Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PREDICTING FRAUD: A MACHINE LEARNING APPROACH TO SECURE TRANSACTIONS IN CREDIT CARD SYSTEM

[1]BASHAR I. HAMEED, [2]MOHAMMED A. MOHAMMED, [3]HUMAM K. YASEEN

[1,2,3] Lecturer, Computer Science Department, Al-Imam Al-Adham University College, Baghdad, Iraq

E-mail: bashar_ibrahim@imamaladham.edu.iq, [2]mohammed.adnan@imamaladham.edu.iq, [3]humam.khalid@imamaladham.edu.iq

ABSTRACT

The expansion of e-commerce has uncovered extensive vulnerabilities in web-based transactions, creating opportunities. The enormous use of credit cards in online transactions, motivated by their perks like discounts and bonuses, has resulted in a substantial upward thrust in credit card fraud. Conventional strategies, including hand checks and inspections, even as traditionally employed, have proven to significant obstacles in identifying fraudulent actions due to their time-intensive nature, high cost, and imprecision. The emergence of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL)-based techniques provides a promising innovative solution for addressing fraudulent activities with the aid of permitting the pattern recognition and anomaly detection of financial transactions. Even with recent advances in research into ML-based credit card fraud detection, the imbalance in credit transaction data makes identifying fraudulent activities a challenging task. This paper presents an advanced credit card fraud detection system using ML and DL algorithms; however, it is very important to investigate the scenario of anomaly detection concerning its characteristics. The paper analyzes a specific case study of the credit card dataset, highlighting the important preliminary steps in creating the necessary processes before the proposed model is applied. Our experimental results demonstrate that the Logistic Regression model achieved superior performance in evaluation metrics compared to the other models tested in our experiment.

Keywords: *Fraudulent Financial Transactions, Credit Card, Fraud Detection, Machine Learning, Deep Learning*

1. INTRODUCTION

According to the 2024 report by way of the Association of Certified Fraud Examiners (ACFE), occupational fraud continues to be a tremendous challenge globally. The report investigated 1,921 cases of occupational fraud analyzed between January 2022 and September 2023 across diverse industries in 138 countries. The general losses attributed to these cases exceeded $3.1 billion [1]. Financial fraud takes place whilst individuals or corporations use illegal or unethical methods to accrue financial benefits, often at the expense of others [2][3]. The impact of financial fraud can disrupt electronic commerce success, strengthen living charges, and erode consumer confidence [4]. Financial fraud incorporates a wide variety of unlawful actions, from common schemes to more elaborate operations. Some of the most widespread forms include [5][6][7]:

Credit and debit card fraud: involves the unlawful use of a person else card information, typically received via robbery or counterfeiting. Criminals may additionally then make unauthorized purchases, withdraw cash, or engage in different fraudulent transactions.

Identity theft: occurs when criminals theft private information, which includes social security numbers or credit card details, to open accounts, benefit financially, or gain loans by the name of the victim.

New bank account fraud: Involves using stolen identities or forged documents to obtain funds, commit other financial crimes, or open fraudulent accounts.

Criminals often close accounts or facilitate further criminal acts.

Recognizing the various methods used in financial fraud is crucial for safeguarding persons and transactions from falling victim to these crimes [8]. Traditional fraud detection methods, advanced

several years ago, depend heavily on manual methods. This method gives has drawbacks, which include time consumption, high costs, and a lack of precision, making it in the end impractical [9]. While several research focused on reducing losses because of fraudulent actions, their effectiveness in accomplishing this goal remains confined [10]. The upward thrust of AI has ushered in a brand-new generation of fraud detection inside the financial sector. ML and data mining techniques are now at the vanguard of this war against financial crime. Both supervised and unsupervised learning methods are used to expect and prevent fraudulent actions [11][12]. Classification techniques have emerged because of dominant approach for figuring out fraudulent financial transactions, presenting a strong and reliable method for protecting financial safety [3].

This paper examines present ML algorithms hired in financial transaction fraud detection. It also discusses the dataset ordinarily used for detecting fraudulent actions within financial transactions. This paper proposed an advanced ML model for detecting credit card fraud. Utilizing real datasets containing imbalanced data from European credit card transactions. ML models regularly face demanding situations whilst handling class imbalance, a situation in which one elegance of data (e.g., Normal) significantly outweighs the opposite (e.g., Fraud). Extensive research has centered on addressing the complexities of classifying fraud transactions from imbalanced datasets. To evaluate the overall performance of the proposed ML model, we employed a set of regular binary classifiers: Logistic Regression (LR), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Decision Tree (DT). These classifiers excel at extracting hidden patterns from financial transaction data to predictable outcomes. Each classifier demonstrates a unique ability to correctly categorize data and selection-making skills, in the end categorizing each instance as either fraudulent or normal behavior.

The proposed system is crucial for securing credit card transactions, benefiting financial institutions, regulators, tech firms, and end-users. By leveraging AI-driven insights, stakeholders can reduce fraud losses, enhance compliance, and improve customer experience in digital payments.

1.1 Problem Statement

The expansion of online transactional activities has led to the development of sophisticated fraudulent activities, which pose issues for existing ML models, even with advancements in fraud detection systems. Most systems continue to struggle with class imbalance (having comparatively low instances of fraud versus legitimate transactions), concept drift (changing tactics of fraudsters), and having high rates of false positives, all of which negatively impact the reliability of systems in practical applications. While prior proposals examined traditional ML approaches, there is a high need for adaptive, powerful, and computationally efficient models that can handle large-scale, imbalanced credit card transaction data without compromising detection accuracy.

1.2 Motivation

The exponential growth of online financial transactions generates huge amounts of information, growing fertile floor for ability financial fraud. This requires the proposition of automated AI structures to locate and prevent financial fraud. The main motivation of this paper is to develop a system for detecting fraudulent financial transactions over credit card data. The proposed system will leverage the power of ML techniques to design a robust and flexible credit card fraud detection system.

1.3 Contributions

1. This paper proposes an ML model that utilizes an LR classifier to detect fraudulent financial transactions.
2. A comparison overall performance of the proposed ML model against several recent ML techniques using credit card fraud detection benchmark dataset.
3. The performance of the proposed ML model was evaluated using several evaluation metrics: accuracy, precision, recall, and F1-score. This multi-faceted method, like shining a spotlight from diverse angles, allowed us to gain a deeper understanding of the model's strengths and weaknesses, ensuring it wasn't solely a master of one instance but capable of successfully detecting fraudulent transactions.

The rest paper is structured as follows. Section II presents a comprehensive review of relevant literature on the subject. Section III delves into the design methodology employed in this research. It emphasizes the ML and DL algorithms used and demonstrates the proposed fraud detection system. The framework and compound components of the system are mentioned in detail. Section IV presents a thorough evaluation of the experimental procedure. It includes a description of the Credit Card Fraud

Detection benchmark dataset utilized, an illustration of the overall performance metrics hired, and an in-depth discussion of the results acquired. The paper concludes in the final section.

2. LITERATURE REVIEW

In [13], the authors reformed the credit card fraud detection dataset to reduce the oversampling problem by creating two datasets from the original. They increased the number of positive (fraud) instances and reduced the number of negative (not fraud) instances with a ratio of 10:90 and 34:64. For the classification process, three different ML models were used, which are KNN, LR, and the Naïve Bayes algorithm. For the examination, many performance measures were utilized, and it was found that the KNN algorithm is the best among the other algorithms used.

The authors in [14] discussed the problem of fraud in credit card transactions and proposed a system to fix this problem. The system begins with preprocessing procedures like normalization and under-sampling to address the issue of imbalanced data. The authors used three different algorithms for the classification process: SVM, KNN, and ANN. The experimental results showed that ANN has the best accuracy with 99.92%, but precision and recall are gone for SVM at 97.43% and 89.76% respectively.

In [15] the authors suggested a framework to detect fraud in credit card transactions. They selected the most important features in the dataset using a light gradient boosting machine (LightGBM) and optimized them using a Bayesian-based hyperparameter optimization algorithm. To fix the problem of the imbalanced data, from their point of view, they used fivefold cross-validation. They have finally compared the results with the state-of-art ML.

The authors in [16] suggested using ML algorithms to classify the dataset into fraud and normal transactions. The algorithms used were random forest and the AdaBoost algorithm. They used many metrics to compare the performance of these algorithms and found that the random forest algorithm is better than the other fraud detection systems.

In [17], the authors also discussed the imbalanced data problem, so they noticed that when using sampling techniques to enhance the model's performance, the unseen data are increased. The authors depended on a convolutional neural network built with twenty layers to fix the problem of detecting fraud in many credit card transaction datasets.

Two stages are suggested in [4]. The first stage ran nine different ML algorithms and chose the best three, which integrated with the second stage with nineteen different resampling techniques. The authors found that using the All KNN as an undersampling technique with the CatBoost algorithm had the best performance of the other algorithms used.

Four ensemble classifiers, i.e., Random Forest, CatBoost, LightGBM, and XGBoost, were used to fix the fraud problem in credit card transactions. The authors investigated the performance of feature extraction and data sampling on the data to obtain the best results. The proposed framework handled the problem in three scenarios: the first was to run the algorithm without any feature extraction or data sampling algorithms, while the second and third used them with an exchange of positions for these algorithms. The best result was obtained by using Random Under Sampling (RUS) techniques followed by Convolutional Auto Encoder (CAE) as a feature extractor [18].

The authors in [19] suggested a stacking framework with two levels. The first level combined two algorithms, i.e., Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) as a base learner. In the second level, they used MultiLayer Perceptron (MLP) as a meta-learner. However, for the imbalanced data problem, the authors used a combination of hybrid synthetic minority oversampling techniques (SMOT) and edited nearest neighbor (ENN). The SMOT technique was used in [20] to fix the problem of imbalanced data in the credit card fraud detection dataset. The authors used five different ML algorithms for the classification. Finally, the voting technique was used to choose the final prediction.

The Binary Brown Bear Optimization Algorithm (BBBOA) was created by [21]. BBBOA was used as a feature selection algorithm to minimize the dimensionality of the fraud detection dataset. This novel optimization algorithm was tested through diverse state-of-the-art datasets and compared with various meta-heuristic algorithms. The BBBOA employed exploration and exploitation to decrease the effect of imbalanced data from their point of

view. The authors also used three different algorithms, i.e., SVM, KNN, and XGB tree, in the classification process.

3. THE RESEARCH METHODOLOGY

Fraud detection methodology normally involves two key phases: financial transactions data acquisition and classification. The classification phase employs a classifier set of rules to differentiate between valid transaction activity and fraudulent transactions.

3.1 Problem Formulation

$Y = \{ y^{(1)}, y^{(2)}, \ldots, y^{(L)} \}$ it is a collection of equivalent labels intended for D, that comprises the input dataset. The input set can be formally represented by $D = \{ x^{(1)}, x^{(2)}, \ldots, x^{(L)} \}$ to symbolize L is a labelled financial transactions data in a network traffic environment. D is formed of F fraud instances and N normal instances, $F + N = L$. To illustrate the fraud detection in an imbalanced dataset, for the sake of this analysis, we will assume $F \ll N$. This study aims to identify whether financial transactions category is fraud or normal instances stated as $y^{(i)}$. Furthermore, every instance $X^{(i)}$ is an n-dimensional feature vector, which can be represented as $X^{(i)} =< x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)} >$ It is observed that $X^{(i)}$ ordinarily is a high-dimensional feature vector from financial transactions data in network traffic environment.

3.2 Modelling And ML

ML offers techniques for fraud detection, able to identify current, contemporary, and future fraudulent actions, even diffused patterns, with minimal human-directed instruction. ML utilizes algorithms that analyze data to reveal patterns and anticipate future events [22]. Classification is a common task in supervised learning, and our proposed system utilizes five popular types of algorithms: LR, KNN, SVM, DT, and CNN. Every algorithm is introduced in-depth, and how these algorithms have been utilized in a fraudulent financial transaction detection system is discussed.

Logistic regression: The LR algorithm is a robust statistical technique used in ML as supervised learning for binary classification. It uses a sigmoid function (a special type of Logistic), which squeezes the output value between 0 and 1, making this choice naturally match our requirement to figure out the chance that the target will happen given some input(s) [23]. It works by creating a linear function of the data features input with coefficients learned during model training. This mixture was later given to the sigmoid function, which yields that as a probability. This model attempts to find the best weights that minimize error, so predictions as close to reality will be. It determines the optimal coefficients that minimize this difference between predicted probabilities and actual observed outcomes to make its predictions as close to actuality as possible. This is frequently achieved through finding the best parameter values that are most probable given the data in keeping with the model's specification [24]. LR can capture artifacts from underlying complex relationships among features and the probability that a given transaction will be fraudulent [25]. It creates a model of the probability that any transaction is fraudulent based on several input variables like timestamp, name, email, address, or IP address, and country. From the identified features and their relationship to fraud, LR estimates a model that predicts whether or not a new transaction is fraudulent by analyzing at historical data.

Decision Tree: DT is a hierarchical structure (a tree) where each internal node represents an option based on one feature. The branches going off of each node are the possible outcomes from choosing that option (i.e., should you proceed with your investigation), and it terminates on end nodes, also known as leaf nodes (the fraud or normal transactions). Tracing a path from the root node all the way to leaf nodes determines which classification rules apply. This path is basically some chosen decisions based on the feature tests at each internal node. It builds the tree by determining attributes, and what values of those attributes produce other branching possibilities. Once that is done, it will then be used to assess the data coming down each intermediate node in the tree. Once the tree is built, it can serve as an early prediction about incoming instances by going from a root feature to the leaf, checking at each node whether the quality of features in every internal node fulfills some criteria. The main difficulty in building a decision tree is to find which value on the node of the tree will be used as its dividing [26]. Many works in the literature have shown that DT is good at solving fraud detection problems, especially for financial transactions. They do so by using past data to create a hierarchical structure of decision rules called the tree. Each of them relates to different characteristics, like amount, location, or timing, etc., and they correspond with a node in the tree. The leaves are then the predictions you want to make (eg, is this transaction likely fraudulent or not), and thus

branches represent different possibilities of what your decision might be [27].

K-Nearest Neighbors: KNN is a simple yet powerful supervised ML algorithm that can be used for regression and classification problems. A fundamental principle was that data points close to one another are likely to be in the same class [28]. KNN finds k number of closest data points to a new unseen data point according to some distance metric (e.g., Euclidean distance); The number of classes among the "k" nearest neighbors is used to determine which class the data point belongs to. This algorithm is also used for complex relationships in a dataset that may not be linear, therefore, it requires minimal model tuning (hyperparameter tuning) that makes many ML tasks easy to perform [29]. KNN classifies a new instance into one of two classes known (one with the highest overall similarity) based on the K most similar records, which were used to classify above nearest neighbors. In case of financial transactions, KNN works this way - comparing a new transaction (their attributes or variables are treated like array elements as its vector also in form simplicial facet/vertex - not testing the intersection just finding vertical projection intersection points for each asset coplanar). This computes the distance between a new transaction and each historical transaction using features like user behavior, time relative to some reference, transaction amount, and geographic locations. Then, the algorithm takes the new transaction as an object and associates it with either the fraudulent or non-fraudulent class by looking at "K" closest transactions in history [30]. Its use case is particularly good to catch the unusual or outlier transactions that might be missed in usual statistical models.

Support vector machine: SVM is a fast and dependable classification algorithm that offers proper precision in comparison to different algorithms. SVM tries to find an optimal hyperplane in the best way possible which can delineate data points for different classes. The data points that are closest to the decision boundary of separating these two classes define a hyperplane, and they are called "support vectors". The idea here is to maximize the margin between the hyperplane and those support vectors giving us a better, more generalized model [31]. SVMs make it possible to deal with more complex classification problems such as non-linear relationships since the mapping of data into a higher dimension allows better discrimination between classes [32]. The same is the case with SVM for detecting fraudulent financial transactions, because of their robustness in handling complex data having very high dimensions and identifying non-linear correlations between features. This function figures out an optimal hyperplane that can divide normal and fake transactions with different attributes such as transaction amount, location, time, and user behavior, etc. SVM is known to have high accuracy and robustness by maximizing the margin between the hyperplanes themselves, as well as support vectors (data points that lie closest of all data in any class), thus being suitable for outlier transactions identifying [33].

Convolutional neural network: CNN is a robust class of DL algorithms that have been very successful in domains where built to analyze and handle data with a grid-like structure, to illustrate images and time series. Instead, each convolutional layer in a CNN focuses on learning different aspects of the image [34]. Their specific architecture, modelled after the brain's visual cortex, which consists of a series of convolutions that extract features from input data. These layers are convolutional, meaning they perform convolutions (applying filters to the input data to identify patterns and features). Subsequent to these convolutions, the outputs of the convolution layers are applied over a pooling layer by which feature maps are reduced and capture main features. This is a process of continuous learning passing through many layers and gradually gathering more comprehensive features and an intrinsic representation from the input data. The last feature extracted is followed by a manifold consisting of connected layers which will perform the classification or predictions given its input. CNN has changed the way ML practitioners think about data, being able to form hierarchical structures of complex patterns automatically and achieving incredible accuracy on a variety of tasks like image recognition, NLP, and time series analysis [35]. In general, CNN has shown a lot of promise in extracting intricate features from various types of data and has an excellent prospect for fraud detection on financial transactions as well. With architectures made up of convolutional layers, pooling layers, and fully connected layers they can learn very complex patterns in transaction data such as the amount attributed with a transaction, time stamps from transactions, and user behavior. The CNN identifies anomalies and unusual activities better than traditional rule-based or statistical models as it learns hierarchical representations of these features [36].

Table 1 explores the strengths and weaknesses of classification algorithms that are used for detecting fraudulent financial transactions in the proposed system. We compare a range of algorithms from 4 different ML and one DL category: statistical-based parametric-LR, decision-based DT, Proximity-based KNN, hyperplane-based SVM, and learning-based CNN. These algorithms leverage powerful techniques, including SMOTE tackling imbalanced data issues seen in fraud detection datasets. They are fast in training too, and hence suitable for deployment. Therefore, to combine these algorithms into the proposed model to detect fraudulent financial transactions, our goal is to maximize the classifier's effectiveness by addressing challenges.

Table 1: Comparison of the advantages and disadvantages of classification algorithms that are used in the proposed fraudulent financial transactions detection [37][38].

Algorithm	Advantages	Disadvantages
LR	• Straightforward: can be understood and applied. • Quick: Training and testing are fast. • Interpretable: Coefficients give comprehension of feature importance. • Robust - Works well with linearly separable data.	• Linear: Supposes a linear connection of results and features. • Overfitting: When the number of features is high dimensionality.
DT	• Explainable: The process is easy to understand and the outputs can be visualized. • Compatible: Can deal both with categorical and numerical variables. • Robust: Resistant to Outliers. Non-parametric: It does not assume specific underlying data distribution.	• Susceptible to overfitting: Easily overfits to the training data, leading to poor generalization. • Sensible: It can be very sensitive to tiny modifies in the data. • Limited: poor with high-dimensional datasets.
KNN	• Intuitive & Explainable: Understand why classifications are made and explain the model decisions. • Training time: short training times, especially on big datasets. • Effective in high-dimensional data: Works well with a large number of features. • Can deal with outliers: Less Influential to outliers.	• Decision Boundary - Linear: Only capable of identifying linear correlations between features and the target. • Susceptible to variations in feature scales: Needs proper features scaling for better performance. • Needs big datasets: Requires a significant amount of training data for accurate classifications.
SVM	• Accuracy: Able to obtain high accuracy (particularly on complex data). • Overfitting: Exhibiting lower susceptibility to overfitting, especially for high dimensional data. • Non-linear Data: Suitable for classifying data with non-linear separability.	• Training: Training time can be slow for big datasets. • Hard to Tune: Hyperparameters must be initialized carefully for best performance. • Hard to Interpret: The decision boundaries of the model are difficult to understand.

CNN	• Image/Video: Excellent for pattern recognition in data images. • Extraction: Less manual effort, automatically learns the relevant features from training data. • Less Overfitting: requires fewer parameters compared to fully connected networks.	• High Computational Cost: Needs lots of resources to train and inference. • Data: needs big datasets to perform better training. • Black Box: Sense that the decision-making process cannot be understood.

3.3 The Proposed Methodology

This section describes the fraud problem in credit card systems, which is a major problem, costing financial institutions and individuals millions of dollars every year. Traditional methods of fraud detection are often ineffective against sophisticated fraudsters.

As we said above, a traditional credit card system is a complex network of institutions, technologies, and processes that enable individuals and businesses to make payments easily using credit cards. It allows consumers to purchase goods and services without immediately paying, while merchants can receive payments without handling cash. In this system, the card is swiped or inserted into the POS terminal or online payment gateway, then by using payment processor verification: The payment processor verifies the card details (account number, expiration date), available credit limit, and checks for fraud detection flags. The payment processor sends an authorization response to the merchant, indicating approval or rejection. If it is approved, it goes to the predictive model. In this step, the predictive model works to detect the fraudulent transaction by using advanced algorithms to analyze transaction patterns, identify potentially fraudulent activities, and trigger alerts and investigations, as shown in Figure 1.

3.4 The Proposed System

The proposed credit card fraud detection system will consist of four main layers. These layers combine to allow the system to detect and prevent credit card fraud accurately. Figure 2 shows the architecture of the proposed system.

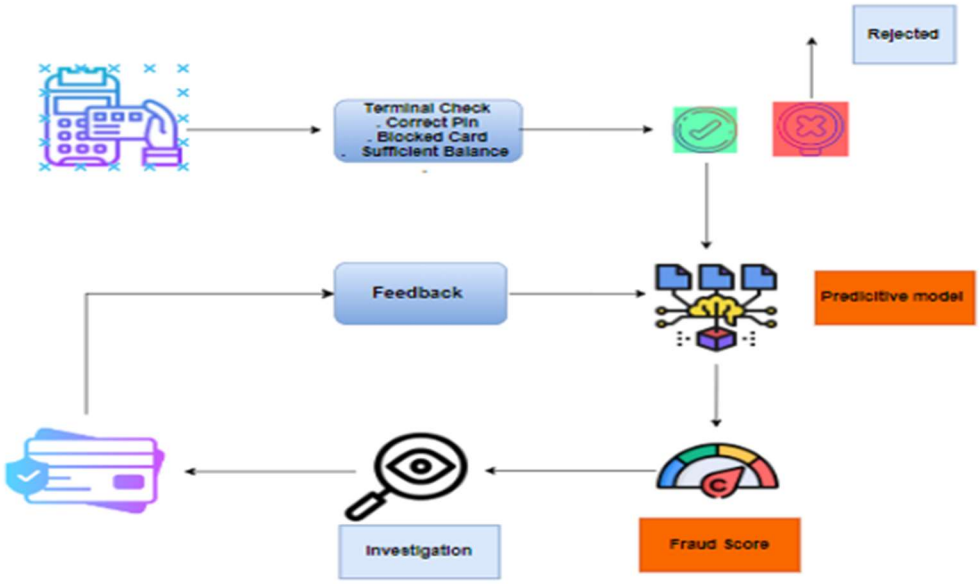

Figure 1: Flow Diagram of Credit Card Fraud Detection System

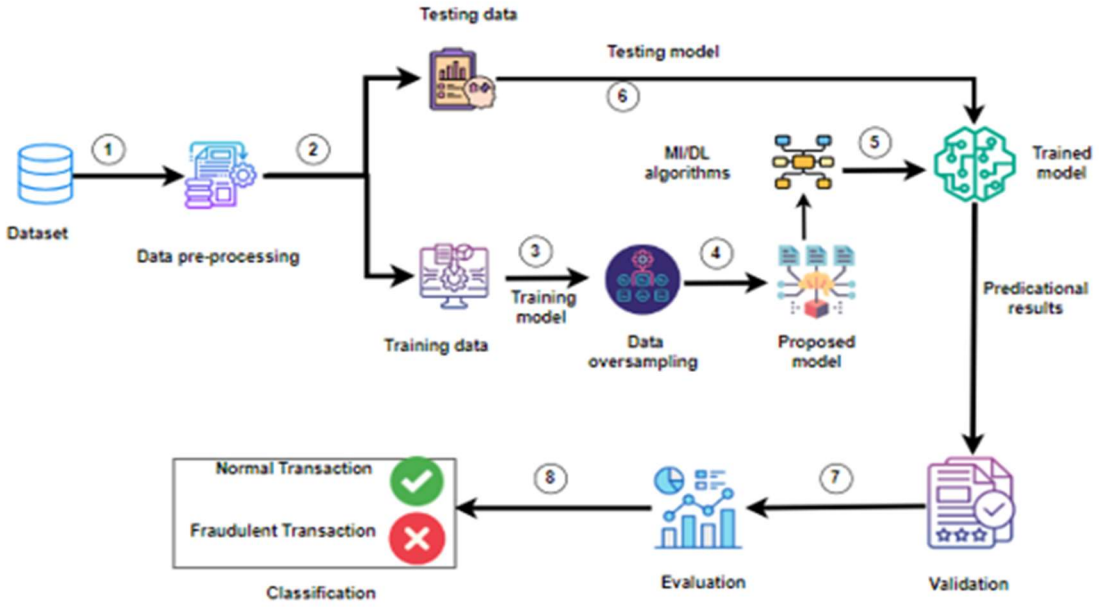

Figure 2: The architecture of the proposed credit card fraud detection system

The layers of the proposed system are described as follows:

- *Data preparation layer:* The Data Preparation layer dives into a detailed exploration of the credit card fraud detection benchmark dataset, feature engineering, and data preparation for modelling. This layer is pivotal to ensuring the ML models are equipped with rich, valuable data and therefore capable of detecting fraud more accurately. This layer involves data normalization or standardization to preprocess the input features ahead of modelling, as well as making the data proper as an input for the next layer.

- *Model development layer*: This layer trains models on data and evaluates model performance to determine the best fit for the task, i.e., credit card fraud detection. This layer includes partitioning, class imbalance mitigation, and classification.

Partitioning means the dataset will split into the train & test datasets with an 80/20 ratio, and make sure that the class distribution (fraud and non-fraud) in both training and test sets is representative of the overall dataset to retain proper evaluation.

In Class Imbalance Mitigation the transaction detection Credit card fraud models are known to have imbalanced data because they usually use a higher rate of valid transactions than fraudulent ones. The class imbalance can result in a biased model towards the majority class, leading to poor detection of the minority class, i.e., fraud instances. The Synthetic Minority Over-Sampling Technique (SMOTE) is a very effective way of dealing with this notion. SMOTE is used on the training dataset to create synthetic instances of the minority class, increasing its presence in fraudulent transactions. It does this by taking each minority class sample and inserting new examples within the line segments that connect any/all of the k-minority class nearest neighbours. The formula for generating synthetic samples can be expressed as:

$$x_{new} = x_i + \text{lambda}(x_j - x_i) \quad (1)$$

Where xi represents a minority class sample, xj is one of the k's nearest neighbours, and lambda takes a random number between 0 and 1. The aim of this is to help the machine learning models see more balanced cases during training, thus enabling them to learn better what any underlying patterns for fraudulent activities look like. This behaviour subsequently enhances the predictive accuracy of models for credit card fraud, especially when those have heavily imbalanced data distributions. Thus, SMOTE makes sure that the machine learning models do not get biased only towards the major class and can have a better approximation of the underlying latent patterns in fraudulent transactions.

Then the classification module, which is considered one of the fundamental components that

form part of the proposed system and it has an important job to identify credit card fraud transactions truthfully. This subsection attempts to obtain reliable and effective ML algorithms using the chosen dataset for the credit card fraud detection problem. In classification models, searching for hyper-parameters is very important to get good performance as expected. Hyper-parameters are model configurations that you select before training. These parameters can dramatically affect the ability of your models to learn, generalize, and converge. Fortunately, a good method called grid search can guide users easily through this hyper-parameter optimization process. The main advantage of grid search performs hyper-parameter choosing in a systematic way. Instead of making guesses or using the trial-and-error technique, you can specify a range for each hyper-parameter to be tested via grid search, where the best combination is selected. This systematic exploration method makes sure you do not overlook some best configurations which is very critical in the case of complex classification problems.

The first model is Logistic Regression with a constant equal to one, Logistic Regression is a very powerful algorithm for binary classification problems, such as Fraud detection, due to its ability to model both the probability of each transaction depending on the input features. The threshold is adjusted to 0.8 to reduce false positives and improve precision for the minority class. Also, logistic regression is prone to over-fitting on imbalanced datasets, so increasing the regularization (decreasing C and increasing lambda) can help prevent over-fitting on the majority class. Furthermore, SVM is famous for dealing with high-dimensional, non-linear data which is why they fit very well when we talk about fraud credit card transaction detection, where it consists of many features on the basis of complex patterns that might exist in them. The Radial Basis Function (RBF) is used in this algorithm as a kernel with C = 10 and gamma = 0.01. In addition, CNNs can automatically learn specific features from the input data, in this way obtaining information about the spatial and temporal dependence of credit card transactions. The CNN was composed of 4 convolutional layers, with 128 filters and a kernel size (3 x 3), followed by a dense with 2 layers and a batch size of 64. The algorithm is also trained with 100 epochs. Similarly, KNN is a simple yet effective algorithm that can identify fraudulent transactions by comparing them to the nearest neighbours in the training data, helping to detect anomalies and outliers. The proposed KNN model used 7 neighbours and the 'Euclidean' distance metric. Finally, DT can provide an interpretable model that captures the complex rules and decision boundaries underlying credit card fraud, allowing for better understanding and explain ability of the detection process. The configuration used with this algorithm was a maximum depth of 10, a minimum of 5 samples per split, and a minimum of 2 samples per leaf.

- *Model Evaluation layer:* Evaluate the results of each model with a wide range of performance metrics (e.g., accuracy, precision, recall, and F1-scores) to make sure that the models are able to detect fraudulent transactions while minimizing false positives.

- *Model Selection and Optimization layer:* In the last step of this system, we exquisitely examine the outputs and select one or multiple fine-tuned models, which can really catch fraudsters who dare to commit credit card fraud. Once the model is chosen, it may undergo fine-tuning by tuning hyper-parameters or extracting useful features to improve its forecasting performance on testing data with a balance between detection accuracy while keeping up the interpretability and computational efficiency required for smooth production implementation.

4. THE EXPERIMENT RESULTS ANALYSIS

4.1 Data Analysis

This paper uses a famous dataset called the credit card fraud detection dataset [39]. This dataset was created by the Machine learning Group in the Université Libre de Bruxelles (ULB), which specializes in fraud detection and big data mining [40]. It represents a snapshot of credit card transactions during 2 days in September 2013 which were made by European cardholders. The dataset consists of 99.83% normal transactions and 0.17% fraudulent transactions, which clearly shows the structure of a highly imbalanced dataset. The imbalanced dataset may cause incorrect predictions when implementing any model on this dataset. The

information in the dataset is sensitive therefore, it has been transformed to another form to keep it private. However, all variables are numeric and they have been masked to names and numbers, such as variables V1/V2...V28 [41]. The "class" feature is very important because it represents the heart of the credit card dataset, it is a binary Boolean value used to detect the true nature of a transaction where number (1) means it is an abnormal (fraudulent) transaction while number (0) means it is a normal transaction. This process is called classification, which represents the main issue to Distinguish between fraud needles (the positives), and the normal haystack (the negatives).

4.2 The Experiment Results

This section demonstrates the performance of the proposed credit card fraud detection system. To integrate the system that was constructed around a set of binary classifiers itself, we played with different discriminating classification techniques to see which works better using some algorithms which are CNN, LR, KNN, SVM, and DT. We report five different reports for each experiment, using distinct datasets and metrics of performance to obtain a comprehensive view of system behaviour.

Using a set of common measures, we evaluated the suggested system. One of the main tools for assessing classification models is the confusion matrix, which can offer a clear, concise picture of how well the system predicts various classes. The model's performance is displayed where it works and where it doesn't using the confusion matrix. True Positive (TP), False Negative (FN), True Negative (TN), and False Positive (FP) are the fundamental metrics upon which it is based. The values utilized to determine the metrics for each model are shown in Figure 3.

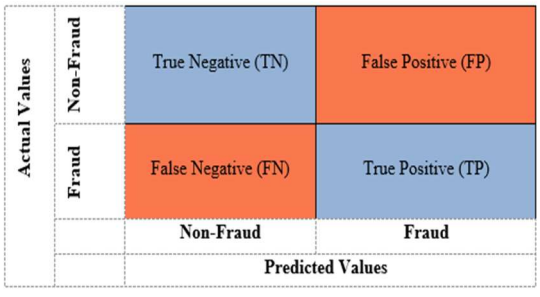

Figure 3: Confusion matrix

The performance of the system was evaluated using the following metrics:

***Accuracy*:** A metric for measuring the performance of the ML models. It simply tells us how many values within each class were correctly classified against the total amount of instances that were used. It can be calculated using the equation below:

$$Accuracy = \frac{TP+TN}{FN+TP+FP+TN} \quad (2)$$

***Precision*:** One of the significant metrics for assessing a positive prediction from the model, it tells us what proportion of the positives are, actually correct predictions, and is a decent way to characterize how effective the model is. It can be calculated using the following equation:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (3)$$

Recall: is an important metric in ML, especially when the success hinges on finding every single positive case. It is the measure of how well a positive class model can detect with respect to total actual positives. This can be calculated using the following equation:

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

***F1-score*:** is considered a more balanced evaluation of ML models than precision and recall. The F1-score is the harmonic mean of precision and recall; thus, it ensures that both are equally accounted for in this calculation. This can be calculated using the following equation:

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (5)$$

As mentioned in the above subsection, the proposed system has five models. Each classifier (LR, KNN, SVM, DT, and CNN) trains the model to identify a specific normal or fraud instance identified in the Credit Card Fraud Detection benchmark dataset that was used. Table 2 and Figure 4 illustrate the experimental results obtained from testing the models trained on a dataset oversampled using the SMOTE technique. SMOTE: Synthetic Minority Over-sampling Technique is a powerful methodology used in the treatment of imbalanced datasets which tend to come up when training Machine Learning models. This helps in reducing class imbalance bias, increasing the accuracy

sensitivity and generalizability of the model while maintaining fairness and interpretability. This makes it a useful weapon to deal with imbalanced classification problems such as fraud detection because over-sampling enables you to use more information from the minority class (the one we are interested in), and that is always beneficial.

Table 2 : Performance evaluation for all models in the proposed system

Model	Accuracy %	Precision%	Recall %	f1-score %
Logistic Regression	96.13	98.66	95.72	97.16
K Nears Neighbors	94.1	96.5	92.02	94.2
Support Vector Machine	96.15	97.18	95.36	96.26
Decision Tree	89.78	86.63	94.82	90.54
Convolutional Neural Network	99.06	73.75	86.35	79.55

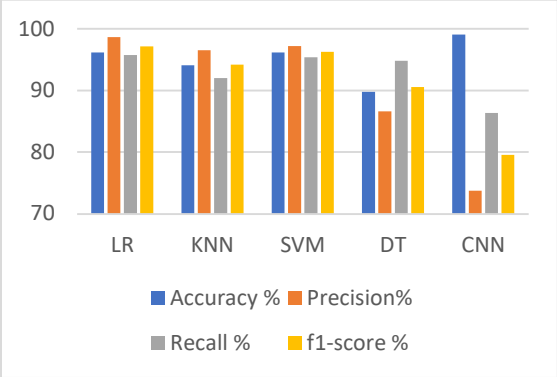

Figure 4: Performance evaluation for all models in the proposed system

As shown in Figure 5, the Convolutional Neural Network model (CNN) is the top-rated model with an accuracy of 99.06%, largely surpassing other models. This is done by the ability to learn hierarchical representations, extract robust features, and perform end-to-end learning in this model.

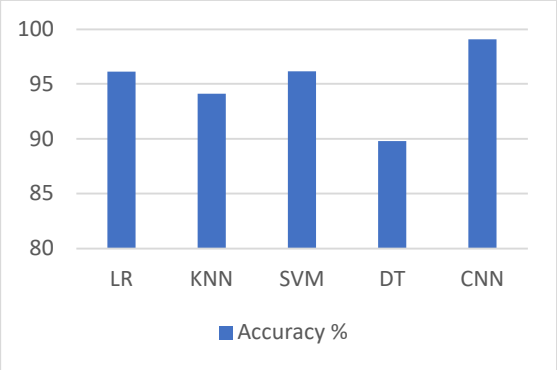

Figure 5: A comparison among the suggested models according to accuracy metric

The Logistic Regression (LR) model obtained the highest precision at 98.66%, with almost minimal false positives in this case. It is an important metric for fraud detection, as it will help in ensuring that fewer genuine transactions are falsely accounted as fraudulent. Figure 6 shows a graphical view of these metrics. The probabilistic approach, linearity, feature selection, interpretability, and handling of imbalanced data enable the logistic regression model to earn the highest precision score, i.e., 98.66 % is possible in the fraud detection problem discussed above. Because of this high precision, the LR model is capable of precisely predicting whether a transaction is fraudulent with a shallow range of false positives, which is indeed very instrumental for all fraud detection systems, as we know.

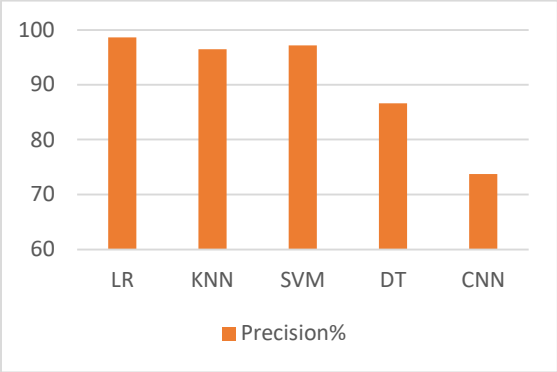

Figure 6: A comparison among the suggested models according to precision metric

It is important to notice the high recall of the Logistic Regression model with 95.72% in comparison with other models, as shown in Figure 7, which can be great for fraud detection. Recall (other names include sensitivity or true positive rate) will show you how many fraudulent transactions were identified by your model correctly. With a 95.72% Recall, it indicates that the Logistic Regression model can recognize most of the true fraud cases, which helps to evade as many mistaken cases so the fraudulent transactions can be identified and taken care of effectively for further steps.

The Decision Tree model on the other hand has a recall of 94.82%, which is also good and close to the Logistic Regression model, however placed slightly behind it. This is a substantial difference and it seems that the Logistic Regression model does a much better job of detecting more fraudulent transactions, which makes sense as we are dealing with a fraud detection problem.

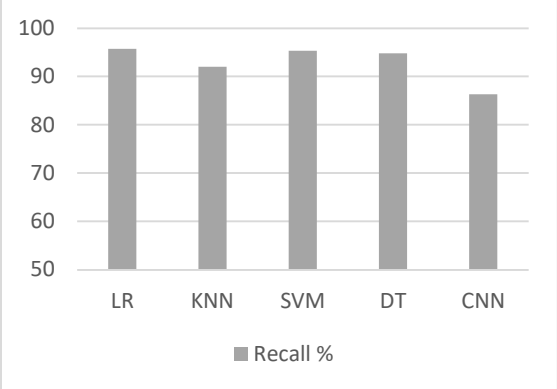

Figure 7: A comparison among the suggested models according to recall metric

The Logistic Regression model also has a high F1-score of 97.16%, showing good performance consistently, as shown in Figure 8. F1-score is the harmonic mean of precision and recall that gives a better measure of overall performance. High F1-score: It means that the Logistic Regression model performs well in balancing missing more frauds (recall) and not having many false positives.

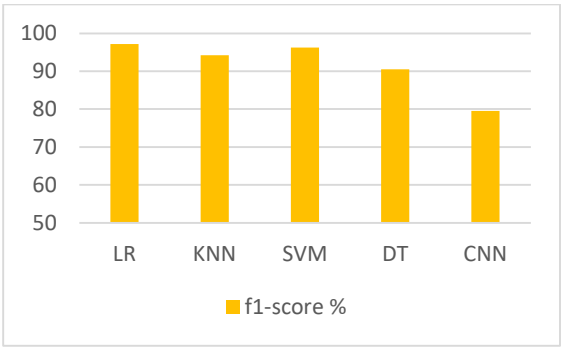

Figure 8: A comparison among the suggested models according to F1-score metric

So now looking at the high precision and recall, we can say that the model is awesome to be a fraud detection system. This exhibits that the model can help catch fraudulent transactions accurately but not miss too many of them, which makes it a beneficial method for companies willing to fight against financial fraud.

As mentioned and illustrated above in Table 2, the evaluation of the proposed model on the Credit Card Fraud Detection benchmark dataset for fraud transaction detection is shown. The performance metrics of the Logistic Regression (LR) model are the highest in all such metrics, which mostly states that LR is best working under different settings with its F1-score, precision, and recall most the highest. These are more complete metrics than just accuracy in this case because they take into account that the classifier has to perform well in identifying frauds (TP) and can rarely classify a normal transaction as fraudulent (FP).

5. DISCUSSION

This section aims to compare the proposed model with other literature studies that focus on the fraud in credit card transaction problem and deal with the same dataset.

Table 3 and Figure 9 illustrate the performance metrics of the financial fraud detection domain experiment comparing two different approaches F. K. Alarfaj et al[17] and N. S. Alfaiz et al[4] with the proposed model.

In terms of recall, if we look at the proposed model, it has a 95.72% where beforehand recall is slightly lower in comparison to N. S. Alfaiz et al[4] which finished with 95.91%. However, the proposed model has a strong performance in other metrics.

The proposed model has an accuracy of 96.13%, which is below very high accuracies, but it reduces the number of false positives and ensures all genuine transactions are correctly authorized. However, the true power of the proposed model lies in its precision, which is a staggering 98.66 %. This in turn results in the model flagging something as fraud, it is doing so with a very high confidence score, thus significantly reducing not only the friction of the entire process for legitimate customers but also the burden on Fraud investigation teams. The Proposed model will allow the financial institutions to dedicate resources only for addressing concrete fraud cases, hence avoiding false positive alerts, which in turn affects their overall efficiency and effectiveness of mitigation strategy against online card, or account fraud.

Table 3: A comparison between the proposed model and a literature works

Algorithm	Accuracy	precision	Recall	F1-Score
F. K. Alarfaj	99.9	93	---	85.71
N. S. Alfaiz	99.96	80.28	95.91	87.4
The proposed model	96.13	98.66	95.72	97.16

From the fraud detection system point of view, precision is a more important metric than accuracy. Precision here refers to the system's capacity to identify how many transactions it believes are fraudulent (frauds detected) and if these cases actually are frauds (true positives). It is important in fraud detection to reduce the number of false positives, since these may require an investigation and inconvenience for a genuine customer. However, precision focuses on true positives, and even worse for fraud detection a high rate of false positives could make the measure deceptive. Prioritizing exactness allows the fraud detection system to be more informed. It will make better decisions, correctly allocate resources, and implement a successful strategy for keeping fraudulent activity at bay. The precision of this fraud detection system ensures that it can identify real fraudulent activities accurately, and this is what makes the model more reliable as well as trustworthy for both organizations & their customers.

The Proposed model is moderately detecting and complements its precision with an impressive 97.16% F1-score. F1-Score is a measure combining precision and recall. For this balanced metric, it shows the incredible ability of our model to find fraud activities without causing too many false alarms.

Given the environment in financial transactions, where fraud detection is of the essence more than ever before, the proposed model proves its efficiency. This means of processing and risk-based decision allows fraud issues to be identified enough that it are reduced in number, while simultaneously protecting cardholders from the destruction brought upon them due to credit side payments caught up in fraudulent activity. Figure 9 shows the superiority of our model in fraud detection than other literature works.

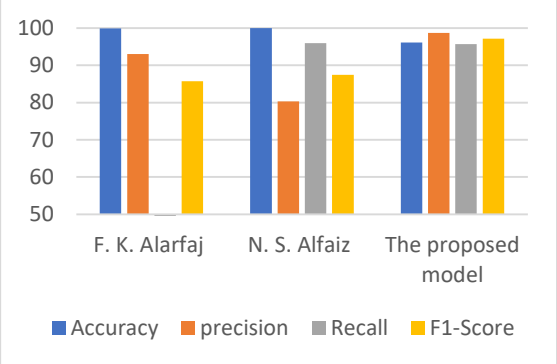

Figure 9: A comparison between the proposed model and a literature works

6. CONCLUSION

The increase in credit card fraud and the rise of non-cash electronic payment methods have serious challenges for cross-border economic activity. It requires powerful and adaptable adversarial fraud detection strategies. This paper has inspected how ML and DL perform with fraudulent transaction detection. This paper suggests a system to detect fraud in credit card transactions by proposing five models which are LR, KNN, SVM, DT, and CNN. The SMOTE technique is also used to reduce the effect of unbalanced data. The proposed system achieved the highest score in detecting fraudulent transactions based on the LR model. While detecting it also indicates that the proposed system can be an efficient tool in terms of reusing detailed features from different data samples, which is quite promising for detecting credit card fraud with the help of refinement continuously. Although much progress has been made, additional research for imbalanced datasets, feature engineering improvements, and hybrid models is required. With ongoing improvements to detection methods, as well as emerging technologies like federated learning for cross-institutional fraud detection without shared data, the system that supports credit card transactions can become safer and more secure - better protecting consumers from identity theft while shielding banks against financial losses.

REFERENCES

[1] ACFE. Association of Certified Fraud Examiners (ACFE) 2024 Report to the Nations. Accessed: 2025. [Online]. Available: https://legacy.acfe.com/report-to-the-nations/2024/".

[2] Hilal.W, Gadsden.S.A, Yawney.J2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances - Expert Syst. Appl., vol. 193, p. 116429.

[3]Ashtiani.M N, and Raahemi. B, (2022). Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. in *IEEE Access*, vol. 10, pp. 72504-72525.

[4]Alfaiz, N. S., & Fati, S. M. (2022). Enhanced Credit Card Fraud Detection Model Using Machine Learning. *Electronics*, *11*(4), 662.

[5]Kamuangu.P.(2024). A Review on Financial Fraud Detection using AI and Machine Learning - J. Econ. Financ. Account. Stud. 6.1, pp. 67–77.

[6]Alfaadhel.A, Almomani, I., & Ahmed, M. (2023). Risk-Based Cybersecurity Compliance Assessment System (RC2AS). Applied Sciences, 13(10), 6145.

[7] Sarma. D, Alam. W, Saha. I, Alam. M. N., Alam. M. J and Hossain. S. (2020). Bank Fraud Detection using Community Detection Algorithm. *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 642-646.

[8] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences*, *12*(19), 9637.

[9] Al-Hashedi, K.G,and Magalingam.P.(2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019 - Comput. Sci. Rev. 40 100402.

[10]Ngai .E. W. T., Hu.Y, Wong Y. H, Chen.Y, and Sun. X.(2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature - Decis. Support Syst. 50.3 559-569.

[11] Chaquet-Ulldemolins. J., Gimeno-Blanes, F.-J., Moral-Rubio, S., Muñoz-Romero, S., & Rojo-Álvarez, J.-L. (2022). On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders. *Applied Sciences*, *12*(8), 3856.

[12] Da'u, A., Salim, N. (2020). Recommendation system based on deep learning methods: a systematic review and new directions. *Artif Intell Rev* **53**, 2709–2748.

[13]Awoyemi.J.O,Adetunmbi.A.O, and Oluwadare. S. A.(2017). Credit card fraud detection using machine learning techniques: A comparative analysis. International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, pp. 1-9.

[14]Asha. R and Suresh. K.(2021).Credit card fraud detection using artificial neural network - Glob. Transitions Proceedings, vol. 2, no. 1, pp. 35-41.

[15] Taha. A & Malebary.S. (2020). An Intelligent Approach to Credit Card Fraud Detection Using

an Optimized Light Gradient Boosting Machine. IEEE Access. 8. 25579-25587.

[16] Sailusha. R, Gnaneswar. V, Ramesh. R and Rao. G. R.(2020). Credit Card Fraud Detection Using Machine Learning. *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 1264-1270.

[17]Alarfaj.F.K, Malik. I, Khan. H. U., Almusallam.N, Ramzan.M and Ahmed.M.(2022)Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. in *IEEE Access*, vol. 10, pp. 39700-39715.

[18]Salekshahrezaee,Z., Leevy, J.L. & Khoshgoftaar, T.M.(2023). The effect of feature extraction and data sampling on credit card fraud detection. *J Big Data* **10**, 6 .

[19]Mienye. D and Sun.Y.(2023).A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection. in *IEEE Access*, vol. 11, pp. 30628-30638.

[20] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. *Big Data and Cognitive Computing*, *8*(1), 6.

[21] Sorour S. E., AlBarrak. K. A, Abohany. A. A, and El-Mageed.A.A. (2024).Credit card fraud detection using the brown bear optimization algorithm - Alexandria Eng. Journal, vol. 104, pp. 171-192.

[22]Alhabshy.A,Hameed.B.I.Eldahshan.K.A.(2022). An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers. IEEE Access, vol. 10, pp. 52724–52743.

[23]James. G,Witten. D,Hastie. T, Tibshirani. T, Taylor.J.(2013). An introduction to statistical learning: with applications. New York, Springer Science and Business Media, eISBN: 978-1-4614-7137-7. *Statistical Theory and Related Fields*.

[24] Aurélien Géron.Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow. Third Ed. O'Reilly Media, Inc, 2022.

[25]Bolton, R.J. and Hand, D.J.Statistical fraud detection: A review - Stat. Sci. 17.3 235-255. 2002.

[26]Save.P,Tiwarekar.P,Jain.K.N,Mahyavanshi.N. (2017). A novel idea for credit card fraud detection using decision tree - Int. J. Comput. Appl. 161.13.

[27]Maira. A, Ali.M.Yadav.A.(2015).A comparative study of decision tree algorithms for class imbalanced learning in credit card fraud detection - Int. J. Econ. Commer. Manag. 3.12 86-102.

[28]Altman N.S.(1992).An introduction to kernel and nearest-neighbor nonparametric regression - Am. Stat. 46.3 175-185.

[29]Hattori. K, Takahashi. M.(2000).A new edited k-nearest neighbor rule in the pattern classification problem - Pattern Recognit. 33.3 521-528.

[30]MaliniN, Pushpa.M(2017).Analysis on credit card fraud identification techniques based on KNN and outlier detection - third Int. Conf. Adv. Electr. Electron. information, Commun. bio-informatics (AEEICB). IEEE.

[31]Bhavsar. H and Panchal. M. H. (2012). A Review on Support Vector Machine for Data Classification.International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, No. 10.

[32]Cervantes.J,García-Lamont.F,Rodríguez-Mazahua.L,&López,A.(2020). A comprehensive survey on support vector machine classification: Applications, challenges and trends. Neurocomputing, 408, 189–215.

[33]Gyamfi. N. K. and Abdulai. J. -D ,(2018).Bank Fraud Detection Using Support Vector Machine," *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada.

[34] Li.Z, Liu. F, Yang. W, Peng.S and Zhou.J.(2022). A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999-7019.

[35] Taye, M. M. (2023). Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions. *Computation*, *11*(3), 52.

[36] Karthika, J., Senthilselvi,(2023). A. Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique. *Multimed Tools Appl* 82, 31691–31708 .

[37] Nazarenko. E, Varkentin. V and Polyakova. T. (2019). Features of Application of Machine Learning Methods for Classification of Network Traffic (Features, Advantages, Disadvantages). *International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, Russia.

[38] Liu, H., & Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*, *9*(20), 4396.

[39] Credit Card Fraud Detection. Accessed: Jun. 2024, 6. [Online]. Available:", [Online]. Available: https://www.kaggle.com/datasets/mlg-lb/creditcardfraud?resource=download

[40] Patel H, Singh Rajput D, Thippa Reddy G, Iwendi C, Kashif Bashir A, Jo O(2020). A review on classification of imbalanced data for wireless sensor networks. *International Journal of Distributed Sensor Networks*.6(4).

[41]Esenogho.E, Mienye. I. D, Swart. T. G., Aruleba.K and Obaido. G, (2022).A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection," in *IEEE Access*, vol. 10, pp. 16400-16407.