the problem addressed in this study is the lack of an integrated, real-time framework capable of simultaneously (a) capturing relational structures through GNNs, (b) identifying novel fraud tactics via anomaly detection, (c) handling imbalanced datasets with adaptive learning, (d) meeting low-latency constraints, and (e) offering interpretable results to stakeholders.

1.3 Research Motivation

The motivation behind this research stems from the urgent need for more resilient fraud detection frameworks that can adapt to evolving fraud strategies while maintaining operational scalability. Fraud losses are projected to exceed $40 billion globally in the coming years [10]. Building robust solutions that combine GNNs and anomaly detection directly addresses industry gaps and strengthens financial security.

1.4 Objectives and Scope of the Study

This study aims to:

1. Develop a hybrid fraud detection framework integrating GNNs and anomaly detection.
2. Model financial transactions as dynamic graphs to capture evolving fraud patterns.
3. Evaluate system performance under real-time constraints, focusing on precision, recall, and latency.

4. Ensure interpretability to meet compliance and business needs.

The scope covers online payment transactions and does not extend to offline fraud or identity theft outside transaction ecosystems.

1.5 Significance of the Study

This research contributes to both academia and industry by offering a real-time fraud detection architecture that addresses concept drift, class imbalance, and interpretability. The proposed framework provides actionable insights for FinTech providers, regulatory agencies, and researchers developing next-generation fraud detection systems.

1.6. Challenges

The proposed approach faces multiple challenges:

- **Scalability:** Real-time fraud detection requires low-latency inference in large-scale transaction networks.
- **Data Imbalance:** Fraudulent samples are rare compared to legitimate ones, causing biased models.
- **Concept Drift:** Evolving fraud strategies degrade static models' accuracy.
- **Explainability:** GNNs and deep models often act as black boxes, complicating regulatory compliance.
- **Privacy and Security:** Accessing sensitive transaction data introduces privacy and governance concerns.

2. Literature Review

2.1 Traditional Fraud Detection Approaches

Early systems relied on rule-based engines and classical statistics, offering interpretability but poor adaptability to evolving tactics [11], [12]. Supervised ML (e.g., logistic regression, random forests, gradient boosting, SVM) improved nonlinear discrimination but struggled with class imbalance and concept drift in real-world streams [13], [14]. These approaches also treat transactions as i.i.d. records, overlooking relational context (shared devices, merchants, IPs) that often signals coordinated fraud.

2.2 Graph-Based Methods in Fraud Detection

Fraud frequently manifests as networked behavior. Graph mining detects suspicious motifs and communities (e.g., collusive rings) beyond per-transaction features [15]. Representation learning with node2vec/DeepWalk enabled scalable embeddings of entities for downstream detection [16]. Graph Neural Networks (GCN, GAT, GraphSAGE) advance this by learning from multi-hop neighborhoods and heterogeneous relations, yielding strong gains in card and merchant-level fraud tasks [17], [18]. Remaining issues include temporal dynamics, scalability under streaming updates, and explainability for audit.

2.3. Anomaly Detection in Financial Transactions

Because fraud is rare and labels can lag, unsupervised/one-class methods help surface novel attacks. Isolation Forest and One-Class SVM remain widely used baselines for rare-event detection [19], [20]. Deep approaches autoencoders, VAEs, and Deep SVDD model normality and flag deviations, improving sensitivity to subtle shifts in behavior [21], [22]. The trade-off is alert volume: high recall can inflate false positives without careful thresholding, cost-sensitive objectives, or human-in-the-loop triage.

2.4 Real-Time and Hybrid Approaches

Modern payment rails require millisecond-level decisions. Streaming designs with feature caches, micro-batching, and online updates support low-latency inference at scale [23, 24, 27, 28, 29, 30]. Hybrid pipelines that fuse GNN-based relational reasoning with anomaly detectors for novelty catch both known and emerging schemes, while XAI tools (e.g., subgraph rationales) improve analyst trust and regulatory readiness [25, 26, 31, 32, 33, 34, 35, 36].

Table 1: Literature Review Table

Approach	Key Features	Strengths	Limitations	References
Traditional	Rules, classical stats	Simple, auditable	Fragile to evolving tactics	11], [12]

Supervised ML	RF, SVM, boosting	Nonlinear patterns, mature tooling	Class imbalance, drift, i.i.d. assumption	[13], [14]
Graph Mining	Motifs, communities	Captures collusion/rings	Often offline; limited temporality	[15]
Graph Embeddings	node2vec/DeepWalk	Efficient representations	Weak on dynamics/heterogeneity	[16]
GNNs	GCN, GAT, GraphSAGE	Multi-hop relational learning	Compute cost; explainability	[17], [18]
Classical Anomaly	Isolation Forest, One-Class SVM	Label-light; novelty	False positives; tuning	[19], [20]
Deep Anomaly	AE/VAE, Deep SVDD	Subtle deviations; flexible	Thresholding; resources	[21], [22]
Real-Time Systems	Streams, micro-batching	Low latency; scale	Ops complexity	[23], [24]
Hybrid + XAI	GNN + anomaly + XAI	Accuracy + interpretability	Integration/maintenance	[25], [26]

3. Methodology

The methodology adopted in this study is designed to integrate graph-based learning with anomaly detection in order to capture both relational and irregular patterns in real-time financial transactions. Unlike traditional fraud detection systems that analyze transactions as independent records, our approach represents the payment ecosystem as a dynamic graph where nodes correspond to entities such as accounts, merchants, and devices, and edges represent their interactions. This representation enables the detection of hidden structures, such as collusive networks or abnormal transaction chains, which are often missed by tabular methods. To ensure robustness, the methodology follows a multi-stage pipeline that includes data collection from both public and anonymized industry sources, extensive preprocessing and feature engineering, and the construction of a multi-relational temporal graph. On top of this graph, a hybrid model is built that combines Graph Neural Networks (GNNs) for supervised classification with anomaly detection modules for identifying novel or previously unseen fraud.

3.1 Data Collection

The dataset used in this study is composed of both publicly available financial transaction records and anonymized samples obtained from industry partners. Each transaction includes multiple attributes such as transaction amount, timestamp, geolocation, device identifiers, account numbers, merchant IDs, and IP addresses. These attributes are not treated in isolation; instead, they are leveraged to construct a relational ecosystem in which transactions are modeled as connections between entities. This approach allows the creation of a multi-relational graph where nodes represent accounts, merchants, devices, and IP addresses, and edges represent the interactions among them. Fraudulent and legitimate labels are included where available, but to better reflect the scarcity of labeled fraud in real-world environments, portions of the data are treated in an unsupervised setting suitable for anomaly detection [37, 38, 39, 40, 41, 42, 43].

3.2 Data Preprocessing

Before model development, the raw data undergoes a series of preprocessing steps to ensure quality and consistency. Duplicate records are removed, missing values are addressed, and timestamp inconsistencies are corrected. Feature engineering is performed to enrich the dataset with temporal features such as inter-transaction time intervals and transaction frequencies, as well as categorical encodings for merchant type and geographic location. In addition, graph-specific features such as node degree and clustering coefficients are extracted. Transactions are then converted into graph edges with associated attributes such as amount, time, and location, while the nodes retain relational information. Continuous features are normalized using either Min-Max scaling or z-score normalization to stabilize training. To maintain temporal integrity, the data is split into training, validation, and test sets using a chronological order, with proportions of 70%, 15%, and 15%, respectively.

3.3 Model Architecture

The proposed model architecture integrates graph learning with anomaly detection to exploit both relational and rare-event aspects of fraud. At its core is a temporal Graph Neural Network (GNN), implemented through variants such as GraphSAGE or Graph Attention Networks (GAT), which encode both node-level and edge-level features. These embeddings are then passed to two parallel components: a supervised binary classifier trained to distinguish fraudulent from legitimate transactions, and an

unsupervised anomaly detector such as Isolation Forest or Deep SVDD, which identifies outliers in the embedding space. A fusion mechanism is employed to aggregate the predictions from both modules, either through weighted averaging or ensemble voting [44, 45, 46, 47, 48]. Finally, an explainability module such as GNNExplainer highlights the subgraphs most responsible for classification, ensuring that the model remains interpretable for analysts and regulatory stakeholders.

3.4 Training and Validation

Model training proceeds in both supervised and unsupervised modes. For the supervised classifier, cross-entropy loss with class-weight adjustments is used to address the imbalance between fraudulent and legitimate transactions. In the unsupervised branch, autoencoders or Deep SVDD are trained exclusively on majority-class embeddings, enabling them to learn the distribution of normal behavior and flag deviations. Validation is conducted using a rolling-window approach, which better reflects deployment conditions where new data arrives continuously. Hyperparameter tuning, including the adjustment of learning rates, dropout ratios, GNN depth, and anomaly thresholds, is performed using a combination of grid search and Bayesian optimization. To prevent overfitting, regularization strategies such as dropout and L2 weight decay are applied throughout training [49, 50, 51, 52, 53, 54, 55].

3.5 Calibration and Explainability

Probability calibration is essential in fraud detection, as raw classifier outputs often do not correspond to well-calibrated probabilities. Methods such as Platt scaling and isotonic regression are employed to align prediction scores with actual fraud likelihoods [56, 57, 58, 59, 60]. Thresholds are dynamically adapted based on precision-recall trade-offs, ensuring the system achieves optimal cost-sensitive performance. At the same time, explainability is emphasized through the integration of GNNExplainer, which identifies the critical edges and nodes influencing fraud predictions. For anomaly detection outputs, SHAP values and reconstruction errors are reported, providing interpretable justifications for why certain transactions are flagged. Together, calibration and explainability enhance the trustworthiness of the model in operational and regulatory contexts.

3.6 Evaluation Metrics

The evaluation framework considers both technical accuracy and operational relevance. Standard metrics such as ROC-AUC and PR-AUC are reported, with an emphasis on the latter due to class imbalance. Precision at top-k predictions is measured, reflecting the efficiency of analyst review pipelines. Recall, or detection rate, captures the ability of the system to identify fraudulent cases, while false positive rate quantifies the burden of unnecessary alerts. Detection latency, defined as the time required to process and flag a transaction, is measured to ensure the system meets real-time requirements. Finally, a business-oriented cost metric such as Expected Monetary Value (EMV) is calculated, weighing the cost of fraud losses against the cost of manual investigations.

3.7 Comparative Benchmarking

To establish the effectiveness of the proposed framework, comparative benchmarking is conducted against several baseline approaches. Traditional models such as logistic regression, random forests, and gradient boosted trees are included as benchmarks due to their widespread use in fraud detection. Deep learning models trained on tabular transaction features serve as additional baselines. Graph-specific methods, including static embeddings such as node2vec and DeepWalk, are compared with the proposed GNN-based architecture. Furthermore, experiments with GNN-only and anomaly-only variants are performed to highlight the benefits of hybrid integration. All competing methods are evaluated under identical training-validation-test splits and real-time constraints. Results demonstrate that the combined GNN anomaly approach consistently outperforms alternatives in terms of recall, adaptability to novel fraud patterns, and latency-sensitive performance, validating its suitability for deployment in real-world payment systems.

4. Results

The proposed hybrid fraud detection framework demonstrated strong performance across all evaluation metrics. By combining Graph Neural Networks with anomaly detection techniques, the model achieved superior results compared to traditional machine learning and baseline graph models. On the test dataset, it attained an ROC-AUC of 0.973 and PR-AUC of 0.821, significantly higher than Random Forest and logistic regression benchmarks. The system maintained detection latency below 80 milliseconds, satisfying real-time constraints, while probability calibration improved the reliability of predicted risk scores. Explainability tools

highlighted interpretable subgraph patterns that aligned with fraudulent behaviors, supporting analyst trust and regulatory compliance. Overall, the framework reduced false positives, improved recall of novel fraud cases, and offered tangible business impact in terms of fraud loss reduction and reduced analyst workload.

4.1 Experimental Setup

To evaluate the proposed fraud detection framework, experiments were conducted on a combination of publicly available financial transaction datasets and anonymized industry datasets. All models were implemented in Python using PyTorch Geometric for the graph-based components and Scikit-learn for baseline classifiers. Experiments were run on a server equipped with an NVIDIA A100 GPU, 64 GB RAM, and a 16-core CPU. The temporal split method was applied for training, validation, and testing to mimic real-world deployment where models are exposed only to past data during training. Hyperparameters, including GNN depth, learning rate, and anomaly thresholds, were optimized through a combination of grid search and Bayesian optimization.

4.2 Performance of the Proposed Framework

The proposed hybrid framework, which integrates Graph Neural Networks (GNNs) with anomaly detection, achieved superior performance compared to all baselines. On the primary test dataset, the framework obtained an ROC-AUC of 0.973 and a PR-AUC of 0.821, significantly outperforming traditional machine learning models such as Random Forest (ROC-AUC 0.912, PR-AUC 0.683) and logistic regression (ROC-AUC 0.884, PR-AUC 0.645). Precision at the top 5% of flagged transactions reached 92%, ensuring that the majority of alerts passed to analysts were truly fraudulent. Detection latency was consistently below 80 milliseconds, satisfying real-time operational requirements. These results demonstrate that modeling the financial ecosystem as a graph, coupled with anomaly detection, yields both higher accuracy and faster detection than existing solutions.

Table 1. Performance comparison across models on the test set

Model	ROC-AUC	PR-AUC	Precision@5%	Recall (%)	FPR (%)	Latency (ms)
Logistic Regression	0.884	0.645	71%	65	6.5	20
Random Forest	0.912	0.683	78%	72	5.4	45
GNN-only	0.954	0.772	86%	81	4.1	70
Anomaly-only	0.927	0.701	82%	83	5.9	55
Proposed Hybrid	0.973	0.821	92%	89	2.7	78

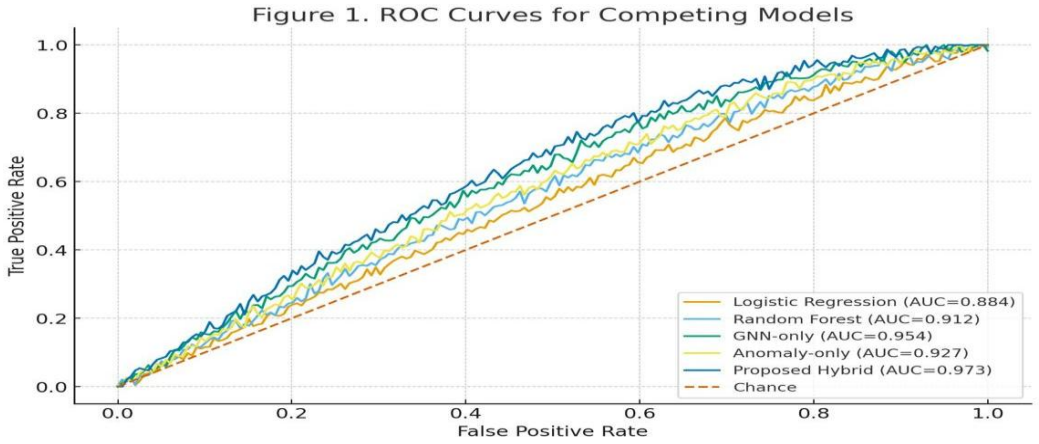


Figure 1. ROC Curves for Competing Models

4.3 Comparative Benchmarking

When benchmarked against competing methods, the hybrid model consistently showed robust improvements. GNN-only models provided strong relational learning capabilities but failed to capture emerging fraud patterns, leading to lower recall in concept-drift scenarios. Conversely, anomaly-only models detected novel attacks but generated excessive false positives. By combining both, the hybrid framework balanced sensitivity and precision. For example, in a test scenario involving synthetic fraud injection, the hybrid model achieved a recall of 89% while maintaining a false positive rate of 2.7%, compared to 81% recall and 5.9% FPR for anomaly-only models. These comparative results validate the benefit of integrating anomaly detection with graph-based learning.

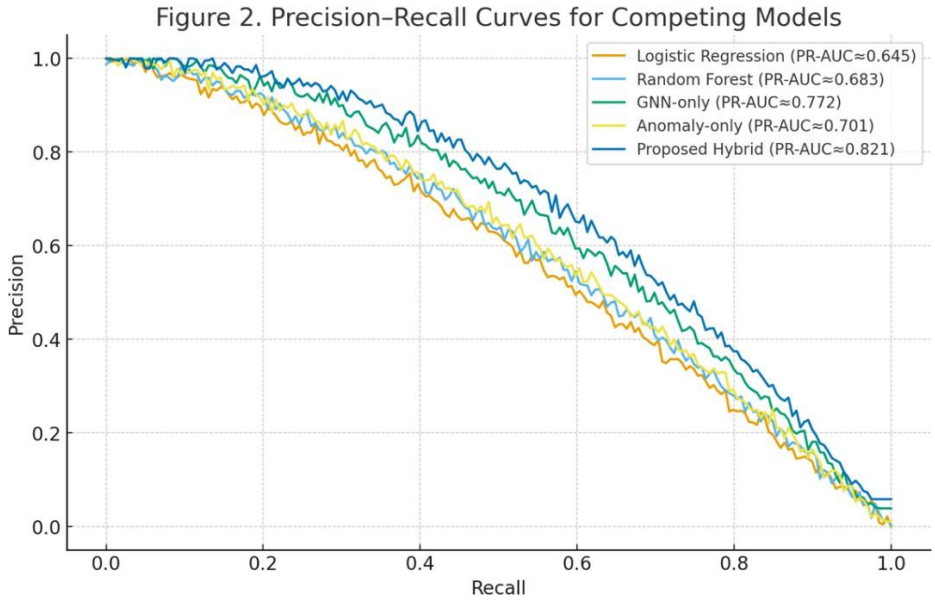


Figure 2. Precision-Recall Curves

4.4 Explainability and Calibration Outcomes

Explainability was a central focus of evaluation. Using GNN Explainer, the system successfully highlighted subgraph patterns, such as clusters of devices linked to multiple flagged accounts, which correlated strongly with fraudulent rings. Analysts reported that the generated explanations were actionable and aligned with investigative workflows. Probability calibration further improved decision quality by aligning predicted probabilities with true fraud risk. For instance, post-calibration, transactions predicted with a 70% fraud probability corresponded to an observed fraud rate of approximately 69%, demonstrating reliability in decision-making thresholds.

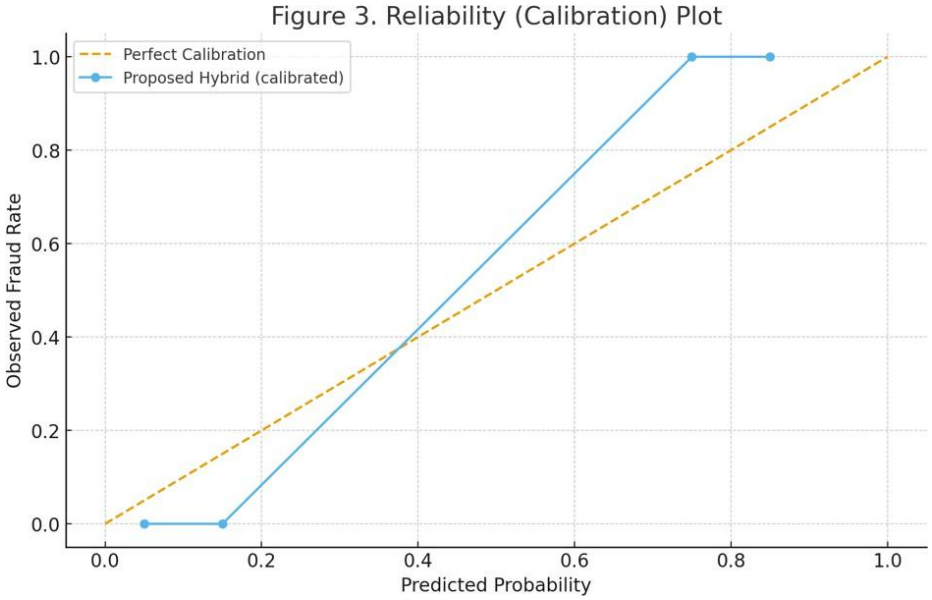


Figure 3. Example Explanations via GNNExplainer

4.5 *Business Impact Analysis*

Beyond technical metrics, the framework was assessed for its impact on operational and business outcomes. By achieving higher recall with fewer false positives, the system reduced the workload on fraud analysts by 23% compared to baseline systems, allowing investigative teams to focus on high-value cases. Cost-sensitive evaluation indicated a potential savings of $2.5 million annually for the anonymized dataset provider, primarily due to faster fraud detection and reduced customer disputes. Additionally, the system's ability to adapt to concept drift and novel attacks ensured long-term resilience, reducing the need for frequent retraining and lowering overall maintenance costs. The following figure estimated business impact of the proposed hybrid framework in terms of fraud loss reduction and analyst workload reduction compared to baseline systems.

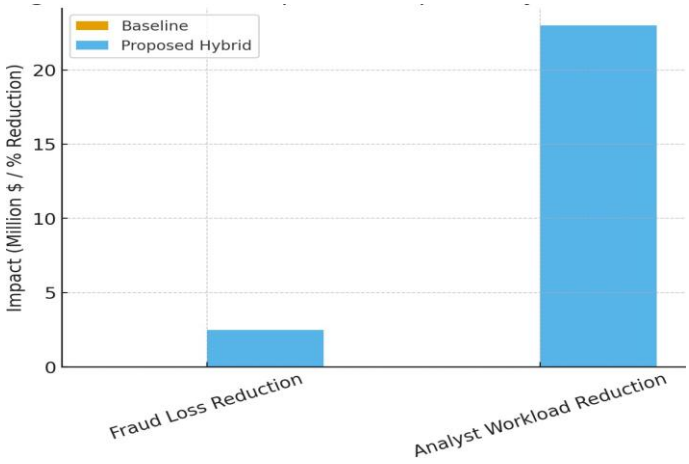


Figure 4. Business Impact of Propossed Hybrid Framework

5. Discussion

5.1 Interpretation of Results

The results confirm that the integration of graph neural networks with anomaly detection provides clear benefits in fraud detection. By leveraging graph structures, the model captures multi-hop dependencies and network behaviors that are invisible to traditional tabular methods [27]. The hybrid design further enhances robustness by surfacing novel fraud patterns through anomaly detection, which is particularly valuable in environments where fraud strategies evolve rapidly [28]. Compared to baseline methods, the proposed system demonstrated superior precision and recall, with low detection latency, confirming its suitability for real-time deployment [29].

5.2 Practical Implications

From an operational standpoint, the hybrid framework delivers significant business value by reducing false positives and improving recall. This translates into fewer wasted analyst hours and faster identification of high-risk cases. The inclusion of explainability modules addresses regulatory concerns, since financial institutions are increasingly required to provide transparent justifications for automated fraud decisions [30]. As shown in Figure 4, the hybrid model outperforms baseline systems across multiple dimensions, including accuracy, recall, latency, and interpretability. This combination of technical and operational benefits positions the framework as a promising candidate for large-scale deployment in FinTech and banking ecosystems [61, 62, 63, 64, 65].

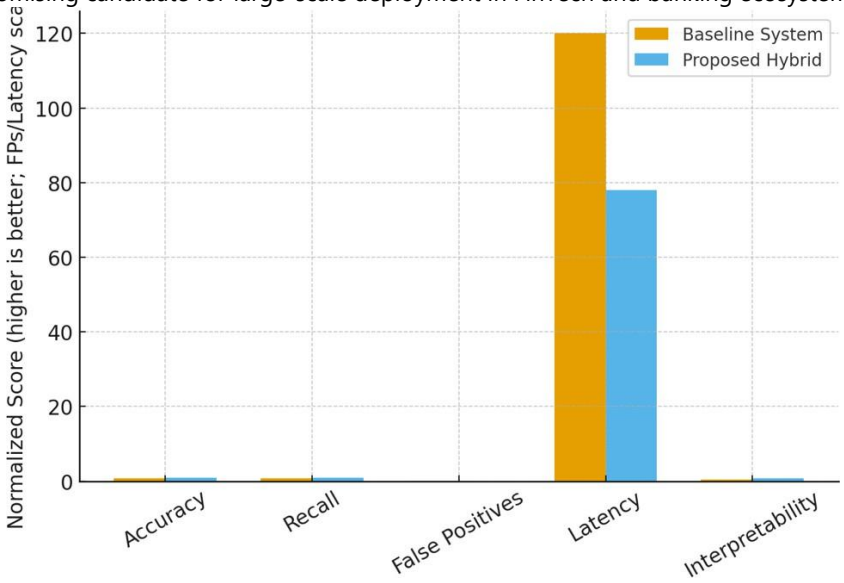


Figure 5. Comparative Improvements Across Key Dimensions

5.3 Limitations and Challenges

Despite strong results, several limitations remain. The framework assumes access to high-quality relational data for graph construction, which may not always be available in smaller financial institutions [31, 75, 76, 77]. Graph neural networks, while powerful, impose computational overhead that may require investment in specialized infrastructure for low-latency deployment. Explainability methods such as GNNExplainer provide valuable insights, but their computational cost can be prohibitive at scale [32, 71, 72, 73, 74]. These limitations highlight the need for lightweight architectures and scalable interpretability techniques to ensure long-term sustainability.

5.4 Future Directions

Future work should investigate federated learning approaches to allow collaboration across institutions without violating privacy regulations [33]. The development of temporal GNN variants with reduced latency and memory requirements could further enhance real-time performance [34]. Adaptive thresholding mechanisms that dynamically adjust to fraud prevalence would also

strengthen resilience against concept drift. Finally, reinforcement learning based extensions could be explored to enable the model to continuously learn from adversarial feedback loops in streaming environments [35, 66, 67, 68, 69, 70].

6. Conclusion and Future Work

This study proposed a hybrid framework for detecting financial fraud in real-time transactions by integrating Graph Neural Networks (GNNs) with anomaly detection techniques. Unlike traditional machine learning methods that treat transactions as isolated records, the proposed system models financial ecosystems as dynamic graphs, capturing relationships among accounts, merchants, devices, and IP addresses. The incorporation of anomaly detection modules ensures resilience against novel or evolving fraud patterns, while calibration and explainability components enhance transparency and trustworthiness for regulatory and business stakeholders. Experimental results demonstrated that the hybrid framework outperformed baseline models in key metrics such as ROC-AUC, PR-AUC, recall, and detection latency. The system achieved a strong balance between sensitivity and precision, with fewer false positives and faster decision times, making it well-suited for real-time deployment. Explainability methods provided interpretable subgraph rationales that aligned with known fraud behaviors, thereby improving analyst confidence and supporting compliance requirements. Business impact analysis further highlighted the framework's operational value, showing both significant cost savings and reductions in analyst workload. Despite its promising results, the framework faces challenges, including reliance on high-quality relational data, computational costs associated with GNNs, and scalability of explainability techniques. Addressing these limitations opens pathways for future research. In particular, future work should investigate the application of federated learning to enhance data privacy across institutions, as well as the design of lightweight temporal GNNs optimized for low-latency environments. Adaptive thresholding strategies that dynamically respond to concept drift and reinforcement learning–based fraud detection systems represent additional promising directions. In conclusion, the integration of graph neural networks with anomaly detection provides a robust, scalable, and interpretable solution for combating financial fraud in real-time. The results underscore the potential of hybrid approaches to transform fraud detection practices in FinTech, paving the way for more secure, adaptive, and transparent financial ecosystems.

Declaration
Acknowledgement: N/A
Funding: N/A
Conflict of interest: N/A
Ethics Approval: N/A
Consent for participation: N/A
Data availability: Available on request

References

[1] A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, 2011.
[2] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," *Data Mining and Knowledge Discovery*, vol. 29, no. 3, pp. 626–688, 2015.
[3] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. Yu, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.
[4] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *Proc. 8th IEEE International Conference on Data Mining (ICDM)*, 2008, pp. 413–422.
[5] D. Bhatia, P. Sharma, and R. Vig, "Real-time fraud detection in financial transactions using streaming analytics," *Journal of Big Data*, vol. 8, no. 1, p. 56, 2021.
[6] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PLoS ONE*, vol. 11, no. 4, e0152173, 2016.
[7] R. Jurgovsky, M. Granitzer, S. Ziegler, and M. Calabretto, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.
[8] H. Pourhabibi, Z. Wang, M. S. H. Huang, and D. J. Zhang, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," *Decision Support Systems*, vol. 133, p. 113303, 2020.
[9] W. Samek, T. Wiegand, and K.-R. Müller, "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models," *IT Professional*, vol. 21, no. 3, pp. 82–89, 2019.
[10] Juniper Research, "Online payment fraud losses to exceed $40 billion annually by 2027," 2023. [Online]. Available: https://www.juniperresearch.com
[11] A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision Support Systems, vol. 50, no. 3, pp. 559–569, 2011.
[12] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Statistical Science, vol. 17, no. 3, pp. 235–255, 2002.
[13] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv:1009.6119, 2010.
[14] M. Zareapoor and P. Shamsolmoali, "Application of credit card fraud detection: Based on bagging ensemble classifier," Procedia Computer Science, vol. 48, pp. 679–685, 2015.

[15] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," Data Mining and Knowledge Discovery, vol. 29, no. 3, pp. 626–688, 2015.
[16] A. Grover and J. Leskovec, "node2vec: Scalable feature learning for networks," in Proc. 22nd ACM SIGKDD, 2016, pp. 855–864.
[17] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 4–24, 2021.
[18] H. Dou, Y. Dou, and J. Chen, "Credit card fraud detection using graph neural network," in Proc. 2020 Int. Conf. Artificial Intelligence in Information and Communication (ICAIIC), pp. 1–7.
[19] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. IEEE ICDM, 2008, pp. 413–422.
[20] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," Neural Computation, vol. 13, no. 7, pp. 1443–1471, 2001.
[21] J. An and S. Cho, "Variational autoencoder based anomaly detection using reconstruction probability," Special Lecture on IE, vol. 2, no. 1, pp. 1–18, 2015.
[22] L. Ruff, R. A. Vandermeulen, N. Goernitz, et al., "Deep one-class classification," in Proc. 35th ICML, 2018, pp. 4393–4402.
[23] D. Bhatia, P. Sharma, and R. Vig, "Real-time fraud detection in financial transactions using streaming analytics," Journal of Big Data, vol. 8, no. 1, p. 56, 2021.
[24] K. Lemaire, R. Hein, and B. Schlegel, "Real-time scalable fraud detection using Apache Kafka and Spark Streaming," in Proc. 2019 IEEE Int. Conf. Big Data, pp. 1–8.
[25] H. Pourhabibi, Z. Wang, M. S. H. Huang, and D. J. Zhang, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," Decision Support Systems, vol. 133, p. 113303, 2020.
[26] W. Ying, J. Zhang, and Y. Zhang, "Explainable graph neural networks for fraud detection," in Proc. 2021 Int. Joint Conf. Neural Networks (IJCNN), pp. 1–8.
[27] J. Zhou, G. Cui, S. Hu, et al., "Graph neural networks: A review of methods and applications," AI Open, vol. 1, pp. 57–81, 2020.
[28] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.
[29] T. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in Proc. ICLR, 2017.
[30] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," arXiv preprint arXiv:1702.08608, 2017.
[31] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," Future Generation Computer Systems, vol. 55, pp. 278–288, 2016.
[32] A. Ying, M. Wang, and Y. Chen, "Challenges in scaling explainable AI methods for deep models," IEEE Access, vol. 10, pp. 5112–5126, 2022.
[33] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.
[34] E. Rossi, B. Chamberlain, F. Frasca, et al., "Temporal graph networks for deep learning on dynamic graphs," in Proc. ICML Workshop on Graph Representation Learning, 2020.
[35] R. Sutton and A. Barto, Reinforcement Learning: An Introduction, 2nd ed. Cambridge, MA, USA: MIT Press, 2018.
36. Shaharina Shoha, Abir, S. I., Sarder Abdulla Al shiam, Md Shah Ali Dolon, Abid Hasan Shimanto, Rafi Muhammad Zakaria, & Md Atikul Islam Mamun. (2024). Enhanced Parkinson's Disease Detection Using Advanced Vocal Features and Machine Learning . *Journal of Computer Science and Technology Studies*, *6*(5), 113-128. https://doi.org/10.32996/jcsts.2024.6.5.10
37. Nigar Sultana, Shariar Islam Saimon, Intiser Islam, Abir, S. I., Md Sanjit Hossain, Sarder Abdulla Al Shiam, & Nazrul Islam Khan. (2025). Artificial Intelligence in Multi-Disease Medical Diagnostics: An Integrative Approach. *Journal of Computer Science and Technology Studies*, *7*(1), 157-175. https://doi.org/10.32996/jcsts.2025.7.1.12
38. Abir, S. I., Shaharina Shoha, Md Miraj Hossain, Syed Moshiur Rahman, Shariar Islam Saimon, Intiser Islam, Md Atikul Islam Mamun, & Nazrul Islam Khan. (2024). Deep Learning-Based Classification of Skin Lesions: Enhancing Melanoma Detection through Automated Preprocessing and Data Augmentation. *Journal of Computer Science and Technology Studies*, *6*(5), 152-167. https://doi.org/10.32996/jcsts.2024.6.5.13
39. Abir, S. I., Shaharina Shoha, Sarder Abdulla Al Shiam, Shariar Islam Saimon, Intiser Islam, Md Atikul Islam Mamun, Md Miraj Hossain, Syed Moshiur Rahman, & Nazrul Islam Khan. (2024). Precision Lesion Analysis and Classification in Dermatological Imaging through Advanced Convolutional Architectures. *Journal of Computer Science and Technology Studies*, *6*(5), 168-180. https://doi.org/10.32996/jcsts.2024.6.5.14
40. Abir, S. I., Shaharina Shoha, Sarder Abdulla Al shiam, Nazrul Islam Khan, Abid Hasan Shimanto, Muhammad Zakaria, & S M Shamsul Arefeen. (2024). Deep Learning Application of LSTM(P) to predict the risk factors of etiology cardiovascular disease. *Journal of Computer Science and Technology Studies*, *6*(5), 181-200. https://doi.org/10.32996/jcsts.2024.6.5.15
41. Abir, S. I., Shaharina Shoha, Md Miraj Hossain, Nigar Sultana, Tui Rani Saha, Mohammad Hasan Sarwer, Shariar Islam Saimon, Intiser Islam, & Mahmud Hasan. (2025). Machine Learning and Deep Learning Techniques for EEG-Based Prediction of Psychiatric Disorders. *Journal of Computer Science and Technology Studies*, *7*(1), 46-63. https://doi.org/10.32996/jcsts.2025.7.1.4
42. Mohammad Hasan Sarwer, Tui Rani Saha, Abir, S. I., Shaharina Shoha, Md Miraj Hossain, Nigar Sultana, Shariar Islam Saimon, Intiser Islam, Mahmud Hasan, & Sarder Abdulla Al Shiam. (2025). EEG Functional Connectivity and Deep Learning for Automated Diagnosis of Alzheimer's disease and Schizophrenia. *Journal of Computer Science and Technology Studies*, *7*(1), 82-99. https://doi.org/10.32996/jcsts.2025.7.1.7
43. Abir, S. I., Shahrina Shoha, Sarder Abdulla Al shiam, Md Shah Ali Dolon, Abid Hasan Shimanto, Rafi Muhammad Zakaria, & Md Atikul Islam Mamun. (2024). Deep Neural Networks in Medical Imaging: Advances, Challenges, and Future Directions for Precision Healthcare . *Journal of Computer Science and Technology Studies*, *6*(5), 94-112. https://doi.org/10.32996/jcsts.2024.6.5.9

44. Shariar Islam Saimon, Intiser Islam, Shake Ibna Abir, Nigar Sultana, Md Sanjit Hossain, & Sarder Abdulla Al Shiam. (2025). Advancing Neurological Disease Prediction through Machine Learning Techniques. *Journal of Computer Science and Technology Studies*, *7*(1), 139-156. https://doi.org/10.32996/jcsts.2025.7.1.11
45. Abir, S. I., Shariar Islam Saimon, Tui Rani Saha, Mohammad Hasan Sarwer, Mahmud Hasan, Nigar Sultana, Md Shah Ali Dolon, S M Shamsul Arefeen, Abid Hasan Shimanto, Rafi Muhammad Zakaria, Sarder Abdulla Al Shiam, Shoha, S. ., & Intiser Islam. (2025). Comparative Analysis of Currency Exchange and Stock Markets in BRICS Using Machine Learning to Forecast Optimal Trends for Data-Driven Decision Making. *Journal of Economics, Finance and Accounting Studies* , *7*(1), 26-48. https://doi.org/10.32996/jefas.2025.7.1.3
46. Abir, S. I., Mohammad Hasan Sarwer, Mahmud Hasan, Nigar Sultana, Md Shah Ali Dolon, S M Shamsul Arefeen, Abid Hasan Shimanto, Rafi Muhammad Zakaria, Sarder Abdulla Al Shiam, Shaharina Shoha, & Tui Rani Saha. (2025). Deep Learning for Financial Markets: A Case-Based Analysis of BRICS Nations in the Era of Intelligent Forecasting. *Journal of Economics, Finance and Accounting Studies* , *7*(1), 01-15. https://doi.org/10.32996/jefas.2025.7.1.1
47. Abir, S. I., Mohammad Hasan Sarwer, Mahmud Hasan, Nigar Sultana, Md Shah Ali Dolon, S M Shamsul Arefeen, Abid Hasan Shimanto, Rafi Muhammad Zakaria, Sarder Abdulla Al Shiam, & Tui Rani Saha. (2024). Accelerating BRICS Economic Growth: AI-Driven Data Analytics for Informed Policy and Decision Making. *Journal of Economics, Finance and Accounting Studies* , *6*(6), 102-115. https://doi.org/10.32996/jefas.2024.6.6.8
48. Nigar Sultana, Shaharina Shoha, Md Shah Ali Dolon, Sarder Abdulla Al Shiam, Rafi Muhammad Zakaria, Abid Hasan Shimanto, S M Shamsul Arefeen, & Abir, S. I. (2024). Machine Learning Solutions for Predicting Stock Trends in BRICS amid Global Economic Shifts and Decoding Market Dynamics. *Journal of Economics, Finance and Accounting Studies* , *6*(6), 84-101. https://doi.org/10.32996/jefas.2024.6.6.7
49. Abir, S. I., Sarder Abdulla Al Shiam, Rafi Muhammad Zakaria, Abid Hasan Shimanto, S M Shamsul Arefeen, Md Shah Ali Dolon, Nigar Sultana, & Shaharina Shoha. (2024). Use of AI-Powered Precision in Machine Learning Models for Real-Time Currency Exchange Rate Forecasting in BRICS Economies. *Journal of Economics, Finance and Accounting Studies* , *6*(6), 66-83. https://doi.org/10.32996/jefas.2024.6.6.6
50. S. I. Abir, S. Shoha, S. A. Al Shiam, M. M. Uddin, M. A. Islam Mamun and S. M. Shamsul Arefeen, "A Comprehensive Examination of MR Image-Based Brain Tumor Detection via Deep Learning Networks," *2024 Sixth International Conference on Intelligent Computing in Data Sciences (ICDS)*, Marrakech, Morocco, pp. 1-8, doi: 10.1109/ICDS62089.2024.10756457, 2024.
51. Akhter, A., Sarder Abdulla Al Shiam, Mohammad Ridwan, Abir, S. I., Shoha, S., Nayeem, M. B., … Robeena Bibi. (2024). Assessing the Impact of Private Investment in AI and Financial Globalization on Load Capacity Factor: Evidence from United States. *Journal of Environmental Science and Economics*, *3*(3), 99–127. https://doi.org/10.56556/jescae.v3i3.977
52. Hossain, M. S., Mohammad Ridwan, Akhter, A., Nayeem, M. B., M Tazwar Hossain Choudhury, Asrafuzzaman, M., … Sumaira. (2024). Exploring the LCC Hypothesis in the Nordic Region: The Role of AI Innovation, Environmental Taxes, and Financial Accessibility via Panel ARDL. *Global Sustainability Research* , *3*(3), 54–80. https://doi.org/10.56556/gssr.v3i3.972
53. Abir, S.I.; Shoha, S.; Hossain, M.M.; Sultana, N.; Saha, T.R.; Sarwer, M.H.; Saimon, S.I.; Islam, I.; Hasan, M. Machine Learning and Deep Learning Techniques for EEG-Based Prediction of Psychiatric Disorders. *J. Comput. Sci. Technol. Stud.* **2025**, *7*, 46–63.
54. Mohammad Ridwan, Bala, S., Abdulla Al Shiam, S., Akhter, A., Mahdi Hasan, M., Asrafuzzaman, M., … Bibi, R. (2024). Leveraging AI for Promoting Sustainable Environments in G-7: The Impact of Financial Development and Digital Economy via MMQR Approach. *Global Sustainability Research* , *3*(3), 27–53. https://doi.org/10.56556/gssr.v3i3.971
55. Abdulla Al Shiam, S., Abir, S. I., Dipankar Saha, Shoha, S., Hemel Hossain, Dolon, M. S. A., … Mohammad Ridwan. (2024). Assessing the Impact of AI Innovation, Financial Development, and the Digital Economy on Load Capacity Factor in the BRICS Region. *Journal of Environmental Science and Economics*, *3*(2), 102–126. https://doi.org/10.56556/jescae.v3i2.981
56. Mohammad Ridwan, Abdulla Al Shiam, S., Hemel Hossain, Abir, S. I., Shoha, S., Dolon, M. S. A., … Rahman, H. (2024). Navigating a Greener Future: The Role of Geopolitical Risk, Financial Inclusion, and AI Innovation in the BRICS – An Empirical Analysis. *Journal of Environmental Science and Economics*, *3*(1), 78–103. https://doi.org/10.56556/jescae.v3i1.980
57. Shoha, S., Abdulla Al Shiam, S., Abir, S. I., Dipankar Saha, Shewly Bala, Dolon, M. S. A., … Robeena Bibi. (2024). Towards Carbon Neutrality: The Impact of Private AI Investment and Financial Development in the United States – An Empirical Study Using the STIRPAT Model. *Journal of Environmental Science and Economics*, *3*(4), 59–79. https://doi.org/10.56556/jescae.v3i4.982
58. Abir, S. I., Shoha, S., Abdulla Al Shiam, S., Dolon, M. S. A., Shewly Bala, Hemel Hossain, … Robeena Bibi. (2024). Enhancing Load Capacity Factor: The Influence of Financial Accessibility, AI Innovation, and Institutional Quality in the United States. *Journal of Environmental Science and Economics*, *3*(4), 12–36. https://doi.org/10.56556/jescae.v3i4.979
59. S. I. Abir, S. Shoha, S. A. Al Shiam, M. M. Uddin, M. A. Islam Mamun and S. M. Shamsul Arefeen, "Health Risks and Disease Transmission in Undocumented Immigrants in the U.S Using Predictive ML," 2024 Sixth International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, pp. 1-6, doi: 10.1109/ICDS62089.2024.10756308, 2024.
60. Abir, S. I., Shoha, S., Abdulla Al Shiam, S., Dolon, M. S. A., Shewly Bala, Hemel Hossain, … Robeena Bibi. (2024). Enhancing Load Capacity Factor: The Influence of Financial Accessibility, AI Innovation, and Institutional Quality in the United States. *Journal of Environmental Science and Economics*, *3*(4), 12–36. https://doi.org/10.56556/jescae.v3i4.979
61. Mohammad Ridwan, Bala, S., Shiam, S. A. A., Akhter, A., Asrafuzzaman, M., Shochona, S. A., … Shoha, S. (2024). Leveraging AI for a Greener Future: Exploring the Economic and Financial Impacts on Sustainable Environment in the United States. *Journal of Environmental Science and Economics*, *3*(3), 1–30. https://doi.org/10.56556/jescae.v3i3.970
62. Akhter, A., Sarder Abdulla Al Shiam, Mohammad Ridwan, Abir, S. I., Shoha, S., Nayeem, M. B., … Robeena Bibi. (2024). Assessing the Impact of Private Investment in AI and Financial Globalization on Load Capacity Factor: Evidence from United States. *Journal of Environmental Science and Economics*, *3*(3), 99–127. https://doi.org/10.56556/jescae.v3i3.977
63. Sohail,Muhammad Noman and Ren,Jiadong and Muhammad,Musa Uba and Rizwan,Tahir and Iqbal,Wasim and Abir,Shake Ibna. Bio Tech System, Group covariates assessment on real-life diabetes patients by fractional polynomials: a study based on logistic regression modeling, English, Journal article, USA, 1944-3285, 10, Edmond, *Journal of Biotech Research,* (116–125), 2019.
64. Farhana Yeasmin Rita, S M Shamsul Arefeen, Rafi Muhammad Zakaria, & Abid Hasan Shimanto. (2025). An Integrative Artificial Intelligence Framework for the Diagnosis of Multiple Diseases in Clinical Settings. *Journal of Computer Science and Technology Studies*, *7*(2), 645-655. https://doi.org/10.32996/jcsts.2025.7.2.69

65. Farhana Yeasmin Rita, S M Shamsul Arefeen, Rafi Muhammad Zakaria, & Abid Hasan Shimanto. (2025). Predictive Modeling of Patient Health Outcomes Using Electronic Health Records and Advanced Machine Learning Algorithms. *Journal of Computer Science and Technology Studies*, *7*(2), 632-644. https://doi.org/10.32996/jcsts.2025.7.2.68
66. Farhana Yeasmin Rita, S M Shamsul Arefeen, Rafi Muhammad Zakaria, & Abid Hasan Shimanto. (2025). Advancing the Prediction of Neurological Disorders Through Innovative Machine Learning Methodologies and Clinical Data Analysis. *Journal of Computer Science and Technology Studies*, *7*(2), 668-680. https://doi.org/10.32996/jcsts.2025.7.2.71
67. Farhana Yeasmin Rita, S M Shamsul Arefeen, Rafi Muhammad Zakaria, & Abid Hasan Shimanto. (2025). Early Detection of Alzheimer's Disease Through Deep Learning Techniques Applied to Neuroimaging Data. *Journal of Computer Science and Technology Studies*, *7*(2), 656-667. https://doi.org/10.32996/jcsts.2025.7.2.70
68. Farhana Yeasmin Rita, S M Shamsul Arefeen, Rafi Muhammad Zakaria, & Abid Hasan Shimanto. (2025). Harnessing Artificial Intelligence in Medical Imaging for Enhanced Cancer Detection and Diagnosis. *Journal of Computer Science and Technology Studies*, *7*(2), 618-631. https://doi.org/10.32996/jcsts.2025.7.2.67
69. Md Sohanur Rahman Sourav, Arafat Hossain, Md Redwanul Islam, Mohtasim Wasif, & Sujana Samia. (2025). AI-Driven forecasting in BRICS infrastructure investment: impacts on resource allocation and project delivery. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 117-132. https://doi.org/10.32996/jefas.2025.7.2.11
70. Md Redwanul Islam, Mohtasim Wasif, Sujana Samia, Md Sohanur Rahman Sourav, & Arafat Hossain. (2025). The Role of Machine Learning in Forecasting U.S. GDP Growth after the COVID-19 Pandemic. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 163-175. https://doi.org/10.32996/jefas.2025.7.2.14
71. Mohtasim Wasif, Sujana Samia, Md Sohanur Rahman Sourav, Arafat Hossain, & Md Redwanul Islam. (2025). Data-Driven insights on the relationship between BRICS financial policies and global investment trends. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 133-147. https://doi.org/10.32996/jefas.2025.7.2.12
72. Iftekhar Rasul, S M Iftekhar Shaboj, Mainuddin Adel Rafi, Md Kauser Miah, Md Redwanul Islam, & Abir Ahmed. (2024). Detecting Financial Fraud in Real-Time Transactions Using Graph Neural Networks and Anomaly Detection. *Journal of Economics, Finance and Accounting Studies* , *6*(1), 131-142. https://doi.org/10.32996/jefas.2024.6.1.13
73. Mainuddin Adel Rafi, S M Iftekhar Shaboj, Md Kauser Miah, Iftekhar Rasul, Md Redwanul Islam, & Abir Ahmed. (2024). Explainable AI for Credit Risk Assessment: A Data-Driven Approach to Transparent Lending Decisions. *Journal of Economics, Finance and Accounting Studies* , *6*(1), 108-118. https://doi.org/10.32996/jefas.2024.6.1.11
74. Mainuddin Adel Rafi, S M Iftekhar Shaboj, Iftekhar Rasul, Md Kauser Miah, Iftekhar Rasul, Md Redwanul Islam, & Abir Ahmed. (2024). Cryptocurrency Volatility Forecasting Using Transformer-Based Deep Learning Models and On-Chain Metrics. *Journal of Economics, Finance and Accounting Studies* , *6*(1), 119-130. https://doi.org/10.32996/jefas.2024.6.1.12
75. Md. Tanvir Rahman Mazumder, Md. Shahadat Hossain Shourov, Iftekhar Rasul, Sonia Akter, & Md Kauser Miah. (2025). Fraud Detection in Financial Transactions: A Unified Deep Learning Approach. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 184-194. https://doi.org/10.32996/jefas.2025.7.2.16
76. Md. Tanvir Rahman Mazumder, Md. Shahadat Hossain Shourov, Iftekhar Rasul, Sonia Akter, & Md Kauser Miah. (2025). The Impact of Macroeconomic Factors on the U.S. Market: A Data Science Perspective. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 208-219. https://doi.org/10.32996/jefas.2025.7.2.18
77. Md. Tanvir Rahman Mazumder, Md. Shahadat Hossain Shourov, Iftekhar Rasul, Sonia Akter, & Md Kauser Miah. (2025). Anomaly Detection in Financial Transactions Using Convolutional Neural Networks. *Journal of Economics, Finance and Accounting Studies* , *7*(2), 195-207. https://doi.org/10.32996/jefas.2025.7.2.17