Enhanced Credit Card Fraud Detection Using Deep Learning Techniques

Ola Imran Obaid[1,*], Ali Yakoob Al-Sultan[1]
[1]College of Science for Women-Computer Science Dept, University of Babylon, Babylon, Iraq
Emails: ola.alghazaly.gsci135@student.uobabylon.edu.iq; ali.alsultan@uobabylon.edu.iq

Abstract

Credit card fraud is a huge challenge in the financial sector, causing huge losses every year. The problem is exacerbated by increased marketing and sophisticated fraudulent activities. This study addresses the important issue of accurate real-time detection of fraudulent transactions to minimize financial losses and enhance transactional security. The main objective of this study is to develop a comprehensive fraud detection algorithm using deep learning techniques, specially designed to address the complexity and volume of modern credit card transactions. Key contributions of this research include the presentation of a new deep learning algorithm optimized for credit card fraud detection, the integration of feature engineering techniques to improve the performance of the model, and a potential scalable solution analysis in real-time Significant improvement in proven rates. The results show that the proposed deep learning-based model achieves higher accuracy and lower false positive rate, giving financial institutions a significant advantage in protecting against fraudulent activities about the character. This study highlights the power of deep learning in reforming fraud detection systems, and lays the foundation for future developments in this important area.

Keywords: Credit Card Fraud Detection; Deep Learning Techniques; Neural Networks; Real-Time Analysis; Feature Engineering; Fraud Detection Accuracy; Financial Security

1. Introduction

Credit card fraud poses a substantial assignment withinside the economic industry, ensuing in full-size economic losses every year [1]. The hassle has been exacerbated with the aid of using the exponential boom withinside the extent of transactions and the growing sophistication of fraudulent schemes [2]. Traditional fraud detection methods, which includes rule-primarily based totally structures and classical system studying algorithms, frequently warfare to maintain tempo with the evolving nature of fraud and the sheer extent of facts generated with the aid of using current economic transactions [3]. Recent improvements in deep studying have proven excellent promise in addressing those demanding situations with the aid of using imparting extra correct and green fraud detection solutions [4]. Deep studying techniques, specifically neural networks, have the cappotential to routinely analyze and extract complicated styles from huge datasets, making them well-suitable for the detection of diffused and complicated fraudulent activities [5]. However, using deep learning models for real-time fraud detection presented its own set of challenges, including the need for efficient data processing, product engineering, and handling unbalanced data sets [6]. The objective of this study is to develop a comprehensive fraud detection algorithm using deep learning to increase the accuracy and efficiency of credit card fraud detection The main objective of this study is to develop robust deep learning algorithms for detecting credit card fraud, effective to improve model performance -Specialties are combining engineering techniques, creating scalable solutions capable of real-time analysis [7]. The proposed model uses neural networks and advanced data pre-processing techniques to handle the complexity and volume of modern credit card transactions [8]. In this paper, we present the design and implementation of the proposed deep learning-based fraud detection algorithm. We also provide a comprehensive evaluation of the performance of the model using a large dataset of anonymous credit card transactions. The results show a significant improvement in the detection accuracy and a decrease in the number

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

of false positives compared to the standard methods. Our contribution highlights the potential of deep learning to transform the fraud detection process and highlights the importance of continued innovation in this important area. This paper is organized as follows: Section 2 presents important related works on credit card fraud detection. Section 3 discusses the methods used in the above thesis. Section 4 presents the results and discussion. Section 5: Comparison of the proposed system with related works. Finally, conclusions and future work.

2. Related Work

Credit card fraud poses a serious threat to the economy, causing significant financial losses each year. Several financial institutions have invested heavily in addressing this issue and established teams of experts to develop effective fraud detection systems [9]. This paper investigates an improved fraud detection method using additive machine learning algorithms and a feedback system. In particular, the random forest (RF) classifier showed excellent performance on the European credit card dataset, achieving an impressive accuracy of 94.9% without feature selection [10]. The main objective of this research is to introduce machine learning algorithms, i.e. Logistic regression (LR) and K-nearest neighbor (KNN) will be used to detect credit card fraud this framework will be applied to the European dataset after a complete preprocessing phase. Among these, the KNN algorithm showed exceptional performance, with an accuracy rate of 95%, a recall rate of 72%, and an f1-score of 82. It is important to note that the data in this study were not generated using the equilibrium the process methodology [11]. This study aims to reduce the misclassification of fraudulent transaction detection by using an under-sampling method to balance the data, followed by developing a classification model using different machine learning techniques Research findings show that the RF algorithm achieved the highest accuracy of 95.19% in European credit card embedded dataset. However under-sampling technique introduced bias towards minority population [12]. To further improve the accuracy of fraud estimation, this study presents a new framework based on short-term memory (LSTM) deep recurrent neural networks by integrating Uniform Manifold Approximation and Projection (UMAP) for feature selection and SMOTE to process dataset is proposed to increase imbalance System robustness Experimental results show that this method achieves an accuracy of 96.7% on the European credit card dataset [13]. Furthermore, this paper presents a two-stage fraud detection framework. The first module consists of a fully integrated anomaly detection model and classifier specifically designed to identify fraudulent activities. The second module, the descriptive module, is responsible for obtaining predictive interpretation. The results show an accuracy of 90.61% on the European credit card data set, although this means that the accuracy is very low [14]. Further research aims to reduce undetected deceptive activities and reduce false positive alerts by combining the resulting scores of three deep learning models: convolutional neural networks (CNN), autoencoders (AE), and recurrent neural networks (RNN).) in tests on the European credit card data set gave an accuracy rate of 94.9%, without selecting the best feature [15]. This study investigates the performance and accuracy of various machine learning techniques such as Support Vector Machine (SVM), RF, LR, and KNN. In particular, the KNN algorithm emerged as an efficient classifier with an accuracy of 95.8% in the European dataset. However, the challenge of data imbalance remains unsolved [16]. In addition, this study investigates two preprocessing methods and uses ensemble classifiers such as RF, CatBoost, and XGBoost. The findings showed that the use of random under-sampling (RUS) and conditional anti-auto-encoder (CAE) methods gave the best results in credit card fraud detection, yielding an average F1 score of 91.1 % in European dataset [17]. In addition, this study presents a framework for fraud detection using under-sampling, feature selection, and support vector data description (SVDD) to increase accuracy The results on the European credit card data set are presented that SVDD achieved an accuracy rate of 93%. However, the under-sampling method resulted in the loss of many data points, affecting overall accuracy [18].

3. Methodology

This section describes in detail the data collection, preprocessing, selection of relevant features, and classifier LSTM used to classify the data, as shown in Figure 1.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

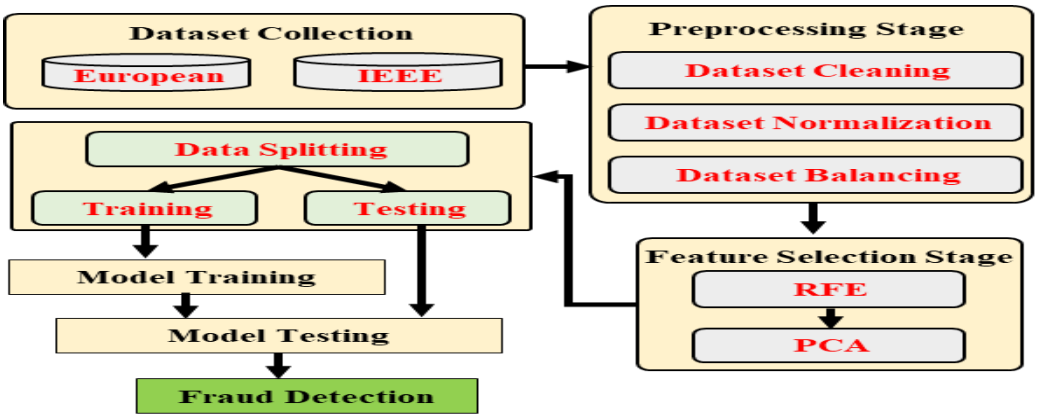

Figure 1. Diagram of the proposed system

3.1 Dataset Description

The proposed algorithm is applied on two datasets: the European credit card dataset and the IEEE dataset.

3.1.1 European credit cards dataset

The European credit card dataset obtained from www.kaggle.com provides valuable information on credit card transactions made by European cardholders over a 48-hour period in September 2013. The dataset contains 284,807 transactions, of which only 492 were identified that it is a fraud, a small part of it. The dataset contains 31 attributes, including usage time, transaction value, and more than 28 products labeled V1 to V28. The primary value label, Class, sets the attributes of each transaction, with a binary value of 1 indicating illegal transactions while 0 indicates legitimate transactions [19].

3.1.2 IEEE credit cards dataset

The IEEE dataset retrieved from www.kaggle.com contains 531,486 transactions and 269 products, initially revealed an imbalance of 18,450 fraudulent and 513,036 non-fraudulent transactions Is Fraud Feature is the binary target feature that transactions legal (0) illegal (1) classified as f.[20].

3.2 Pre-processing stage

Before applying machine learning algorithms to the data, some preprocessing is required. Model performance and data quality improve during this phase. The procedures followed in data preprocessing are clarified:

3.2.1 Dataset Cleaning

The purpose of this phase is to clean the data to fine-tune it for the classification phase of training. Data in the real world often exhibit some noise. Data correction helps in deletion process of missing values [15].

3.2.2 Dataset Normalization

Dataset normalization is an important process in data management and analysis, aimed at improving the efficiency and accuracy of data processing. Training data sets with multiple dimensions requires a large amount of computing power [21]. Normalization methods to overcome these problems. It is denoted by the following equations.

$$S = \frac{x - \mu}{\eth} \quad (1)$$

$$mean\ (\mu) = \frac{1}{N}\sum_{i=1}^{n}(\text{Xi}) \quad (2)$$

$$standard\ deviation(\eth) = \sqrt{\frac{1}{N}\sum_{i=1}^{n}(x_i - \mu)^2} \quad (3)$$

Where S represents the dataset normalization, N represents the number of changes, and x represents the number of items. normalization is a method of storing data with mean 0 and standard deviation 1. Machine learning often uses this method to normalize different features or variables to increase the performance of algorithms [22].

3.2.3 Dataset Balancing

The term data imbalance describes a situation where the amount of data from one part is more or less than the amount of data from another part now the part with more data is called the majority group, while the part with data is called few in it as few category ignore class A [23]. To overcome this problem, the Synthetic Minority Oversampling Technique (SMOTE) deals with class imbalance by increasing a few classes. SMOTE provides artificial models to balance the data set rather than relying solely on existing models of subgroups. This is done by

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

generating nearest neighbor models using the K-Nearest Neighbors (KNN) algorithm for each model in the minority class and generating synthetic instances on the line segments connecting them [24]. As shown in Algorithm 1 [25].

Algorithm 1: SMOTE

Input:
K: number of nearest neighbors
Xminor: number of minority class
Npercent: Quantity of synthetic to be produced n%
Output: Xsmote
Function SMOTE (Xminor, Npercent, K)
Xsmote = {}
For j=1 to len (Xminor) do
U=K Nearest Neighbor (Xj, Xminor, K)
C= [Npercent /100]
While C! =0 do
Xneighbor= select random (U)
Xsmote=Xj+rand (0,1) * |Xneighbor-Xj|
C=C-1
End while
End for
Rreturn Xsmote

3.3 Feature Selection Stage

Feature selection is a useful way to improve the performance of the model. Feature selection removes unnecessary and unnecessary features that do not provide any significant benefit to the model. The selection method reduces the robustness of the proposed method and the computation time [7]. We use RFE and PCA as feature selection methods on two different datasets.

3.3.1 Recursive Feature Elimination

RFE is a feature selection method that uses machine learning algorithms to select the most important features for fraud detection. RFE uses iterative feature resolution and cross-validation to identify features of the model that improve model performance [26]. RFE uses a classification machine learning algorithm to assign a score to each item and gradually remove items that do not improve classification accuracy Algorithm 2 describes the feature search method, which starts at the entire list of items and removes items that do not the increase in classification accuracy is removed. RFE). [27]. As shown in Algorithm 2 [28]. In this study, the European dataset contains 30 items, of which 25 items are selected. The IEEE dataset contains 296 features, of which 150 features are selected to improve the accuracy of the proposed algorithm.

Algorithm 2: Recursive Feature Elimination with DT

Input:
S: Training set
Z: Set of n features {f1, f2…, fn}
Ranking method DT (S, Z)
Output: R: Final Ranks
For x = 1 to n
Rank set Z using DT (S, Z)
F* ⟵ last ranked feature in Z
R (n-x+1) ⟵F*
Z ⟵Z- F*
End for

3.3.2 Principal Component Analysis

Principal component analysis (PCA) is a technique for feature extraction and dimensionality reduction in machine learning and data analysis. Principal Component Analysis (PCA) aims to convert the original components of a dataset into new variables, called principal components, which are not associated These principal components are

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

designed to capture significant differences in the data, reduce dimensionality, . and preserve most important information The covariance matrix determines its own vectors and its own values [29], as shown in equation (4). It is customary to standardize features by adjusting their mean to 0, standard deviation to 1, before applying PCA[30].

$$Cov(Yi, Yj) = \frac{1}{n-1} \sum_{k=1}^{n} (Yik - \overline{Yı}) (Yjk - \overline{Yj}) \quad (4)$$

Where: Yik represents the standard value of attribute i for k data points, is the average of attribute i over all data points, and n represents the number of samples (data points).

Eigenvectors (V) refer to the principal components, while eigenvalues(Λ) refer to the number of variations each principal component has. It is customary to rank them based on their own value. The eigenvector associated with the largest eigenvalue represents the first principal, while the subsequent eigenvalues correspond to the next principal to represent the second principal [30]. Interpolation involves mapping the original data to selected principal features and obtaining new, reduced-size data. As shown in Equation(5).

$$PCA\ Projection: W = Y\ std.Vr \quad (5)$$

Where: W is the reduced data, Y is the std standardized data, and Vr is the matrix containing the first r principal components. The above equations [30] . In this study, 20 features were selected for the European data, while 100 features were selected for the IEEE data.

3.4. The Classification Stage

The synthesis phase is an important part of data processing, with two important steps: LSTM sampling and analysis.

3.4.1 Long Short Term Memory (LSTM) Model

LSTM is an artificial recurrent neural network (RNN) commonly used to represent time series data in deep learning. Unlike traditional feedforward neural networks, LSTM incorporates feedback relationships between hidden units. This allows the model to capture long-term sequential relationships and to predict behavioral scripts based on historical behavioral sequences [31]. The LSTM is a memory cell that holds information and is modulated by three types of gates: an input gate, a forget gate, and an output gate. Three gates control the flow of information into and out of the cell [32].

You forget the table (ft) determines the information to be retained or destroyed. The tanh function is used to combine the data from the previous hidden state (h_(t-1)) with the data from the current input (Xt). The sigmoid function maps values to a range from -1 to 1. A value close to -1 indicates a tendency to forget, while a value close to 1 indicates a tendency to hold. The cell position Ct-1 controls which components will them they will be forgotten [33]. Eq. (6) shows the statistics of the forgotten gate

$$ft = tanh(Wf.[h_{t-1}, xt] + bf) \quad (6)$$

where bf and Wf represented the biases and input weights of the forget gate (ft) arrays.

The input gate (It) specifies the relevant data to be added from the current input (Xt). It updates the cell state appropriately, as shown in Eq. (7) no. These gates used a function (tanh) to cut the current input and hidden state, producing values from -1 to 1, which helped to manage the network.

Moreover, in order to create a new memory, the memory of the previous cell state (Ct-1) is subsequently used at time t-1, resulting in a new cell state (Ct) at time t [34], as described in Eq. (8,9).

$$It = tanh(Wi.[h_{t-1}, xt] + bi) \quad (7)$$

$$Nt = tanh(Wn.[h_{t-1}, xt] + bn) \quad (8)$$

$$Ct = C_{t-1} * ft + Nt * It \quad (9)$$

where bi and Wi represented the biases and input weights of the input gate (It) arrays.

The output gate (Ot) controls the data from the previous hidden state (h_(t-1)) by the sigmoid of the data from the current input (Xt). [35], as outlined in Eq.(10). The above equations [34].

$$Ot = \sigma(Wo.[h_{t-1}, xt] + bo) \quad (10)$$

Where bo and Wo represented the biases and input weights arrays of the output gate (Ot).

The LSTM Structure is constructed:

- Input Layer: LSTM Layer (units=200, return sequences=True, activation='tanh'):
- LSTM Layer (units=100, return sequences=False, activation='tanh'):
- Dropout Layer (rate=0.3): Introduces dropout with a rate of 0.3 to mitigate overfitting.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

- Dense Layer (units=50): Adds a densely connected layer with 50 units.
- Output Layer (units=1, activation='sigmoid'): Produces the final output with a single unit and utilizes the sigmoid activation function for binary categorization.
- The model is compiled using an A optimizer with a learning rate of 0.0001 and binary cross-entropy as the loss function.
- The accuracy metric is employed for monitoring model performance during training.

3.4.2 Evaluation Methodology

Various metrics are used to evaluate performance, such as accuracy, recall, accuracy, F1-score, and Area under Curve, as shown in Eqs

$$Accuracy = (TP + TN)/(TP + FP + FN + TN) \quad (11)$$

$$Precision = TP/(TP + FP) \quad (12)$$

$$\text{Sensitivity (Recall)} = \text{TP}/(\text{TP} + \text{FN}) \quad (13)$$

$$\text{F1 score} = 2 * ((\text{precision } * \text{recall})/(\text{precision} + \text{recall})) \quad (14)$$

$$\text{Specificity} = TN/(TN + FP \quad (15)$$

$$AUC = (Sensitivity + Specificity)/2 \quad (16)$$

Based on the comparison of actual and expected values in the credit card fraud detection data set. A false positive (FP) refers to a particular purchase being mistaken for fraud. A False Negative (FN) indicates a fraud that was not incorrectly classified as normal. True positives (TP) refer to cases of fraudulent transactions that are alleged to be very fraudulent. True Negative (TN) Legitimate transactions marked as fully valid [36].

4. Results and Discussion

The balanced results of the two data sets and the LSTM results will be discussed.

4.1 Balancing Results

The initially unbalanced European credit card dataset with 284,807 transactions (492 fraudulent and 284,315 normal) involves synthetic minority oversampling technique (SMOTE) After SMOTE, total transactions increased to 568,630, giving the dataset balance effectively It starts with 531,486 transactions (18,450 deceptive and 513,036 normal) in the IEEE dataset and extends to 1,026,072 balanced connections.

4.2 The Result of LSTM

The proposed algorithm is evaluated with two data sets: European and IEEE. The dataset was divided into two groups: 80% training data and 20% testing.

The proposed algorithm was first applied on the European dataset without feature selection, obtaining 92% and 90% accuracy for the IEEE dataset Table 1 shows the performance parameters of the proposed model (LSTM a feature selection).

Table 1: Results LSTM with feature selection

Dataset	Accuracy	Precision	Recall	F1-score	AUC
European	0. 9988	1.00	1.00	1.00	0.99
IEEE	0.9591	0.96	0.96	0.96	0.99

Figure 2 shows the confusion matrix of the European data with an accuracy of 99.8%. Both the correct fraud classification (TP=56533) and the correct biological interaction classification (TN=57061) are good indicators of the robustness of the proposed algorithm due to the basic processing function, materials for selection and change. The total number of misclassifications indicates (FP=129) (FN=3) that it failed to classify because some samples contain fraudulent classifications similar to natural variation that cannot be distinguished

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

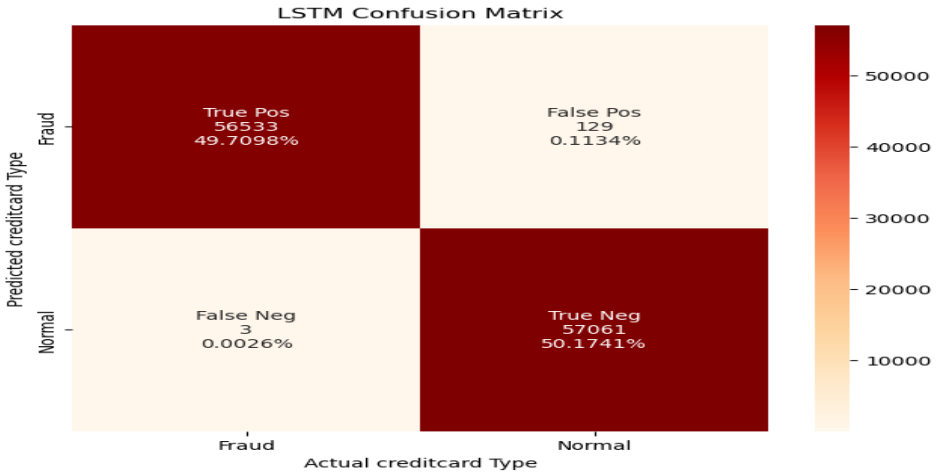

Figure 2. Confusion matrix for test data in a European credit card dataset

Figure 3 shows the confusion matrix of the IEEE data with an accuracy of 95.9%. Total number of correctly classified fraudulent behaviors (TP=99662) and correctly classified natural behaviors (TN=97173). Mean total number of misclassifications (FP=2951) (FN=5429).

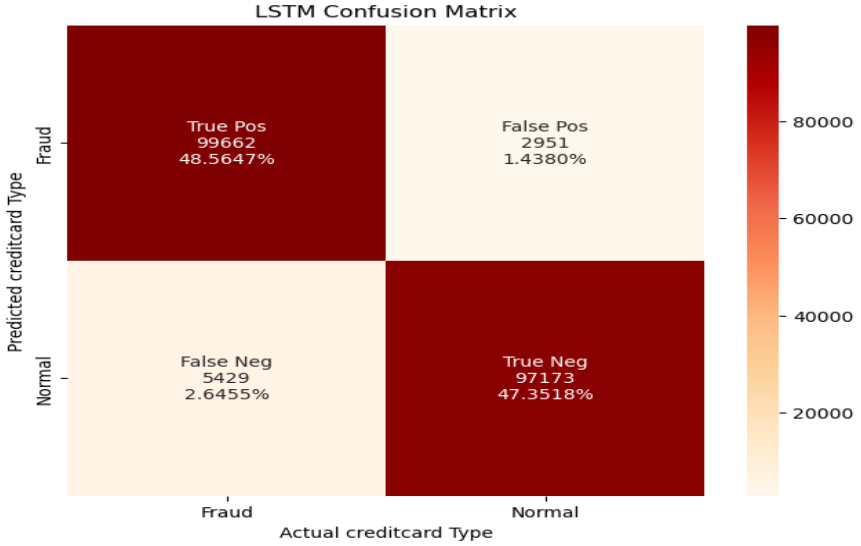

Figure 3. Confusion matrix for test data in the IEEE Credit Cards dataset

Figure 4 (a) shows that the loss function for training is 0.0049, and for testing is 0.0043 using 70 periods, indicating that the model is well trained using European credit card datasets. The loss function represents the difference between the actual yield and the expected yield. Figure 4 (b) shows that the loss function for training is 0.1150, and for testing is 0.1130 using 70 epochs, indicating that the model is well trained by the IEEE credit card dataset.

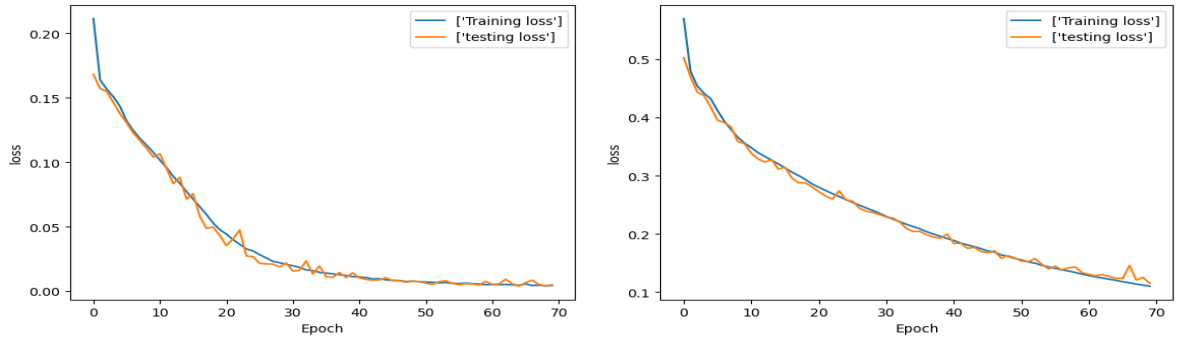

Figure 4. (a) A job loss for Europeans. (b) Loss function for IEEE

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

Figure 5 (a) shows the training and testing accuracy values of 70 occasions using European credit card datasets. The precision for training is 0.9986, while in testing it is 0.9988.

Figure 5 (b) shows the training and testing accuracy values of 70 seasons using IEEE credit card datasets. Precision for training is 0.9587, time for testing is 0.9587. 9591 square feet.

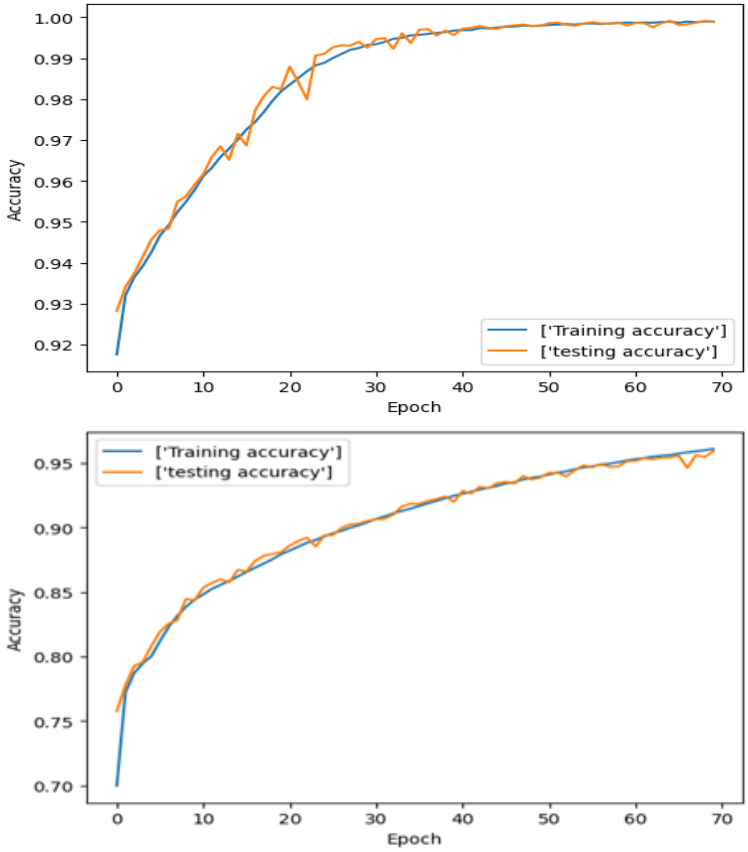

Figure 5. (a) Accuracy for the European dataset. (b) Accuracy for the IEEE dataset.

Considering that the total number of measurements (248,807) in the European data is relatively small and the number of items is 30, which is considered relatively simple, an accuracy of 0.998 was obtained compared to the IEEE data with the total number of a they are concepts. There are (531,486) interactions and the number of attributes is 269, which is considered highly complex. A precision of 0.9591 is considered acceptable in deceptive data detection because deceptive data involves normal data, and it is difficult to detect The results are good due to reduced loss in training and accuracy due to increased. The proposed model had good results on both data sets.

5. Comparison of the Proposed System with Related Works

Table 2 compares the fraud detection methods for credit cards by using machine learning and deep learning algorithms, and evaluates the effectiveness of the proposed algorithm with the same data ara in the process. The proposed system outperformed previous researchers who used the same dataset of accuracy, precision, recall, F1-score, (AUC) and other classification metrics. Then, PCA was used to select features that would reduce the number of effects and increase computational efficiency. Secondly, the structure of the LSTM system has 5 layers which are efficiently used to handle big data in credit card fraud detection using accurate data. It is perfect for capturing temporal relationships in sequential data. The Adam optimizer can handle large data.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

Table 2: Comparison with related works

Reference	Technique	Dataset	Accuracy	Precision	Recall	F1 score	AUC
[9]	RF	European	0.949%	0.959%	0.951%	0.951%	-
[10]	KNN	European		0.95%	0.72%	0.82%	-
[11]	RF	European	0.9519%	0.979%	0.922%	-	-
[12]	LSTM	European	0.967%	0.988%	0.919%	-	-
[13]	Anomaly detection model and fully connected classifier	European	0.9061%	0.921%	0.887%	0.904%	-
[14]	Ensemble (CNN, AE, RNN)	European	0.949%	0.971%	0.838%	-	-
[15]	KNN	European	0.958%	0.967%	0.744%	-	-
[16]	Ensemble Classifiers (RF, CatBoost, XGBoost)	European	0.911%	-	0.802%	-	-
[17]	Fraud Detection Framework (FFD) with Support Vector Data Description SVDD	European	0.93%	0.90%	0.97%	0.93%	-
[18]	attentional anomaly detection-based credit card fraud detection network	IEEE	-	0.941%	0.602%	0.734%	0.839%
		European	-	0.975%	0.751%	0.848%	0.943%
Proposed system	LSTM with RFE and PCA	IEEE	0.9591%	0.96%	0.96%	0.96%	0.99%
		European	0.9988%	100%	100%	100%	0.99%

Letter 18 is closest to my work. It used two datasets (IEEE, European). In the IEEE dataset, Precision, recall, f1-score, and AUC are 0.941%, 0.602%, 0.734%, and 0.839%, respectively. On the other hand, the European dataset produced Precision, recall, f1-score, and AUC values f0 974%, 0.751%, 0.848%, and 0.943%, respectively. The proposed model achieved maximum Precision of 0.96, recall of 0.96, f1-score of 0.96, and AUC of 0.99 on the IEEE dataset. In the European data set, the model achieved a precision of 100, a recall of 100, an f1-score of 100, and an AUC of 0.99. The observed improvements can be attributed to improved system operations and feature selection methods used by RFE and PCA. The proposed model has the potential to be further adapted to achieve higher accuracy when applied to large data sets with multiple features.

6. Conclusion and Future Works

The aim of this study was to increase the prediction accuracy of illegal behavior detection by integrating different machine learning algorithms. These methods include the RFE-based feature selection method, the PCA method for dimensionality reduction, the synthetic minority oversampling method (SMOTE) for dealing with imbalanced data, and the LSTM network for sampling time length of reliance so that our proposed model can identify valuable patterns in consumer behavior They enable accurate distinctions between different behaviors. To verify the findings, we ran our model on two different credit card datasets, showing that it can achieve high sensitivity in fraudulent content detection, which is very important in this case and also, us the model exhibits good performance compared to recent research. This study contributes to our understanding of applying artificial intelligence to credit card security, providing valuable insights for continuing to improve fraud detection systems. Thus, opening new opportunities for research and innovation to ensure the survival and growth of these systems in the face of future challenges If the proposed system is trained in future on multiple machine learning algorithms and with voting algorithm used, it can increase the prediction accuracy, detect whether a transaction is fraudulent or normal and that we can apply the proposed algorithm in real time because our algorithm works better and more accurate. The proposed system can be applied in the banking system.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

References

[1] H. John and S. Naaz, "Credit Card Fraud Detection using Local Outlier Factor and Isolation Forest International Journal of Computer Sciences and Engineering Open Access Credit Card Fraud Detection using Local Outlier Factor and Isolation," no. April, 2019, doi: 10.26438/ijcse/v7i4.10601064.

[2] C. Jiang, "Mitigating Cybersecurity challenges in the Financial Sector with Arti fi cial Intelligence," *Univ. Strat. Glas.*, no. 2021, pp. 1–15, 2021, [Online]. Available: https://strathprints.strath.ac.uk/75985/1/Jiang_Broby_CeFRI_2021_Mitigating_cybersecurity_challenges_in_the_financial_sector_with_Artificial_Intelligence.pdf

[3] M. Alamri and M. Ykhlef, "Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques," *Electron.*, vol. 11, no. 23, 2022, doi: 10.3390/electronics11234003.

[4] E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," *PeerJ Comput. Sci.*, vol. 9, pp. 1–66, 2023, doi: 10.7717/PEERJ-CS.1278.

[5] Vimala, S. Krishnan, V. Raj, M. Kumar, A. Janakiraman, M. "Object Detection Using Deep Learning," Journal of Journal of Cognitive Human-Computer Interaction, vol. 6, no. 1, pp. 32-38, 2023. **DOI:** https://doi.org/10.54216/JCHCI.060103

[6] D. Trisanto, N. Rismawati, M. F. Mulya, and F. I. Kurniadi, "Modified Focal Loss in Imbalanced XGBoost for Credit Card Fraud Detection," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 4, pp. 350–358, 2021, doi: 10.22266/ijies2021.0831.31.

[7] Asad, R. Hajjari, A. "Intelligent Data Processing and Mining of Histopathological Images using Improved Tunicate Swarm Algorithm with Deep Learning," Journal of International Journal of Advances in Applied Computational Intelligence, vol. 5, no. 1, pp. 40-55, 2024. **DOI:** https://doi.org/10.54216/IJAACI.050104

[8] I. Benchaji, S. Douzi, and B. El Ouahidi, "Credit card fraud detection model based on LSTM recurrent neural networks," *J. Adv. Inf. Technol.*, vol. 12, no. 2, pp. 113–118, 2021, doi: 10.12720/jait.12.2.113-118.

[9] N. K. Trivedi, S. Simaiya, and U. K. Lilhore, "An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods," no. June, 2020.

[10] K. Vengatesan, A. Kumar, S. Yuvraj, V. D. Ambeth Kumar, and S. S. Sabnis, "Credit card fraud detection using data analytic techniques," *Adv. Math. Sci. J.*, vol. 9, no. 3, pp. 1185–1196, 2020, doi: 10.37418/amsj.9.3.43.

[11] E. Amusan *et al.*, "Credit Card Fraud Detection on Skewed Data using Machine Learning Techniques," *LAUTECH J. Comput. Informatics*, vol. 2, no. 1, pp. 49–56, 2021, [Online]. Available: https://www.researchgate.net/publication/354780529

[12] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," *J. Big Data*, 2021, doi: 10.1186/s40537-021-00541-8.

[13] T. Y. Wu and Y. T. Wang, "Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection," *Proc. - 2021 Int. Conf. Technol. Appl. Artif. Intell. TAAI 2021*, pp. 25–30, 2021, doi: 10.1109/TAAI54685.2021.00014.

[14] Audumbar, A. Singh, S. K., H. Gadilkar, S. Benisemeni, Z. Shivaji, G. Imuede, J. "Investigating Recent Advances In Coded Diffraction Patterns using Deep Learning," Journal of International Journal of Wireless and Ad Hoc Communication, vol. 7, no. 1, pp. 62-71, 2023. **DOI:** https://doi.org/10.54216/IJWAC.070106

[15] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, and A. B. Rajendra, "Exploratory analysis of credit card fraud detection using machine learning techniques," vol. 3, no. April, pp. 31–37, 2022, doi: 10.1016/j.gltp.2022.04.006.

[16] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.

[17] A. Mniai, M. Tarik, and K. Jebari, "A Novel Framework for Credit Card Fraud Detection," *IEEE Access*, vol. 11, no. October, pp. 112776–112786, 2023, doi: 10.1109/ACCESS.2023.3323842.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024

[18] S. Jiang, R. Dong, J. Wang, and M. Xia, "Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network," *Systems*, vol. 11, no. 6, pp. 1–14, 2023, doi: 10.3390/systems11060305.

[19] V. N. Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," *Procedia Comput. Sci.*, vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.

[20] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, "Credit Card Fraud Detection Based on Machine and Deep Learning," *2020 11th Int. Conf. Inf. Commun. Syst. ICICS 2020*, no. May, pp. 204–208, 2020, doi: 10.1109/ICICS49469.2020.239524.

[21] S. Rao, P. Poojary, J. Somaiya, and P. Mahajan, "a Comparative Study Between Various Preprocessing Techniques for Machine Learning," *Int. J. Eng. Appl. Sci. Technol.*, vol. 5, no. 3, pp. 431–438, 2020, doi: 10.33564/ijeast.2020.v05i03.069.

[22] Z. S. Rubaidi, B. Ben Ammar, and M. Ben Aouicha, "Fraud Detection Using Large-scale Imbalance Dataset," *Int. J. Artif. Intell. Tools*, vol. 31, no. 8, 2022, doi: 10.1142/S0218213022500373.

[23] U. Ependi, A. F. Rochim, and A. Wibowo, "A Hybrid Sampling Approach for Improving the Classification of Imbalanced Data Using ROS and NCL Methods," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 3, pp. 345–361, 2023, doi: 10.22266/ijies2023.0630.28.

[24] A. O. Salau, E. D. Markus, T. A. Assegie, C. O. Omeje, and J. N. Eneh, "Influence of Class Imbalance and Resampling on Classification Accuracy of Chronic Kidney Disease Detection," *Math. Model. Eng. Probl.*, vol. 10, no. 1, pp. 48–54, 2023, doi: 10.18280/MMEP.100106.

[25] Y. Sun *et al.*, "Borderline SMOTE Algorithm and Feature Selection-Based Network Anomalies Detection Strategy," *Energies*, vol. 15, no. 13, 2022, doi: 10.3390/en15134751.

[26] M. Awad and S. Fraihat, "Recursive Feature Elimination with Cross-Validation with Decision Tree: Feature Selection Method for Machine Learning-Based Intrusion Detection Systems," *J. Sens. Actuator Networks*, vol. 12, no. 5, 2023, doi: 10.3390/jsan12050067.

[27] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," *Math. Probl. Eng.*, vol. 2020, 2020, doi: 10.1155/2020/2835023.

[28] C. V. Priscilla and D. P. Prabha, "A two-phase feature selection technique using mutual information and XGB-RFE for credit card fraud detection," *Int. J. Adv. Technol. Eng. Explor.*, vol. 8, no. 85, pp. 1656–1668, 2021, doi: 10.19101/IJATEE.2021.874615.

[29] B. Dhomse Kanchan and M. Mahale Kishor, "Study of machine learning algorithms for special disease prediction using principal of component analysis," *Proc. - Int. Conf. Glob. Trends Signal Process. Inf. Comput. Commun. ICGTSPICC 2016*, no. February, pp. 5–10, 2017, doi: 10.1109/ICGTSPICC.2016.7955260.

[30] K. Pothuganti, "Overview on Principal Component Analysis Algorithm in Machine Learning," *@International Res. J. Mod. Eng.*, no. October, 2020, [Online]. Available: www.irjmets.com

[31] I. Md. Sanzidul, S. M. Sadia Sultana, S. Abujar, and S. A. Hossain, "Sequence-to-sequence Bangla sentence generation with LSTM recurrent neural networks," *Procedia Comput. Sci.*, vol. 152, pp. 51–58, 2019, doi: 10.1016/j.procs.2019.05.026.

[32] M. H. Al-Tai and B. M. Nema, "Detecting Arabic Misinformation Using an Attention Mechanism-Based Model," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 1, pp. 285–298, 2024, doi: 10.52866/ijcsm.2024.05.01.020.

[33] Y. Murugan, M. Vijayalakshmi, L. Selvaraj, and S. Balaraman, "Credit Card Fraud Detection Using CNN," *Lect. Notes Networks Syst.*, vol. 340 LNNS, no. 1, pp. 194–204, 2022, doi: 10.1007/978-3-030-94507-7_19.

[34] A. Yara, A. Albatul, and R. M. A, "A Financial Fraud Detection Model Based on LSTM Deep Learning Technique," *J. Appl. Secur. Res.*, vol. 0, no. 0, pp. 1–19, 2020, doi: 10.1080/19361610.2020.1815491.

[35] M. Ala'raj, M. F. Abbod, and M. Majdalawieh, "Modelling customers credit card behaviour using bidirectional LSTM neural networks," *J. Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00461-7.

[36] A. Mohari, J. Dowerah, K. Das, F. Koucher, and D. J. Bora, "Credit Card Fraud Detection Techniques: A Review," no. July, pp. 157–166, 2021, doi: 10.1007/978-981-16-1048-6_12.

DOI: https://doi.org/10.54216/JCIM.140223
Received: January 28, 2024 Revised: April 05, 2024 Accepted: July 11, 2024