

Enhancing credit card fraud detection with synthetic minority over-sampling technique-integrated extreme learning machine

Iman Kadhim Ajlan¹, Mohammed Ibrahim Mahdi², Hayder Murad¹, Fahad Taha AL-Dhief³,
Nurhizam Safie⁴, Yasir Hussein Shakir⁵, Ali Hashim Abbas⁶

¹Department of Computer Science, College of Education for Pure Science, Wasit University, Kut, Iraq

²Department of Computer Science, College of Computer Science and Information Technology, Wasit University, Kut, Iraq

³Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia

⁴Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor

⁵College of Graduate Studies, Universiti Tenaga Nasional, Kajang, Malaysia

⁶Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq

Article Info

Article history:

Received Mar 13, 2025

Revised Sep 25, 2025

Accepted Oct 16, 2025

Keywords:

Class imbalance

Credit card fraud detection

Cybersecurity

Extreme learning machine

SMOTE

ABSTRACT

Many works in cybersecurity detection suffer from low accuracy rates, particularly in real-world applications, where imbalanced datasets and evolving fraud strategies pose significant hurdles. This study introduces an optimized extreme learning machine (ELM) algorithm to address these challenges by dynamically adjusting hidden nodes ranging from 10 to 100 with an increment step of 10 and integrating two activation functions. The proposed method utilizes the synthetic minority over-sampling technique (SMOTE) to handle class imbalance effectively and incorporates a comprehensive evaluation using descriptive statistics, visualization, and significance testing. The proposed ELM-SMOTE method achieves the highest results including an accuracy of 99.710%, recall of 85.811%, specificity of 99.743%, and G-mean of 92.068%. These outcomes reflect the robustness and adaptability of the proposed ELM algorithm in detecting fraudulent transactions. This study emphasizes the importance of a holistic performance analysis, addressing gaps in existing methods and providing a scalable framework for real-world fraud detection applications.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Fahad Taha AL-Dhief

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia

Bangi 43600, Malaysia

Email: fahad@ukm.edu.my

1. INTRODUCTION

In recent years, the exponential growth of digital transactions has brought convenience and efficiency to global commerce [1]. However, this rise in digital payments has also given rise to an alarming increase in fraudulent activities, particularly in credit card transactions [2]. Credit card fraud detection becomes a critical challenge in the field of cybersecurity, requiring innovative and effective solutions to protect financial systems and consumer trust [3]. Systems of cybersecurity detection have developed significantly over recent years, leveraging advancements in artificial intelligence (AI), machine learning (ML), and deep learning (DL) [4]. Among these, extreme learning machines (ELM) have garnered attention for their rapid learning capabilities and minimal computational requirements [5]. ELM, a single-layer feedforward neural network (SLFN), offers an advantage in handling large datasets, making it a promising candidate for real-time fraud detection [6]. Despite its potential, the application of ELM algorithm in credit

card fraud detection remains underexplored, especially in addressing class imbalances and incorporating robust statistical evaluations [7].

In general, security is a critical component of every system and organization [8]–[10]. In particular, credit card fraud detection poses unique challenges because of the complexity and evolving tactics involved in fraudulent activities [11]. In the systems of credit card fraud detection, the datasets are typically highly imbalanced, with legitimate transactions vastly outnumbering fraudulent ones [12]. This imbalance often skews the performance of models, where it may obtain high overall accuracy but poor sensitivity and specificity for the minority class (i.e., fraudulent transactions). As fraudulent activities continue to grow in sophistication, conventional detection systems often find it difficult to keep pace, highlighting the importance of adopting more adaptive and versatile approaches [13]. Previous research has explored a wide range of ML techniques for credit card fraud detection, including logistic regression (LR) [14], support vector machines (SVMs) [15], random forests (RFs) [16], and neural networks (NNs) [17]. Although these algorithms have produced encouraging results, many still depend on architectures with a fixed number of neurons, which restricts their capacity to handle diverse and complex data patterns. In addition, several cybersecurity detection studies have reported suboptimal accuracy, particularly when applied to real-world datasets that contain noise and irregularities.

Another significant gap identified in the existing literature is the absence of thorough statistical evaluations. Many studies assess model performance using only a limited range of metrics, typically accuracy or precision, while overlooking crucial measures such as specificity, G-mean and F-measure. This narrow evaluation approach hampers a comprehensive understanding of model effectiveness, especially in the context of imbalanced datasets where accuracy alone fails to capture true performance. Moreover, the limited use of descriptive statistics, visualization, and significance testing further reduces the interpretability and reliability of the reported results. In contrast, these techniques are fundamental to validating the robustness of ML models. Descriptive statistics offer valuable insights into data distribution and variability, visualization helps uncover underlying trends and anomalies, and significance testing determines whether observed differences in performance are statistically meaningful rather than due to random variation. Despite their importance, such methods are frequently neglected in credit card fraud detection research. Overall, existing studies in this domain continue to face several limitations, summarized as i) many models rely on a fixed number of neuron nodes, reducing adaptability to diverse datasets; ii) cybersecurity detection systems often exhibit low accuracy, particularly when tested on real-world data; iii) descriptive statistics, visualization, and significance testing are commonly excluded from evaluation frameworks; and iv) most cybersecurity detection systems are assessed using a limited set of evaluation metrics, ignoring a holistic performance analysis.

The current study aims to address these limitations by exploring the application of ELM for credit card fraud detection using a dynamic approach. The proposed methodology incorporates varying numbers of hidden nodes and evaluates two activation functions to identify the optimal configuration. Additionally, this study emphasizes a comprehensive evaluation framework, including accuracy, precision, recall, specificity, F-measure, G-mean, descriptive statistics, visualization, and significance testing. In addition, to overcome the previously mentioned limitations, this paper summarizes the following key contributions: i) dynamic hidden node configurations: unlike traditional approaches, this study evaluates ELM with varying numbers of hidden nodes, ranging from 10 to 100, to identify the optimal configuration for credit card fraud detection; ii) comparison of activation functions: two widely used activation functions (i.e., sigmoid and rectified linear unit (ReLU)) are assessed to determine their impact on model performance; iii) comprehensive statistical evaluation: the proposed methodology includes a thorough evaluation framework, such as accuracy, precision, recall, specificity, F-measure, G-mean, and confusion matrices. Descriptive statistics, visualization, and significance testing are utilized to ensure a robust analysis; iv) addressing class imbalance: the synthetic minority over-sampling technique (SMOTE) is employed to balance the dataset, ensuring equitable learning for both majority and minority classes; and v) holistic performance insights: by integrating multiple metrics and statistical techniques, this study provides a nuanced understanding of ELM's effectiveness in credit card fraud detection.

The rest of the current paper is structured as follows: section 2 presents the related works presented in detecting credit card fraud. Section 3 delivers and explains the proposed method in terms of the database and the proposed ELM algorithm. Section 4 gives the experimental setup and results analysis. Section 5 provides the discussion of the experimental results. Finally, section 6 presents the conclusion of this paper.

2. RELATED WORK

Recently, researchers are highly interested in fraud detection due to the increasing prevalence of fraudulent activities, particularly in the financial sector [18]. As the volume of financial transactions continues

to grow, so does the complexity of detecting fraudulent behavior. ML techniques have gained considerable attention for their ability to identify patterns in large datasets, making them effective tools for fraud detection. Researchers have explored a variety of algorithms, ranging from traditional methods like decision tree (DT) and LR to more advanced approaches such as DL and ensemble methods. Trivedi *et al.* [19] presented an effective credit card fraud detection mechanism that incorporates a feedback system based on ML methodologies. The feedback approach enhances the classifier's detection rate while ensuring cost-effectiveness. The study evaluates the performance of several ML models, including RF, DT, artificial neural networks (ANN), SVM, naïve Bayes (NB), LR, and gradient boosting classifier (GBM), applied to a slightly imbalanced credit card fraud dataset. The dataset consists of transaction data from European account holders, with 284,807 transactions. Both raw and pre-processed data were used in the experiments. The results showed that RF achieved an accuracy of 94.99%, NB 91.88%, LR 90.44%, SVM 93.96%, k-nearest neighbors (KNN) 94.99%, DT 90.99%, and GBM 94.00%. However, this work has been ignored the statistical analysis of the presented methods. Another work has been focused on utilizing multiple ML algorithms, such as SVM algorithm, KNN algorithm, and ANN algorithm, to predict the occurrence of fraud [20]. The study compares the performance of these supervised ML techniques with DL approaches to distinguish between fraudulent and non-fraudulent transactions. The results show that the KNN algorithm achieved an accuracy of 0.9982, followed by the ANN with 0.9992, and the SVM with 0.9349. Although this work achieved high results in the fraud detection, the suggested work has not been evaluated in terms of other important measures such as specificity, F-measure, and G-mean. Moreover, there was no statistical evaluation.

Alarfaj *et al.* [21] has been aimed to address challenges in credit card fraud detection, including the availability of public data, high class imbalance, changes in fraud patterns, and high false alarm rates. The existing literature presents several ML-based approaches for fraud detection, such as ELM, DT, RF, SVM, LR, and extreme gradient boosting (XGBoost). However, due to low accuracy, there remains a need to implement state-of-the-art DL algorithms to reduce fraud losses. The study focuses on leveraging recent developments in DL to improve fraud detection performance. A comparative analysis between ML and DL algorithms was conducted to identify the most efficient methods. The empirical analysis was carried out using the European card benchmark dataset for fraud detection. Initially, ML algorithms were applied to the dataset, resulting in some improvement in fraud detection accuracy. Subsequently, three architectures based on convolutional neural networks (CNN) were used to further enhance detection performance. The addition of more layers led to increased accuracy. The study also explored variations in the number of hidden layers, epochs, and the latest models to optimize results. The evaluation demonstrated that the proposed DL model achieved improved results, with an accuracy of 99.9%, F1-score of 85.71%, precision of 93%, and area under the curve (AUC) of 98%, outperforming existing ML and DL algorithms for credit card fraud detection. However, the authors have not evaluated the presented algorithms in terms of G-mean, F-measure, and specificity. Besides, they have not assessed their methods statistically.

Ileberi *et al.* [22] has been proposed a ML-based credit card fraud detection engine that utilizes a genetic algorithm (GA) for feature selection. Once the optimal features are selected, the proposed detection engine employs several ML classifiers, including DT, RF, LR, ANN, and NB. To validate its performance, the engine was evaluated using a dataset generated from European cardholders. The results showed that the GA-RF classifier achieved an accuracy of 99.98%, followed by GA-DT with 99.92%, GA-LR with 99.91%, and GA-NB with 99.44%. A limitation of this work is that it has not been evaluated in terms of statistical analysis. While the study focuses on optimizing ML classifiers and feature selection, it does not provide an in-depth statistical evaluation of the results. This omission limits the understanding of the model's performance in terms of statistical significance, which could offer more robust insights into the reliability and generalizability of the proposed fraud detection engine.

Another study has been presented an effective approach for credit card fraud detection using a NN ensemble classifier paired with a hybrid data resampling technique [23]. The ensemble classifier is built by integrating a long short-term memory (LSTM) NN as the base model within the adaptive boosting (AdaBoost) framework. The hybrid resampling method is implemented using the SMOTE combined with the edited nearest neighbor (ENN) method. The proposed approach is tested on publicly available real-world credit card transaction datasets, and its performance is compared with several algorithms, including SVM, multilayer perceptron (MLP), DT, traditional AdaBoost, and LSTM. The experimental findings indicate that classifiers trained on resampled data achieved better results, with the LSTM ensemble outperforming other models, attaining a sensitivity of 0.996 and specificity of 0.998. However, the limitation of this work is that it has been evaluated in terms of sensitivity, specificity, and AUC only, without considering other important performance metrics or a more comprehensive statistical analysis.

Aghwar *et al.* [24] has been investigated the performance of five ML algorithms, trained both with and without the SMOTE, to assess their effectiveness in credit card fraud detection. The algorithms tested include RF, KNN, NB, SVM, and LR. The methodology was implemented and evaluated through an application programming interface (API) using Flask and Streamlit in Python. Prior to applying SMOTE, the

RF classifier demonstrated the highest performance with an accuracy of 0.9802, while LR, KNN, NB, and SVM algorithms have been achieved accuracies of 0.9219, 0.9435, 0.9508, and 0.9008, respectively. After the application of SMOTE, the RF classifier achieved a higher accuracy of 0.9919, while LR, KNN, NB, and SVM algorithms reached accuracies of 0.9805, 0.9210, 0.9125, and 0.8145, respectively. These results emphasize the advantage of combining RF with SMOTE to improve prediction accuracy in fraud detection tasks. Nevertheless, the limitation of this work is that the evaluation was solely based on accuracy, precision, and recall, without considering other important performance metrics or conducting a more comprehensive statistical analysis.

3. METHOD

This section describes the methodology adopted for credit card fraud detection, including details about the database and the SMOTE method. It also covers the implementation of the proposed ELM algorithm used for detecting credit card fraud. Subsequent sections will explain the credit card transaction database and the proposed ELM algorithm.

3.1. Database

The credit card fraud detection dataset used in this study was sourced from Kaggle [25], a widely recognized platform for data science research and competitions. The dataset comprises 284,807 transactions conducted by European cardholders in September 2013. It is characterized by a strong class imbalance, containing only 492 fraudulent transactions, which represent approximately 0.172% of the total records. Each transaction is described by 30 numerical features, including the attributes time and amount, while the remaining 28 features were derived through principal component analysis (PCA) to protect sensitive information and reduce dimensionality. The target variable, class, denotes whether a transaction is legitimate '0' or fraudulent '1'. To mitigate the issue of class imbalance, the SMOTE was applied to the training set. SMOTE generates synthetic samples for the minority class, allowing for a more balanced and representative dataset during model training. Additionally, the time and amount features were normalized using min-max scaling, and all input features were standardized to ensure compatibility and stable performance of the ELM algorithm.

3.1.1. Data preprocessing

In this study, the SMOTE technique is applied exclusively to the training dataset in order to address class imbalance between legitimate and fraudulent transactions. The SMOTE technique operates by generating synthetic instances of the minority class (fraud) using the KNNs approach. Specifically, for each minority instance, new samples are created by interpolating between it and its nearest neighbors in the feature space, thereby enriching the training data without simply duplicating original examples. To avoid overfitting, the SMOTE technique was not applied to the test data, ensuring that model evaluation was conducted on original, unseen data. While synthetic sampling improves the model's ability to learn from rare fraud cases, care was taken to apply SMOTE only before the model was trained to preserve the integrity and realism of the performance evaluation. To prepare the credit card fraud dataset for further analysis, the following preprocessing steps were performed:

- i) Normalization: the 'time' and 'amount' features were normalized using min-max scaling to ensure all variables are on a similar scale.
- ii) Feature scaling: all features were rescaled to a range between 0 and 1 using the min-max scaler.
- iii) Class imbalance handling: the SMOTE was applied to the training dataset in order to balance the class distribution, enabling the model to learn effectively from both majority and minority samples.
- iv) Train-test split: the dataset was divided into training (70%) and testing (30%) subsets using stratified sampling to maintain the original class distribution across both sets.

3.2. Extreme learning machine classifier

Credit card fraud detection plays a vital role in helping financial institutions prevent unauthorized transactions and minimize financial losses. In this study, the ELM is employed as the primary ML algorithm due to its efficiency in handling large datasets and its high computational speed. The ELM algorithm is proposed as an effective and scalable approach for detecting fraudulent activities in credit card transactions. It is based on the concept of SLFNs, which are known for their ability to manage high-dimensional and imbalanced datasets [26]. In other words, the ELM algorithm is a type of SLFN characterized by fast training and low computational cost. Within the ELM framework, the input weights and biases of the hidden layer are randomly assigned and remain fixed, while the output weights are calculated analytically using a closed-form solution, often through the Moore-Penrose pseudoinverse [27]. This design removes the need for iterative optimization of hidden layers, enabling the model to achieve faster convergence. Owing to its computational efficiency and capacity to process large-scale data, ELM is particularly well-suited for fraud detection

applications that require real-time or near-real-time performance. The proposed ELM framework demonstrates rapid training capability, strong generalization performance, and the integration of synthetic oversampling methods to address class imbalance issues. The initial stage of the framework involves preparing the dataset to ensure optimal performance of the ELM algorithm. The credit card dataset is first loaded, and the time and amount features are normalized using the min-max scaling technique to bring their values within the range of [0, 1]. This normalization step ensures that all input features contribute uniformly during model training. The dataset is then divided into input features (x) and the target variable (y), where the class attribute identifies fraudulent transactions '1' and legitimate transactions '0'. To avoid data leakage, the data is further split into training and testing subsets using 70:30 ratio.

One of the major challenges in credit card fraud detection is the extreme class imbalance, where fraudulent transactions represent less than 1% of the total dataset. This imbalance often biases ML models toward predicting the majority class, resulting in high overall accuracy but poor fraud detection performance. To overcome this issue, the SMOTE is integrated into the training process. SMOTE generates synthetic samples of the minority class by interpolating between existing minority instances, thereby increasing their representation within the dataset [28]. Balancing the dataset through SMOTE enables the model to learn more effectively from fraudulent transaction patterns. This approach is particularly beneficial for the ELM algorithm, as it enhances the model's ability to differentiate between minority and majority classes, improves recall, and reduces false negatives. Since fraudulent transactions are significantly fewer than legitimate ones, SMOTE is applied only to the training data to maintain realistic evaluation conditions. The ELM model is initialized by defining a range of hidden nodes, typically between 10 and 100, and by selecting suitable activation functions such as sigmoid or ReLU. These configurations allow experimentation to identify the optimal combination of hidden nodes and activation functions for achieving higher accuracy in fraud detection. As a binary classification task characterized by high data imbalance, this setup ensures that the ELM model can achieve balanced and reliable performance across both classes.

- i) Sigmoid: the sigmoid function is one of the most widely used activation functions in classification tasks, especially when the goal is to output probabilities [29]. It maps any real-valued number into a range between 0 and 1, which aligns well with binary classification objectives, such as distinguishing between fraudulent and legitimate transactions [30]. However, it may suffer from the vanishing gradient problem, which can hinder training in deeper or more complex models.
- ii) ReLU: the ReLU is a piecewise linear activation function those outputs zero for negative input values and returns the input value itself for positive inputs. This property introduces sparsity in neural activations, leading to faster convergence and lower computational complexity. These advantages make ReLU highly effective for large-scale and real-time fraud detection applications [31]. In addition, ReLU helps reduce the impact of the vanishing gradient problem, thereby improving the learning efficiency of models such as ELM [32].

These two activation functions were selected to assess the ELM model's adaptability to different activation behaviors. The sigmoid function provides smooth probabilistic mapping, aiding in the detection of minority classes such as fraud cases, while ReLU emphasizes computational efficiency and scalability, which are essential for large-scale financial applications. The ELM algorithm trains the single-layer feedforward network using randomization and least-squares optimization, as outlined in the following mathematical steps.

- i) Hidden layer computation: let the input dataset be $X \in \mathbb{R}^{N \times M}$, where N is the number of samples and M is the number of features. Randomly initialize the input weight matrix $W \in \mathbb{R}^{M \times L}$ and bias vector $b \in \mathbb{R}^L$, where L is the number of hidden nodes. The hidden layer output, $H \in \mathbb{R}^{N \times L}$ is calculated as (1).

$$H = f(XW + b) \quad (1)$$

Here, $f(\cdot)$ represents the activation function (e.g., sigmoid or ReLU). Where the activation functions of sigmoid and ReLU are computed as shown in (2) and (3), respectively.

$$\text{Sigmoid} = f(x) = \frac{1}{1+e^{-x}} \quad (2)$$

$$\text{ReLU} = f(x) = \max(0, x) \quad (3)$$

- ii) Output weight calculation: the output weights $\beta \in \mathbb{R}^{L \times 1}$ are computed using the Moore-Penrose pseudo-inverse of the hidden layer output matrix H , as shown in (4).

$$\beta = H^\dagger T \quad (4)$$

Where, H^\dagger is the pseudo-inverse of H , and T is the target vector, $T \in \mathbb{R}^{N \times 1}$ (class labels: 0 for non-fraud and 1 for fraud). The pseudo-inverse of H , H^\dagger is computed as shown in (5).

$$H^\dagger = (H^T H)^{-1} H^T \quad (5)$$

iii) Prediction: For a given test input $X_{\text{test}} \in R^{N_{\text{test}} \times M}$, the predicted output $Y_{\text{pred}} \in R^{N_{\text{test}} \times 1}$ is calculated as (6).

$$Y_{\text{pred}} = f(X_{\text{test}}W + b)\beta \quad (6)$$

Thresholding is applied to Y_{pred} to obtain binary predictions (fraud or non-fraud), as given in (7).

$$\hat{y}_i = \begin{cases} 1, & \text{if } y_{\text{pred},i} \geq 0.5 \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

Where, \hat{y}_i is the binary prediction for the i -th sample, where 1 indicates fraud and 0 indicates non-fraud.

Furthermore, the proposed ELM model is trained using the balanced training dataset. During evaluation, the test data is passed through the model to compute predictions. Binary labels are generated by applying a threshold of 0.5 to the predicted values. Key evaluation metrics are calculated, including accuracy, precision, recall (sensitivity), specificity, F-measure, and G-mean. These metrics comprehensively assess the model's performance in identifying fraudulent transactions. In addition, the results are subjected to descriptive statistical analysis to summarize the performance across various configurations of hidden nodes and activation functions. Significance testing is conducted to ascertain whether observed differences in metrics are statistically meaningful. Visualizations, such as line plots, compare metrics (e.g., specificity vs. hidden nodes) to identify optimal configurations. Figure 1 illustrates the flowchart and the key steps of the proposed ELM algorithm in detecting credit card fraud.

In the proposed method, the dataset will be load and preprocess. Then, the SMOTE method is applied to balance the training data. The proposed model is initialized by defining the hidden nodes (10 to 100) and activation functions (sigmoid and ReLU). After the initialization step, the proposed model will be trained by computing hidden layer outputs and output weights. Subsequently, predictions and binary labels are generated. The performance of the proposed model will be evaluated by calculating metrics and save results. Lastly, based on the experimental result, the statistical analysis and visualization are performed.

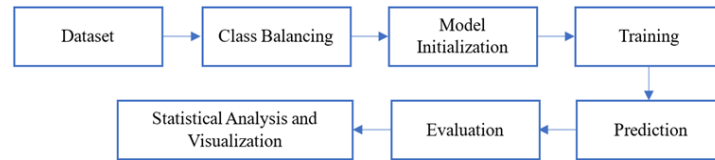


Figure 1. The flowchart of the proposed ELM model for credit card fraud detection

4. EXPERIMENTAL SETUP AND RESULTS ANALYSIS

The proposed ELM model was implemented to detect credit card fraud in a highly imbalanced dataset. The dataset consisted of legitimate and fraudulent transactions, where the latter constituted only a small fraction of the total samples. To address this imbalance, the SMOTE technique was applied exclusively to the training set, ensuring an equal representation of both classes while maintaining the integrity of the testing set. The dataset was preprocessed by normalizing numerical features, including the transaction "amount" and "time," using min-max scaling. Subsequently, the features were scaled to ensure uniformity. The data was split into training and testing sets with a 70:30 ratio. The proposed ELM model employed two activation functions for the hidden layer, sigmoid and ReLU, to evaluate their impact on performance. The number of hidden nodes was varied from 10 to 100, with increments of 10, to analyze the influence of the hidden layer's complexity. In other words, to determine the optimal configuration of hidden nodes in the ELM, we conducted various experiments. For each configuration, the ELM model was trained and evaluated using the same dataset and experimental conditions. The selection criterion for the best configuration was primarily the accuracy achieved on the test set, as it reflects the model's overall performance. The configuration that yielded the highest accuracy was selected as the optimal setup. While other metrics such as recall, specificity, and G-mean were also considered, accuracy served as the decisive factor in finalizing the best number of hidden nodes. The proposed model has been evaluated in terms of many evaluation metrics which can be listed as follows [33]–[36].

- Accuracy: the proportion of correctly classified transactions among all transactions. It is calculated as shown in (8).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

- Precision: the proportion of correctly classified fraudulent transactions among all predicted fraudulent transactions. This metric is computed as given in (9).

$$Precision = \frac{TP}{TP + FP} \quad (9)$$

- Recall (sensitivity): the proportion of correctly classified fraudulent transactions among all actual fraudulent transactions. It is computed as shown in (10).

$$Recall = \frac{TP}{TP + FN} \quad (10)$$

- Specificity: the proportion of correctly classified legitimate transactions among all actual legitimate transactions. This metric is calculated as shown in (11).

$$Specificity = \frac{TN}{TN + FP} \quad (11)$$

- F-measure: the harmonic means of precision and recall metrics. The performance metric can be computed as shown in (12).

$$F - Measure = \frac{2 \times Precision \times Recall}{Recall + Precision} \quad (12)$$

- G-mean: the geometric mean of sensitivity and specificity metrics. The G-mean metric is calculated as shown in (13).

$$G - Mean = \sqrt[2]{\frac{tp}{p} \times \frac{tn}{n}} \quad (13)$$

In the context of credit card fraud detection, evaluating model performance using a diverse set of metrics is essential due to the inherent class imbalance. While accuracy provides a general measure of correctness, it can be misleading in imbalanced datasets where the majority class dominates. For example, a model predicting all transactions as legitimate may still achieve high accuracy. To address this, recall (sensitivity) is particularly important as it measures the model's ability to correctly identify fraudulent transactions, a critical aspect in minimizing financial losses. Specificity, on the other hand, evaluates how well the model identifies legitimate transactions, which helps reduce false alarms. Additionally, the G-mean metric offers a balanced measure by combining recall and specificity, providing insight into the model's ability to perform well on both classes. By using multiple metrics, this study ensures a holistic evaluation of the proposed method's performance and its practical relevance in real-world fraud detection systems.

The activation function plays a critical role in determining the learning and representation capacity of the ELM model. Results show that both sigmoid and ReLU exhibit distinct patterns in performance as the number of hidden nodes increases. Table 1 shows the experimental results of the proposed ELM algorithm in detecting credit card fraud. The sigmoid function demonstrates consistent improvements in key metrics, particularly accuracy and recall, as the number of hidden nodes increases. For instance, with 30 hidden nodes, the sigmoid activation achieves an accuracy of 99.225%, recall of 81.757%, and a G-mean of 90.082%, indicating a balanced performance in detecting both legitimate and fraudulent transactions. In contrast, the ReLU activation function shows a more gradual improvement across the metrics, achieving competitive results at higher hidden node counts. While ReLU's precision is slightly lower compared to sigmoid at lower node counts, it gains stability and achieves comparable recall and G-mean values as the number of hidden nodes increases. This trend highlights ReLU's potential for scalability in complex models. Table 2 shows the confusion matrix values for the highest results achieved by the proposed method concerning true positives, true negatives, false positives, and false negatives. Figure 2 shows the best results of the proposed ELM algorithm for detecting credit card fraud.

The results demonstrate that the number of hidden nodes significantly influences the performance of the ELM model. When using the sigmoid activation function, accuracy improved markedly from 95.906% at 10 hidden nodes to a peak of 99.225% at 30 nodes. Beyond this point, the performance began to plateau, with accuracy fluctuating slightly within the range of 98.7 to 98.9%, indicating diminishing returns from adding more nodes. Similarly, with the ReLU activation function, the highest accuracy of 99.710% was also achieved at 30 hidden nodes. Subsequent increases in hidden nodes produced marginal variations, with accuracy ranging between 98.3 and 99.3%. These findings suggest that an optimal configuration likely exists

within the 30–40 hidden node range. Increasing the number of hidden nodes beyond this threshold does not result in substantial performance gains and may lead to unnecessary computational complexity.

Based on the experimental results obtained from the proposed ELM algorithm, the best performance for each evaluation metric and important insights into the achieved results can be summarized as follows:

- i) Accuracy: the overall accuracy of the model improves with an increase in hidden nodes for both activation functions, reaching over 99% in multiple configurations. This high accuracy reflects the model's effectiveness in correctly classifying transactions.
- ii) Precision: precision, which measures the proportion of correctly identified fraudulent transactions, remains relatively low for both activation functions at smaller node counts but improves as hidden nodes increase. For example, sigmoid achieves a precision of 16.005% with 30 hidden nodes, while ReLU achieves 35.207% precision at similar higher node.
- iii) Recall: recall, a critical metric for fraud detection, consistently improves with the number of hidden nodes. The sigmoid activation reaches a recall of 85.811% with 80 hidden nodes, showcasing its robustness in identifying fraudulent transactions. ReLU follows a similar pattern but lags slightly behind in lower configurations. In other words, the proposed ELM algorithm achieved 84.459% recall at 70 hidden nodes using the ReLU activation function.
- iv) Specificity: specificity remains high across all configurations, indicating the model's ability to correctly classify legitimate transactions. Both activation functions maintain specificity above 98% in most cases, ensuring a low false-positive rate.
- v) F-measure: the F-measure balances precision and recall, and its trends reflect the trade-offs between these metrics. Sigmoid achieves higher F-measure values at moderate hidden node counts, while ReLU closes the gap at higher counts. However, the highest F-measure is 48.971%, obtained using ReLU at 30 hidden nodes.
- vi) G-mean: as a combined measure of recall and specificity, G-mean highlights the overall balance of the model's performance. Both activation functions exhibit a steady increase in G-mean with more hidden nodes, reaching above 90% in optimal configurations. In addition, the highest G-mean result is 92.068%, where it has been obtained using sigmoid at hidden nodes of 80.

Table 1. The experimental results of the proposed ELM algorithm

Activation function	H. N.	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F-measure (%)	G-mean (%)
Sigmoid	10	95.906	2.897	69.595	95.952	5.562	81.717
	20	98.618	9.680	83.784	98.644	17.355	90.911
	30	99.225	16.005	81.757	99.256	26.770	90.082
	40	98.962	12.334	81.757	98.992	21.435	89.962
	50	98.854	11.563	84.459	98.879	20.342	91.385
	60	98.903	11.810	82.432	98.932	20.660	90.306
	70	98.710	10.513	85.811	98.733	18.732	92.045
	80	98.758	10.883	85.811	98.781	19.316	92.068
	90	98.748	10.531	83.108	98.775	18.693	90.603
	100	98.689	10.294	85.135	98.713	18.367	91.673
ReLU	10	97.312	4.257	67.568	97.363	8.010	81.109
	20	97.305	4.708	75.676	97.342	8.864	85.828
	30	99.710	35.207	80.405	99.743	48.971	89.554
	40	99.302	17.155	79.054	99.338	28.193	88.617
	50	99.224	16.252	83.784	99.251	27.223	91.190
	60	98.332	7.910	81.081	98.362	14.414	89.305
	70	98.550	9.321	84.459	98.574	16.790	91.244
	80	99.178	15.375	83.108	99.206	25.949	90.801
	90	98.986	12.836	83.784	99.013	22.262	91.081
	100	99.246	16.667	83.784	99.273	27.803	91.200

Table 2. The confusion matrix values for the highest achieved results

Activation function	Metric highlights	True positives	True negatives	False positives	False negatives
Sigmoid	Highest recall and G-mean	127	84255	1040	21
ReLU	Highest accuracy, precision, specificity, and F-measure	119	85076	219	29

According to the statistical analysis of the proposed ELM model, the experimental results demonstrate notable performance across various metrics for both activation functions. Table 3 presents the statistical analysis of the proposed model in detecting credit card fraud. In terms of accuracy, the ReLU activation function achieved a mean accuracy of 98.715%, accompanied by a small standard deviation of 0.836%, reflecting consistent and reliable performance across trials. The sigmoid activation function

performed slightly lower, with a mean accuracy of 98.537% and a standard deviation of 0.941%, indicating marginally higher variability compared to ReLU. Precision results highlight some challenges in identifying fraudulent transactions. The ReLU activation function achieved an average precision of 13.969%, with a relatively high standard deviation of 8.915%, suggesting variability in its ability to minimize false positives. In contrast, the sigmoid activation function recorded a lower average precision of 10.651% but exhibited greater consistency, as evidenced by its smaller standard deviation of 3.248%.

Recall, a critical metric for detecting fraudulent cases, showed strong performance for both activation functions. The ReLU activation function achieved an average recall of 80.270%, with a standard deviation of 5.242%, indicating its effectiveness in identifying fraudulent transactions. The sigmoid activation function performed slightly better, with an average recall of 82.365% and a standard deviation of 4.740%, reflecting its robustness and slightly superior detection capability. Specificity remained consistently high across both activation functions, demonstrating the model's ability to accurately classify legitimate transactions. The ReLU activation function achieved a mean specificity of 98.747%, with a standard deviation of 0.831%, while the sigmoid activation function recorded a slightly lower mean specificity of 98.565%, with a standard deviation of 0.935%. Both results underscore the model's strong performance in minimizing false positives.

The F-measure, which balances precision and recall, revealed some trade-offs. The ReLU activation function achieved a mean F-measure of 22.848%, but with a relatively high standard deviation of 11.964%, indicating variability in balancing these two metrics. The sigmoid activation function, with a mean F-measure of 18.723% and a smaller standard deviation of 5.313%, showed less variability but a slightly less optimal balance between precision and recall. Finally, the G-mean, which combines recall and specificity to assess overall balance, demonstrated strong performance for both activation functions. The ReLU activation function achieved a mean G-mean of 88.993%, with a standard deviation of 3.251%, indicating a well-balanced performance. The sigmoid activation function achieved a slightly higher mean G-mean of 90.075%, with a standard deviation of 3.037%, reflecting its slightly better overall balance between detecting fraudulent transactions and minimizing false positives.

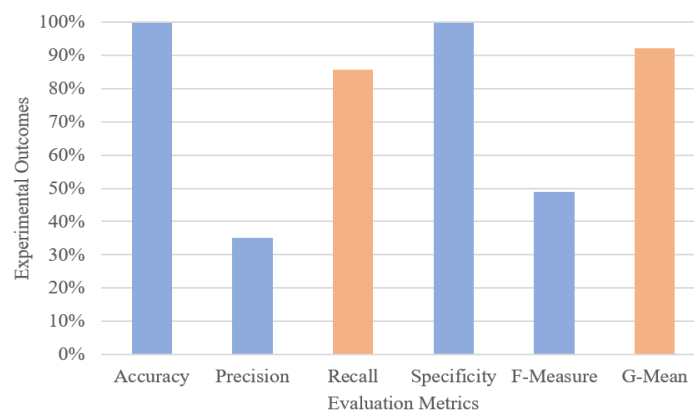


Figure 2. The highest obtained results of the proposed ELM algorithm for detecting credit card fraud

Table 3. The statistical analysis results of the proposed model

Evaluation measurements	ReLU		Sigmoid	
	Mean (%)	STD (%)	Mean (%)	STD (%)
Accuracy	98.715	0.836	98.537	0.941
Precision	13.969	8.915	10.651	3.248
Recall	80.270	5.242	82.365	4.740
Specificity	98.747	0.831	98.565	0.935
F-measure	22.848	11.964	18.723	5.313
G-mean	88.993	3.251	90.075	3.037

5. DISCUSSION

The experimental results demonstrate that the proposed ELM model effectively addresses the challenges of credit card fraud detection in imbalanced datasets. Applying the SMOTE technique to the training set helps balance class representation, which significantly contributes to improved recall and specificity. The choice of activation function also influences learning behavior, with the sigmoid function yielding stronger initial performance and the ReLU function showing better scalability. Adjusting the number of hidden nodes

revealed that model complexity plays a key role in achieving optimal results. Increasing the number of hidden nodes enhances the model's ability to capture complex relationships, improving accuracy and overall performance. However, excessive complexity can lead to diminishing returns or overfitting, highlighting the importance of careful hyperparameter tuning. Statistical analysis further supports the effectiveness of the ELM model using both ReLU and sigmoid activation functions. Both functions achieved high accuracy and specificity, consistently exceeding 98%, which indicates the model's strong ability to identify legitimate transactions and maintain a low false-positive rate, which is an essential aspect of reliable fraud detection. In terms of recall, which measures the detection of fraudulent transactions, the sigmoid function performed slightly better, achieving an average recall of 82.365% compared to 80.270% for ReLU. This suggests that sigmoid is more suitable when minimizing false negatives is critical. However, precision values for both activation functions remained relatively low, with ReLU achieving 13.969% and sigmoid 10.651% on average. This outcome reflects the inherent difficulty of detecting fraudulent transactions in datasets dominated by legitimate ones and underscores the persistent challenge of achieving high precision in highly imbalanced financial data.

The F-measure, showed that ReLU had a slightly better overall balance in some configurations. However, when considering the G-mean, which accounts for both recall and specificity, sigmoid performed slightly better with a mean G-mean of 90.075% compared to ReLU's 88.993%. This indicates that while sigmoid may not excel in precision, it provides a more balanced overall performance across metrics. Variability in performance was another important aspect to consider. The standard deviations for precision and F-measure were higher for ReLU, suggesting greater inconsistency in its performance across trials. In contrast, Sigmoid demonstrated more stable results, making it potentially more reliable for consistent fraud detection in different scenarios. Based on the experimental results, it demonstrated that the choice of activation function should depend on the specific priorities of the fraud detection system. Sigmoid is more suitable for applications that prioritize recall and overall balance, as reflected in its superior recall and G-mean. On the other hand, ReLU might be preferred in scenarios where precision and consistency are more critical. In general, the proposed ELM model demonstrates strong potential for real-world fraud detection applications. The insights gained from the experimental results provide valuable guidance for optimizing ELM configurations and addressing the unique challenges posed by imbalanced datasets. However, although the proposed model achieves high results in terms of accuracy, recall, specificity, and G-mean, it still suffers from low precision and F-measure, which are considered limitations of the proposed model in detecting credit card fraud.

The use of SMOTE had a significant impact on the model's ability to detect fraudulent transactions. By generating synthetic samples for the minority (i.e., fraud) class, SMOTE effectively balanced the dataset, enabling the ELM algorithm to better learn and recognize patterns associated with fraudulent behavior. This resulted in notable improvements in recall, which is a crucial metric for fraud detection since minimizing false negatives is of primary importance. As commonly observed with oversampling methods, this improvement came with a slight reduction in specificity, as the model became somewhat more likely to classify legitimate transactions as fraudulent, leading to an increase in false positives. Nevertheless, the overall performance, reflected in metrics such as G-mean and F-measure, improved, suggesting that SMOTE enhanced the model's robustness when dealing with imbalanced data. These findings highlight the importance of applying data balancing techniques in fraud detection to ensure that minority class patterns are effectively captured during the training process.

Furthermore, the proposed ELM algorithm has been compared with the state-of-the-art methods for detecting credit card fraud in terms of accuracy. Table 4 presents the comparative performance of the proposed ELM algorithm against state-of-the-art methods for credit card fraud detection. The proposed ELM algorithm demonstrates a significant improvement in detecting credit card fraud compared to state-of-the-art methods. While traditional approaches like LR [7] and RF [37] achieved moderate accuracy levels up to 94.425 and 82.5%, respectively. Meanwhile, the proposed ELM surpasses them with an impressive accuracy of 99.710%. In addition, LSTM networks [38] and ANN [39] show lower performance, achieving 90 and 70%, respectively, indicating their limited effectiveness in this context. Notably, the standard ELM implementation achieved 87.32% [40], highlighting the enhancements made in the proposed ELM algorithm. The near-perfect accuracy achieved by the proposed method underscores its robustness and potential as a superior tool for credit card fraud detection, outperforming conventional and state-of-the-art methods across the board.

The superior performance of the proposed ELM model is attributed to several key factors. First, the dynamic adjustment of hidden nodes allowed for finding an optimal network size (around 30–40 nodes) that balances learning capacity and prevents overfitting. Second, the integration of SMOTE effectively handled the severe class imbalance by generating synthetic minority samples, improving the model's ability to detect fraudulent transactions. Lastly, comparing activation functions revealed that ReLU's computational efficiency and ability to mitigate vanishing gradients further enhanced accuracy. These combined improvements enable the proposed method to outperform traditional models by better capturing complex fraud patterns and maintaining high detection accuracy.

The proposed ELM-SMOTE framework offers significant potential for integration into real-world fraud detection systems. Due to the fast-training speed and low computational complexity of the ELM algorithm, this model is highly suitable for real-time or near real-time applications in financial institutions. Moreover, the modular nature of our approach allows easy integration into existing fraud detection pipelines with minimal infrastructure modification. The use of SMOTE can be incorporated as a pre-processing stage, while the ELM can function as a plug-and-play classification technique. These attributes make the model scalable and adaptable for deployment in large-scale financial environments.

Table 4. Performance comparison of the proposed ELM algorithm with state-of-the-art methods

Methods	Accuracies (%)
Proposed ELM	99.710
LR [7]	94.425
LR [7]	82.5
LSTM [38]	90
ANN [39]	70
ELM [40]	87.32

6. CONCLUSION

This study presented an optimized ELM algorithm designed to address key challenges in credit card fraud detection, including low accuracy, limited adaptability to diverse datasets, and narrow evaluation metrics. By dynamically varying the number of hidden nodes (from 10 to 100 with an increment of 10) and integrating the SMOTE to mitigate class imbalance, the proposed model achieved strong performance, recording an accuracy of 99.710%, recall of 85.811%, specificity of 99.743%, and a G-mean of 92.068%. In addition, the inclusion of descriptive statistics, visualization, and significance testing provided a more comprehensive evaluation of model performance, addressing common gaps in prior research that often overlook detailed statistical analysis. Although the proposed ELM model demonstrates excellent results in terms of accuracy, recall, specificity, and G-mean, certain limitations remain. The relatively lower precision and F-measure indicate persistent challenges in reducing false positives. Future research should aim to improve these metrics through advanced feature selection, hybrid learning strategies, and ensemble-based methods. Incorporating online learning techniques may also allow the model to adapt continuously to new and evolving fraud patterns, supporting real-time detection. Evaluating the model on larger and more diverse datasets would further confirm its robustness and generalizability. Moreover, integrating interpretability frameworks such as local interpretable model-agnostic explanations (LIME) or shapley additive explanations (SHAP) could enhance transparency and trust in the model's decision-making process, which is critical for its adoption in financial institutions. Overall, this work contributes a scalable and reliable solution for credit card fraud detection and provides a foundation for further advancements in cybersecurity and financial fraud prevention systems.

ACKNOWLEDGMENTS

We would like to thank the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, for the Faculty Income Generation Grant (FTM1)

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Iman Kadhim Ajlan	✓			✓			✓		✓					
Mohammed Ibrahim Mahdi		✓				✓			✓		✓		✓	
Hayder Murad		✓	✓	✓					✓	✓				
Fahad Taha AL-Dhief	✓			✓	✓					✓				
Nurhizam Safie		✓					✓			✓				✓
Yasir Hussein Shakir	✓		✓	✓				✓	✓		✓			
Ali Hashim Abbas	✓				✓			✓		✓				

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are openly available in Kaggle at <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>, reference number [25].




REFERENCES

- [1] A. S. Sikder and S. Rolfe, "The power of e-commerce in the global trade industry: a realistic approach to expedite virtual market place and online shopping from anywhere in the world," *International Journal of Imminent Science & Technology*, vol. 1, no. 1, pp. 79–100, 2023, doi: 10.70774/ijist.v1i1.3.
- [2] M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, "An intelligent payment card fraud detection system," *Annals of Operations Research*, vol. 334, no. 1, pp. 445–467, 2024, doi: 10.1007/s10479-021-04149-2.
- [3] E. O. Paul *et al.*, "Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors," *International Journal on Soft Computing*, vol. 14, no. 3, pp. 1–16, 2023, doi: 10.5121/ijsc.2023.14301.
- [4] N. A. A. Bakar, K. Sekaran, S. S. Hussein, H. Salehuddin, and F. Yahya, "A knowledge management-driven framework for strengthening social engineering awareness in public sector cybersecurity," in *International Conference on Knowledge Management in Organizations*, Springer, 2025, pp. 315–328, doi: 10.1007/978-3-031-95898-4_22.
- [5] J. Wang, S. Lu, S.-H. Wang, and Y.-D. Zhang, "A review on extreme learning machine," *Multimedia Tools and Applications*, vol. 81, no. 29, pp. 41611–41660, 2022, doi: 10.1007/s11042-021-11007-7.
- [6] F. Z. El Hlouli, J. Riffi, M. A. Mahraz, A. Yahyaouy, K. El Fazazy, and H. Tairi, "Weighted binary ELM optimized by the reptile search algorithm, application to credit card fraud detection," *Multimedia Tools and Applications*, pp. 1–22, 2024, doi: 10.1007/s11042-024-19508-x.
- [7] A. R. Khalid, N. Owah, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing credit card fraud detection: an ensemble machine learning approach," *Big Data and Cognitive Computing*, vol. 8, no. 1, pp. 6, 2024, doi: 10.3390/bdcc8010006.
- [8] S. H. M. A. S. Abdullah and M. Mukhtar, "The implementation strategy of DNSSEC in strengthening digital government security in Malaysia," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 11, no. 1, pp. 26–38, Jun. 2022, doi: 10.17576/apjitm-2022-1101-03.
- [9] A. A. Abdulsahib, "Anatomy of network security execution through utilizing spss to evaluate public Wi-Fi," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 12, no. 1, 2023, doi: 10.17576/apjitm-2023-1201-06.
- [10] B. Zyoud and S. L. Lutfi, "Adapting zero trust: information security cultural factors considerations in the UAE context," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 13, no. 2, 2024, doi: 10.17576/apjitm-2024-1302-09.
- [11] I. D. Mienye and N. Jere, "Deep learning for credit card fraud detection: a review of algorithms, challenges, and solutions," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3426955.
- [12] A. Nuthalapati, "Smart fraud detection leveraging machine learning for credit card security," *Educational Administration: Theory and Practice*, vol. 29, no. 2, pp. 433–443, 2023, doi: 10.53555/kuey.v29i2.6907.
- [13] K. Patel, "Credit card analytics: a review of fraud detection and risk assessment techniques," *International Journal of Computer Trends and Technology*, vol. 71, no. 10, pp. 69–79, 2023, doi: 10.14445/22312803/IJCTT-V71I10P109.
- [14] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *International Journal of Information Technology*, vol. 13, no. 4, pp. 1503–1511, 2021, doi: 10.1007/s41870-020-00430-y.
- [15] S. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, "Credit card fraud detection using support vector machine," in *Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications (ICMISC 2021)*, Springer, 2022, pp. 27–37, doi: 10.1007/978-981-16-6407-6_3.
- [16] M. S. Kumar, V. Soundarya, S. Kavitha, E. Keerthika, and E. Aswini, "Credit card fraud detection using random forest algorithm," in *2019 3rd International Conference on Computing and Communications Technologies*, IEEE, 2019, pp. 149–153, doi: 10.1109/ICCCT2.2019.8824930.
- [17] S. Georgieva, M. Markova, and V. Pavlov, "Using neural network for credit card fraud detection," in *AIP Conference Proceedings*, AIP Publishing, 2019, doi: 10.1063/1.5127478.
- [18] O. Cherkaoui, H. Anoun, and A. Maizate, "A benchmark of health insurance fraud detection using machine learning techniques," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 2, pp. 1925–1934, 2024, doi: 10.11591/ijai.v13.i2.pp1925-1934.
- [19] N. K. Trivedi, S. Simaiya, U. K. Lilhore, and S. K. Sharma, "An efficient credit card fraud detection model based on machine learning methods," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 3414–3424, 2020.
- [20] S. C. Dubey, K. S. Mundhe, and A. A. Kadam, "Credit card fraud detection using artificial neural network and backpropagation," in *2020 4th International Conference on Intelligent Computing and Control Systems*, 2020, pp. 268–273, doi: 10.1109/ICICCS48265.2020.9120957.
- [21] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
- [22] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, p. 24, 2022, doi: 10.1186/s40537-022-00573-8.




- [23] 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*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.
- [24] F. O. Aghwar *et al.*, "Enhancing the random forest model via synthetic minority oversampling technique for credit-card fraud detection," *Journal of Computing Theories and Applications*, vol. 1, no. 4, pp. 407–420, 2024, doi: 10.62411/jcta.10323.
- [25] L. Toni, Y.-A. L. Borgne, J. De Stefani, Andrea, and F. Carcillo, "Credit card fraud detection dataset," *Kaggle*, 2018. [Online]. Available: <https://www.kaggle.com/mlg-ulb/creditcardfraud>
- [26] P. A. Alaba *et al.*, "Towards a more efficient and cost-sensitive extreme learning machine: a state-of-the-art review of recent trend," *Neurocomputing*, vol. 350, pp. 70–90, 2019, doi: 10.1016/j.neucom.2019.03.086.
- [27] M. A. A. Albadr, S. Tiun, M. Ayob, M. Z. A. Nazri, and F. T. Al-Dhief, "Grey wolf optimization-extreme learning machine for automatic spoken language identification," *Multimedia Tools and Applications*, vol. 82, no. 18, pp. 27165–27191, 2023, doi: 10.1007/s11042-023-14473-3.
- [28] N. Nasaruddin, N. Masseran, W. M. R. Idris, and A. Z. Ul-Saufie, "Reduced noise SMOTE in machine learning model: application in water quality classification with imbalanced datasets," in *2024 5th International Conference on Artificial Intelligence and Data Sciences*, 2024, pp. 87–92, doi: 10.1109/AiDAS63860.2024.10730391.
- [29] S. R. Dubey, S. K. Singh, and B. B. Chaudhuri, "Activation functions in deep learning: a comprehensive survey and benchmark," *Neurocomputing*, vol. 503, pp. 92–108, 2022, doi: 10.1016/j.neucom.2022.06.111.
- [30] Y. Singh and M. Saini, "Impact and performance analysis of various activation functions for classification problems," in *2023 IEEE International Conference on Contemporary Computing and Communications*, 2023, pp. 1–7, doi: 10.1109/InC457730.2023.10263129.
- [31] M. Goyal, R. Goyal, P. V. Reddy, and B. Lall, "Activation functions," in *Deep Learning: Algorithms and Applications*, 2020, pp. 1–30, doi: 10.1007/978-3-030-31760-7_1.
- [32] T. Szadala, "Review and comparison of commonly used activation functions for deep neural networks," in *Bio-Inspired Neurocomputing*, 2021, pp. 203–224, doi: 10.1007/978-981-15-5495-7_11.
- [33] F. T. Al-Dhief, N. M. A. Latiff, N. N. A. Malik, M. M. Baki, N. Sabri, and M. A. A. Albadr, "Dysphonia detection based on voice signals using naive Bayes classifier," in *2022 IEEE 6th International Symposium on Telecommunication Technologies*, IEEE, 2022, pp. 56–61, doi: 10.1109/ISTT56288.2022.9966535.
- [34] M. A. A. Albad *et al.*, "Fast learning network algorithm for voice pathology detection and classification," *Multimedia Tools and Applications*, vol. 84, no. 17, pp. 18567–18598, 2025, doi: 10.1007/s11042-024-19788-3.
- [35] F. T. Al-Dhief *et al.*, "Voice pathology detection using decision tree classifier," in *2023 14th International Conference on Information and Communication Technology Convergence*, 2023, pp. 36–41, doi: 10.1109/ICTC58733.2023.10392786.
- [36] N. A. N. Za'im, F. T. Al-Dhief, M. Azman, M. R. M. Alsemawi, N. M. A. A. Latiff, and M. M. Baki, "The accuracy of an online sequential extreme learning machine in detecting voice pathology using the Malaysian voice pathology database," *Journal of Otolaryngology-Head & Neck Surgery*, vol. 52, no. 1, 2023, doi: 10.1186/s40463-023-00661-6.
- [37] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *Proceedings of the 4th International Conference on Smart City Applications*, 2019, pp. 1–4, doi: 10.1145/3368756.3369082.
- [38] T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep learning methods for credit card fraud detection," *arXiv:2012.03754*, 2020.
- [39] R. Asha and S. K. K. R., "Credit card fraud detection using artificial neural network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, 2021, doi: 10.1016/j.gltp.2021.01.006.
- [40] F. Z. El Houl, J. Riffi, M. A. Mahraz, A. Yahyaoui, K. E. Fazazy, and H. Tairi, "Towards maximum efficiency: combining ELM with BA for Credit Card Fraud Detection," in *2024 International Conference on Intelligent Systems and Computer Vision*, 2024, pp. 1–8, doi: 10.1109/ISCV60512.2024.10620081.

BIOGRAPHIES OF AUTHORS






Iman Kadhim Ajlan    received the B.S. in Computer Science from Al Rafidain University College, Iraq in 1996 and also received M.S. in Information Technology from University Utara Malaysia (UUM), Katak, Malaysia in 2014. She currently studying at Universiti Teknologi Malaysia (UTM) for a Ph.D. in Information Technology. Lecturer at University of Wasit. Iraq, she is scientific researcher in different healthcare applications. Her research interests are, deep learning, social networks, internet of things, and location-based service. She can be contacted at email: eajlan@uowasit.edu.iq.






Mohammed Ibrahim Mahdi    received the B.S. in Software Engineering from Al Rafidain University College, Iraq in 2011 and also received M.S. in Information Technology from THK University (THK), Ankara, Turkey in 2017. He is currently studying at Qom University for a Ph.D. in Information Technology. He is lecturer and web programming expert experience in IT management, education, and research. He can be contacted at email: mmahdi@uowasit.edu.iq.






Hayder Murad    received B.Sc. in Information Engineering from Al-Nahrain University-College of Information Engineering, Iraq in 2005 and also received M.Sc. in Information Engineering from Al-Nahrain University-College of Information Engineering in 2009. He also received Ph.D. in Artificial Intelligence from University of Portsmouth, School of Energy and Electronics Engineering, United Kingdom in 2019. He is scientific researcher in different healthcare applications. His research interests are machine learning, deep learning, recommender systems, natural language processing, information retrieval, big data, context-aware computing as well as their applications in internet, business, social networks, and health-informatics. He can be contacted at email: hayder.murad@uowasit.edu.iq.






Fahad Taha AL-Dhief    received the B.S. in Software Engineering from Imam Jaafar Al-Sadiq University, Iraq in 2013 and also received M.S. in Computer Science from University Kebangsaan Malaysia (UKM), Malaysia in 2016. He also received Ph.D. in Department of Communication Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Malaysia in 2023. Currently, he is a lecturer at Faculty of Information Science and Technology (FTSM), UKM, Malaysia. He is scientific researcher in different healthcare applications. He is an active student member of IEEE, and a member of IEEE Communications Society. His research interests are machine learning, artificial neural networks, deep learning, sensor networks, routing protocols, mobile ad-hoc networks, social networks, internet of things, and location-based service. He can be contacted at email: fahad@ukm.edu.my.






Nurhizam Safie    received the master's degree in information technology from UKM, in 1999, the M.B.A. degree from Anglia Ruskin University, U.K., in 2019, and the Ph.D. degree in Management Information Systems (MIS). He is an Associate Professor and the Dean of the Faculty of Information Science and Technology. Before this position, he was a Research Fellow with United Nations University, a United Nations Academic Arm. He has conferred the Professional Technologist [Ts/P.Tech. (IT)] credential from the Malaysian Board of Technology (MBoT), in 2018. During the Ph.D. study, he received the National Science Fellowship (NSF) Scholarship from the Malaysian Ministry of Science, Technology, and Innovation (MoSTI). He can be contacted at email: nurhizam@ukm.edu.my.



Yasir Hussein Shakir    is a software engineer who obtained his B.Sc. degree in software engineering from Baghdad College of Economic Sciences University in 2014. He further pursued his education and received his M.Sc. degree in Computer and Communication, specializing in Computer Programming, from the Faculty of Engineering at the Islamic University of Lebanon (IUL) in 2018. His areas of interest include data mining, image medical processing, medical electronic systems, machine learning, deep learning, and artificial intelligence. Currently, he is a Ph.D. student in the Department of Engineering at Universiti Tenaga Nasional (UNITEN) in Malaysia. He can be contacted at email: yasserhessein19855@gmail.com.



Ali Hashim Abbas    received the B.S. degree in communication engineering from Al-Furat Al-Awsat Technical University/Engineering Technical College of Al-Najaf, in 2010 and the M.S. degree in Digital System and Computer Electronics (DSCE) from Jawaharlal Nehru Technological University Hyderabad (JNTU), Hyderabad, India, in 2014, and Ph.D. degrees in Communication Engineering, Clustering of Vehicular Ad-Hoc Networks (VANETs) from University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia, in 2019. Where he is currently working Head of Department of Scientific Affairs and Promotions at the Department of Computer Technical Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq. His research interests are cluster stability for intervehicle communication and distributed algorithms, for vehicular ad hoc networks. He can be contacted at email: alsalamy1987@gmail.com.