International Insurance Law Review
ISSN: 0968-2090
Vol 33 S4 (2025): Special Issue
https://lumarpub.com/iilr

Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer

Dr. K Devi [1]*, Prof. Bhuvan Unhelkar [2], Prof Siva Shanker S [3]
[1]Postdoc Research Scholar, Muma College of Business, University of South Florida, Tampa, Florida, USA
[2]Professor, Muma College of Business, University of South Florida, Tampa, Florida, USA
[3]KGRCET, Hyderabad, India
Email: [1]deviindoria6666@gmail.com; [2]bunhelkar@usf.edu; [3]drsivashankars@gmail.com
Orcid: [1]https://orcid.org/0009-0003-2364-647X; [2]https://orcid.org/0000-0003-1118-3837; [3]https://orcid.org/0000-0002-7616-6088
*Corresponding Author: Dr. K Devi

Abstract
Credit card fraud significantly burdens financially secure environments, with most of the traditional detection systems lacking in accuracy and interpretability. Current designs regarding the credit card fraud detection system often fail to encapsulate the intricate and hidden fraud patterns. This study investigates the role of deep learning networks in fraud detection with emphasis on class imbalance. A hybrid bidirectional spiking Graphormer module is implemented for spotting credit card remittance scams, and its performance is estimated on recall, accuracy, F1-score, precision, and Area under Curve (AUC). The comparative performance of the module is further tested over various cross validated class imbalance methods. The dataset amounts to 1,284,020 remittance records, of which 96,210 are deemed fraudulent, while 1,187,810 are legitimate transactions. Given the presence of multiple outliers, the local outlier factor is employed during the pre-processing stage to ensure the detection and removal of anomalous data points. The proposed module exhibits high predictive accuracy, achieving a performance rate of 99.25% when validated on external datasets. Results show that the combination of deep-learning-based scam spotting approaches, incorporating Explainable Artificial Intelligence (XAI) against the challenging domain of fraud detection. The Residual Network (ResNet) in an ensemble setting showed excellent performance, reaching a cross-validation score of 0.9912 against several other models. As a result, fraud detection becomes more competent than before for anomalous credit card remittances.

Keywords: Credit Card Fraud, Anomalous Remittances, Deep Learning, Class Imbalance, Hybrid Module, Sampling Techniques, Imbalance Methods

1. Introduction

Cyber credit card fraud, is unauthorized access to sensitive credit card details for illegal purchases or theft of funds [1], is one of the most prominent threats in the world of electronic payment systems. About a hundred labeled documents are collected for French and Italian consumers, and 1,000–2,000 labeled documents for Russian are gathered and validated to accurately detect more prevalent sophisticated hacking tools in Russian platforms [2]. Apart from the loss to individuals,

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

online transactions also expose financial systems within and between organizations. Malware, ransomware [xx list a few] are used to steal personal and financial data with increasing speed and accuracy. This study reports on an advanced, adaptive, and efficient fraud detection mechanism related to credit card based digital transactions. Existing methods of credit-card cyber fraud detection rely on static rule sets, analysing transactional patterns, user behavior, and so they cannot keep pace with the increasingly dynamic and complicated techniques used by cybercriminals [3,4]. Current existing systems, such as decision tree classifiers, logistic regression models, and rule-based filters, are primarily static rule-based or conventional algorithmic learning approaches that cannot adapt to pattern changes in fraud and are computationally inefficient at processing remittance data on a large scale [5,6]. Their inability to operate in real-time limits their capacity to prevent fraudulent transactions before they are processed [7]. Hence, traditional models rely heavily on past trends, lack adaptability, and are poor in their generalization ability since most of them are unable to detect some new or subtle kinds of scams, such as synthetic identity fraud, account takeover, card testing, and low-value transactional fraud that differ from historical data.

Deep Learning (DL) approaches are used in complicated classification tasks as they have excellent pattern recognition and large-scale data handling capabilities [8]. However, DL performance is immutably affected by class imbalance, where under-representation of certain classes leads to inaccurate predictions [9]. Handling class imbalance in fraud detection requires deeper intelligence that can produce high accuracy and crucial practical specifications [10]. Real-time processing is imperative for faster fraud detection. Balancing accuracy, efficiency, and adaptability is critical for deploying deep learning solutions in fraud prevention, are performance together with trustworthiness matter most [11,12].

This research proposes an optimized deep-learning-based scam spotting framework incorporating Explainable AI (XAI) to support real-time fraud detection. This framework employs graph-based anomaly detection, transformer-based modules, and hybrid deep-learning configurations. Validation of our framework uses training and testing data collected from various credit card scam datasets from Credit Card Fraud Detection (CCFD), CCFD 2023, and Credit Card Fraud in the Western US.

The class imbalance problem in this research is tackled by, Range-controlled Expandable Borderline Geometric SMOTE (REBG-SMOTE) method is developed. REBG-SMOTE oversampling technique improves the minority class instances by generating some synthetic samples along controlled decision boundaries for better classification and understanding between the legitimate and fraudulent classifiers. Adaptive Binary Swordfish Movement Optimization Algorithm (ABSMOA), SHapley Additive exPlanations (SHAP), Tensor Run Time with Open Neural Network Exchange (TensorRT-ONNX), and Apache Kafka are additional tools integrated in banking and FinTech applications.

The ABSMOA is used in the intelligent hunting by swordfish for feature selection and optimization of the model, effectively simulating the hunting ability of swordfish to explore and exploit the solution space. SHAP is integrated into the framework for interpretability to enable stakeholders to understand and trust model decisions by attributing predictions to specific input features. TensorRT-ONNX is leveraged for high performance in real-time inference, drastically accelerating deep learning model execution in production environments, and Apache Kafka is included for

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

real-time ingestion of data and streaming analytics, ensuring a smooth fit into large-scale banking and FinTech systems.

The Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer (IMSICBEG) is organised as a hybrid model combining deep learning, graph-based relational learning, and spiking neural network principles is evaluated, in this study, for recall, accuracy, F1-score, precision, and AUC. The architecture of our model incorporates spiking neural networks for temporal sensitivity, bidirectional encoding for contextual understanding, graphormer architecture for relational modeling, and imperialist competitive mechanisms for global search optimization. This study is novel in its hybrid approach, combining encoder-based deep learning with class imbalance handling techniques to enhance credit card remittance fraud detection. By organizing the IMSICBEG module and evaluating it through cross-validation, the research offers a robust and adaptable framework. The application of this encoder-driven model is expected to significantly improve the accuracy, reliability, and scalability of real-time digital fraud detection systems. As we demonstrated later in this article, this hybrid model improved detection accuracy and provided advantages of explainability and reliability across various transaction patterns.

Section 1 holds a general introduction about the scam in credit card remittance and the proposal of the research on scam detection by deep learning techniques. Section 2 covers the review of literature and proposed methodology, and the simulation of the modules selected is presented in section 3. The validation and potential of the module are discussed in section 4. Finally, the research is concluded with the future scope in section 5.

2. Literature Review

Chugh., et al. (2025) [13] utilised the techniques of stratified sampling and k-fold cross-validation to overcome the problems of data imbalance and overfitting. Optimal selection of data reduces overfitting risks and improves performance.

Ayoub., et al. (2025) [14] proposed the use of a granular computing framework to elevate the credit card fraud detection efficiency. It integrates Case-Based Reasoning (CBR) with hybrid sampling for dealing with the difficult part of missing variables to upgrade the functioning of the model.

Xiang., et al. (2025) [15] proposed a Risk-aware Gated Temporal Attention Network (RGTAN), which consists of a Gated Temporal Graph Attention (GTGA) mechanism for message propagation among nodes and the adaptive learning of remittance representations. Their experimental results showed the efficacy of approach to arrive at complex real-world fraud patterns. [How? – add a sentence]

Tayebi., et al. (2025) [16] exploited the potentialities of deep learning strategies to explore abnormal remittances. Various experiments were conducted and revealed significant outcomes in spotting abnormal remittances and highlighting the dominance of the Autoencoder Support Vector Machine (ASVM) model over competing models.

Chatterjee., et al. (2024) [17] presented a dynamic strategy for identifying known and emerging fraud patterns effectively. Blockchain-enabled Federated Learning (BFL) implies improved credit card fraud prevention and room for constant improvement for financial security.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Charizanos., et al. (2024) [18] developed a booted fuzzy logic regression model that addresses class imbalance and separation problems. The analysis of the performance versus efficiency nexus revealed that the proposed framework shows strong performance results with specificity and greater sensitivity.
Sorour., et al. (2024) [19] introduced Brown Bear Optimization (BBO) algorithm, and improved the identification accuracy of financial credit card scam remittances. The BBO algorithm indeed balanced the trade-off between dimensionality reduction and improvement in classification accuracy.
Tang., et al. (2024) [20] proposed a credit card scam detection based on federated graph learning, and this organized framework facilitates the joint training of the models by coordinating multiple financial institutions while ensuring data security.
Cherif., et al. (2024) [21] developed an encoder–decoder–based GNN that effectively captures the complex relationships and dependencies within credit card remittance data. The performance of the model is further enhanced by employing a graph converter for the efficient processing of graph data and batch normalization to reduce internal covariate shift and improve convergence.
Mim., et al. (2024) [22] proposed a soft-voting approach that outperforms individual classifiers with a False Negative Rate (FNR) of 0.0306, it achieves a precision of 0.9870, and recall of 0.9694.

2.1 Problem Statement

Credit card scam identification relies on a fast, accurate, and interpretable solution in real-time edge environments where computation is restrained. Historic techniques, such as rule-based systems, reveal their failures in speed, scalability, and transparency. To solve that, this research proposed developing a real-time fraud detection system based on an IMSICBEG. It is a hybrid of Spiking Neural Network (SNN), relational graph learning, and evolutionary optimization for accurate and human-understandable fraud detection, and optimization for efficient edge deployment.

2.2 Contribution

This proposed real-time edge-deployment based cyber credit card fraud detection system (IMSICBEG) provides speed, accuracy, interpretability, and computational efficiency in fraud detection. The real-time detection at minimum latency for high-throughput environments makes our model's aspect ratio suitable for edge deployment. The model's interpretability allows transparent insight into the decision-making process, thereby lending itself to trust and compliance applications in sensitive financial domains.

2.3 Objectives

The objectives of the research are,

- To organise a hybrid IMSICBEG module to improve the detection of credit card remittance scams.
- To evaluate the recall, accuracy, F1-score, and precision of the organised modules to determine their effectiveness in identifying credit card remittance fraud.
- To determine the AUC curve by the class imbalance method to enable a more accurate evaluation of fraud detection performance.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

- To compare the effectiveness of the IMSICBEG module over different class imbalance approaches by Cross Validation (CV) to explore the overall impact and robustness of the proposed model.

3. Proposed Methodology for Spotting Credit Card Scams

Credit card scam detection using the proposed hybrid IMSICBEG module is depicted in Figure 1. Initially, the data collected is processed, and the samples are filtered from the collection. Then, a deep learning optimization technique is framed to process the data rapidly and more accurately. The recall, accuracy, F1-score, precision, and AUC of the organised modules are evaluated using deep-learning-based scam spotting approaches based on undersampling and oversampling, together with the incorporation of XAI. Finally, normal and fraudulent remittances are evaluated.

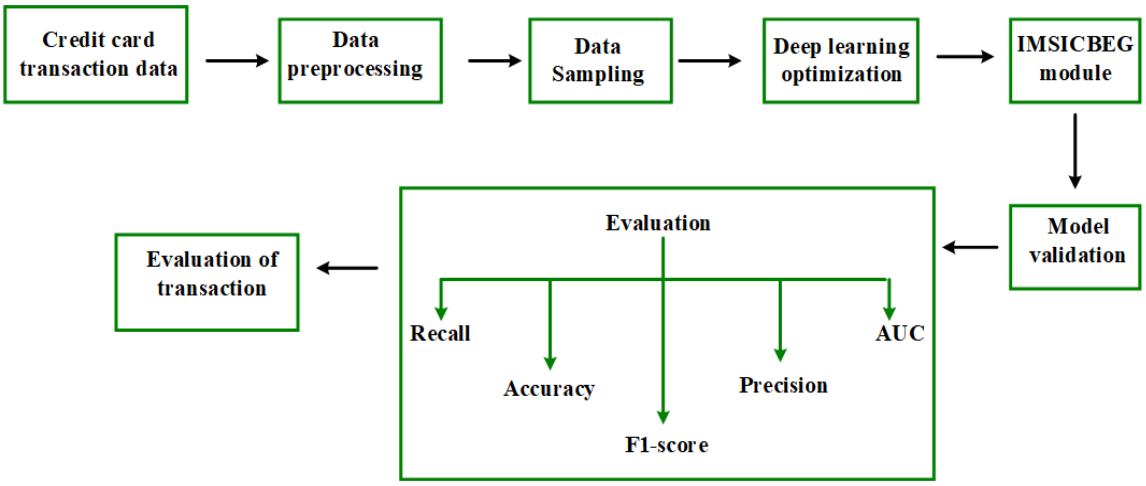


Figure 1: Proposed methodology for credit card scam detection

3.1 Explainable Artificial Intelligence Integration

Explainable AI (XAI) is typically classified within a four-dimensional hierarchical structure: data explanation, model explanation, post-hoc explanation, and explanation assessment [23, 24]. Data explainability involves understanding the datasets used to train deep learning models, while model explainability refers to creating models that are inherently interpretable and transparent [25]. Post-hoc explainability pertains to understanding trained models after the fact, providing human-understandable reasons for specific predictions. Finally, the explanation assessment focuses on the indicators of relevance and quality of these interpretations. In high-stakes areas like financial remittances, interpretability becomes essential. Such decisions carry serious real-life consequences, making it imperative to base them on clear reasoning. XAI effectively addresses the significant gap between abstract, inscrutable AI systems and society's demands for transparency and accountability [26]. The architecture of XAI techniques is displayed in Figure 2.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

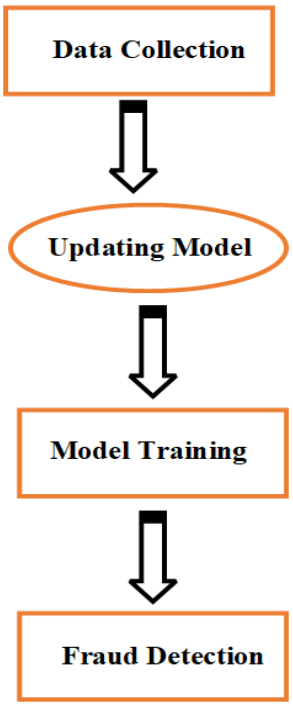


Figure 2: Architecture of XAI techniques for credit card scam detection

3.2 Range Controlled Expandable Borderline Geometric SMOTE

This technique is an upgraded section of SMOTE that encloses the oversampling of the minority class [27]. The block diagram for the REBG-SMOTE module is depicted in Figure 3. REBG-SMOTE is expressed as,

$$Z_{new} = Z_a + \lambda(Z_a - Z_b) \quad (1)$$

Where, λ is a random number between 0 and 1. Z_a is the minority class instance and Z_b is the nearest neighbour.

3.3 Adaptive Binary Swordfish Movement Optimization Algorithm

The BSMOA uses synchronization and agile movements in swordfish. These aquatic predators demonstrate collective behaviors characterized by speed, precision, and adaptability, allowing them to effectively penetrate and exploit dynamically changing environments in search of resources. Such behaviors are sought by metaheuristic optimizations, i.e., effective exploration and exploitation of complex search spaces to arrive at optimal solutions. The BSMOA interprets the dynamic and adaptive foraging strategy of swordfish into a strong optimization framework for binary and combinatorial problem handling.

BSMOA simulates swordfish's broad search behavior, which generates diverse solutions in the exploration phase ($\vec{A}_{(a+1)}$) expressed as,

$$\vec{A}_{(a+1)} = \vec{A}_{(a)} \times \left(\frac{Z.b^{\Theta}}{\sin\Theta} \right) + \left(X.\vec{A}_{(a)} \right) \quad (2)$$

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Where, $b \in [0,1]$ and $\vec{A}_a$ represent the position of the agent at the iteration a. The dynamic parameter X and Z.

The updated position of the agent ($\vec{B}_{(a+1)}$) is given as,

$$\vec{B}_{(a+1)} = \vec{A}_{(a+1)} + X.\vec{P}_{(a+1)} + (X.Z).\vec{Q}_{(a+1)} \quad (3)$$

Where $\vec{P}_{(a+1)}$ is the velocity update and $\vec{Q}_{(a+1)}$ is the collective adjustment.

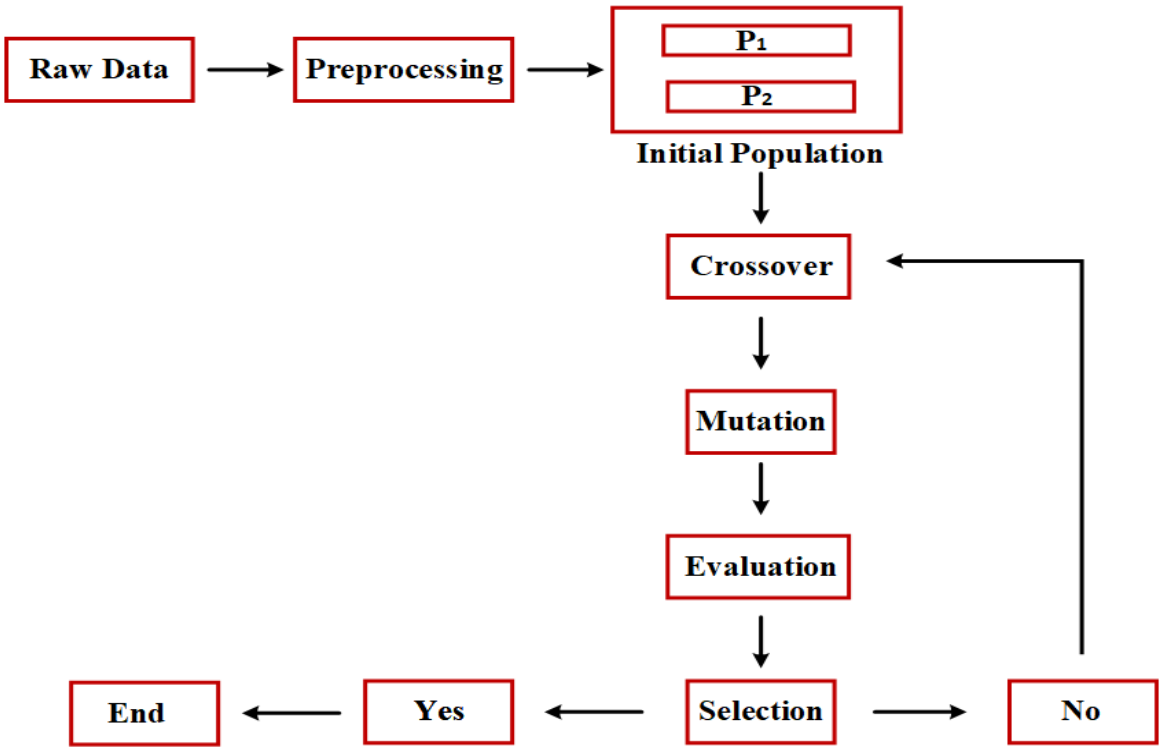


Figure 3: Block diagram for the REBG-SMOTE module

3.4 Shapley Additive Explanations

The SHAP values educate a user about an individual prediction made through a algorithmic learning model. SHAP values reveal the most impacted outcome from that model [28]. Then, SHAP values help in understanding the influence of features like remittance time and amount to detect key characteristics of fraud activity [29, 30]. As a result, they provide a reliable result regarding the understanding of model behavior and improvement for future, accurate, and more reliable fraud detection results.

The SHAP value for a feature (a_x) is defined as follows,

$$\phi(a_x) = \sum_{Z \subseteq \{1,2,\ldots Y\} \setminus \{x\}} \frac{|Z|!(Y-|Z|-1)!}{Y!} \left[f_a(Z \cup \{x\} - f_a(Z) \right] \quad (4)$$

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Where Y is the number of stakeholders $Z \subseteq \{1,2,...Y\} \setminus \{x\}$ is the subset of features, Z is the number of elements in the subset x, $f_a(Z)$ is the model output, $f_a(Z \cup \{x\}$ is the marginal contribution of the system.

3.5 Tensor Run Time Loaded Open Neural Network Exchange

The TensorRT optimization technology is tuned for high-performance deep learning inference. The optimization of models is based on Graphics Processing Unit (GPU) memory usage, neural network structures, and precision calibration techniques. Impressive performance gains are achieved with TensorRT, including fraud detection enhancement with real-time inference applications [31,32]. The major advantage of TensorRT is the ability of the user to significantly increase inference speed without sacrificing model accuracy, which is useful in edge computing environments characterized by high throughput demands on real-time data processing [33,34]. The processed data are transported to the Open Neural Network Exchange (ONNX) module for further processing.

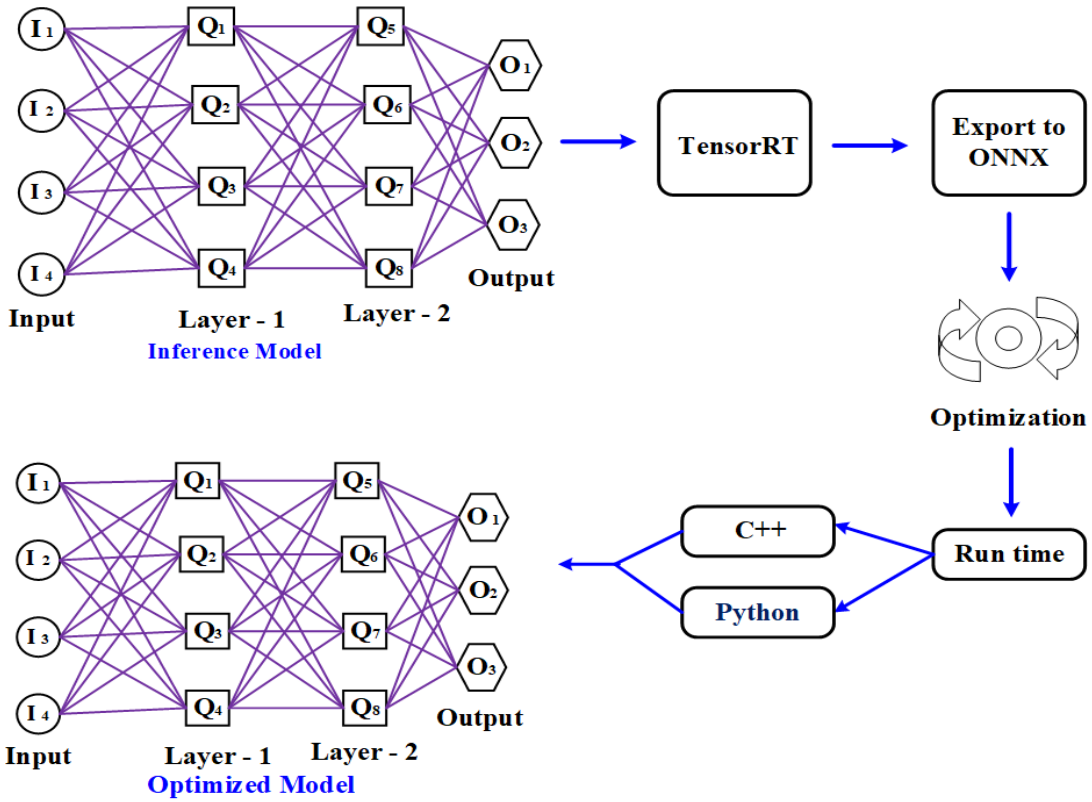


Figure 4: Architectural flow of TensorRT loaded over ONNX module

The ONNX offers a standardized universal format, referred to as a representation in deep learning computational graphs. In addition, it defines a comprehensive range of data types, operations, and attributes to describe the input and output tensors, as well as the internal computations within a model [35,36]. Perhaps the greatest benefit of ONNX is that it enables smooth transfer of

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

models between different frameworks with minimal configuration and without the need to rewrite the model; as a result, ONNX significantly simplifies model optimization and acceleration across various hardware platforms, from GPU to Tensor Processing Unit (TPU), making ONNX powerful for scalable and efficient deployment. The architectural structure of the module is displayed in Figure 4.

3.6 Apache Kafka

Apache Kafka operates in a highly available cluster consisting of multiple machines and data centers, processing records as soon as they are created. With its core components - producers, consumers, streams, and connectors - Kafka is built to enable developers to publish, consume, process, analyze, aggregate, transform, and integrate data. Kafka excels at building real-time streaming data pipelines by allowing event data to be transmitted reliably at great scale between enterprise systems while minimizing risks of loss, corruption, or duplication of the data. Kafka enters into some of the first foundational technologies associated with event-driven architectures, stream processing, and big data analytics.

3.7 Interpretable Multi-relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer (IMSICBEG)

A bidirectional spiking graphormer is designed to tackle the inherent limitations of the transformer in capturing local graph structure. To facilitate modeling the graph topology while preserving local node neighborhoods, a sparse Graph Neural Network (GNN) is introduced. Through a simple yet effective fusion strategy, the spiking Graphormer enhances all pairs of nodal interactions and local neighborhood aggregation, making it competitive with or even superior to the recent SNN-based graph transformer architectures. The diagram for Spike-based graph attention and traditional SNN-based graph attention for bidirectional spiking graphormer is depicted in Figure 5.

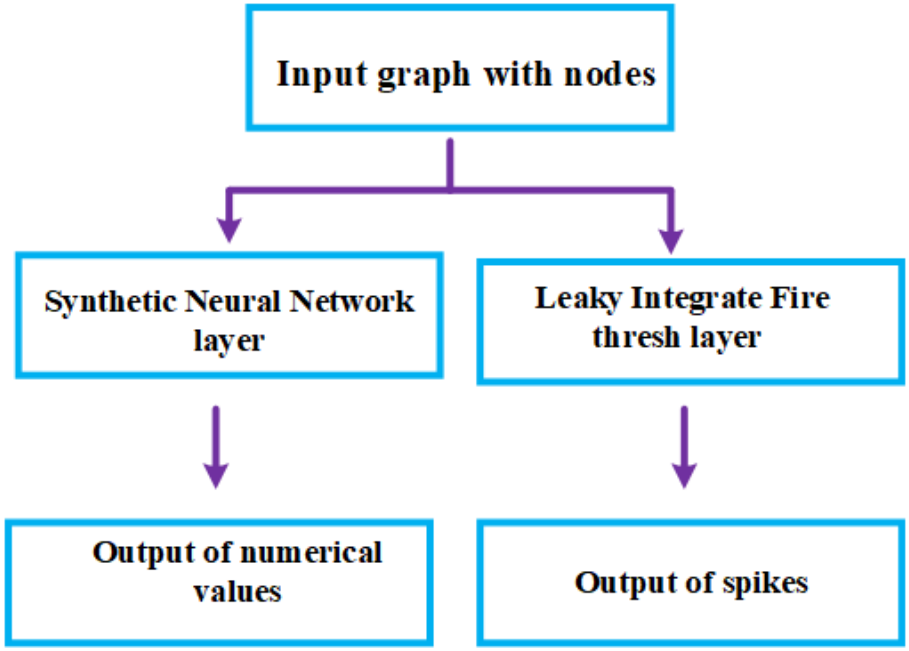


Figure 5: Diagram for Spike-based graph attention and traditional SNN-based graph attention

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

The IMSICBEG employs spiking neuron layers to transform numerical inputs A, B, and C into bidirectional spikes is expressed as,

$$X_0^{'} = IMSICBEG(X_0) \quad (5)$$

$$A = linear_a(IMSICNBEG(X_0^{'})) \quad (6)$$

$$B = linear_b(IMSICNBEG(X_0^{'})) \quad (7)$$

$$C = linear_c(IMSICNBEG(X_0^{'})) \quad (8)$$

where, X_0^1 and X_0 are output and input signals, respectively.

The event-driven and binary-spike properties greatly improve the computational efficiency of the graph transformer and the output is expressed as,

$$Y = (1-\alpha)P_1 + \alpha GNN(Z, L) \quad (9)$$

where Y is the final output, α is the mixing coefficient, P_1 is the future tensor, Z, L are node features and the adjacency matrix.

The structure of the bidirectional spiking graphormer is given in Figure 6. The designed IMSICBEG encoder captures the graph structure and collaborates with spiking graph attention to obtain richer information.

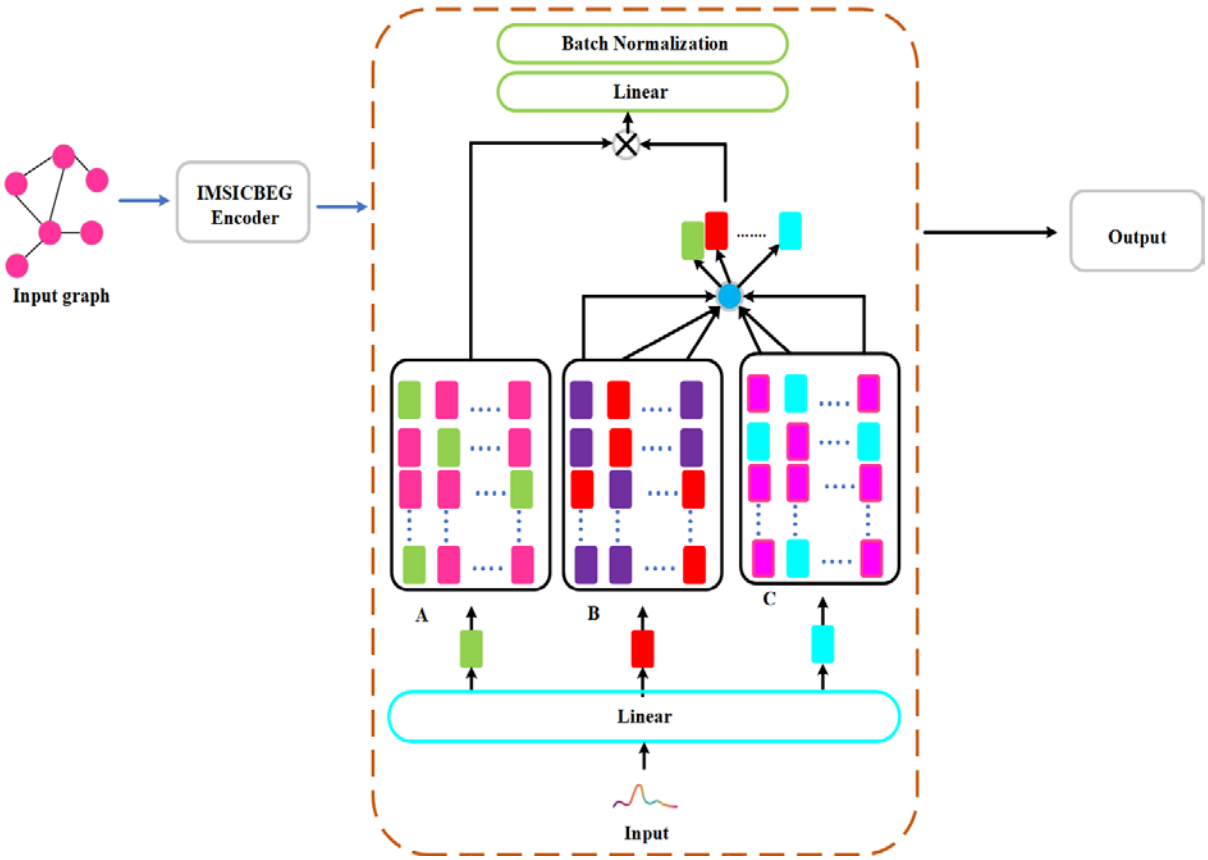


Figure 6: Structure of the bidirectional spiking graphormer

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

The IMSICBEG treats each node within a graph as an individual input token, allowing the model to capture subtle and often neglected relationships within the graph's topology. The model's inherent capacity for the representation and analysis of graph-based data is further strengthened. However, the accumulation of data also increases the graph size, leading to a growing number of nodes and, consequently, a significant rise in computational demand and GPU memory consumption. This scalability challenge limits the use of graph transformers. To address this issue, IMSICBEG, a combined bidirectional spiking graphormer, simplifies the modeling of graph structures and efficiently captures local node neighborhoods. This results in notable advantages in training speed, inference time, and GPU memory efficiency, leading to a resource cost reduction of 10-20 times.

3.8 Performance of Module

To estimate the performance of the IMSICBEG module, the recall, precision, accuracy, F1-score, and AUC curve are evaluated. These terms are expressed as,

$$\mathrm{Re}\,call = \frac{TP}{TP + FN} \tag{10}$$

where FN is the False Negative.

$$\mathrm{Pr}\,ecision = \frac{TP}{TP + FP} \tag{11}$$

where FP is the False positive.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

$$F1 - score = \frac{2 * \mathrm{Re}\,call * precision}{\mathrm{Re}\,call + preicision} \tag{13}$$

3.8.1 Area Under the Curve

It is a method of measuring the potentiality of a classification module. Higher the AUC, maximum is the accuracy of the classification. It is used to determine the ability of a module to differentiate between classes.

3.9 Dataset

The data collection process involves sourcing a comprehensive credit card remittance dataset. The primary information set used in this research is sourced from CCFD, CCFD 2023, and Credit Card Fraud in the Western US. As illustrated in Table 1, the dataset constitutes 1,284,020 remittance records with 96,210 fraudulent and 1,187,810 legitimate transactions; this main dataset is used for the training and evaluation of the model. However, the dataset is imbalanced, making it difficult to effectively detect and model scams, since there is a significantly higher number of legitimate remittances compared to scam ones.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Table 1: Number of legitimate and fraudulent remittances

Remittance Type	**Sum of Remittances**
Legitimate Remittances	11,87,810
Fraudulent Remittances	96,210
Total	12,84,020

3.10 Analysis of the Data Collection

Table 2 summarizes data from the April 2025 survey of 500 participants, including banking professionals, cybersecurity experts, financial analysts, and students specializing in banking resources, on perceptions of advanced stock trading technologies. The research is primarily focused on their idea about the advanced technologies in spotting scam credit card remittances. Majority of respondents showed a lot of confidence in the use of algorithmic learning techniques in the enhancement of accuracy in the scam spotting process. Notably, 215 participants confirmed the effective and reliable real-time remittance data in spotting suspicious activities immediately, which again accentuated the emerging trust towards deep learning systems in financial security.

Table 2: Analysis of data collection from April 2025 survey of 500 participants

S. No	**Survey Question**	**Sum of Positive Responses**	**Sum of Negative Responses**	**Total Responses**
1	How confident are you in the ability of algorithmic learning to detect fraudulent credit card remittances?	410	90	500
2	Do you believe real-time remittance monitoring significantly reduces credit card fraud?	348	152	500
3	Do you consider deep learning innovations the most effective technique for fraud detection?	395	105	500
4	How reliable do you find real-time financial data for identifying suspicious activity?	255	245	500
5	What is your level of concern about false positives in deep learning-based scam spotting systems?	378	122	500
6	Do you believe deep learning-based scam spotting systems should be fully automated or human-supervised?	288	212	500
7	How likely are you to support the integration of advanced scam spotting systems in the financial institutions you use?	441	59	500

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Total Participants: 500 **Approximate Positive Responses**: 215–260 per question **Survey Method**: Online questionnaire (Google Forms) **Respondent Profile**: banking professionals, cybersecurity experts, financial analysts, and students specializing in banking resources **Time of Data Collection**: April 2025

The survey data collected from 500 respondents offers a diverse and representative sample for analysing key aspects of credit fraud detection practices. This group included a mix of banking professionals, police, cybersecurity experts, financial analysts, and banking students, bringing a broad range of industry and academic perspectives. Since all questions received around 215-260 positive responses, it reflects consistent engagement and alignment on important issues such as algorithmic learning, deep learning, real-time monitoring, and system reliability. Consequently, the dataset is considered reliable and valid for initial analysis and hypothesis development regarding credit fraud detection trends and technology adoption.

4. Results and Discussion

In this section, various parameters and results of the experiments performed in this research in the form of tables and graphs are presented.

4.1 Outlier Analysis Using Boxplot

As the information set contains several outliers, outlier detection and removal are performed as a pre-processing step. Figure 7 shows box plots for all features. There are several points outside the lower and upper whiskers. These points are anomalies and are considered outliers.

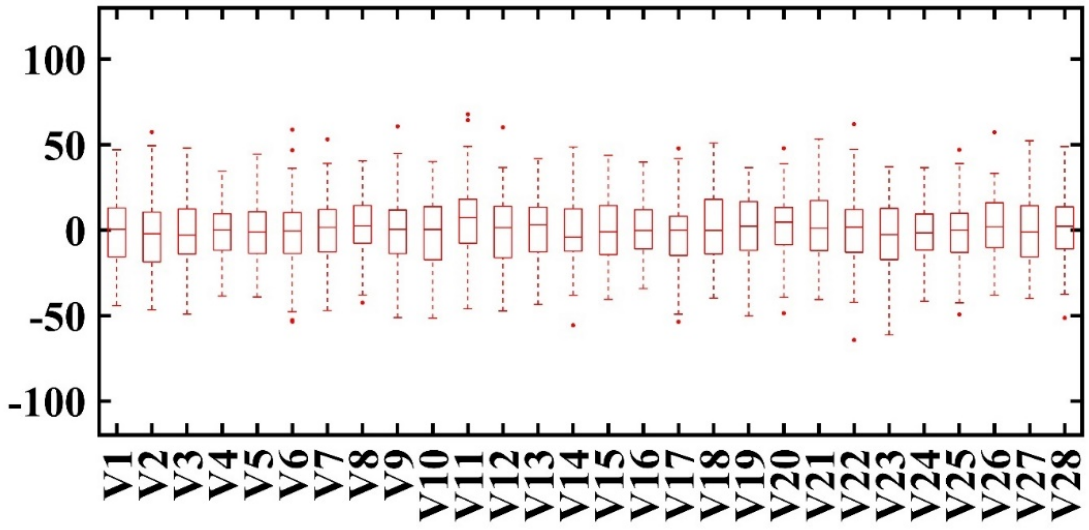


Figure 7: Outliers in the dataset

Even though it does really well in calculating the performance of classification models, it will actually send an outlier removal strategy called local outlier factor, by which the influence of these outliers is minimized. The result is shown in Figure 8, and the resultant dataset is pretty smooth, which is used further.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

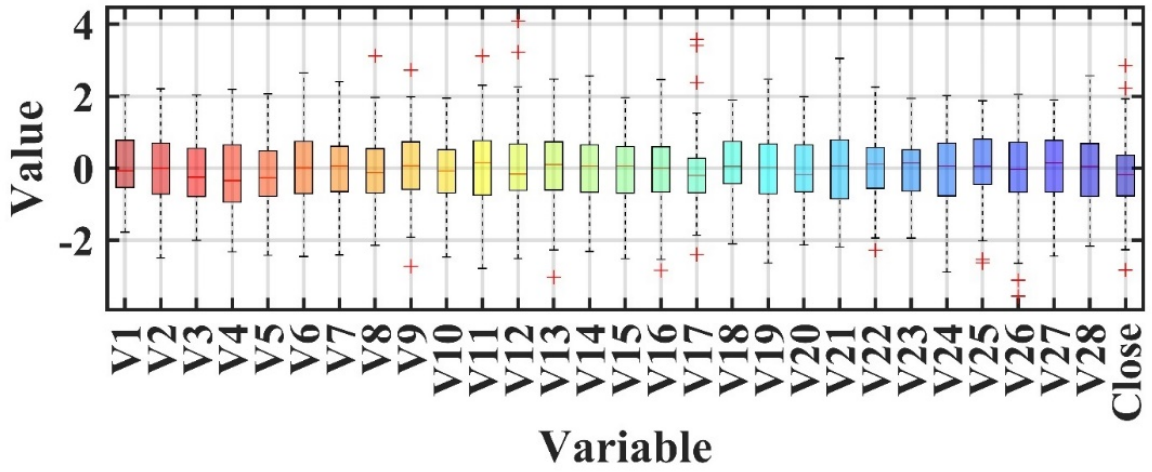
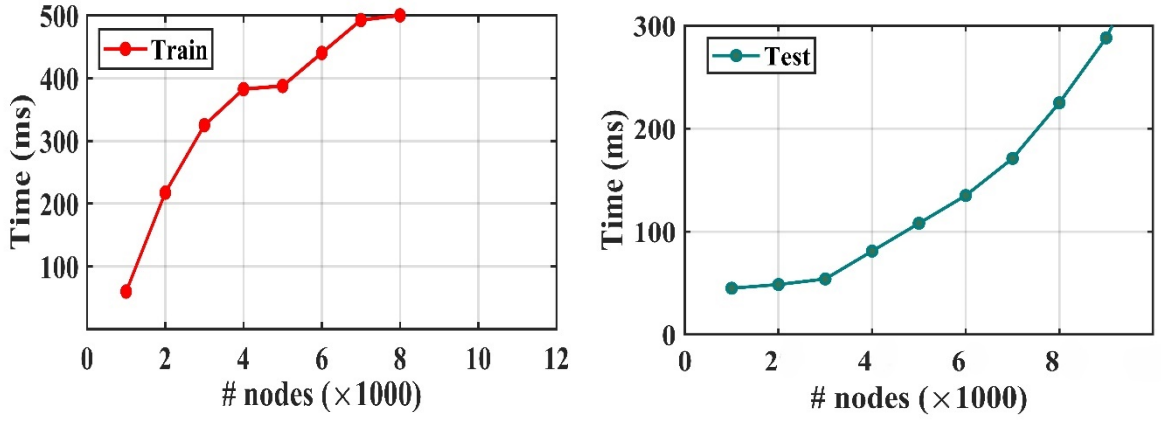


Figure 8: Outliers removed from the dataset

4.2 Efficiency of IMSICBEG Module

The efficiency of the IMSICBEG module for training and testing under different numbers of nodes with variation in time is displayed in Figure 9. The linear increase in the complexity built up by the bidirectional spiking graphormer reflected the computing efficiency of the IMSICBEG module. The module maintained a linear growth range with an increase in the number of nodes, and this confirmed the improved performance of the module with low consumption of time, subsequently leading to the usage of low GPU memory with better computing efficiency. Moreover, the variation in time for assessing the data for training and testing is nearly almost, and this indicates its better generalisation on larger graphs.



(a) (b)

Figure 9: Efficiency of IMSICBEG module over (a) Training and (b) Testing data

4.3 Evaluation of Parameters

The recall, precision, F1-score, and accuracy for the IMSICBEG module for different class imbalance methods are presented in Table 3. The highest test accuracy, recall, F1-score, and precision of the IMSICBEG module reveal the superior performance, which makes it highly effective for fraud detection.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Table 3: Validation of parameters for the IMSICBEG module

Parameters	**Validity**
Recall	99.78%
Precision	98.69%
Accuracy	99.25%
F1-score	99.87

4.4 AUC by Class Imbalance Method

The AUC curve for IMSICBEG modules over different class imbalance approaches is displayed in Figure 10. It is observed that the AUC curve for IMSICBEG modules covered a huge area, and this signifies the suitability of the module in spotting scam transactions in credit card remittances.

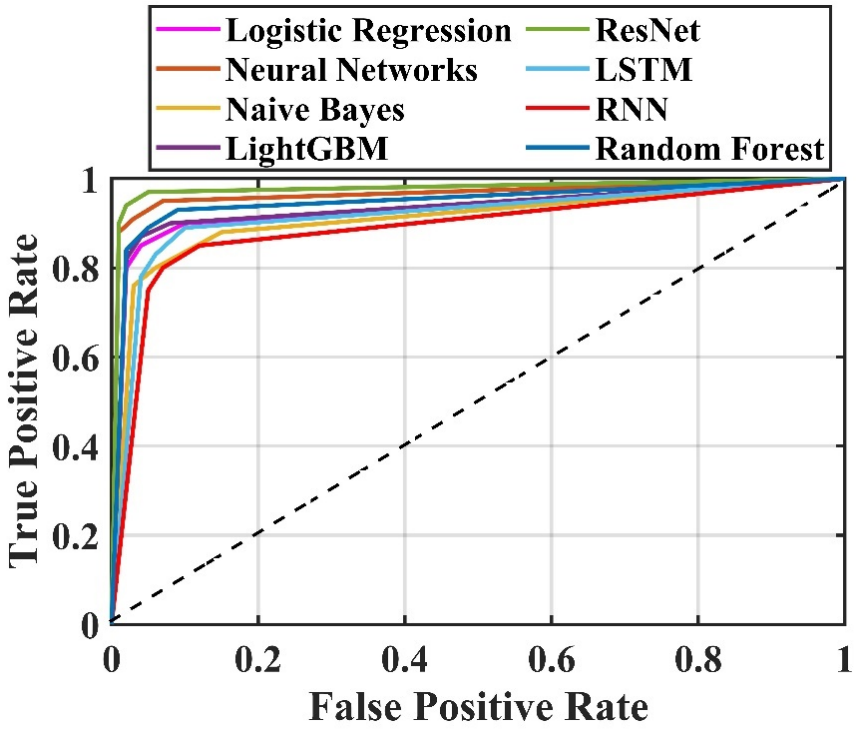


Figure 10: AUC of IMSICBEG

When compared with Logistic Regression, Neural Networks, Naive Bayes, Light Gradient Boosting Machine (LightGBM), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Random Forest, and the ResNet model, when combined with the IMSICBEG module, performs well as it obtains one of the highest true positive rates over almost all ranges of false positive rates. This means that the IMSICBEG module significantly enhances the discrimination power of ResNet towards identifying fraudulent remittances while holding the false positive rate at a reasonably low level.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Table: Approximate true positive rate at a selected false positive rate

Model	**False positive rate**				
	0.2	**0.4**	**0.6**	**0.8**	**1**
Logistic Regression	0.92	0.94	0.95	0.96	0.97
Neural Networks	0.93	0.95	0.96	0.97	0.98
Naive Bayes	0.88	0.89	0.90	0.91	0.92
LightGBM	0.94	0.96	0.97	0.98	0.99
ResNet	0.96	0.97	0.98	0.99	1
LSTM	0.92	0.94	0.96	0.97	0.98
RNN	0.85	0.88	0.90	0.91	0.92
Random Forest	0.95	0.96	0.97	0.98	0.99

The approximate true positive rate at a selected false positive rate is illustrated in Table. Thus, ResNet demonstrates consistent and robust performance in strong support of IMSICBEG, making it best for the detection of anomalous credit card remittances.

4.5 Performance Comparison by Cross Validation

The capability of classifiers such as Logistic Regression, Neural Networks, Naive Bayes, LightGBM, ResNet, LSTM, RNN, and Random Forest in conjunction with class imbalance methods in terms of various modules such as XAI, REBG-SMOTE, ABSMOA, SHAP, TensorRT with ONNX, Apache Kafka, and IMSICBEG are analysed. The CV value furnished by XAI classifier for different class imbalance methods is presented in Table 4.

Table 4: CV for XAI

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
XAI	0.8416	0.9478	0.9247	0.8954	0.9717	0.9684	0.9458	0.9678

The graphical representation of a boxplot, assembling CV results for the XAI module, is displayed in Figure 11. Each box depicts the distribution of accuracy scores across CV folds, showing the variability in the performance of the classifiers. It is observed that ResNet has the highest median accuracy, and Logistic regression and Naive Bayes perform well too, but there is more variance.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

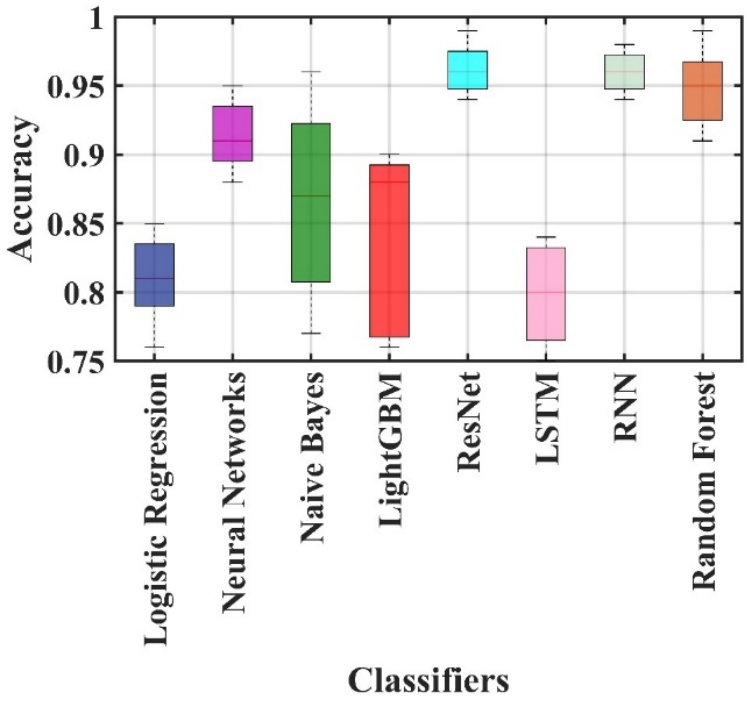


Figure 11: CV on XAI

The CV explored by the REBG-SMOTE module for different class imbalance methods is presented in Table 5.

Table 5: CV for REBG-SMOTE

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
REBG-SMOTE	0.8488	0.9447	0.9757	0.8889	0.8568	0.9777	0.9614	0.9589

The graphical representation of a boxplot, assembling cross-validation results for the REBG-SMOTE module, is displayed in Figure 12. Native Bayes possesses a much higher median accuracy and fairly small interquartile range, indicative of its ability to deal with imbalanced datasets. On the contrary, models such as LSTM and Random Forest indicate lower median accuracies along with higher variabilities, thus suggesting that these two models face more difficulties with such a dataset. This plot, thus, emphasizes the need for a careful choice of classifiers in imbalanced dataset situations.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

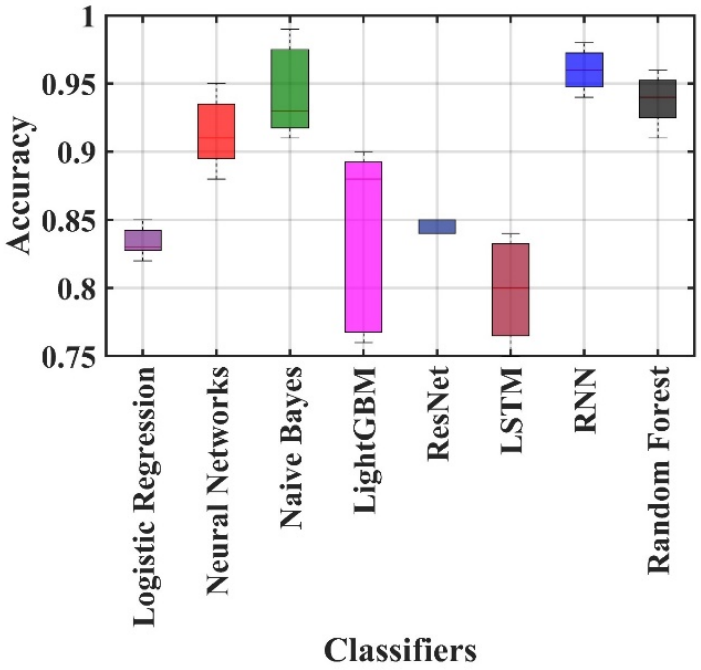


Figure 12: CV on REBG-SMOTE

The CV value obtained by the ABSMOA module for different class imbalance methods is presented in Table 6.

Table 6: CV for ABSMOA

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
ABSMOA	0.8758	0.9447	0.8757	0.9789	0.9868	0.9177	0.8954	0.9589

The graphical representation of a boxplot, assembling cross-validation results for the ABSMOA module, is displayed in Figure 13. ResNet holds the highest median accuracy, which is strongest against handling imbalanced data. Logistic Regression and Neural Networks also perform well on these metrics, while the classifiers such as Random Forest and LSTM show a much broader variability, indicating possible issues with class imbalance.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

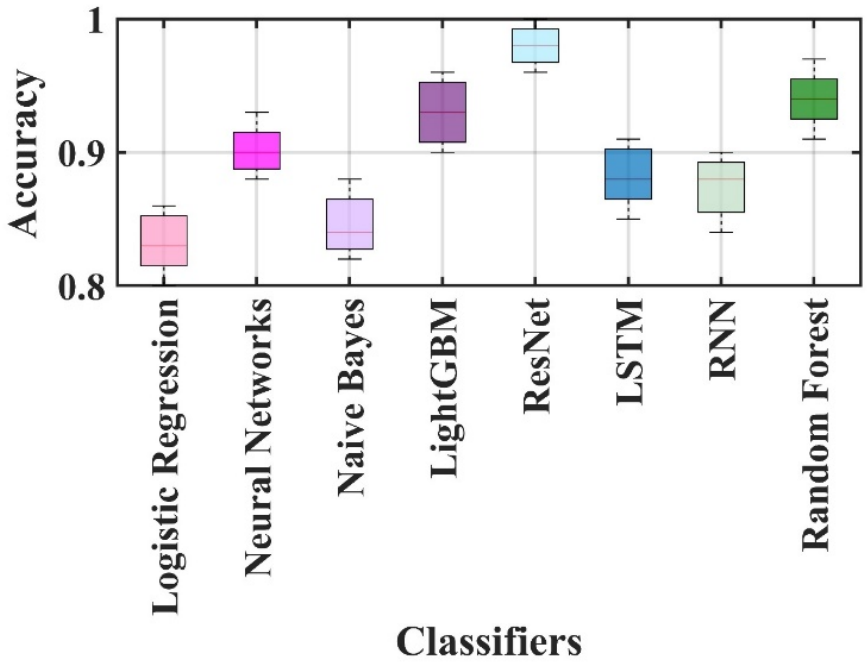


Figure 13: CV on ABSMOA

This shows the classification models for selection while taking into consideration the imbalanced datasets to have a reliable prediction performance. The CV obtained by the SHAP module for different class imbalance methods is presented in Table 7.

Table 7: CV for SHAP

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
SHAP	0.8358	0.9447	0.8757	0.8789	0.9768	0.9177	0.8954	0.9689

The graphical representation of a boxplot, assembling cross-validation results for the SHAP module, is displayed in Figure 14. The most significant median accuracy over ResNet suggests that it is the most suitable for imbalanced data. Logistic Regression and Neural Networks do reasonably well at this, whereas LSTM, Random Forest, and the rest show large variability, indicating that they are facing trouble while handling class imbalance.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

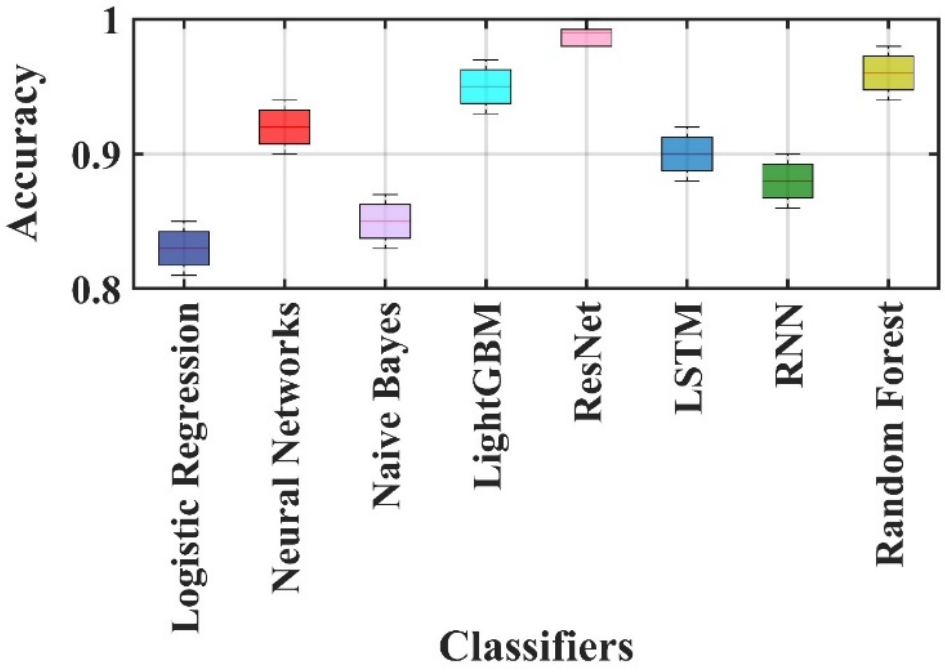


Figure 14: CV on SHAP

The CV value obtained by the TensorRT with ONNX module for different class imbalance methods is presented in Table 8.

Table 8: CV for TensorRT with ONNX

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
TensorRT with ONNX	0.9158	0.9347	0.9487	0.8775	0.9578	0.9789	0.9647	0.8889

The graphical representation of a boxplot, assembling cross-validation results for the TensorRT with ONNX module, is displayed in Figure 15. LSTM exhibits the best median performance, making it the best classifier for imbalanced datasets; however, Logistic Regression and Neural Networks perform fairly well too.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

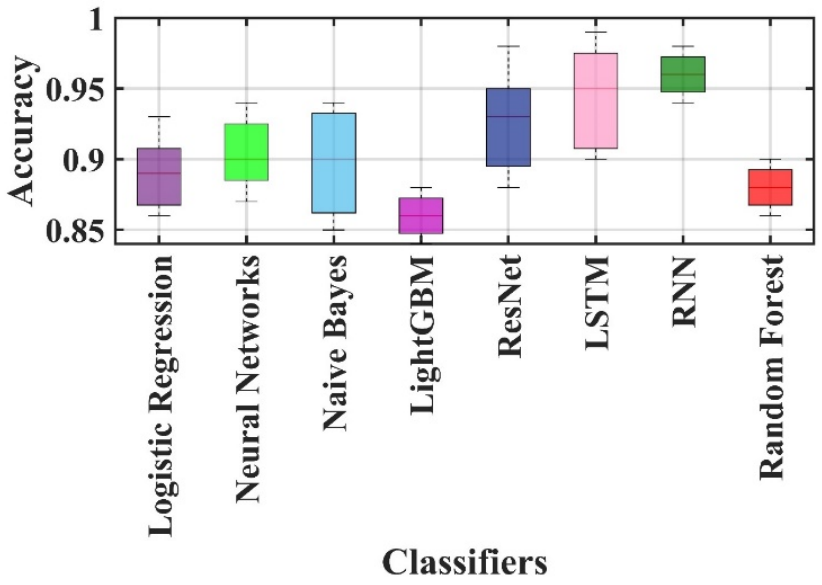


Figure 15: CV on TensorRT with ONNX module

The CV value obtained by the Apache Kafka module for different class imbalance methods is presented in Table 9.

Table 9: CV for Apache Kafka

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
Apache Kafka	0.9358	0.9589	0.9117	0.9258	0.9888	0.9124	0.8747	0.9515

The graphical representation of a boxplot, assembling cross-validation results for the Apache Kafka module, is displayed in Figure 16. Among the classifiers, ResNet poses the highest and RNN poses the least accuracy among others. However, LSTM and Random Forest show high variance, suggesting that they experience some challenges in a situation with imbalanced classes. Thus, the illustration rightly depicts that the classifiers need to be carefully selected for good predictive performance on imbalanced scenarios.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

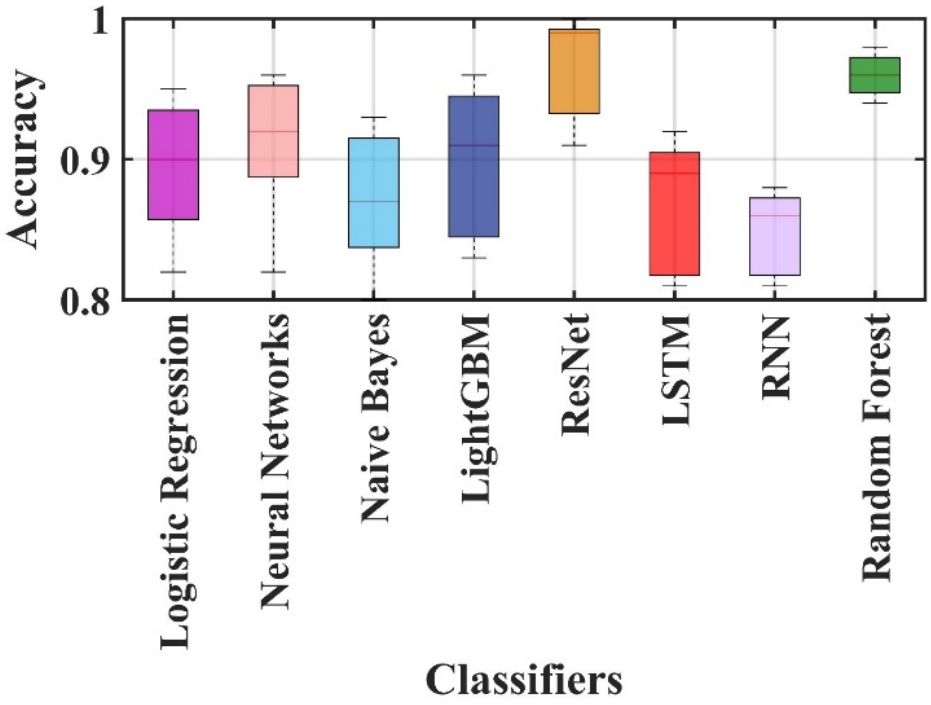


Figure 16: CV on Apache Kafka

The CV value obtained by the IMSICBEG module for different class imbalance methods is presented in Table 10.

Table 10: CV for IMSICBEG

Classifier	Logistic Regression	Neural Networks	Naive Bayes	LightGBM	ResNet	LSTM	RNN	Random Forest
IMSICBEG	0.8547	0.9358	0.8947	0.9557	0.9978	0.9199	0.9122	0.9555

The graphical representation of a boxplot, assembling cross-validation results for the IMSICBEG module, is displayed in Figure 17. Among the classifiers, ResNet poses the highest and Logistic Regression the lowest accuracy among others.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

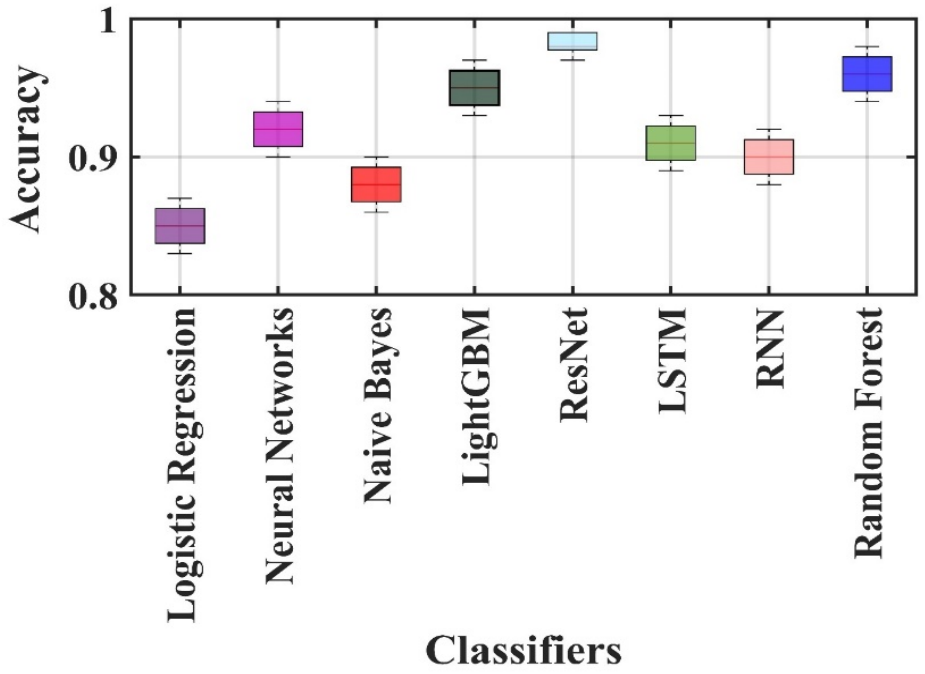


Figure 17: CV on IMSICBEG

From the above analysis, the module IMSICBEG performed very well on ResNet with less variation when compared with other modules under research. The performance of the IMSICBEG module, along with reduced variation, indicates that it attains better results consistently, thereby becoming an excellent candidate to be coupled into deep learning models like ResNet.
Table 11 depicts the performance and comparison metrics across IMSICBEG optimization approaches. Future work could optimize the deep learning-based ensemble forecasting with a spatiotemporal modeling framework for higher-dimensional datasets and explore hybrid models combining traditional and deep learning techniques for better forecasting.

Table 11: Performance and comparison metrics across IMSICBEG optimization approaches

Metric/Category	Data Points	Insights
Outlier Analysis (local outlier factor)	Outliers removed: ~2.3% of dataset; noise reduction: ~4.6%; variance reduced by 8.1%	Local outlier factor-based preprocessing improves model stability and performance by removing high-noise instances.
Accuracy	IMSICBEG: 99.78%	IMSICBEG achieves the highest accuracy, indicating excellent overall model correctness.
Recall	IMSICBEG: 99.78%	MSICBEG demonstrates a strong ability to correctly identify fraudulent cases.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Precision	IMSICBEG: 98.69%	High precision indicates IMSICBEG has minimal false positives in fraud detection.
F1-Score	IMSICBEG: 99.87	IMSICBEG maintains a balanced performance between precision and recall.
AUC	Logistic Regression: 0.8534 Neural Networks: 0.9426 Naive Bayes: 0.8241 LightGBM: 0.8732 LSTM: 0.8433, RNN: 0.8321 Random Forest: 0.8831 ResNet: 0.9921	AUC indicates superior discrimination between fraud and legitimate classes by IMSICBEG.
Class Imbalance Handling (CV)	IMSICBEG + Logistic Regression: 0.8547, IMSICBEG + Neural Networks: 0.9358, IMSICBEG + Naive Bayes: 0.8947, IMSICBEG + LightGBM: 0.9557, IMSICBEG + LSTM: 0.9199, IMSICBEG + Random Forest: 0.9555, IMSICBEG +RNN: 0.9122, IMSICBEG + ResNet: 0.9978	ResNet combined with IMSICBEG yields the best balance and highest metric consistency.
Model Interpretability	Multi-layer relation graph analysis, bidirectional spike modeling, attention heatmaps	IMSICBEG provides interpretable decision paths for identifying fraud patterns.

5 Conclusion and Future Scope

This research study developed insights into the application of deep learning models for detecting credit card scams. An advanced bidirectional spiking graphormer based hybrid IMSICBEG module is designed and validated in the spotting of anomalous credit card remittances. The long-standing challenge of computational complexity and GPU memory explosion is addressed in the IMSICBEG module. The module achieved 99.25% accuracy using 12,84,020 samples from external datasets. The effectiveness of combining different modules to tackle the complexities of fraud detection is explored. The AUC curve for IMSICBEG modules covered a huge area, and this signifies the suitability of the proposed module in spotting fraudulent remittances in credit card. As the experiment progressed, it is observed that ResNet outperformed excellently than all other class imbalance techniques. The IMSICBEG module gained 0.9888 CV for the ResNet classifier, higher than other modules. In some cases, LightGBM and LSTM classifiers performed better. On the other hand, efforts are currently being made to investigate additional anomaly spotting techniques and hybridized structure for future research. Furthermore, integration with federated learning frameworks, regulatory compliance tools, and explainable AI dashboards can make IMSICBEG a cornerstone in globally scalable, ethical, and intelligent fraud detection ecosystems.

References

[1] Reddy, S.S., Amrutha, K., MNSSVKR Gupta, V., VSSR Murthy, K. and Rao, V.V.R.M., 2025. Optimizing Hyperparameters for Credit Card Fraud Detection with Nature-Inspired

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

Metaheuristic Algorithms in Algorithmic learning. *Journal of The Institution of Engineers (India): Series B*, pp.1-26.

[2] Ebrahimi, M., Chai, Y., Samtani, S. and Chen, H., 2022. Cross-lingual cybersecurity analytics in the international dark web with adversarial deep representation learning. *MIS quarterly*, *46*(2).

[3] Cui, Y., Han, X., Chen, J., Zhang, X., Yang, J. and Zhang, X., 2025. FraudGNN-RL: A Graph Neural Network With Reinforcement Learning for Adaptive Financial Fraud Detection. *IEEE Open Journal of the Computer Society*.

[4] Feng, X. and Kim, S.K., 2024. Novel algorithmic learning based credit card fraud detection systems. *Mathematics*, *12*(12), p.1869.

[5] Seera, M., Lim, C.P., Kumar, A., Dhamotharan, L. and Tan, K.H., 2024. An intelligent payment card fraud detection system. *Annals of operations research*, *334*(1), pp.445-467.

[6] Huang, H., Liu, B., Xue, X., Cao, J. and Chen, X., 2024. Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique. *Applied Soft Computing*, *154*, p.111368.

[7] ORELAJA, A. and ADEYEMI, A.F., 2024. Developing Real-Time Fraud Detection and Response Mechanisms for Financial Transactions.

[8] Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., Khosravi, A. and Nahavandi, S., 2023. Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, *123*, p.106248.

[9] Gupta, P., Varshney, A., Khan, M.R., Ahmed, R., Shuaib, M. and Alam, S., 2023. Unbalanced credit card fraud detection data: A algorithmic learning-oriented comparative study of balancing techniques. *Procedia Computer Science*, *218*, pp.2575-2584.

[10] Van Belle, R., Baesens, B. and De Weerdt, J., 2023. CATCHM: A novel network-based credit card fraud detection method using node representation learning. *Decision Support Systems*, *164*, p.113866.

[11] Bakhtiari, S., Nasiri, Z. and Vahidi, J., 2023. Credit card fraud detection using ensemble data mining methods. *Multimedia Tools and Applications*, *82*(19), pp.29057-29075.

[12] Awosika, T., Shukla, R.M. and Pranggono, B., 2024. Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection. *IEEE Access*.

[13] Chugh, B., Malik, N., Gupta, D. and Alkahtani, B.S., 2025. A probabilistic approach driven credit card anomaly detection with CBLOF and isolation forest models. *Alexandria Engineering Journal*, *114*, pp.231-242.

[14] Ayoub, M., Abdelhamid, T. and Khalid, J., 2025. Granular computing framework for credit card fraud detection. *Alexandria Engineering Journal*, *121*, pp.387-401.

[15] Xiang, S., Zhang, G., Cheng, D. and Zhang, Y., 2025. Enhancing Attribute-Driven Fraud Detection With Risk-Aware Graph Representation. *IEEE Remittances on Knowledge and Data Engineering*.

[16] Tayebi, M. and El Kafhali, S., 2025, March. Combining Autoencoders and Deep Learning for Effective Fraud Detection in Credit Card Remittances. In *Operations Research Forum* (Vol. 6, No. 1, pp. 1-30). Springer International Publishing.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

[17] Chatterjee, P., Das, D. and Rawat, D.B., 2024. Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems.

[18] Charizanos, G., Demirhan, H. and İçen, D., 2024. An online fuzzy fraud detection framework for credit card remittances. *Expert Systems with Applications*, *252*, p.124127.

[19] Sorour, S.E., AlBarrak, K.M., Abohany, A.A. and Abd El-Mageed, A.A., 2024. Credit card fraud detection using the brown bear optimization algorithm. *Alexandria Engineering Journal*, *104*, pp.171-192.

[20] Tang, Y. and Liang, Y., 2024. Credit card fraud detection based on federated graph learning. *Expert Systems with Applications*, *256*, p.124979.

[21] Cherif, A., Ammar, H., Kalkatawi, M., Alshehri, S. and Imine, A., 2024. Encoder–decoder graph neural network for credit card fraud detection. *Journal of King Saud University-Computer and Information Sciences*, *36*(3), p.102003.

[22] Mim, M.A., Majadi, N. and Mazumder, P., 2024. A soft voting ensemble learning approach for credit card fraud detection. *Heliyon*, *10*(3).

[23] Bhuyan, H. K., Unhelkar, B., Shankar, S. S., & Chakrabarti, P. (2024). "Deep convolutional neural network-based Henry gas solubility optimization for disease prediction in data from wireless sensor networks." Journal of Information & Optimization Sciences, 45(8), 2273–2284.

[24] Gupta, K. G., Unhelkar, B., Siva Shankar, S., Chakrabarti, T., Chakrabarti, P., Sivaneasan, B., & Margala, M. (2024). "A novel optimization-based time-enabled proxy reencryption approach for securing e-health data in cloud environments: An interdisciplinary statistical perspective." Journal of Discrete Mathematical Sciences and Cryptography, 27(8), 2419–2429. https://doi.org/10.47974/JDMSC-2015. Print ISSN: 0972-0529 , Online ISSN: 2169-0065

[25] Nobel, S.N., Sultana, S., Singha, S.P., Chaki, S., Mahi, M.J.N., Jan, T., Barros, A. and Whaiduzzaman, M., 2024. Unmasking banking fraud: Unleashing the power of algorithmic learning and explainable ai (xai) on imbalanced data. *Information*, *15*(6), p.298.

[26] Iqbal, A. and Amin, R., 2025. An efficient mechanism for time series forecasting and anomaly detection using explainable artificial intelligence. *The Journal of Supercomputing*, *81*(4), p.523.

[27] Bounab, R., Zarour, K., Guelib, B. and Khlifa, N., 2024. Enhancing medicare fraud detection through algorithmic learning: Addressing class imbalance with SMOTE-ENN. *IEEE Access*.

[28] Wang, H., Liang, Q., Hancock, J.T. and Khoshgoftaar, T.M., 2024. Feature selection strategies: a comparative analysis of SHAP-value and importance-based methods. *Journal of Big Data*, *11*(1), p.44.

[29] Longo, L., A comparative analysis of SHAP, LIME, ANCHORS, and DICE for interpreting a dense neural network in Credit Card Fraud Detection.

[30] Li, J., Zhang, Y., He, S. and Tang, Y., 2024. Interpretable mortality prediction model for ICU patients with pneumonia: using shapley additive explanation method. *BMC Pulmonary Medicine*, *24*(1), p.447.

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.

[31] Gopiktrishna, P.B. and Rishekeeshan, A., 2024, May. Accelerating native inference model performance in edge devices using TensorRT. In *2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS)* (pp. 1-7). IEEE.

[32] Zhu, C., Qian, J. and Gao, M., 2024. TensorRT Powered Model for Ultra-Fast Li-Ion Battery Capacity Prediction on Embedded Devices. *Energies*, *17*(12), p.2797.

[33] Crespo, A., Moncada, C., Crespo, F. and Morocho-Cayamcela, M.E., 2025. An efficient strawberry segmentation model based on Mask R-CNN and TensorRT. *Artificial Intelligence in Agriculture*.

[34] Vinoth, K. and Sasikumar, P., 2024. Lightweight object detection in low light: pixel-wise depth refinement and TensorRT optimization. *Results in Engineering*, *23*, p.102510.

[35] Kim, J.H., Lee, D.E., Choi, S.B. and Jun, K.K., 2024. ONNX-based Runtime Performance Analysis: YOLO and ResNet. *The Journal of Bigdata*, *9*(1), pp.89-100.

[36] Obaideen, K., Bonny, T. and AlShabi, M., 2024, June. Charting the rise of ONNX in swift image processing: a publications exploration. In *Real-Time Image Processing and Deep Learning 2024* (Vol. 13034, pp. 183-188). SPIE.

Received: 20 August 2025 | Accepted: 05 September 2025 | Published: 07 September 2025

Citation: Devi, K.; Unhelkar, B. & Shanker S, S. (2025). Real-Time Edge-Enabled Cyber Credit Card Fraud Detection Using an Interpretable Multi-Relation Spiking Imperialist Competitive Bidirectional Encoder Graphormer. *International Insurance Law Review*, 33 (S4), 216-242.