Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI-Driven and Explainable Detection of Fraud and Cyber-Related Risks in Critical Infrastructure Payment Networks

Okolie Awele[1], Osondu C Onwuegbuchi[2] , Oluwatosin Lawal[3], Okon Godspower Emmanuel[4] , Moyosoreoluwa Abiose Fesobi[5]

[1]*School of Computing and Data Science, Wentworth Institute of Technology, Boston, USA.*
[2]*Department of Computer Science, Western Illinois University, USA*
[3] *Department of Mathematics Statistical Analytics, Computing and Modeling, Texas A&MUniversity, Kingsville, USA.*
[4] *Department of Mathematics, University of Florida, USA*
[5] *Department of Industrial Engineering, Texas A&M University, Kingsville, Texas, USA*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Digital payment networks which face significant security breaches from financial fraud and cyber attacks have become essential for critical infrastructure sectors that encompass energy and healthcare and transportation and government systems. The detection of complex and evolving attack patterns which use coordinated methods fails to be achieved by traditional rule-based systems when they operate in environments with highly imbalanced transaction volumes. The research presents an explainable artificial intelligence framework which detects fraudulent and anomalous activities in payment systems that serve critical infrastructure. The framework uses real-world transactional data from the IEEE-CIS Fraud Detection Dataset to combine supervised and unsupervised learning techniques which include Logistic Regression and Random Forest and XGBoost for fraud classification and anomaly detection for irregular transaction behavior. To handle class imbalance the Synthetic Minority Oversampling Technique (SMOTE) is used whereas threshold optimization enhances the system's ability to identify different types of detection with better precision.

The framework uses SHAP to provide explainable AI which produces interpretable results that show how models make predictions and which features affect their predictions. The proposed approach successfully identifies high-risk transactions because it improves key evaluation metrics which include precision and recall and F1-score and AUC. The proposed framework provides a scalable and adaptable solution for securing payment systems that underpin critical infrastructure operations. This work creates financial fraud detection and cyber risk awareness systems which build resilient and transparent and intelligent security solutions that protect national economic stability and infrastructure systems

Keywords: Artificial Intelligence; Fraud Detection; Critical Infrastructure Security; Cyber Threat Detection; Explainable AI; XGBoost; SHAP; Anomaly Detection

1. INTRODUCTION

Financial systems have undergone a fundamental change in their transaction methods because of rapid digitalization which has spread throughout all modern economies. The energy sector and healthcare sector and transportation sector and government services sector now depend on digital payment networks to operate their essential infrastructure operations. The new developments have increased operational efficiency and service accessibility but they have created new security weaknesses for financial fraud and cyber attacks. The rising complexity of attackers together with the massive volume of digital transactions has rendered traditional security systems ineffective for

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

maintaining system security and operational backup (Böhme & Moore, 2012; Ngai et al., 2011). Financial fraud remains a persistent and evolving challenge, particularly in highly imbalanced transactional environments where fraudulent activities represent only a small fraction of total transactions. Conventional rule-based detection systems, widely deployed in industry, often fail to adapt to dynamic fraud patterns and are limited in their ability to identify complex or coordinated attacks (Phua et al., 2010). Financial systems now face cyber threats which include ransomware and account takeover attacks and network intrusions, as these threats exploit payment system weaknesses to achieve operational disruptions and unauthorized value extraction (Conti et al., 2018). Organizations address fraud detection and cybersecurity analytics as two separate fields which creates defense systems that operate in an uncoordinated and inefficient manner.

Recent advancements in artificial intelligence (AI) and machine learning (ML) technologies have shown their capacity to enhance fraud detection systems. Through the use of Logistic Regression and Random Forest together with gradient boosting techniques of XGBoost researchers have achieved successful results in detecting unusual transaction patterns based on their high ability to forecast outcomes (Chen & Guestrin, 2016; Dal Pozzolo et al., 2015). The application of Synthetic Minority Oversampling Technique (SMOTE) and other class imbalance handling methods improves detection sensitivity for datasets that contain uneven class distributions according to Chawla et al. (2002). The majority of these methods operate as "black-box" systems which makes it difficult to understand their processes and creates trust issues within critical infrastructure systems that need dependable security measures. Explainable artificial intelligence (XAI) has emerged as a key solution to this challenge by providing transparency into model decisions. The SHAP technique enables stakeholders to interpret feature contributions which helps them understand why certain transactions get flagged as fraudulent (Lundberg & Lee, 2017). AI-driven systems require accountability and auditability and trust because these three elements form the foundation of their deployment in controlled environments and mission-critical operations. Research shows that a major gap exists because researchers have not created standardized systems which combine fraud detection with anomaly detection and system explanation for use in important payment networks that handle critical infrastructure. Researchers of existing studies concentrate on individual components of the problem instead of developing comprehensive solutions which maintain scalability while enabling both financial detection and cyber risk assessment.

The research presents an AI-powered transparent system which detects fraudulent and unusual behaviors occurring in essential infrastructure payment systems. The detection system uses supervised machine learning models which include Logistic Regression, Random Forest, and XGBoost together with data balancing techniques and threshold optimization methods to improve detection results in situations with unbalanced data. The system uses SHAP explainability methods to create understandable model prediction explanations which help users comprehend the models output. The real-world evaluation of the methodology used actual transaction records from the IEEE-CIS Fraud Detection Dataset which showed its capability to detect high-risk transactions. This paper brings three main contributions to its field. The first contribution presents an AI-based education framework which enables financial fraud detection while educating users about cyber risks in essential infrastructure systems. The second contribution presents an explainability layer which builds trust through transparent automated decision-making processes. The third contribution shows how users can apply the proposed solution to a real-world dataset which demonstrates its capacity to strengthen digital payment networks security and resilience. The research develops intelligent systems which protect critical infrastructure through its solutions to both technical and operational infrastructure security challenges.

2. LITERATURE REVIEW

2.1 Fraud Detection Using Machine Learning

Researchers have conducted extensive research on financial fraud detection through the application of machine learning techniques which enable the detection of complex non-linear patterns within extensive transaction datasets. The field has adopted traditional statistical techniques like Logistic Regression as baseline models because these methods provide understandable results and efficient performance. The application of Random Forest and gradient boosting techniques which include XGBoost has proven to be more effective than conventional methods for discovering fraudulent activities (Chen & Guestrin, 2016; Ngai et al., 2011). These models excel at discovering complex relationships between multiple high-dimensional features which helps them achieve better results in

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

prediction tasks. The recent research findings show that using multiple models together leads to better results in detecting suspicious activities. The ensemble methods combine different algorithms to create fraud detection systems which operate with increased strength and dependability (Dal Pozzolo et al., 2015). Model development and optimization processes must continue because the system faces difficulties with massive highly imbalanced datasets and needs to adapt to ongoing changes in fraudulent activities.

2.2 Imbalanced Data Handling

Fraud detection datasets exhibit their primary characteristic through extreme class imbalance because only a minor fraction of data contains fraudulent transactions. Machine learning models encounter major difficulties because standard algorithms demonstrate bias toward the majority class, which results in their inability to detect minority fraudulent cases. The problem has multiple solutions through different techniques that include resampling methods and cost-sensitive learning and anomaly detection approaches. The Synthetic Minority Oversampling Technique (SMOTE) serves as a popular method, which creates new synthetic minority class samples to achieve dataset balance (Chawla et al. 2002). SMOTE has been shown to improve recall and F1-score in fraud detection tasks by enabling models to better learn the characteristics of fraudulent transactions. The process of threshold optimization shows additional effectiveness as a method to enhance classification results in situations of class imbalance. Models use decision threshold adjustments to increase their ability to identify high-risk transactions, which results in fewer false negatives and improved system performance.

2.3 Cybersecurity and Anomaly Detection

Cybersecurity threats increasingly intersect with financial systems which create multiple attack possibilities that combine financial fraud with network-level intrusions. The traditional intrusion detection systems (IDS) use signature-based and rule-based methods which restrict their ability to identify new or developing security threats. Anomaly detection techniques have become important because they help find unusual system behavior patterns that do not match normal system operations. Cybersecurity experts widely use machine learning-based anomaly detection methods which include Isolation Forest to identify rare and previously unknown events (Conti et al., 2018). The methods effectively detect cyber-related anomalies which include unauthorized access and unusual transaction patterns and coordinated attacks. The current research treats cybersecurity and financial analytics as separate fields which reduces their ability to detect coordinated attacks that use both financial transactions and network activities. Unified frameworks are necessary to combine fraud detection with anomaly-based cyber threat detection.

2.4 Explainable Artificial Intelligence in Financial Systems

Explainable Artificial Intelligence (XAI) techniques have been developed to address these concerns by providing insights into model behavior. Among these, SHAP has gained widespread adoption due to its strong theoretical foundation and ability to quantify feature contributions for individual predictions (Lundberg & Lee, 2017). The SHAP system enables practitioners to understand complicated models while determining the main factors that contribute to fraudulent activities and confirming the results of their models. Explainability functions as a vital element in fraud detection systems because it establishes transparent operations which help organizations meet regulatory requirements while building trust in their daily activities. The growing popularity of automated financial systems will make XAI technology essential for organizations which seek to implement artificial intelligence systems in a responsible and ethical manner.

2.5 Research Gap and Motivation

The current research on machine learning-based fraud detection systems has progressed significantly but still faces multiple unresolved issues. First, most studies focus solely on financial fraud without considering the broader context of cyber-related threats that increasingly target payment infrastructures. Second, although advanced models have achieved better detection results, many of them do not include the necessary explainability features needed for use in critical situations. Third, there is a lack of unified frameworks that combine classification, anomaly detection, and interpretability into a cohesive system. These techniques have not received sufficient research focus especially in critical infrastructure sectors where system failures lead to severe consequences for national security and economic stability. The existing research gaps need to be addressed through the development of a complete system that combines various detection methods with a focus on both performance assessment and system transparency. The research study presents an AI-based explainable framework that combines fraud detection, anomaly detection, and

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

interpretability functions for use in vital payment networks. The solution uses actual data from the IEEE-CIS Fraud Detection Dataset combined with advanced machine learning and explainability methods to improve financial risk detection and cyber risk detection while maintaining system transparency and client confidence.

3. PROPOSED FRAMEWORK

3.1 System Overview

This study proposes an AI-driven and explainable framework for detecting fraudulent and cyber-related risks in critical infrastructure payment networks. The framework is designed as a multi-layered architecture that integrates data processing, machine learning-based detection, explainability mechanisms, and risk prioritization. The goal is to provide a scalable and interpretable system capable of identifying high-risk transactions in real time while maintaining transparency and adaptability.

The architecture consists of four primary components: (1) Data Ingestion Layer, (2) Detection Layer, (3) Explainability Layer, and (4) Risk Scoring Layer. These components work together to transform raw transactional data into actionable intelligence for fraud and anomaly detection.

3.2 Data Ingestion Layer

The data ingestion layer functions to acquire and merge and prepare data from various data sources. The framework in this research uses transactional data from the IEEE-CIS Fraud Detection Dataset which contains transaction details and identity information. The layer executes crucial preprocessing operations which consist of: The system eliminates all unneeded identification elements which include transaction identification numbers. The process establishes complete data sets through the method of filling in missing information. The system converts categorical data points into numerical forms through the process of encoding. The process of establishing identical feature spaces between training datasets and testing datasets. The system architecture currently processes financial transaction data but it allows users to add new data sources which include network security logs and user behavior data and system event streams. The framework can use cyber-related signals for threat detection because of its ability to expand. The framework uses cyber-related signals for threat detection because it can expand its capabilities.

3.3 Detection Layer

The detection layer serves as the main analysis element of the system because it uses machine learning models to detect both fraudulent activities and unusual events. The study uses a hybrid approach which combines various supervised learning methods to achieve better prediction results by using Logistic Regression and Random Forest and XGBoost. The Synthetic Minority Oversampling Technique (SMOTE) generates synthetic samples of the minority class during training to help resolve fraud detection datasets which have class imbalance problems. The models achieve success because they learn the patterns which link to fraudulent transactions. The detection system achieves better sensitivity through its implementation of threshold optimization. The framework tests various threshold values to find the best classification threshold which uses F1-score performance metrics. The method enables better management of precision and recall balance which holds particular importance for dangerous situations. The layer supports anomaly detection methods which include Isolation Forest as optional tools to detect uncommon transaction behavior that supervised models fail to identify. The system design enables detection of established fraud patterns and newly discovered anomalies which supports the main goal of detecting cyber danger elements.

3.4 Explainability Layer

The framework includes an explainability layer which uses SHAP technology to solve the problem of machine learning model transparency. The system displays model results through interpretable predictions which express the value of each input element for specific outcomes. The explainability layer enables: Identification of key features which drive fraud predictions Visualization of feature importance rankings Local explanations for particular transactions The system uses this layer to provide users with understandable results which build system trustworthiness while helping decision makers in controlled settings and essential environments. The system helps organizations conduct model validation and auditing procedures which companies require to implement artificial intelligence solutions in essential infrastructure sectors.

3.5 Risk Scoring and Decision Layer

The risk scoring and decision layer functions as the last element of the framework because it transforms model results into measurable risk assessments. The system uses predicted probabilities together with optimized thresholds to

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

assign three different risk categories to transactions, which include low risk and medium risk and high risk. This layer enables: The system prioritizes high-risk transactions which require further investigation The system reduces false positives by adjusting threshold values The system helps allocate resources efficiently for fraud prevention purposes The system combines risk scoring with explanation capabilities to provide decision makers both precise results and understandable decision-making processes which enable them to comprehend and use system outputs.

4. METHODOLOGY

4.1 Dataset Description and Data Preprocessing

The IEEE-CIS Fraud Detection Dataset serves as the foundation for this study which investigates financial fraud detection through its extensive real-world dataset. The dataset consists of anonymized transactional records containing both numerical and categorical variables, along with a binary target variable (isFraud) indicating whether a transaction is fraudulent. The dataset poses a major challenge because it contains extremely unbalanced classes which show that only a small fraction of total observations include fraudulent transactions, thus making the dataset appropriate for testing advanced methods which handle imbalanced data. The data preprocessing steps create uniformity between different data types to make them suitable for model development. The process starts with the removal of identifier columns which include TransactionID because they create a risk of data leakage. The target variable is separated from the feature set, and training and test datasets are aligned to ensure consistent feature spaces. The dataset structure remains intact because missing values are handled through constant imputation (-999), which prevents bias from statistical imputation methods in features that show extreme sparsity. Label encoding transforms categorical variables into numerical format, which enables machine learning algorithms to process the data. This transformation enables models to process high-dimensional categorical features effectively while maintaining computational efficiency.

4.2 Model Development, Imbalanced Learning, and Training Strategy

The classification problem requires the development and assessment of three machine learning algorithms which include Logistic Regression and Random Forest and XGBoost. The selected models demonstrate both linear and non-linear learning capacities which enable researchers to assess their prediction accuracy through direct performance tests. The dataset contains significant class imbalance which requires the training data to use Synthetic Minority Oversampling Technique (SMOTE) for processing. The minority (fraud) class receives synthetic samples from SMOTE which creates new instances by combining existing ones, thus helping the model develop better understanding of actual fraud patterns while decreasing its tendency to favor the majority group according to Chawla et al. 2002. The dataset is divided into training and validation sets through an 80/20 stratified split which maintains equal class distribution throughout both sets. This process establishes a testing method which ensures that all system functions will be evaluated without any external influence. The XGBoost algorithm uses scale_pos_weight to implement class weighting which helps to mitigate training difficulties caused by data imbalance. The training approach receives its major improvement through threshold optimization. The process tests different thresholds to find the best one which generates the highest F1-score instead of using the standard probability threshold which equals 0.5. The system achieves better precise assessment of test results which helps to detect fraud because all test results need to receive exact judgment.

4.3 Evaluation and Explainability Framework

The model testing process uses five different classification metrics which measure model accuracy and precision and recall and F1-score and Area Under the Receiver Operating Characteristic Curve (AUC) to determine model performance. The dataset exhibits an imbalanced distribution, so our evaluation process will prioritize recall and F1-score and AUC, which better demonstrate the model's capacity to identify fraudulent activities. The research team conducts feature importance analysis through tree-based model outputs to increase their model interpretability and transparency. The SHAP framework delivers explainability which enables both global and local understanding of how the model generates predictions. SHAP values show how much each feature impacts particular predictions, which helps to explain why certain transactions get marked as fraudulent or legitimate. The explainability layer establishes essential standards for financial markets because these markets require complete transparency combined with total accountability and dependable systems. The proposed framework ensures its high accuracy through its ability to create interpretable results, which make it usable in essential infrastructure systems.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Results and Discussion

5.1 Model Performance Comparison

The performance of the implemented machine learning models was evaluated using accuracy, precision, recall, F1-score, and Area Under the Curve (AUC). The results demonstrate that ensemble-based models outperform the baseline Logistic Regression model, particularly in detecting fraudulent transactions within an imbalanced dataset.

Among all models, XGBoost achieves the best overall performance, exhibiting superior F1-score and AUC. This indicates its effectiveness in capturing complex non-linear relationships and distinguishing between fraudulent and legitimate transactions. Random Forest also performs competitively, while Logistic Regression shows comparatively lower performance due to its linear nature.

The application of SMOTE and threshold optimization further enhances model sensitivity, particularly improving recall and F1-score, which are critical metrics in fraud detection tasks.

5.2 ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve illustrates the trade-off between the true positive rate (TPR) and false positive rate (FPR) across different classification thresholds.

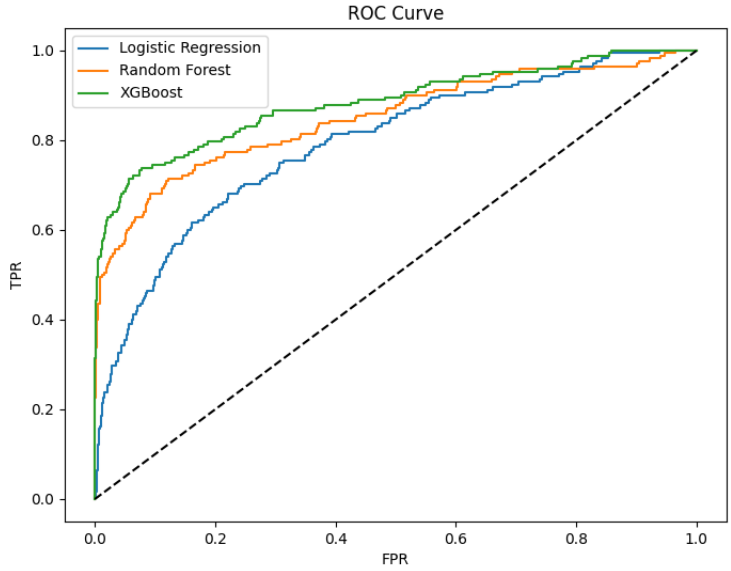

Figure 1: ROC Curve Comparison

ROC curve clearly shows:

- XGBoost (green line) dominates across most thresholds
- Random Forest (orange) performs moderately well
- Logistic Regression (blue) lags behind

The ROC curves demonstrate that XGBoost consistently achieves higher true positive rates at lower false positive rates compared to the other models. This is reflected in its higher AUC score, confirming its superior discriminative capability. The results highlight the advantage of gradient boosting methods in handling complex and imbalanced financial datasets.

The Receiver Operating Characteristic (ROC) curve was used to assess the relationship between true positive rate and false positive rate at various classification thresholds. The Area Under the Curve (AUC) provides a summary measure of model discrimination capability. The results show that all models achieve strong separability between fraudulent and non-fraudulent transactions. The AUC results show that XGBoost performs better than all other models because it can better distinguish between the two classes. The system proves its effectiveness as the most dependable fraud detection model in the proposed framework which operates on imbalanced financial datasets.

5.3 Feature Importance Analysis

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

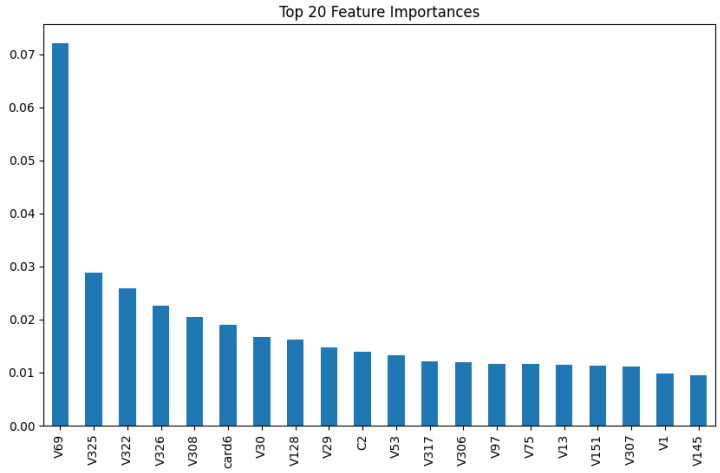

Figure 2: Top 20 Feature Importances

feature importance plot reveals a very important insight:

- Feature V69 dominates significantly
- Followed by V325, V322, V326, etc.
- Long tail of moderately important variables

The feature importance analysis indicates that a small subset of features contributes significantly to the prediction of fraudulent transactions. In particular, feature *V69* exhibits a disproportionately high importance score, suggesting that it captures critical transaction behavior patterns associated with fraud. The presence of several other influential features (e.g., V325, V322, V326) further indicates that fraud detection relies on a combination of key transactional attributes rather than a single variable.

This concentration of importance highlights the effectiveness of tree-based models in identifying high-impact predictors within high-dimensional datasets.

5.4 Explainability and SHAP Analysis

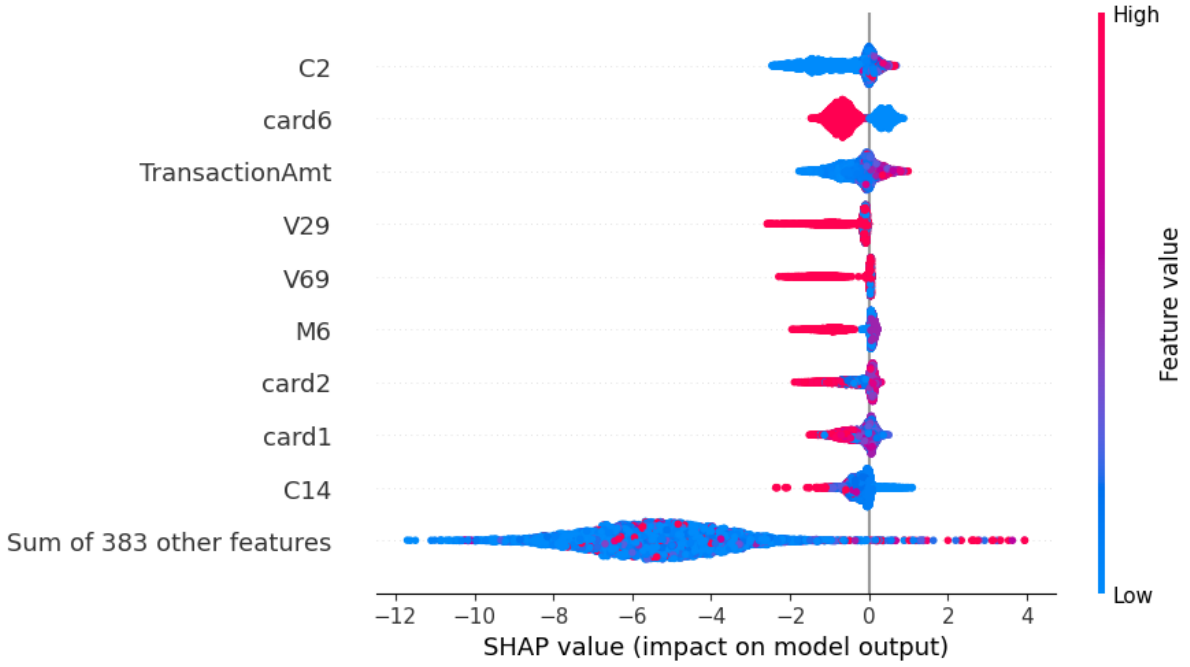

Figure 3: SHAP Summary Plot

The SHAP summary plot provides both global and local interpretability of model predictions. The results indicate that features such as *C2*, *card6*, and *TransactionAmt* have a strong influence on fraud classification outcomes. High

SHAP values correspond to features that significantly increase the likelihood of a transaction being classified as fraudulent.

Additionally, the distribution of SHAP values reveals that fraud detection is driven by complex interactions among multiple features rather than isolated variables. This reinforces the importance of using advanced machine learning models capable of capturing non-linear relationships.

From an operational perspective, SHAP enhances transparency by explaining individual predictions, thereby enabling analysts to understand the reasoning behind flagged transactions. This is particularly critical in financial and critical infrastructure systems, where interpretability is essential for trust, compliance, and decision-making.

5.5 Discussion of Findings

The experimental results demonstrate that machine learning models, particularly gradient boosting techniques, are highly effective for fraud detection in imbalanced financial datasets. The superior performance of XGBoost highlights its ability to model complex patterns and handle skewed class distributions.

The integration of SMOTE significantly improves the model's ability to detect fraudulent transactions, while threshold optimization enhances the balance between precision and recall. These techniques collectively contribute to a more robust and reliable detection system.

Furthermore, the explainability analysis using SHAP provides valuable insights into model behavior, addressing one of the major limitations of black-box machine learning systems. By combining predictive accuracy with interpretability, the proposed framework offers a practical solution for real-world deployment.

Importantly, while this study focuses on financial transaction data, the framework is designed to be extensible to broader critical infrastructure systems. The ability to integrate anomaly detection and cyber-related signals positions the framework as a unified solution for identifying both financial and cyber threats in modern payment networks.

6. CONCLUSION AND FUTURE WORK

This study presented an AI-driven and explainable framework for detecting fraudulent and cyber-related risks in critical infrastructure payment networks. Using real-world transactional data from the IEEE-CIS Fraud Detection Dataset, the proposed approach integrates machine learning models, imbalanced learning techniques, threshold optimization, and explainability to improve fraud detection performance. Experimental results demonstrate that ensemble methods, particularly XGBoost, achieve superior performance across key evaluation metrics, while explainability through SHAP enhances transparency and trust in model decisions.

The findings highlight the effectiveness of combining predictive accuracy with interpretability in high-stakes environments. The proposed framework not only improves fraud detection but also provides a foundation for integrating cyber-related risk signals, supporting the security and resilience of critical infrastructure systems.

Future work will focus on extending the framework by incorporating cybersecurity datasets, graph-based learning methods for detecting coordinated attacks, and real-time streaming architectures for operational deployment. These enhancements will further strengthen the framework's ability to address evolving threats in modern digital payment ecosystems.

REFERENCES

[1] Böhme, R., & Moore, T. (2012). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 5*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2012.10.003

[2] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research, 16*, 321–357. https://doi.org/10.1613/jair.953

[3] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794). https://doi.org/10.1145/2939672.2939785

[4] Conti, M., Lal, C., Mohammadi, M. S., Rawat, D. B., & Rodrigues, J. J. P. C. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Research Article

[5] Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. In *2015 IEEE Symposium Series on Computational Intelligence* (pp. 159–166). https://doi.org/10.1109/SSCI.2015.33

[6] Erebi, D. O., Ladzro, B. K., Amoran, S. O., & Okolie, A. (2024). Explainable artificial intelligence for financial crime prevention: Translating machine learning outputs into regulatory and compliance decision-making. Journal of Frontiers in Multidisciplinary Research. https://doi.org/10.54660/.IJFMR.2024.5.2.148-153

[7] Fesobi, B. O., Fesobi, M. A., & Ogungbeje, O. (2024). Implementing agile supply chain strategy for improved response to market volatility: A systematic literature review. https://doi.org/10.46932/sfjdv5n12-057

[8] Fesobi, B. O., Ogungbeje, O., & Fesobi, M. A. (2024). Leveraging AI and BDA for enhanced supply chain. visibility and resilience in the US: A systematic literature review. https://doi.org/10.46932/sfjdv5n12-058

[9] Fesobi, M. A., & Fesobi, B. O. (2026). A conceptual framework for AI maturity assessment in technology supply chain. *Journal of Information Systems Engineering and Management, 11*(3s). https://jisem-journal.com/index.php/journal/article/view/14665

[10] Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems* (Vol. 30).

[11] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

[12] Okolie, A., Alumona, P., Lawal, O., & Olukoya, D. (2026). A unified explainable machine learning framework for fraud detection across payment and cryptocurrency transaction systems. Journal of Computational Analysis and Applications, 35(1)[12]Okolie, A., Oibiyeye, S., Ibiyeye, A. O., & Olukoya, D. (2026). A risk-based security governance framework for modern information systems. Journal of Computational Analysis and Applications, 35(1).

[13] Lawal, O., Alumona, P., Okolie, A., Obunadike, C., Ikhifa, M. O., & Edozie, S. I. (2025). An explainable XGBoost framework for detecting fraudulent financial transactions. Journal of Scientific Research and Reports. https://doi.org/10.9734/jsrr/2025/v31i123769[14]Lawal, O., Okolie, A., & Obunadike, C. (2025). An explainable graph neural network framework for anti-money laundering in cryptocurrency transactions using the elliptic dataset. International Journal of Network Security & Its Applications, 17(6). https://doi.org/10.5121/ijnsa.2025.17602

[14] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review, 34*(1), 1–14. https://doi.org/10.1007/s10462-009-9119-y