


RESEARCH ARTICLE

Hybrid Neural Network Methods for the Detection of Credit Card Fraud

Mahmoud Ahmad Al-Khasawneh¹ | Muhammad Faheem² | Deema Mohammed Alsekait³ | Adamu Abubakar⁴  | Ghassan F. Issa¹

¹School of Computing, Skyline University College, University City Sharjah, Sharjah, UAE | ²VTT Technical Research Center of Finland Ltd., Espoo, Finland |

³Department of Computer Science and Information Technology, Applied College, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia |

⁴Department of Computer Science International Islamic University Malaysia, Kuala Lumpur, Malaysia

Correspondence: Mahmoud Ahmad Al-Khasawneh (mahmoud@outlook.my) | Muhammad Faheem (muhammad.fatheem@vtt.fi)

Received: 5 October 2024 | **Revised:** 24 November 2024 | **Accepted:** 26 December 2024

Funding: This study was supported by Princess Nourah Bint Abdulrahman University, Project number (PNURSP2024R435), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

Keywords: artificial intelligence | fraud | fraud detection | hybrid-neural network | machine learning

ABSTRACT

The purpose of research on fraud detection is to discover methods that are superior and more effective in detecting fraudulent activity. Because of the difficulties that are associated with single models, this research proposes a hybrid model neural network be utilized in order to overcome such difficulties. A very effective binary classification system is produced as a result of the multimodal neural network (MNN) model, which combines continuous and categorical data channels. The hybrid model neural network model demonstrates some extraordinary effectiveness in detecting cases of credit card fraud, according to the results of experimental investigation. The findings on accuracy, precision, recall, and area under the curve (AUC) give evidence of its robustness and reliability in identifying fraudulent transactions while simultaneously reducing the number of false positives and false negatives. In particular, it proved that the performance of the model is exceptional, with a test accuracy of 99.47%, precision of 99.82%, recall of 97.87%, and an AUC of 98.99%. Furthermore, these findings provide evidence of a robust model that is capable of effectively detecting fraudulent transactions with a high degree of accuracy, while simultaneously lowering the occurrence of both false positives and false negatives. Consequently, this guarantees a fraud detection system that is dependable and effective.

1 | Introduction

The fact that fraudulent activity using credit cards is an expensive problem that can have significant repercussions for the economy highlights the significance of fraud detection for financial institutions [1]. Sustainable fraud detection is not only improving the fraud detection capability but also understanding the relationships between fraud detection and other operating factors like company competitiveness, operating specifications, and customer relationships. It includes the effects of incorrect

classification on other financial performance measures and strategies [2]. In recent years, some machine learning methods have been applied to perform the card fraud detection task [3–8]. However, these methods cannot achieve optimized or even acceptable performance under the circumstance of having extreme imbalanced class distributions between normal and fraudulent transactions [9].

Conventional machine learning models frequently have difficulties when dealing with highly skewed fraud datasets [10]. Recent

progress in neural networks, particularly multimodal neural networks that can handle many forms of data at the same time, provide encouraging answers to this issue [11]. Typically, this involves using a wide range of attributes from transaction data. Effective fraud detection requires enhancing fraud detection capabilities and comprehending the interconnections between fraud detection and aspects such as firm competitiveness, operational standards, and customer relationships. Although machine learning techniques such as back-propagation neural networks, Bayes classifiers, decision trees, fuzzy neural networks, and support vector machines have been used, they frequently struggle to achieve satisfactory results when dealing with highly imbalanced datasets.

The research problem this current research dwells on relies within the majority of research in fraud detection which primarily aims to enhance efficiency and effectiveness through the utilization of many models. Critically, these problems of efficiency and effectiveness frequently fail to account within the basic machine learning model. Even though multimodal model characteristics tend towards going deeper to bring out the optimized results, yet where data becomes imbalance between fraudulent and non-fraudulent transactions tends to possess another challenges. In order to tackle these difficulties, the research suggests employing a multimodal neural network that utilizes addressing imbalance situation techniques. The usage of credit cards has been simplified because to the proliferation of online financial services; nevertheless, this has also led to a rise in the likelihood of fraudulent activity, which presents a significant challenge for both customers and financial institutions. In what ways can online financial services keep the convenience of using credit cards while simultaneously reducing the likelihood of fraudulent activity? Also, in the context of online financial services, what are the most successful ways for detecting and preventing fraudulent activity, specifically with credit cards?

The justification of adopting “Multimodal neural network” lies with the fact that it utilizes several sets of variables to analyse and identify more accurate and distinguishing patterns, resulting in notable benefits compared to current approaches in detecting instances of credit card fraud [11]. Furthermore, by practical implications, criminals employing diverse techniques to exploit pilfered card information, such as vending it on the clandestine internet or promptly utilizing it, with this method this approach, it will be able to detect even before it happened. Similarly, payment cancellations and disruptions that usually can result from fraudulent transactions, underscoring the importance for merchants to employ sophisticated algorithms and technology to differentiate criminals and safeguard against fraudulent transactions will be established.

The present study suggests that incorporating models into multimodal neural networks significantly enhances the detection of credit card fraud. Therefore, the research contributes in the following ways:

- This research contributes in highlighting that, multimodal neural networks have the ability to successfully integrate and combine many elements such as “Continuous Pathway,” “Categorical Pathway,” “Combined Features,”

“Post-Concatenation Layers,” and “Output Layer” that enables efficient detection of credit card fraud.

- This research also contributes in highlighting the most important feature of credit card transactions from European cardholder’s dataset captured over a period of 2 days. Where it was revealed that “purchase rate” transactions, is found to be the most important criteria that effectively used to detect fraud.
- This research also contributes in highlighting that the balanced approach to handling class imbalance, contributed to high level of performance, where the performance of our model is outstanding, with a test accuracy of 99.92%, precision of 99.17%, recall of 99.87%, and an AUC of 99.99%. The results demonstrate that the model is very strong and effectively detect fraudulent transactions with high accuracy, while also reducing the occurrence of both false positives and false negatives.

Apart from the current section, which provides the background of the research, the remaining sections are organized as follows: Section 2 present the “Related Work,” Section 3 discuss the research models, Section 4 present the experimental analysis and presentation of the results, Section 5 present the discussion, Section 6 discuss the implications of the study, Limitations, and recommendations for future work, finally Section 7 present the conclusion of the research.

2 | Related Work

Credit card fraud is a serious problem in the financial sector, resulting in huge monetary losses for both customers and financial institutions. Researchers have recently investigated the utilization of new technology, such as neural networks, to improve the detection of credit card fraud. The work of Varmedja [3] is essential in this context, which found that many machine learning algorithms can achieve high accuracy in detecting credit card fraud. This highlights the potential of using different machine learning methods to address this issue. Credit card fraud detection is a crucial concern in financial security, and many machine learning methods have been utilized to enhance the precision of fraud detection. Various methodologies, such as data mining, machine learning, and diverse algorithms, have been investigated for the purpose of detecting credit card fraud [3]. These strategies have proven to be successful in identifying fraudulent transactions, achieving high levels of accuracy.

A study conducted by Aftab et al. [8] found that credit card fraud involves illegal activities aimed at acquiring confidential information for unauthorized transactions. The research aimed to determine the most appropriate supervised machine learning algorithm for detecting credit card fraud by comparing Logistic Regression, Random Forest, Support Vector Machine, and Decision Trees. The findings indicated that Random Forests outperformed other algorithms, earning a recall score of 84%.

Fu et al. [12] suggested employing Convolutional Neural Networks (CNNs) to detect credit card fraud. The authors showcased the efficacy of CNNs in identifying fraudulent activity through the analysis of transaction data. Their research indicated that

CNNs have the ability to accurately identify intricate patterns in credit card transactions, resulting in enhanced accuracy in detecting fraudulent activities.

Expanding upon the research conducted by Fu et al. [12] in 2016, Jin et al. [13] in 2017 proposed the idea of combining many modes of information using Recurrent Neural Networks (RNNs) to detect rumors on microblogs. Although not directly pertaining to credit card fraud detection, their research offers useful insights into the potential of multimodal neural networks for detecting fraudulent activities. By combining data from several sources, such as transaction metadata and user behavior, multimodal neural networks have the potential to improve the identification of fraudulent credit card transactions.

Dou et al. [14] conducted research on improving Graph Neural Network-based fraud detection systems to better identify camouflaged crooks. While their study focused on fraud detection in a different environment, the idea of utilizing graph neural networks for fraud detection coincides with the main objective of improving fraud detection through advanced neural network models. This underscores the capacity to utilize graph neural networks to enhance the capabilities of credit card fraud detection.

Seera et al. [15] found that creating accurate predictive models for fraud detection is difficult because of the secrecy surrounding actual transaction information. The research investigates 13 statistical and machine learning models to detect payment card fraud. It utilizes both publicly available and genuine transaction records. The study's findings validate the efficacy of utilizing aggregated features to tackle practical issues in payment card fraud detection.

Ordonez and Roggen [16] proposed a multi-modal Recurrent Neural Network (m-RNN) model. This model is designed to generate new picture captions by directly estimating the probability of creating a word based on past words and an image. This approach demonstrates the proficiency of multimodal neural networks in comprehending and producing natural language descriptions based on visual inputs.

Awoyemi et al. [4] did a study to examine the effectiveness of naïve bayes, k-nearest neighbor, and logistic regression algorithms on credit card fraud data that had a significant degree of skewness. The researchers discovered that the effectiveness of fraud detection in credit card transactions is significantly influenced by the sampling methodology employed on the dataset, the selection of variables, and the detection algorithms utilized.

Randhawa et al. [17] found that the majority voting method is highly effective in accurately detecting instances of credit card fraud. The discovery indicates that utilizing ensemble approaches like AdaBoost and Majority Voting can greatly enhance the precision of credit card fraud detection. In their study, Xuan et al. [18] compared two random forests that utilized various basis classifiers and evaluated their effectiveness in detecting credit fraud. The results showed that both methods achieved high levels of accuracy.

Makki et al. [9] found that imbalanced classification methods are not effective, particularly when dealing with extremely imbalanced data. This discovery emphasizes the necessity for more powerful and equitable classification techniques to tackle the difficulties presented by uneven credit card fraud data.

In their study, Khalid et al. [7] found that the utilization of machine learning models, namely ensemble approaches, enhances the detection of credit card fraud. This conclusion was drawn following a thorough literature search that revealed shortcomings in existing technology. The ensemble model, which incorporates Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Bagging, and Boosting classifiers, is designed to address dataset imbalance by utilizing under-sampling and the Synthetic Over-Sampling Technique (SMOTE). The study emphasizes the efficacy of ensemble approaches in countering fraudulent transactions and lays the groundwork for the development of more robust and adaptable fraud detection systems to tackle evolving fraud schemes.

Taha and Malebary [6] introduced an intelligent method to enhance credit card fraud detection. Their approach surpassed other techniques and achieved the highest levels of accuracy, Area under receiver operating characteristic curve (AUC), Precision, and F1-score. This discovery highlights the capacity of sophisticated machine learning methods to improve the precision and efficacy of credit card fraud detection.

In addition, Yang et al. [19] proposed a unique method for detecting credit card fraud using federated learning approaches. This methodology offers a new way to tackle fraud detection. Lastly, Itoo et al. [5] performed a comparative analysis of logistic regression, Naïve Bayes, and KNN machine learning algorithms for the purpose of credit card fraud detection. Their study shed light on the effectiveness of various machine learning techniques in this specific domain.

Paldino et al. [20] shown that conventional machine learning techniques frequently struggle to adjust to the dynamic nature of client behavior, which entails ongoing fluctuations in data distribution for the purpose of credit card fraud detection. The research suggests a learning technique that leverages diversity-based ensemble learning to retain previous notions and utilize them for faster adaptation to changes. The results clearly indicate the efficacy of this method in improving the identification of fraudulent transactions.

The literature review suggests that the effectiveness of credit card fraud detection significantly impacted by the selection of machine learning methods, sampling strategies, and data attributes. The research gaps established from the reviews empirical research studies dwells on the fact that the current status Coe offers useful insights on the utilization of neural networks, such as CNNs, RNNs, to improve credit card fraud detection [21–24]. Nevertheless, it is necessary to examine the particular characteristics and methods that provide the most valuable information for identifying fraudulent activity in credit card transactions. In addition, the advancement of strong multimodal fusion techniques into credit card fraud detection systems offer interesting opportunities. That is why this current study established that ultimately,

the combination of multimodal neural networks has significant potential to improve credit card fraud detection techniques.

2.1 | The Model Configuration and Architecture

Multimodal learning seeks to acquire knowledge by utilizing several modalities. Multi-modality is the process of extracting and combining important information from different sources and using it to solve a problem. This approach results in a more comprehensive representation and better performance compared to using each source alone [11, 16]. The neural network developed for this study is designed to handle both continuous and categorical data inputs. It utilizes discrete paths within the model to take use of the unique characteristics of each data type. This methodology enables a sophisticated comprehension

of intricate connections within the data, which is crucial for detecting fraudulent transactions. The general architecture of the model is presented in Figure 1.

The model's overall structure consists of five main components: the "Continuous Pathway," the "Categorical Pathway," the "Combined Features," the "Post-Concatenation Layers," and the "Output Layer." Therefore, the result of the dense layer, which is obtained by applying the ELU (Exponential Linear Unit) activation function, is calculated using Equation (1) for various dimensions.

$$Z_1 = \text{elu}(W_n i_{cont} + b_n) \in \mathbb{R}^x \quad (1)$$

The input vector for continuous data is represented by $i_{cont}t$, which can have varied shapes indicating the properties of the transaction. The weight matrix $W_n \in \mathbb{R}^x$ is used for the dense layer in the continuous data pathway. The shape of the variables

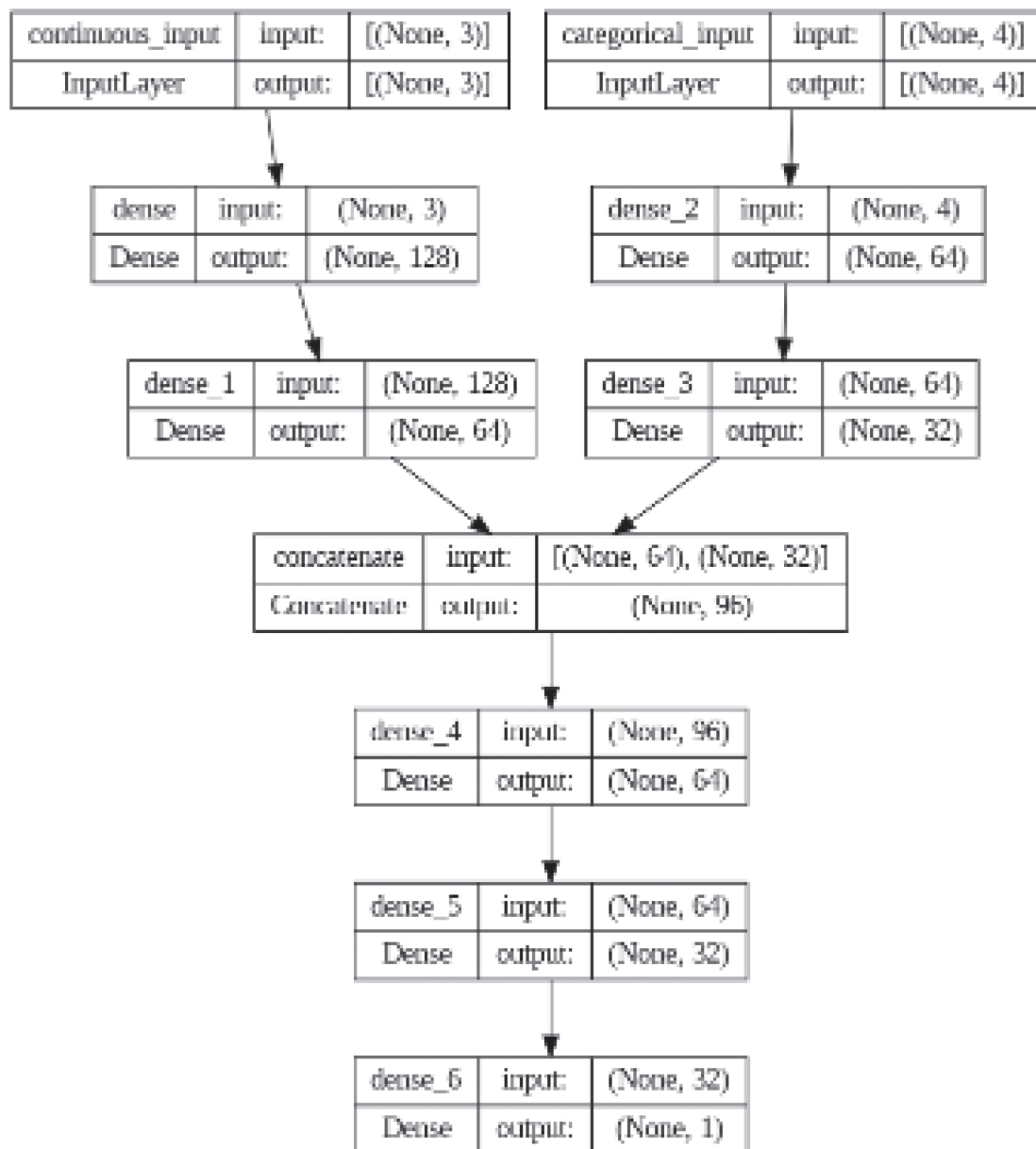


FIGURE 1 | The architectural model of the multimodal neural networks.

determines the direction and specifies the number of units in the dense layer, as well as the size of the input vector. The vector $bW_n \in \mathbb{R}^x$ represents the bias for the dense layer, and its shape is determined by the dimension. The Exponential Linear Unit (ELU) is an activation function that is applied element-wise to the output of the affine transformation.

The input layer consists of a continuous pathway and a categorized pathway. This layer processes three continuous features, namely transaction distances and ratios, by utilizing a series of dense layers. The initial layer comprises 128 neurons, while the subsequent layer contains 64 neurons. Both layers utilize the exponential linear unit (ELU) activation function to effectively process non-linear input. The first layer, known as “layer 1 (Dense Layer),” is evaluated using Equation (2):

$$z_1 = \text{elu}(W_1 i_{\text{cont}} + b_1) \in \mathbb{R}^{128} \quad (2)$$

The input vector for continuous data is presented by i_{cont} when it has a shape of (3). This pertains to characteristics such as transaction distances and ratios. W_1 is the weight matrix corresponding to the initial dense layer in the continuous data pipeline? The shape of the input vector is (128, 3) with 128 units in the dense layer and a size of 3 for the input vector. b_1 is the bias vector for the first dense layer has a form of (128). The activation function applied element-wise to the result of the affine transformation is called Elu. The output represents the result obtained from the first dense layer after the application of the ELU activation function. It has a form of (128).

The second “Layer 2 (Dense Layer)” is evaluated by Equation (3)

$$z_2 = \text{elu}(W_2 z_1 + b_2) \quad (3)$$

z_2 is the input vector from the first dense layer, denoted as is of shape (128). W_2 is the weight matrix for the second dense layer, denoted as, is of shape (64, 128). The bias vector for the second dense layer has a form of (64,). z_2 is the output corresponding to the result of the second dense layer following the application of the ELU activation function, and it has a shape of (64).

The categorical pathway refers to a specific route or process that is organized or classified according to distinct categories or groups. The input layer handles four category features, which consist of transaction methods such as chip usage and online orders. It is followed by two dense layers, one with 64 neurons and the other with 32 neurons, both utilizing the ELU activation function. Equation (4) evaluates the first categorical data pathway at “Layer 1 (Dense Layer)”:

$$z_3 = \text{elu}(W_3 i_{\text{cat}} + b_3) \quad (4)$$

i_{cat} is the input vector for categorical data, and has a shape of (4). This vector represents the features of the state. W_3 is the weight matrix corresponding to the initial dense layer in the pathway for categorical data? The shape of the object is (64, 4). b_3 is the bias vector for the first dense layer has a form of (64). z_3 is the output refers to the result obtained from the second dense layer after the application of the ELU activation function? It has a shape of (64). The second Categorical Input “Layer 2 (Dense Layer)” is evaluated by Equation (5):

$$z_4 = \text{elu}(W_4 z_3 + b_4) \quad (5)$$

z_3 is the input vector from the first dense layer is denoted as and has a shape of (64). W_4 is the weight matrix for the second dense layer is denoted as and has a shape of (32, 6). b_4 is the bias vector for the second dense layer is denoted as and has a shape of (32). The output z_4 represents the result obtained from the second dense layer after applying the ELU activation function. It has a form of (64).

2.2 | Combination and Prediction Layer

The results of the combined pathways mentioned before are joined together to create a merged feature set. This merged feature set is then passed through further dense layers, consisting of 64 and 32 neurons, to successfully combine the learnt representations. Hence, the combination of both paths is assessed using Equation (6):

$$z_{\text{combined}} = [z_2, z_4] \quad (6)$$

The outputs from the continuous data pathway z_2 and the categorical data pathway z_4 are merged to create a single feature vector. The output from the second dense layer of the continuous pathway z_2 is denoted as a tensor with a shape of (64). The output from the second dense layer of the categorical pathway z_4 is a tensor with a form of (32,). Therefore, z_{combined} is the resulting output is the combined feature vector, which has a shape of (96,). Equation (7) evaluates the post-concatenation dense layers at “Layer 1 (Dense Layer)”

$$z_5 = \text{elu}(W_5 z_{\text{combined}} + b_5) \quad (7)$$

The concatenated feature vector from the previous phase, denoted as z_{combined} , has a shape of (96). The weight matrix W_5 for the dense layer, denoted as, has a shape of (64, 96). The bias vector b_5 for the dense layer has a form of (64). The output z_5 corresponds to the result obtained from the dense layer after the application of the ELU activation function. It has a form of (64,). Immediately following this process, the “Layer 2 (Dense Layer)” is evaluated using Equation (8):

$$z_6 = \text{elu}(W_6 z_5 + b_6) \quad (8)$$

The input vector from the previous dense layer is denoted as z_5 “input vector” and has a shape of (64). The weight matrix W_6 for the dense layer has a form of (32, 64). The bias vector b_6 for the dense layer has a form of (32). The output z_4 is the result of the dense layer after the ELU activation function has been applied. It has a shape of (64).

The ultimate output layer comprises a solitary neuron with a sigmoid activation function, intended to categorize the input as either fraudulent or non-fraudulent. Therefore, it is determined by the Equation (9):

$$\hat{y} = \sigma(W_7 z_6 + b_7) \quad (9)$$

The input vector z_6 is derived from the preceding dense layer and has a form of (32). The weight matrix W_7 for the output layer has a shape of (1, 32). The bias vector b_7 for the output layer has a form

of (1). The sigmoid activation function σ is defined as $\sigma(i) = \frac{1}{1+e^{-i}}$ ultimately, the result obtained is the estimated likelihood of the transaction being deceitful, represented as a numerical number ranging from 0 to 1.

2.3 | Performance Measurement

Model efficacy is evaluated by tracking performance parameters such as binary accuracy, precision, recall, and the area under the receiver operating characteristic (AUC) curve [25, 26]. Using recognized operational performance assessors that are derived from a confusion matrix, an evaluation was conducted to determine whether or not the strategy that was presented was effective. In this matrix, the components that are included are as follows: true positives (TPs), true negatives (TNs), false positives (FPs), and false negatives (FNs). As a result, the performance measures Precision, Recall, F1-score, and Accuracy (Acc) have been defined (please refer to Table 2 for further information).

The term “Precision Metric” refers to a quantitative measurement that evaluates the percentage of positive predictions that are accurate in comparison to the total number of positive class values that are predicted. It is calculated using Equation (10):

$$Precision = \frac{TP}{TP + FP} \quad (10)$$

The “Recall Metric” is determined by Equation (11) through dividing the total number of True Positives (TPs) and False Negatives (FNs) by the number of True Positives (TPs) that have been obtained.

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

There is a numerical metric known as the “F1-score” that is used to evaluate the accuracy of a classifier through the use of Equation (12):

$$F_1 - score = \frac{TP}{TP + \frac{1}{2}(FP + FN)} \quad (12)$$

The “Accuracy metric,” also known as ACC for short, is determined by Equation (13) as the rating system that determines how effective the model is in general.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \quad (13)$$

3 | Research Methodology

The research employs a multimodal neural network to address the challenges of credit card fraud detection within a highly imbalanced dataset. When utilizing a multimodal neural network for credit card fraud detection, the typical workflow consists of multiple essential stages. Every step plays a distinct role in guaranteeing the effectiveness and accuracy of the model. Below is a detailed description of each stage within this particular context:

The initial stage entails “Data Acquisition,” where the aim is to collect the essential data needed for training the neural network. This study involves the collection of transaction data. The

dataset used for this study was already produced by [27] and was obtained from [27] as the primary sources. The dataset may contain transaction amounts, time stamps, location data, and other relevant information as specified in Section 3.1. The subsequent stage involves data pre-processing, which aims to purify and convert the un-processed data into a format that is appropriate for training the model.

The task has been completed without any missing values, duplication, or errors in the data. Next, the research advanced by encoding categorical variables and performing feature engineering to generate additional features that could potentially provide more insightful information for the model. Examples of this can be consolidating transaction amounts across various time intervals, computing metrics that are specific to individual users, or extracting characteristics from textual data. Finally, the data is partitioned into training, validation, and test sets to accurately assess the performance of the model. The “Model Building” phase involves the creation of a multimodal neural network. This network consists of input layers that are responsible for handling different types of features, such as extraction layers and fusion layers. Ultimately, these levels combine to generate the output layer.

3.1 | Dataset

The dataset utilized in this study was acquired from Kaggle [26]. The dataset includes transactions that were done with credit cards by cardholders in Europe during the month of September 2013. There was a span of 2 days during which the transactions were documented. There are approximately one million transactions included in the dataset, and 87 403 of those transactions have been determined to be fraudulent. The fact that fraudulent transactions only account for 0.172% of the total implies that there is a large class imbalance. One of the most significant challenges that must be overcome in order to successfully identify fraudulent operations is this difference.

The dataset features can be summarized as follows: The characteristic “distance_from_home” represents the distance between the cardholder’s home and the location where the transaction took place. The “distance_from_last_transaction” feature represents the spatial separation between the location of the previous transaction and the current transaction location. The characteristic “ratio_to_median_purchase_price” represents the proportion of the transaction amount to the median purchase price. The “repeat_retailer” attribute indicates if the transaction took place at a retailer where the card-holder has previously made a purchase. The “used_chip” characteristic indicates if the transaction was conducted using a card that has a chip for enhanced security. The “used_pin_number” feature content entries indicate if the transaction was authorized using a PIN number. The “online_order” content entries indicate if the transaction was made online. The “fraud” feature determines whether the transaction has been identified as fraudulent.

This dataset is well-suited for training machine learning models to identify fraudulent transactions. It includes a wide range of features that encompass different elements of transaction patterns and behaviors generate the output layer.

3.2 | Experimental Set Up and Analysis

The experiment with the multimodal neural network model was conducted out via Google Colab, which offers a more convenient method of uploading datasets directly to either Colab or loading them from Google Drive.

To begin, we import all of the libraries that are required for the management of data, the creation of visualizations, and the construction of our model. Following the completion of preprocessing, in which no missing values were discovered, scaling features were carried out, and the data was partitioned into training and test sets, the end resultant sample of the data that was created is displayed in Table 1. The features are coded as follows: “distance_from_home (DFH),” “distance_from_last_transaction (DFL),” “ratio_to_median_purchase_price (RMP),” “repeat_retailer (RRT),” “used_chip (UCP),” “used_pin_number (UPN),” “online_order (OOD),” and “fraud (FRA).”

The interrelationship among the features was evaluated, and the result of these evaluation is presented in Figure 2. It was revealed that an interrelationships exist between these features, a multi-dimensional perspective on transaction behaviors was obtained. Identifying patterns of fraudulent behavior can be accomplished through the examination of these linkages, particularly when specific security features (UCP, UPN) and types of transactions (OOD, RRT) are present. There is the potential for a multimodal neural network to utilize these interrelationships in order to enhance the accuracy of fraud detection.

The result in Figure 2 clearly indicate that the highest correlation value of 0.46 was obtained from the relationship that exists between RMP and FRA, it can be deduced that unforeseen purchase rate are a significant indicator of fraudulent conduct. This finding is consistent with theoretical frameworks that place an emphasis on behavioral anomalies as principal markers of fraudulent activity [28–30]. It is possible for financial institutions to

TABLE 1 | Selected features from credit card transactions of European cardholder’s dataset.

DFH	DFL	RMP	RRT	UCP	UPN	OOD	FRA
57.87786	0.31114	1.94594	1	1	0	0	0
10.82994	0.17559	1.29422	1	0	0	0	0
5.091079	0.80515	0.42772	1	0	0	1	0
2.247564	5.60004	0.36266	1	1	0	1	0
44.19094	0.56649	2.22277	1	1	0	1	0

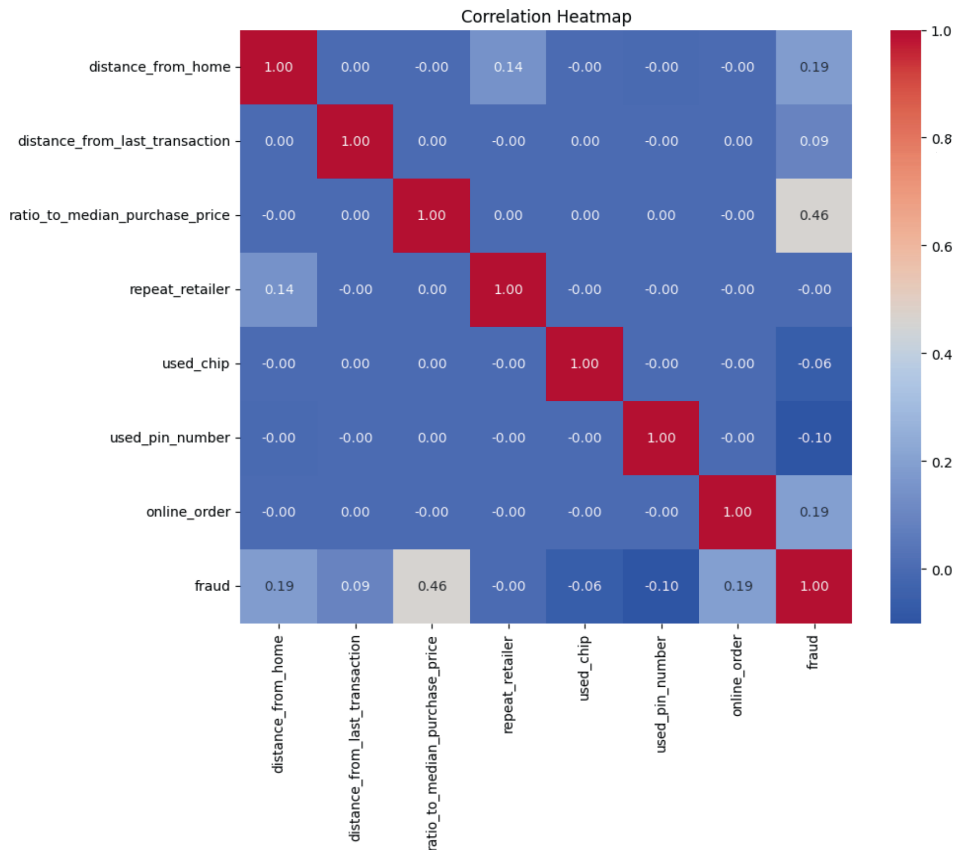


FIGURE 2 | The correlation heatmap among the features.

improve their capacity to identify fraudulent transactions and efficiently reduce their impact by including RMP as an essential component in fraud detection models and systems.

Given the evident imbalance in the data, which has an impact on our approach to developing the model, we are tackling the issue of imbalanced classes in our dataset. In order to address this issue, we employ the Synthetic Minority Over-Sampling Technique (SMOTE) to artificially equalize the distribution of classes in the training data. This procedure entails manufacturing artificial samples from the minority class (frauds) in order to provide a training environment that is more evenly distributed. After applying SMOTE, we transform the datasets into NumPy arrays to ensure compatibility with TensorFlow. Subsequently, we divide the features into continuous and categorical inputs in order to utilize them in our multimodal neural network model.

Applying SMOTE has equalized the dataset, ensuring a balanced representation of both classes (fraud and non-fraud), which is essential for training a resilient fraud detection model. Moreover, transforming data into NumPy arrays and explicitly defining the data type guarantees compatibility with machine learning packages and enables efficient numerical computations. By dividing the features into continuous and categorical, it becomes possible to apply specific preprocessing and modeling techniques to each type of data, resulting in enhanced model performance and interpretability.

4 | Data Analysis and Presentation of the Results

We design and build a developed multimodal neural network model specifically for the purpose of fraud detection. To ensure a clean setup, we begin by deleting any previous TensorFlow sessions. The model utilizes “elu” (exponential linear unit) activations to improve learning capabilities, especially when dealing with non-linear data transformations. The network architecture comprises distinct input layers for continuous and categorical data. The continuous data pipeline consists of two densely connected layers that handle inputs such as transaction distances and ratios. Simultaneously, the categorical data, which represents transaction features such as chip usage and online ordering, is processed through its own set of thick layers. Subsequently, both routes merge, integrating their characteristics into a unified flow, which proceeds through further compact layers, culminating in a sigmoid output layer for the purpose of binary classification. This output provides a prediction on the likelihood of a transaction being fraudulent. The model is compiled using the Adam optimizer and its performance is evaluated using metrics such as binary accuracy, precision, recall, and AUC, which collectively provide a thorough assessment of its performance. The network’s architecture is assessed to confirm its configuration and preparedness for training. Subsequently, we commence training our neural network model utilizing the evenly distributed training data. We employ both continuous and categorical inputs, ensuring that the model acquires knowledge from the varied characteristics at its disposal. The training procedure involves doing validation stages utilizing distinct test data to assess the model’s performance and prevent overfitting.

The training was configured to run for a maximum of 50 epochs, using a batch size of 32. In order to optimize the training process, we employ an early stopping callback. This callback tracks the validation loss and stops the training process if there is no improvement over multiple epochs. This ensures that we retain the best model without performing needless computations.

Typically, after preparing the entire dataset, the analysis was conducted in three different phase as follows:

- The first phase uses the first three variables to detect fraud (see Figure 3). “the distance from home where the transaction happened,” “the distance from last transaction happened,” and “Ratio of purchased price transaction to median purchase price” and “Is the transaction fraudulent.”
- The second phase use the four variables to detect fraud (see Figure 4) “Is the transaction happened from same retailer,” “Is the transaction through chip (credit card),” “Is the transaction happened by using PIN number,” “Is the transaction an online order,” “Is the transaction fraudulent.”
- The last phase of the experimental setup uses all the variables to detect fraud (see Figure 5). These are, (“the distance from home where the transaction happened,” “the distance from last transaction happened,” and “Ratio of purchased price transaction to median purchase price”) and (“Is the transaction happened from same retailer,” “Is the transaction through chip (credit card),” “Is the transaction happened by using PIN number,” “Is the transaction an online order”) with “Is the transaction fraudulent.”

Figure 5 illustrates the direct relationships between the variables and the FRA outcome, as indicated by the arrows. The left-side

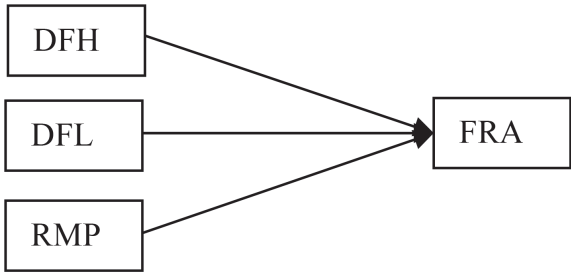


FIGURE 3 | The first experimental training setup.

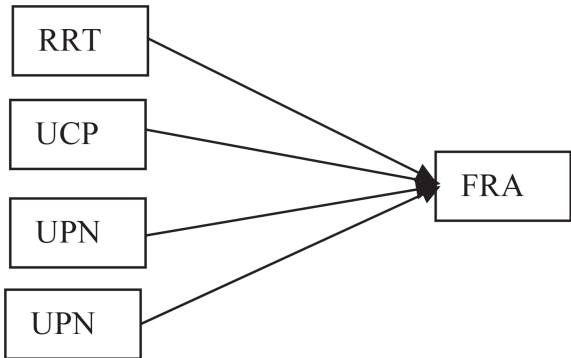


FIGURE 4 | The second experimental training setup.

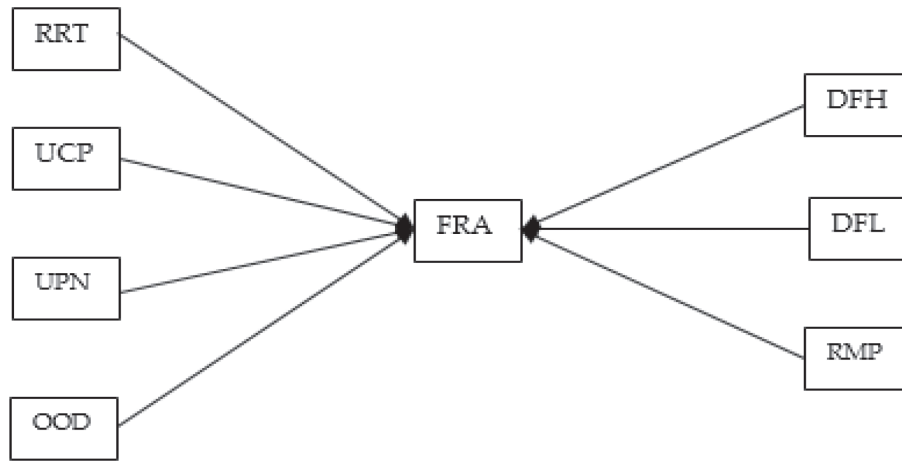


FIGURE 5 | The final experimental training setup.

features (RRT, UCP, UPN, OOD) denote interactions associated to the transactions. The right-side features (DFH, DFL, RMP) primarily address the spatial and financial aspects of the transaction. This research established an integration for fraud detection by combining variables used to predict the likelihood of a transaction being fraudulent (FRA). Interactions related data (RRT, UCP, UPN, OOD) is analyzed in conjunction with contextual and financial data (DFH, DFL, RMP) to identify anomalies that could suggest fraudulent activity. This configuration establishes the foundation for the ultimate experimental model, wherein all input features collectively influence the probability of a fraudulent transaction. The system analyzes these interrelationships to discern patterns characteristic of fraudulent behavior.

5 | Presentation of the Results

The training and evaluation of the multimodal neural network model for fraud detection have produced highly promising results, showcasing remarkable performance metrics that highlight the model's usefulness in this crucial application. An exhaustive examination of the training logs and validation data uncovers a distinct pattern of progress and strong ability to apply knowledge to new situations. The model's training phase was characterized by a substantial decrease in loss, which dropped from an initial value of 0.0153 to 0.0031 after 20 epochs. The consistent decrease in loss indicates that the model was successfully acquiring knowledge and fine-tuning its parameters, resulting in reduced prediction errors. Simultaneously, the model's binary accuracy experienced a significant improvement, rising from 99.47% to 99.90% (see Table 2). The enhanced precision demonstrates that the model's forecasts became more dependable as the training advanced, showcasing its capacity to effectively apply learned patterns to the training data.

Initially, the model demonstrated excellent precision and recall metrics, which showed a little improvement as the training progressed. Precision quantifies the model's capacity to accurately identify instances of fraud that are actually present, hence indicating its effectiveness in reducing the occurrence of false positive results. Recall, however, evaluates the model's ability to accurately detect most real instances of fraudulent transactions, thus

TABLE 2 | The multimodal neural network model.

Metric	Training	Validation	Test
Accuracy	99.88%	99.91%	99.92%
Precision	99.84%	99.07%	99.17%
Recall	99.93%	99.90%	99.87%
F1-score	99.88%	99.48%	99.52%

reducing the occurrence of false negatives. The elevated values in both metrics suggest that the model was not only precise but also efficient in accurately detecting and capturing fraudulent actions.

The training and validation loss curves demonstrate the model's successful convergence behavior. Both curves exhibit a consistent decline, with the validation loss closely mirroring the training loss (refer to Figure 6). The parallel movement seen indicates that the model is effectively generalizing to new, unknown data, hence avoiding the problem of overfitting. Overfitting is a common issue where the model performs well on the training data but badly on the validation data. The accuracy plots for both the training and validation data exhibit a constant and continuous rising trend, which provides evidence of the model's resilience and reliability (refer to Figure 7). The progressive enhancement in precision throughout the epochs strengthens the model's capacity to enhance its predictive abilities over time, successfully adjusting to the patterns in the data.

After being assessed on the test dataset, the model demonstrated exceptional performance characteristics. The model achieved a precision of 99.92%, indicating its exceptional accuracy in making predictions. The model's precision of 99.17% showcases its capacity to properly detect fraudulent transactions while minimizing the occurrence of false positives (refer to Figure 8). In addition, the recall rate was 99.87%, demonstrating that the model accurately detected almost all real fraudulent transactions, effectively reducing the occurrence of false negatives (refer to Figure 9). The Area Under the Curve (AUC) was an impressive 0.9999, indicating the model's extraordinary ability to differentiate between fraudulent and non-fraudulent transactions (refer to Figure 10). The confusion matrix showed a low number of incorrect positive

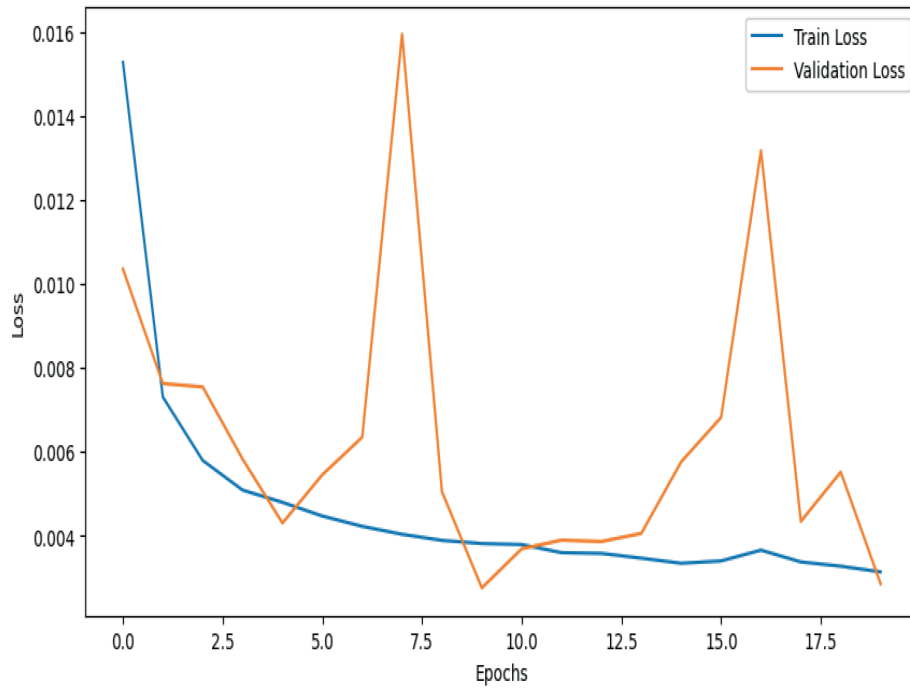


FIGURE 6 | The model loss performance.

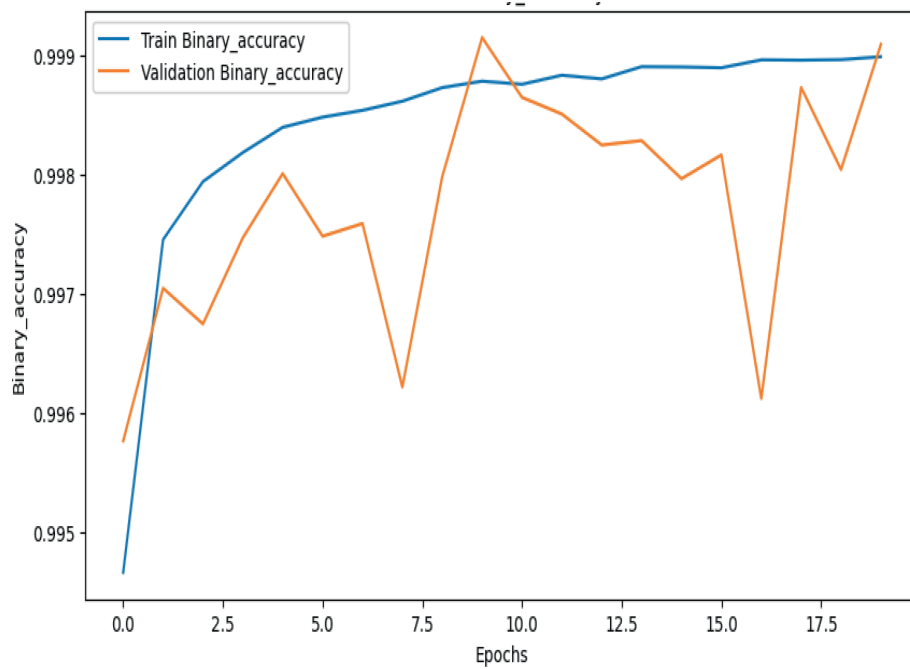


FIGURE 7 | The model accuracy performance.

and negative predictions, which strengthens the high precision and recall scores. The matrix is an essential instrument for assessing the model's performance, as it offers a distinct representation of the true positives, true negatives, false positives, and false negatives (see Figure 11).

In addition, the Receiver Operating Characteristic (ROC) curve demonstrated an AUC that was close to perfection, indicating the model's exceptional capacity to distinguish between the classes (refer to Figure 12). A large Area Under the Curve (AUC) implies that the model exhibits strong performance across various

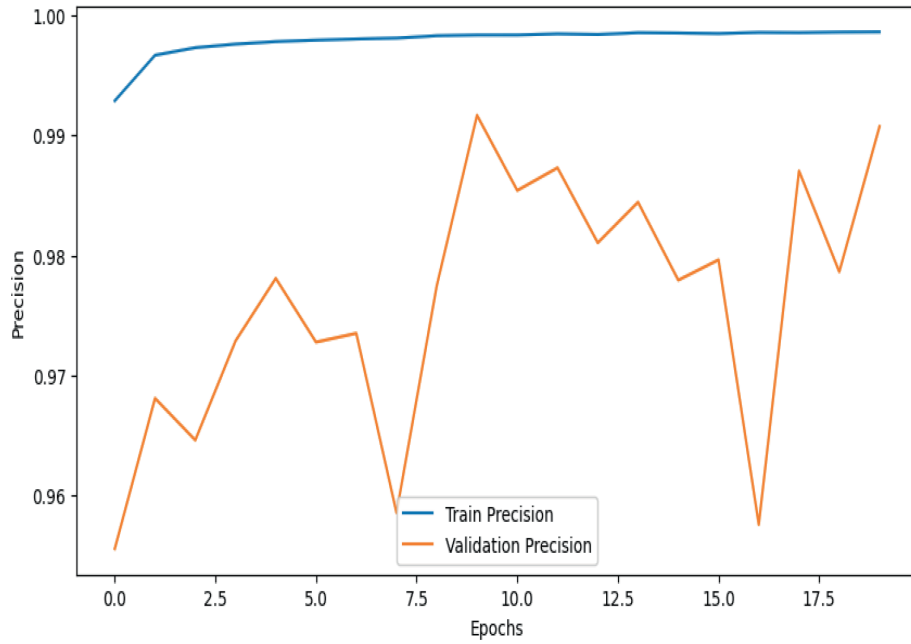


FIGURE 8 | The model precision performance.

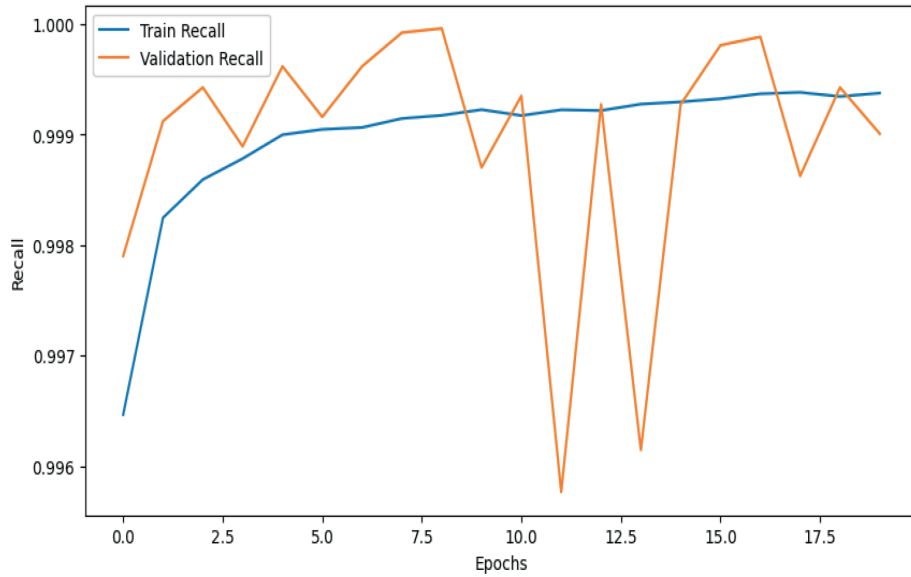


FIGURE 9 | The model recall performance.

thresholds, effectively balancing sensitivity and specificity, as evidenced by the findings of this research.

6 | Discussion

When it comes to the topic of detecting fraudulent credit card transactions, the results that were acquired from the training and evaluation of the multimodal neural network model for fraud detection have significant implications. The efficiency of the model, the practical ramifications, and the opportunities for further progress are all factors that can be taken into consideration while attempting to appreciate these implications [32–34]. The model displays exceptional performance over a wide range of

criteria, emphasizing both its robustness and its effectiveness in identifying fraudulent transactions. Over the course of 50 epochs, the model was able to effectively achieve a considerable reduction in loss, specifically a reduction from 0.0153 to 0.0031. This shows that the model not only learned effectively from the training data but also performed well on new data that it had not previously seen. The drop in loss, together with an improvement in binary accuracy from 99.47% to 99.90%, points to this conclusion.

In addition to having a high level of accuracy and completeness, the model also offers precision and recall rates that continue to increase during the training process. The fact that this is the case demonstrates that the model is able to effectively identify relevant instances of fraud (precision) and catch a significant number

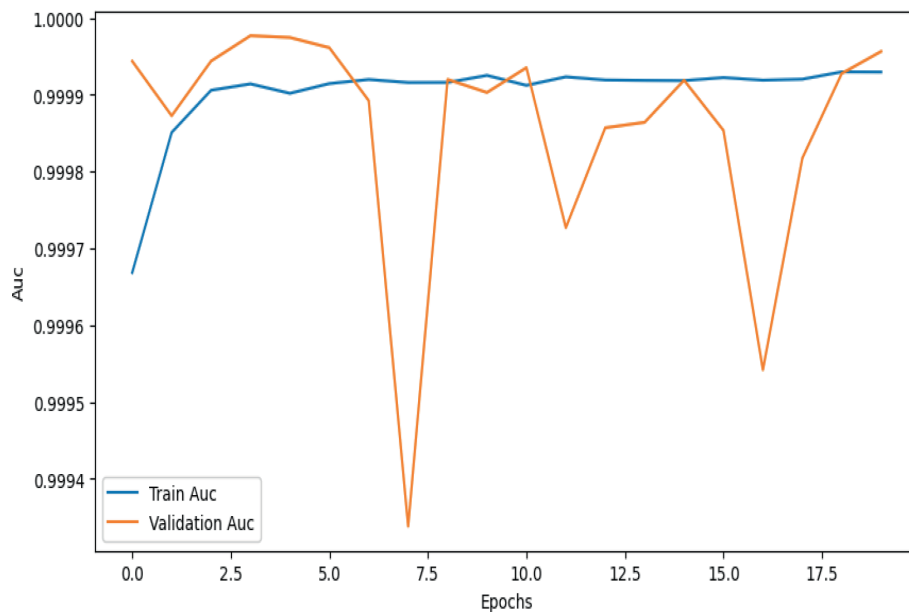


FIGURE 10 | The model AUC performance.

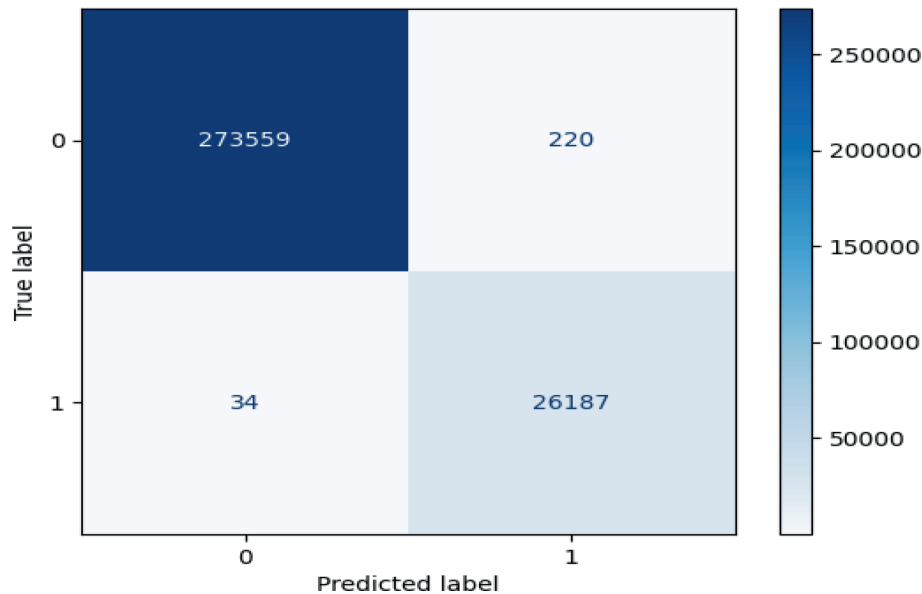


FIGURE 11 | The model confusion matrix.

of positive fraud cases (recall). With an accuracy of 99.92%, precision of 99.17%, recall of 99.87%, and an area under the curve (AUC) of 0.9999, the model shown remarkable performance on the test dataset. These metrics provide evidence that the model is able to detect fraudulent transactions in a reliable and efficient manner while simultaneously reducing the number of instances of both false positives and false negatives.

The findings will have substantial repercussions for the operational environments of establishments that deal with financial matters. By ensuring high levels of accuracy and precision, the

likelihood of legitimate transactions being wrongly classified as fraudulent is decreased. This helps to reduce the amount of irritation that customers feel and increases their trust in the institution's procedures that detect fraudulent activity. The system has the potential to effectively identify the majority of fraudulent transactions if it is able to achieve a high recall rate. This will result in a reduction in financial losses and will protect the assets of customers. Furthermore, the F1-score, which is a measure that takes into account both precision and recall, offers additional evidence that the model is reliable when applied to events that occur in the real world. It is clear that the model is capable of

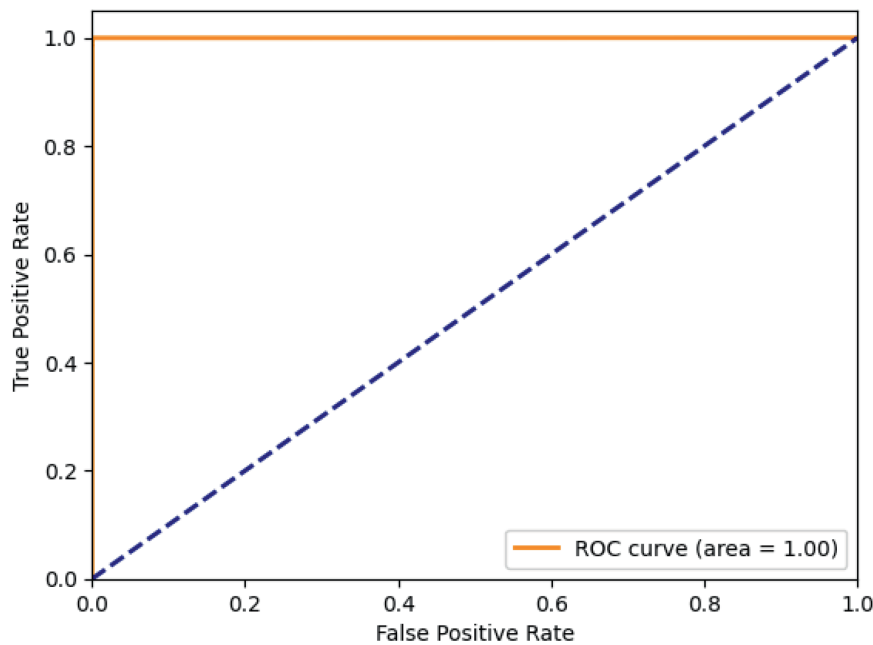


FIGURE 12 | The model receiver operating characteristic (ROC) curve.

effectively detecting fraud while simultaneously reducing the number of false alarms, as evidenced by the F1-score of 99.52% that it achieved on the test data. For the purpose of maximizing operating efficiency and maintaining the satisfaction of customers, this equilibrium is absolutely necessary.

As a result of the depiction of training and validation loss curves, which display good convergence behavior, it appears that the model did not suffer from over-fitting. The implication of this is that the capability of the model to function on new data that it has not before encountered is anticipated to be just as effective as it was throughout the training phase. In a similar manner, the accuracy plots demonstrate a consistent growth pattern for both the training and validation sets. This demonstrates that the model is robust and has the ability to perform dependably in situations that resemble those that occur in the real world. These additional insights into the performance of the model are provided by the confusion matrix as well as the ROC curve. There is a low occurrence of both false positives and false negatives in the confusion matrix, which helps to improve the high precision and recall values. A further demonstration of the model's outstanding capability to differentiate between fraudulent and legitimate transactions is provided by the nearly perfect area under the curve (AUC) in the ROC equation.

The performance of the model establishes a stringent standard for fraud detection systems that will be developed in the future. By demonstrating that multimodal neural networks are capable of effectively capturing detailed patterns in transactional data that may potentially suggest fraudulent conduct, this model demonstrates that it is effective in doing so. To further enhance the accuracy and robustness of the model, it is recommended that future enhancements give priority to the incorporation of additional data sources, such as data on behavioral patterns or transaction information that is more comprehensive. Furthermore, the model can be guaranteed to adapt to ever-changing fraud

patterns and methods if it is being monitored on a constant basis and retrained on a regular basis utilizing new data.

The deployment of this proactive strategy for detecting fraud has the potential to significantly improve an organization's ability to protect itself against fraudulent strategies that are always evolving for new purposes. It is not enough to simply measure the performance of the model; the implications of these discoveries extend well beyond that. The authors highlight the enormous impact that contemporary machine learning techniques can have on the enhancement of the dependability and security of financial transactions. The multimodal neural network model is able to properly detect fraudulent transactions, which leads to a reduction in financial losses as well as an improvement in customer trust and satisfaction. As financial institutions are confronted with increasingly complicated fraud efforts, it will be essential for them to make use of advanced models in order to ensure the continued existence of a transactional environment that is both secure and successful.

Machine learning techniques have been extensively utilized [35–39] and researched in the domain of detecting fraudulent credit card transactions. The performance of these algorithms is compared in Table 3 based on key parameters such as Accuracy, Precision, Recall, and F1-score. The present study employs a multimodal neural network model and compares its performance to that of previous investigations.

After analyzing multiple investigations, it has been determined that the current study, which utilizes multimodal neural networks, achieves the highest performance. It attains the utmost level of accuracy (99.88%), precision (99.84%), recall (99.93%), and F1-score (99.88%), outperforming all other models in each performance category. This demonstrates the superior proficiency of multimodal neural networks in precisely and reliably detecting fraudulent credit card transactions.

TABLE 3 | Comparison of previous research studies findings.

Study	Algorithm	Accuracy	Precision	Recall	F1-score
[3]	Random Forest	99.96%	96.38%	81.63%	—
[4]	KNN	97.92%	—	—	—
[6]	Gradient boosting	98.40%	97.34%	—	56.95%
[31]	Random Forest	98.912%	98.912%	98.912%	98.924%
Current Study	Multimodal Neural Networks	99.88%	99.84%	99.93%	99.88%

The comparison highlights the exceptional performance of the multimodal neural network model in the present study, namely in terms of its well-balanced and highly accurate precision, recall, and F1-score. This indicates that the model not only precisely detects fraudulent transactions but does so regularly and dependably, which is essential for practical situations where both incorrect identifications and missed identifications have important repercussions. The exceptional performance indicators indicate that this model has the potential to greatly enhance the security and efficiency of fraud detection systems, resulting in reduced financial losses and increased customer trust in financial institutions.

7 | Conclusion

The research being conducted into creating a multimodal neural network model for detecting fraudulent credit card transactions has produced extremely promising outcomes. The model exhibited outstanding performance in various parameters, including as accuracy, precision, recall, and F1-score, attaining a test accuracy of 99.92% and an AUC of 0.9999. The measurements demonstrate the model's resilience and its ability to effectively and consistently detect fraudulent transactions while minimizing both type I and type II errors. The substantial decrease in loss and enhancements in binary accuracy across 50 epochs demonstrate that the model successfully acquired knowledge and demonstrated strong generalization capabilities from the training data. The model's high precision and recall values confirm its effectiveness in accurately detecting relevant fraud cases and capturing the bulk of fraudulent transactions. The model's performance has practical implications in terms of minimizing customer pain and enhancing trust in fraud detection systems. This is achieved by reducing the likelihood of legal transactions being mistakenly marked and accurately identifying the majority of fraud cases. The balanced F1-score high-lights the model's dependability in preserving operational efficiency and customer happiness. The visualization of training progress, which includes plots of loss and accuracy, along with the confusion matrix and ROC curve, provides evidence of the model's successful convergence and exceptional discriminatory capacity. This research establishes a rigorous standard for future fraud detection systems, showcasing the capabilities of modern machine learning approaches in improving the security of financial transactions. Consistent surveillance and regular reeducation will guarantee that the model adjusts to changing fraud tendencies, hence enhancing the defenses against complex fraudulent schemes. The results emphasize the significant influence of these powerful models

in pre-serving a safe and effective financial system, eventually leading to enhanced financial stability and customer confidence.

There is a significant amount of potential for value in enhancing the capabilities of hybrid neural network methods to enable quick model responses that could help to prevent the execution of fraudulent transactions. This is due to the fact that the ability to detect fraudulent card activity in real time or near real time was reported to be one of the most important priorities in the finance sector. As a result, it is possible that future research may concentrate on improving the performance of hybrid neural network models like these, drawing particular attention to the enhancement of the models' capacity to rapidly interpret transactional data streams.

Acknowledgments

This study was supported by Princess Nourah Bint Abdulrahman University, Project number (PNURSP2024R435), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. P. O. Shoetan, A. T. Oyewole, C. C. Okoye, and O. C. Ofodile, "Reviewing the Role of Big Data Analytics in Financial Fraud Detection," *Finance & Accounting Research Journal* 6, no. 3 (2024): 384–394.
2. D. Jamil, A. Iqbal, B. Bhattarai, et al., "Sustainable Fraud Detection in Green Finance Empowered With Machine Learning Approach," *Remittances Review* 9, no. 1 (2024): 1897–1914.
3. D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit Card Fraud Detection-Machine Learning Methods," in *2019 18th International Symposium Infoteh-Jahorina (INFOTEH)* (IEEE, 2019), 1–5.
4. J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis," in *2017 International Conference on Computing Networking and Informatics (ICCNi)* (IEEE, 2017), 1–9.
5. F. Itoo and S. S. Meenakshi, "Comparison and Analysis of Logistic Regression, Naïve Bayes and KNN Machine Learning Algorithms for Credit Card Fraud Detection," *International Journal of Information Technology* 13, no. 4 (2021): 1503–1511.
6. A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," *IEEE Access* 8 (2020): 25579–25587.

7. A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," *Big Data and Cognitive Computing* 8, no. 1 (2024): 6.
8. A. U. Aftab, I. Shahzad, M. Anwar, A. Sajid, and N. Anwar, "Fraud Detection of Credit Cards Using Supervised Machine Learning," *Pakistan Journal of Emerging Science and Technologies (PJEST)* 4, no. 3 (2023): 38–51.
9. S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," *IEEE Access* 8, no. 7 (2019): 93010–93022.
10. S. Warghade, S. Desai, and V. Patil, "Credit Card Fraud Detection From Imbalanced Dataset Using Machine Learning Algorithm," *International Journal of Computer Trends and Technology* 68, no. 3 (2020): 22–28.
11. G. Joshi, R. Walambe, and K. Kotecha, "A Review on Explainability in Multimodal Deep Neural Nets," *IEEE Access* 9 (2021): 59800–59821.
12. K. Fu, D. Cheng, Y. Tu, and L. Zhang, "Credit Card Fraud Detection Using Convolutional Neural Networks," in *Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III* (Springer International Publishing, 2016), 483–490.
13. Z. Jin, J. Cao, H. Guo, Y. Zhang, and J. Luo, "Multimodal Fusion With Recurrent Neural Networks for Rumor Detection on Microblogs," in *Proceedings of the 25th ACM International Conference on Multimedia* (2017), 795–816.
14. Y. Dou, Z. Liu, L. Sun, Y. Deng, H. Peng, and P. S. Yu, "Enhancing Graph Neural Network-Based Fraud Detectors Against Camouflaged Fraudsters," in *Proceedings of the 29th ACM International Conference on Information & Knowledge Management* (2020), 315–324.
15. M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, "An Intelligent Payment Card Fraud Detection System," *Annals of Operations Research* 334, no. 1 (2024): 445–467.
16. F. J. Ordóñez and D. Roggen, "Deep Convolutional and LSTM Recurrent Neural Networks for Multimodal Wearable Activity Recognition," *Sensors* 16, no. 1 (2016): 115.
17. K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *IEEE Access* 6 (2018): 14277–14284.
18. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random Forest for Credit Card Fraud Detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)* (2018), 1–6, <https://doi.org/10.1109/ICNSC.2018.8361343>.
19. W. Yang, Y. Zhang, K. Ye, L. Li, and C. Z. Xu, "Ffd: A Federated Learning Based Method for Credit Card Fraud Detection," in *Big Data – BigData 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings* (Springer International Publishing, 2019), 18–32.
20. G. M. Paldino, B. Lebiclot, Y. A. Le Borgne, et al., "The Role of Diversity and Ensemble Learning in Credit Card Fraud Detection," *Advances in Data Analysis and Classification* 18, no. 1 (2024): 193–217.
21. M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach," *Journal of Theory and Practice of Engineering Science* 4, no. 2 (2024): 23–30.
22. E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection," *IEEE Access* 31, no. 10 (2022): 16400–16407.
23. S. L. Marie-Sainte, M. B. Alamir, D. Alsaleh, G. Albakri, and J. Zouhair, "Enhancing Credit Card Fraud Detection Using Deep Neural Network," in *Intelligent Computing: Proceedings of the 2020 Computing Conference*, Volume 2 (Springer International Publishing, 2020), 301–313.
24. I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced Credit Card Fraud Detection Based on Attention Mechanism and LSTM Deep Model," *Journal of Big Data* 8 (2021): 1–21.
25. P. Fränti and R. Marinescu-Istodor, "Soft Precision and Recall," *Pattern Recognition Letters* 167 (2023): 115–121.
26. J. Cook and V. Ramadas, "When to Consult Precision-Recall Curves," *Stata Journal* 20 (2020): 131–148, <https://www.kaggle.com/datasets/dhanushnarayanar/credit-card-fraud/data>.
27. W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications* 193 (2022): 116429.
28. S. Khodabandehlou and A. H. Golpayegani, "FiFrauD: Unsupervised Financial Fraud Detection in Dynamic Graph Streams," *ACM Transactions on Knowledge Discovery from Data* 18, no. 5 (2024): 1–29.
29. M. G. Nakitende, A. Rafay, and M. Waseem, "Frauds in Business Organizations: A Comprehensive Overview," *Research Anthology on Business Law, Policy, and Social Responsibility* 18, no. 5 (2024): 848–865.
30. G. L. Sahithi, V. Roshmi, Y. V. Sameera, and G. Pradeepini, "Credit Card Fraud Detection using Ensemble Methods in Machine Learning," in *Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 28–30 April 2022, 1237–1241.
31. D. Prusti and S. K. Rath, "Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning Techniques," in *Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 6–8 July 2019, 1–6.
32. S. A. Ebiaredoh-Mienye, E. Esenogho, and T. G. Swart, "Artificial Neural Network Technique for Improving Prediction of Credit Card Default: A Stacked Sparse Autoencoder Approach," *International Journal of Electrical and Computer Engineering* 11, no. 5 (2021): 4392.
33. S. A. Ebiaredoh-Mienye, E. Esenogho, and T. G. Swart, "Integrating Enhanced Sparse Autoencoder-Based Artificial Neural Network Technique and Softmax Regression for Medical Diagnosis," *Electronics* 9, no. 11 (2020): 1963.
34. S. A. Ebiaredoh-Mienye, T. G. Swart, E. Esenogho, and I. D. Mienye, "A Machine Learning Method With Filter-Based Feature Selection for Improved Prediction of Chronic Kidney Disease," *Bioengineering* 9, no. 8 (2022): 350.
35. M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldahri, A. Alzahrani, and A. A. Alarood, "A MapReduce Based Approach for Secure Batch Satellite Image Encryption," *IEEE Access* 11, no. 8 (2023): 62865–62878.
36. M. Faheem and M. A. Al-Khasawneh, "Multilayer Cyberattacks Identification and Classification Using Machine Learning in Internet of Blockchain (IoBC)-Based Energy Networks," *Data in Brief* 54, no. 8 (2024): 110461.
37. N. Ahmed, A. A. Hashmani, S. Khokhar, M. A. Tunio, and M. Faheem, "Fault Detection Through Discrete Wavelet Transform in Overhead Power Transmission Lines," *Energy Science & Engineering* 11, no. 11 (2023): 4181–4197.
38. F. Ullah, M. Faheem, M. A. Hashmi, R. Bashir, and A. R. Khan, "A Novel 1-Dimensional Cosine Chaotic Equation and Digital Image Encryption Technique," *IEEE Access* 12, no. 6 (2024): 118857–118874.
39. A. Raza, Z. H. Qaisar, N. Aslam, M. Faheem, M. W. Ashraf, and M. N. Chaudhry, "TL-GNN: Android Malware Detection Using Transfer Learning," *Applied AI Letters* 5, no. 3 (2024): 1–14.