The Scientific Temper (2024) Vol. 15 (2): 2216-2224
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.2.34
https://scientifictemper.com/

RESEARCH ARTICLE

A combined framework based on LSTM autoencoder and XGBoost with adaptive threshold classification for credit card fraud detection

D. Padma Prabha[1*], **C. Victoria Priscilla**[2]

Abstract

The digital invasion of the banking and financial sectors made life simple and easy. Traditional machine learning models have been studied in credit card fraud detection, but these models are often difficult to find effective for unseen patterns. This study proposes a combined framework of deep learning and machine learning models. The long short term memory autoencoder (LSTMAE) with attention mechanism is developed to extract high-level features and avoid overfitting of the model. The extracted features serve as input to the powerful ensemble model XGBoost to classify legitimate and fraudulent transactions. As the focus of fraud detection is to increase the recall rate, an adaptive threshold technique is proposed to estimate an optimal threshold value to enhance performance. The experiment was done with the IEEE-CIS fraud detection dataset available in Kaggle. The proposed model with optimal threshold has an increase in predicting fraudulent transactions. The research findings are compared with conventional ensemble techniques to find the generalization of the model. The proposed LSTMAE-XGB w/ attention method attained a good precision and recall of 94.2 and 90.5%, respectively, at the optimal threshold of θ = 0.22. The experimental results proved that the proposed approach is better at finding fraudulent transactions than other cutting-edge models.

Keywords: Credit card fraud detection, LSTM, Autoencoder, XGBoost, Threshold, Classification.

Introduction

Credit card is a widely used payment method for online and offline transactions. However, the mass evolution of credit cards paved the way for different fraudulent actions. Fraudsters use multiple approaches to do an illegal transaction. They try to mimic the behavior of legitimate users to create fake cards. Today, researchers have to strive hard to develop an efficient fraud detection system. Machine learning and deep learning methods are used to design a sophisticated credit card fraud detection (CCFD) system to sustain cardholders and banks, preventing them from phishing threats (Cherif *et al*., 2023). During the process of building an intelligent system, there are many challenges to be addressed, like imbalances in data, concept drift, lack of real-time data, etc.

Among the above challenges, the most important is the class imbalance present in the dataset. This encourages the research community to find the best solution to overcome this problem (Benchaji *et al*., 2021). The effective way to tackle the imbalance problem to predict accurate fraud patterns is quite a critical problem to be addressed (Jiang *et al*., 2023). In a binary classification, the positive class is much less than the negative class. This kind of data appears in various fields, like churn prediction, medical diagnosis, image recognition, and fraud detection. In credit card fraud detection, legitimate transactions are more than fraudulent transactions, which creates a bias in the model by inclining toward the prediction of the majority class while ignoring the positive class (Ding *et al*., 2023). Figure 1 shows the process of online transactions using stolen credit cards. Despite numerous studies aimed at providing an efficient

[1]Department of Computer Applications, Madras Christian College, Affiliated to University of Madras, Chennai, India.

[2]PG Department of Computer Science, Shrimathi Devkunvar Nanalal Bhatt Vaishnav College for Women, Affiliated to University of Madras, Chennai, India.

***Corresponding Author:** D. Padma Prabha, Department of Computer Applications, Madras Christian College, Affiliated to University of Madras, Chennai, India., E-Mail: padmaprabha@mcc.edu.in

How to cite this article: Prabha, D. P., Priscilla, C. V. (2024). A combined framework based on LSTM autoencoder and XGBoost with adaptive threshold classification for credit card fraud detection. The Scientific Temper, **15**(2):2216-2224.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.2.34

Source of support: Nil

Conflict of interest: None.

Received: 13/04/2024 **Accepted:** 14/05/2024 **Published** : 15/06/2024

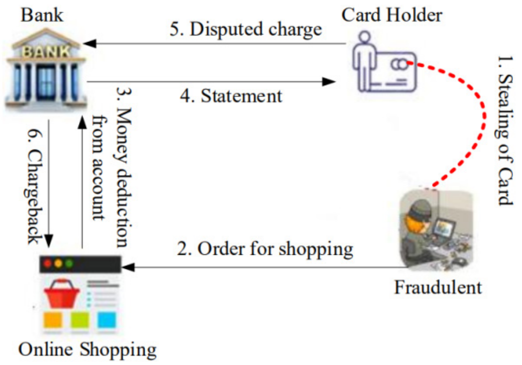

Figure 1: Credit card fraud transaction process during online purchase (Razaque *et al.*, 2023)

solution, fraudsters continue to find more sophisticated ways to engage in cyber theft. Deep learning architectures such as recurrent neural networks (RNN), autoencoders (AE), convolutional neural networks (CNN), and long short term memory (LSTM) have emerged in the latest studies (Tayeh *et al.*, 2022). To elucidate the aforementioned challenges, deep learning models can solve the issue of imbalanced datasets.

This study was motivated by our prior work (Prabha & Priscilla, 2023), where a normal deep autoencoder was used as a dimensionality reduction method to extract the reduced feature subset present in the latent space. The obtained features are the input for the XGBoost model to detect fraudulent transactions. Since the dataset is highly imbalanced, we have to monitor the chance of overfitting. Hence, we set dropout and early stopping parameters to train the autoencoder. As it is a binary classification problem, therefore, a threshold technique with a maximized F1 score is introduced to handle the imbalance during the classification. In this study, two powerful machine learning (ML) and deep learning (DL) techniques are combined to build an enhanced framework of CCFD. The classification of the positive and negative classes is based on the selection of the optimal threshold. The essential contributions of our proposed fraud detection framework are:

- To extract potential features in the form of lower dimensions from the latent space of credit card dataset, the conventional neurons present in the autoencoder are replaced with LSTM.
- Constructing an attention mechanism for the LSTM network is to inform the network where to give exact attention for the input sequence.
- The XGBoost model receives the reduced features from the latent representation to classify fraudulent and normal transactions.
- We introduce the probabilistic threshold method with a maximized f1 score to increase the detection rate of fraudulent transactions (Recall).

Following this introduction, the related works section will outline previous research with LSTM autoencoders across many domains. The methodology section elucidates our proposed approach by creating an integrated framework of machine learning and deep learning approaches. The experimental study section outlines the experimental evaluation using performance measures, explains the results, and compares them with other methods employed in credit card fraud detection. Finally, the paper concludes and proposes ideas for future research directions.

Related Works

Credit card fraud is a prevalent global issue, resulting in financial losses growing every year. Traditional machine learning models frequently combat this problem by detecting credit card fraud. Researchers frequently used state-of-the-art machine learning models like random forest, support vector machine, and Bayesian models to solve the problem of credit card fraud detection. De Sá *et al.* (de Sá *et al.*, 2018) designed a fraud-BNC algorithm using a customized Bayesian network classifier for credit card fraud detection. Considering the economic inferences of misclassifications, they addressed the challenge of classifying legitimate or fraudulent transactions. Seeja and Zareapoor (Seeja & Zareapoor, 2014) emphasized the intricate nature of accurately identifying fraudulent transactions when they overlap. They proposed a model named Fraud Miner to efficiently identify fraudulent transactions. Ahmad and Kasasbeh (Ahmad & Kasasbeh, 2022) introduced a unique technique for detecting fraud across various stages, utilizing fuzzy C-means clustering algorithms. They also identified the normal usage pattern of credit card users based on their past transactions. The readers are referred to the review paper (C. V. Priscilla & Prabha, 2020) for a detailed description of the methods used by several researchers in the field of credit card fraud detection, like supervised, unsupervised, and ensemble learning.

Recently, new researchers in the field of CCFD have suggested deep learning techniques that can effectively detect fraudulent transactions, similar to machine learning methods (Alyami & Meraj, 2022); (Kang *et al.*, 2021). Deep learning techniques are applied in several fields, such as object recognition, classification, and predictions for large datasets (Park *et al.*, 2022). Recent studies have introduced architectures like recurrent neural networks, autoencoders, convolutional neural networks, and long short-term memory networks (Tayeh *et al.*, 2022) in different domains. Autoencoders have become popular for generating new feature representations with reduced dimensions compared to other supervised methods (Fanai & Abbasimehr, 2023). (Bampoula *et al.*, 2021) developed an autoencoder model utilizing LSTM for analyzing machinery data in order to forecast the equipment's longevity. Alghofaili *et al.* (Alghofaili *et al.*, 2020) utilized the LSTM model for CCFD and found that it outperformed other machine learning and deep learning models, demonstrating superior performance. Li *et al.*

(Li *et al*., 2021) developed an innovative hybrid model to address class imbalance and overlap by employing the divide-and-conquer technique. They isolated the overlapped subset of data using an evaluation criteria known as dynamic weighted entropy on a real-time credit card dataset. Dasan and Panneerselvam (Dasan & Panneerselvam, 2021) proposed a novel concept by integrating convolutional denoising autoencoder and LSTM. An LSTM network was constructed following the encoder section to decrease computation time. Mushtaq *et al*. (Mushtaq *et al*., 2022) introduced a hybrid architecture that combines a deep LSTM autoencoder with bidirectional LSTM for classifying anomalies in intrusion detection. Zhao *et al*. (Zhao *et al*., 2022) presented a dual attention network architecture that combines LSTM and VAE for analyzing time series data. They determined the anomaly score using an adaptive threshold approach to establish a precise threshold value. Ghrib *et al*. (2020) designed an anomaly detection approach that utilizes an LSTM autoencoder trained on normal data and integrated with an SVM classifier. They proposed that encoding data diminishes the correlations between anomaly and normal data by consistently segregating the two categories. Fanai and Abbasimehr (2023) developed an innovative system that utilizes a deep autoencoder for dimensionality reduction to create a fresh dataset with fewer features. Advanced classifiers such as ANN, RNN, and a combination of RNN and CNN are employed to identify fraudulent transactions. Oluwasanmi *et al*. (Oluwasanmi *et al*., 2022) developed a model that incorporated an attention mechanism into the latent space representation to capture the activations of encoded features. They developed a variational autoencoder and LSTM specifically for analyzing time series data.

By combining supervised and unsupervised techniques, researchers developed a hybrid approach to enhance the accuracy of fraud detection systems (Giannini *et al*., 2020). Alarfaj *et al*. (2022) conducted a comparison between the algorithms of machine learning (ML) and DL to determine the efficiency of each learning method. After the analysis, they concluded that the efficiency of the model depends on the nature of the input. Recent works in the field of CCFD with an ensemble framework show tremendous performance when compared with individual models (Forough & Momtazi, 2020). Since the dataset is highly imbalanced, fixing the threshold during the classification process plays a vital role instead of keeping the default threshold during the classification process. To distinguish between valid and fraudulent transactions, Lin and Jiang (Lin & Jiang, 2021) introduced a bootstrap aggregation model with deterministic threshold classification. In our previous work (Prabha & Priscilla, 2024), we proposed a threshold technique based on F1-score and G-mean to estimate the optimal threshold for the classification of fraudulent and legitimate transactions. In this study, we formulate a new framework with two powerful combinations of DL and ML methods to enhance the performance of fraud detection systems. The framework specifically addresses the issue of data imbalance in the model, which may have a negative impact on its effectiveness.

Methodology

Deep learning algorithms have attracted researcher's interest in recent years for their high performance and promising results across numerous artificial intelligence applications (Forough & Momtazi, 2020). However, the works on deep neural networks for investigating the occurrence of fraud transactions in credit card fraud detection need more attention. We proposed a new hybrid model using an LSTM autoencoder with an attention mechanism to learn and extract the most significant features from the training dataset by forcing the latent space to have lower dimensional features than the original features. The latent features are subsequently entered into the ensemble-supervised model XGBoost, which uses the threshold approach to classify legitimate and fraudulent transactions. The following section provides a detailed introduction to the proposed framework for detecting credit card fraud.

Long Short-Term Memory

LSTM is similar to RNN, where the recurrent nodes are replaced with memory cells. The LSTM introduces a storage type called a memory cell. Each memory cell is a composite unit of three different gates equipped with input $\mathrm{I_t}$, forget $\mathrm{F_t}$ and output $\mathrm{O_t}$ neural network. The values of three gates are computed using the sigmoid activation function σ, which ranges between 0 and 1. Gates interact within the memory units during training to identify significant data to retain or forget (Alhnaity *et al*., 2021). Figure 2 represents the architecture of the LSTM network. An input gate's input signal monitors the state of the memory cell undergoing change. The forget gate determines whether to discard or preserve the previous signal it received from the input gate. The output gate controls the memory cell that receives the input signal (Benchaji *et al*., 2021). The gates in the LSTM network can learn sequential data as the gates control the flow of information (Razaque *et al*., 2023). Given the input $\mathrm{x_t}$, the previous hidden state $\mathrm{h_{t-1}}$, previous cell memory

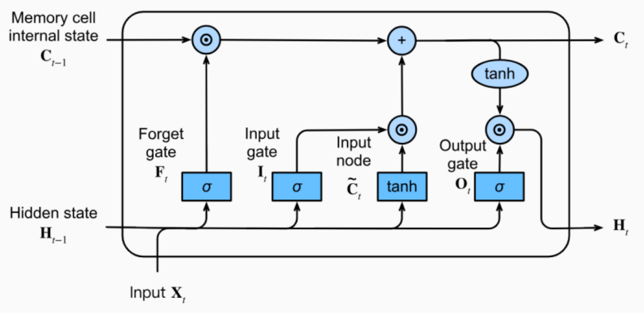
Memory cell internal state $\mathbf{C}_{t-1}$
⊙
+
$\mathbf{C}_t$
tanh
⊙
⊙
Forget gate $\mathbf{F}_t$
Input gate $\mathbf{I}_t$
Input node $\tilde{\mathbf{C}}_t$
Output gate $\mathbf{O}_t$
σ
σ
tanh
σ
Hidden state $\mathbf{H}_{t-1}$
$\mathbf{H}_t$
Input $\mathbf{X}_t$

Figure 2: The architecture of LSTM unit

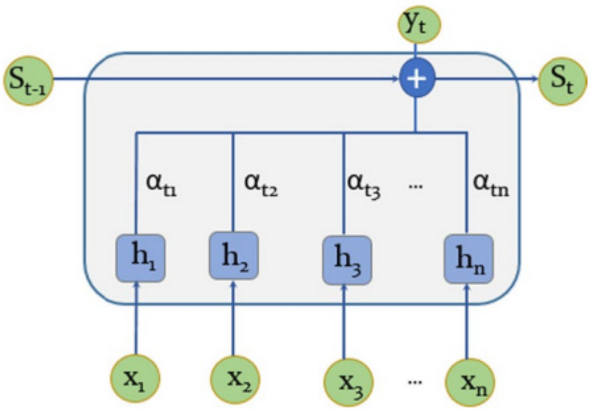

Figure 3: Attention mechanism (Benchaji *et al*., 2021)

$c_{t-1}$and the hidden state of the current LSTM h_t for time step t, then

$$I_t = \sigma\left(x_t w_{xi} + h_{t-1} w_{hi} + b_i\right) \quad (1)$$

$$F_t = \sigma\left(x_t w_{xf} + h_{t-1} w_{hf} + b_f\right) \quad (2)$$

$$O_t = \sigma\left(x_t w_{xo} + h_{t-1} w_{ho} + b_o\right) \quad (3)$$

where w and b are weight and bias parameters respectively.

Attention mechanism

To improve the performance of the LSTM autoencoder, Abu *et al*. (Abu *et al*., 2015) proposed an attention mechanism to address the performance of the bottleneck layer of traditional encoder and decoder architectures. The attention mechanism is similar to human attention intelligence (Kong *et al*., 2021). The attention mechanism in Figure 3 selects the most important data from the input sequences using weights. The implementation of the attention mechanism involves constructing the most relevant data using a context vector, which then serves as an input to the next layer. The attention layer focuses on the most significant data points automatically to improve the efficiency of classification based on a weighted average of the information present. The attention mechanism builds a context vector with the most important data from the weighted average of a set of vectors that becomes the input for the succeeding layers.

eXtreme Gradient Boosting (XGBoost)

The sparsity-aware algorithm, a tree-boosted ensemble model, was developed by Chen and Guestrin (Chen & Guestrin, 2016) to handle sparse data. The XGBoost algorithm is efficient due to its parallel processing technique and the ability to tackle missing data by itself when compared with the gradient boosting machine (GBM). Trisanto (Trisanto, 2021) developed a modified focal loss method to address imbalanced datasets by utilizing weighted binary cross-entropy, eliminating the need for pre-processing techniques like sampling and outlier detection. The nodes of the tree split until they reach the maximum depth, and the pruning is used to remove the splits that result in a negative loss. The XGBoost model is built using the additive tree boosting technique, which includes the derivatives gradient g_i and hessian h_i. To tackle class imbalance, these derivatives generate the boosting tree independently (Wang *et al*., 2020).

Algorithm 1: To find the best threshold

```
Step 1 : Train the XGBoost model with the training dataset.
Step 2 : Find the prediction score of each test data for threshold between 0 to 1
Step 3 : Store the maximum prediction score attained
Step 4 : Initialize the best f1-score and best threshold value as 0
Step 5 : Repeat for each current threshold $\in$ maximum prediction score
            Current f1-score = f1-score at current threshold
            if Current f1-score > best f1-score
                best f1-score = Current f1-score
                best threshold = current threshold
Step 6 : Return best threshold
```

Estimating Optimal Threshold

We determined the ideal threshold by analyzing the F1-score and G-mean metrics in our prior research. Threshold shifting (Collell *et al*., 2018) alters the decision threshold of the classifiers according to the class priors. Adjusting the decision threshold in a dataset with imbalanced binary classification can enhance efficiency by taking into account the problem's characteristics. Adjusting the threshold away from the default value can improve the performance of severely unbalanced datasets. Modifying the threshold can lead to improved outcomes depending on the issue. The following algorithm provides a better understanding of finding the best threshold using the metric F1-score.

In the Algorithm 1, the maximized F1-score is identified by comparing the current threshold with the best threshold for each iteration.

Proposed LSTMAE-XGB Framework

Autoencoder is a class of deep learning that solves the problem of dimensionality reduction for CCFD (Zhao *et al*., 2022). Studies reveal that LSTM autoencoders have the ability to deal with time series data as input for prediction when compared with regular autoencoders. To extract the significant features in order to reduce the dimensionality, the LSTM autoencoder framework is designed by adding an attention layer. This layer is embedded with the encoder of the framework to generate a latent space representation of input data with a reduced feature set. Figure 4 displays the proposed framework of long short-term memory autoencoder with XGBoost (LSTMAE-XGB). This CCFD framework at first pre-processes the data using a label encoder to convert the categorical data to numeric data, and the min-max scalar is used to scale the data range

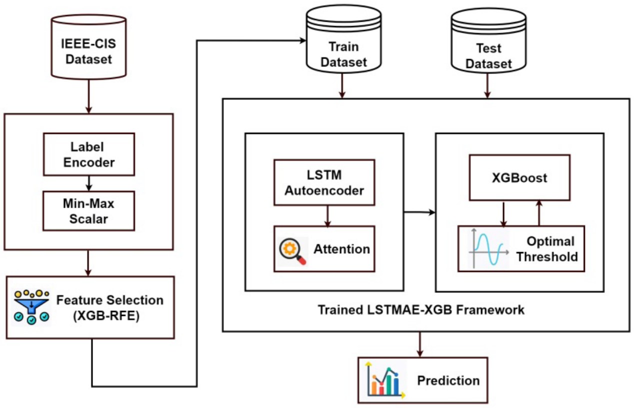

Figure 4: Schematic diagram of the enhanced credit card fraud detection framework based on the LSTM autoencoder and the XGBoost with attention mechanism

Algorithm 2: LSTMAE-XGB/w attention

```
Step 1:  Start
Step 2:  Train the LSTMAE network layers with the training dataset.
Step 3:  Add the attention layer at the encoder part of the LSTMAE
Step 4:  Train the XGBoost with the extracted low-dimensional
features from latent representation.
Step 5: Identify the best threshold using Algorithm 1.
Step 6:  Apply the test dataset to the trained LSTMAE
Step 7:  Repeat for each feature of LSTMAE
             Obtain prediction score of XGBoost for each test data
             if the prediction score > best threshold, then
                  Alert Fraudulent
             else
                  Allow transaction
Step 8 :  End
```

from 0 to 1. Since the features of the dataset are very high, which leads to poor performance of the model, MI-XGB (Priscilla & Prabha, 2021) is a two-phase feature selection technique used to identify the most important features. The proposed model is designed with two powerful methods: the LSTM autoencoder and XGBoost. We employ an LSTM autoencoder to reduce the data dimensionality and extract features from the latent space representation, thereby overcoming the curse of dimensionality. In addition, to make the model learn better, an attention mechanism is embedded in the encoder layers.

The model effectively learns the abstract features during the training process. We utilize these feature codes to train the XGBoost model, which subsequently categorizes the data as either genuine or fraudulent according to a predefined classification threshold. Finally, the trained LSTMAE and XGBoost models, along with the estimated threshold, can be applied to each test data to predict whether it is fraudulent or legitimate. Fine-tuning the threshold θ can provide tailored classification results, depending on the problem. The algorithm of the proposed LSTMAE-XGB with attention mechanism is given in Algorithm 2:

Experimental Study

To experiment the proposed methodologies, this study has used the IEEE-CIS credit card dataset from Kaggle ("IEEE-CIS Fraud Detection | Kaggle). This section details the dataset specification and the evaluation metrics performed.

Dataset

The real-world credit card fraud detection dataset from Kaggle is an imbalanced dataset that consists of identity and transaction files with 41 and 394 features, respectively. The TransactionID column links these two files together. Hence, we obtain a total transaction of 590, 540 and 433 features. We remove the unimportant features because they negatively impact the model's performance. There is a huge difference in the size of the positive and negative classes, accounting for only 3.5% of fraudulent transactions. Therefore, to mitigate the problem of data imbalance, an advanced learning method can be effectively utilized. Moving from traditional supervised learning models, this paper designs an ingenious framework to circumvent the impact of imbalanced data in credit card fraud detection.

Evaluation Metrics

To validate the performance of the developed hybrid framework, the metrics for evaluating the performance of classifiers are derived from the conventional confusion matrix shown in Table 1. The possible outcomes of classification are true positive (TP), false positive (FP), true negative (TN) and false negative (FN).

TP is the number of positive transactions that are truly positive. TN is the number of transactions that are predicted properly as negative. FP is the number of transactions that are labeled as positive but actually negative. FN is the number of transactions predicted as negative but actually positive. Precision, recall, and f1_Score are commonly used measures for imbalanced classification.

$$\text{Precision} = \frac{\text{TP}}{\text{TP + FP}} \tag{4}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP + FN}} \tag{5}$$

$$\text{F1} - \text{score} = 2 \text{ x } \frac{\text{Precision x Recall}}{\text{Precision+ Recall}} \tag{6}$$

The area under the precision-recall curve (AUC-PR) is a metric used to measure the performance of classifiers on imbalanced datasets. Other statistical metrics are supportively used to identify the classification performance.

$$\text{MCC} = \frac{\text{TP X TN} - \text{FP X FN}}{\sqrt{(\text{TP+FP})(\text{TP+FN})(\text{TN+FP})(\text{TN+FN})}} \tag{7}$$

Table 1: Confusion matrix

Actual	*Predicted*	
	Fraudulent	*Legitimate*
Fraudulent	TP	FN
Legitimate	FP	TN

$$G - \text{mean} = \sqrt{\text{TPR X TNR}} \quad (8)$$

$$\text{Balanced Accuracy} = \frac{1}{2}\,(\text{TPR} + \text{TNR}) \quad (9)$$

Experimental Results and Discussion

Deep learning has gained popularity in recent years due to its ability to automatically extract useful features from the original data, resulting in the composition of high-level features from low-level features. This study aims to enhance the recall rate for detecting fraudulent activities, particularly in areas such as credit card fraud detection. Therefore, we developed the LSTMAE-XGB with an attention model, which reduces the feature dimension and performs classification using the probabilistic threshold method. We split the dataset into training and testing sets. The autoencoder network was built with an LSTM network and an attention layer with a dropout and repeat vector. We built the model with the parameters of learning rate, batch size, epoch, and early stopping to prevent overfitting. The loss function, binary cross-entropy, and Adam optimizer are all defined to minimize the loss. The feature representations obtained in the bottleneck layer are fed to the classifier XGBoost, and the classification of legitimate and fraudulent is done with the optimal threshold estimated by maximizing the f1-score. In Table 2, the performance of the proposed LSTMAE-XGB w/ Attention for default and optimal thresholds is compared with other models.

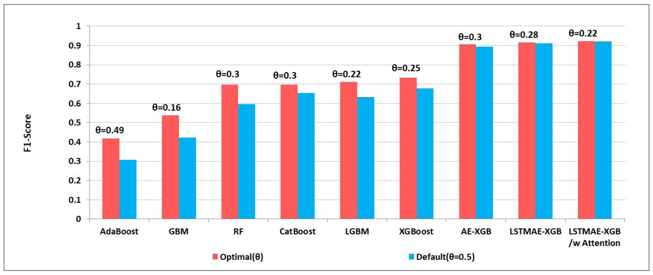

Figure 5: Comparison of F1-scores between suggested AE-XGB and LSTMAE-XGB models w/ attention mechanism and other boosting models using both default (θ = 0.5) and optimal thresholds. XGBoost with attention mechanism

Figure 5 displays a comparison of the performance of the proposed LSTMAE-XGB with attention against other ensemble algorithms based on F1-score using optimal and default thresholds.

The confusion matrix illustrates the classification performance of distinguishing between legitimate and fraudulent transactions for the proposed LSTMAE-XGB model with an attention mechanism, as shown in Figure 6 (a&b). The classification performance is shown both before and after implementing the adaptive threshold. Upon examining the confusion matrix, there was a 1.12% rise in correctly identifying true positive class (Fraudulent) after adjusting the threshold from 0.5 to 0.22. This demonstrates that the approach may effectively decrease the number

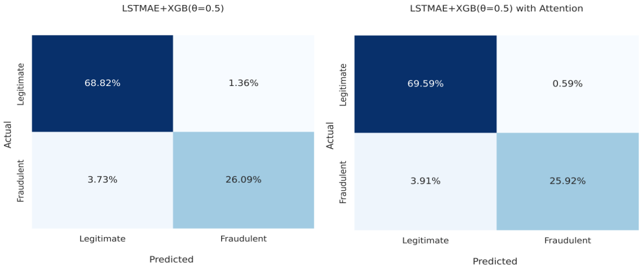

Figure 6(a): Confusion matrix for LSTMAE-XGB and LSTMAE-XGB /w attention mechanism for the default threshold value of 0.5

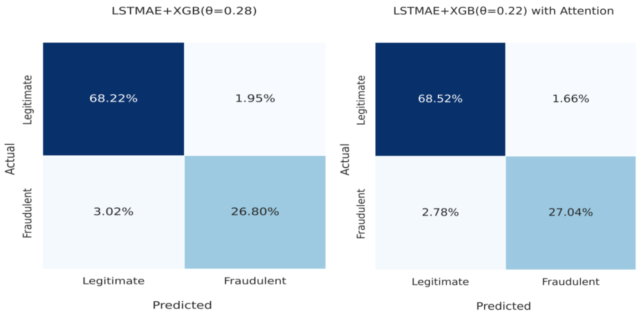

Figure 6(b): Confusion matrix for the LSTMAE-XGB and LSTMAE-XGB /w attention mechanism for the adaptive threshold values of 0.28 and 0.22, respectively.

Table 2: Performance outcome of proposed AE-XGB and LSTMAE-XGB w/Attention for default and optimal thresholds on IEEE-CIS fraud detection dataset

Model	*Default threshold (θ = 0.5)*				*Optimal threshold*			
	XGB	*AE-XGB*	*LSTMAE-XGB*	*LSTMAE-XGB w/ Attention*	*XGB (θ = 0.24)*	*AE-XGB (θ = 0.3)*	*LSTMAE-XGB (θ = 0.28)*	*LSTMAE-XGB w/ Attention (θ = 0.22)*
Precision	0.971	0.961	0.950	0.978	0.883	0.907	0.934	0.942
Recall	0.522	0.835	0.875	0.869	0.626	0.905	0.899	0.905
F1_Score	0.679	0.894	0.911	0.920	0.733	0.906	0.916	0.923
G-mean	0.722	0.907	0.926	0.928	0.790	0.932	0.935	0.940
Cohen (K)	0.672	0.853	0.876	0.976	0.672	0.866	0.881	0.941
MCC	0.707	0.857	0.877	0.889	0.707	0.866	0.882	0.891
Bal-Accu	0.761	0.926	0.928	0.930	0.812	0.933	0.936	0.941

Table 3: Performance comparison of LSTMAE-XGB and other research work conducted using IEEE-CIS dataset

Research	*Methods*	*Precision*	*Recall*	*F1-score*
(Malik *et al.* 2022)	AdaBoost+XGB	0.94	0.59	0.73
(Siddharth, 2021)	Deep-Q NR	0.48	0.35	0.41
(Ruangsakorn & Yu, 2021)	XGBoost	0.95	0.57	0.72
(Jiang *et al.* 2023)	UAAD-FDNet w/FA	0.93	0.63	0.73
This research	LSTMAE+XGB w/o Attention (θ = 0.28)	0.93	0.90	0.92
This research	LSTMAE+XGB w/ Attention (θ = 0.22)	0.94	0.91	0.92

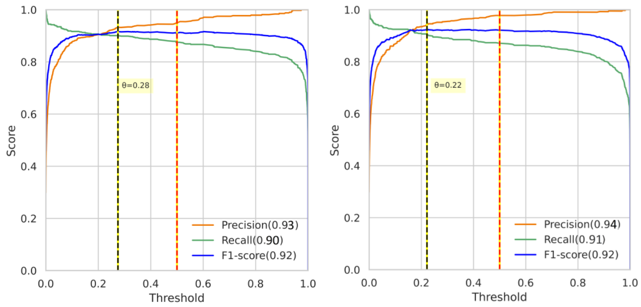

Figure 7: Precision, recall, and F1-score curve for the optimal threshold values for the proposed LSTMAE-XGB w/o attention (θ = 0.28) and LSTMAE-XGB w/ attention (θ = 0.22)

of fraudulent transactions labeled as legitimate while identifying the critical few fraudulent transactions that are significant for financial service providers.

The precision, recall, and f1-score plots for both proposed models applied to the same dataset are presented in Figure 7, from which we observe that our model LSTMAE-XGB, achieved a high precision and recall rate with an optimal threshold value of 0.22. This significant increase is due to the attention layer embedded with the LSTM autoencoder, which extracts the more relevant patterns from sequence transactions. Here, the F1-score is the harmonic mean between precision and recall.

Financial organizations are focusing on detecting fraud to save customers from financial damages. The measure of recall (sensitivity) is highly important in the field of fraud detection. Our suggested model outperforms existing ensemble models based on the experimental findings, as shown in Figure 5. The LSTMAE-XGB model with attention mechanism and optimal threshold estimation shows improved performance in detecting fraudulent credit card transactions. Table 3 presents a comparison of the performance achieved by the proposed study with existing research studies using the IEEE-CIS fraud detection dataset. Our objective was to enhance the recall rate for identifying fraudulent transactions. Through our investigation, we successfully increased the recall rate by 91% using a threshold-shifting approach.

Conclusion

In this study, we proposed combining the deep learning model LSTMAE-XGB with an attention mechanism to extract high-level features from a latent representation. These features are loaded into XGBoost, a machine-learning ensemble model that classifies legitimate and fraudulent transactions. Because the problem is most critical for capturing fraudsters and protecting the customers of financial institutions. Hence, the increase in recall is efficiently managed by calculating the appropriate threshold using the maximal F1-score. The proposed architecture outperforms conventional ensemble models such as AdaBoost, GBM, RF, CatBoost, LGBM, and our AE-XGB in terms of generalization. The experiment is carried out using the IEEE-CIS credit card fraud detection dataset available on Kaggle. The proposed strategy efficiently prevents the problem of class imbalance while also increasing fraud detection rates (recall).

Future work could involve using a more skewed dataset to determine the reliability of the suggested model. Classification can be performed solely using deep learning, with CNN and MLP replacing XGBoost.

References

Abu, O., Mohammed, A., Momani, A. S., & Hayat, T. (2015). Numerical solutions of fuzzy differential equations using reproducing kernel Hilbert space method. *Soft Computing*, *20*, 3283–3302. https://doi.org/https://doi.org/10.1007/s00500-015-1707-4

Ahmad, H., & Kasasbeh, B. (2022). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology*, *15*, 325–333. https://doi.org/10.1007/s41870-022-00987-w

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access*, *10*(April), 39700–39715. https://doi.org/https://doi.org/10.1109/ACCESS.2022.3166891

Alex Gedeon, Park, E., Jang, J., & Yoo, Y. (2022). Attention-Based Distributed Deep Learning Model for Air Quality Forecasting. *Sustainability*, *14*(6), 119562. https://doi.org/https:// doi.org/10.3390/su14063269 Academic

Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A Financial Fraud Detection Model Based on LSTM Deep Learning Technique A Financial Fraud Detection Model Based on LSTM. *Journal* *of Applied Security Research*, *15*(4), 1–19. https://doi.org/10.1080/19361610.2020.1815491

Alhnaity, B., Kollias, S., Leontidis, G., Jiang, S., Schamp, B., & Pearson, S. (2021). An autoencoder wavelet based deep neural network with attention mechanism for multi-step prediction of plant growth. *Information Sciences*, *560*, 35–50. https://doi.org/https://doi.org/10.1016/j.ins.2021.01.037

Alyami, H., & Meraj, T. (2022). A Novel text2IMG Mechanism of Credit Card Fraud Detection : A Deep Learning Approach. *Electronics*, *11*(5), 1–18. https://doi.org/https://doi.org/10.3390/electronics11050756

Bampoula Xanthi, Siaterlis, G., & Nikolakis, N. (2021). A Deep Learning Model for Predictive Maintenance in Cyber-Physical Production Systems Using LSTM Autoencoders. *Sensors*, *3*, 972. https://doi.org/https://doi.org/10.3390/s21030972

Benchaji, I., Douzi, S., Ouahidi, B. El, & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*(151), 1–21. https://doi.org/10.1186/s40537-021-00541-8

Chen, T., & Guestrin, C. (2016). Xgboost: A scalable tree boosting system. *Proceedings of the 22nd Acm Sigkdd International Conference on Knowledge Discovery and Data Mining*, 785–794. https://doi.org/https://doi.org/10.1145/2939672.2939785

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies : A systematic review. *Journal of King Saud University - Computer and Information Sciences*, *35*(1), 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008

Collell, G., Prelec, D., & Patil, K. R. (2018). A simple plug-in bagging ensemble based on threshold-moving for classifying binary and multiclass imbalanced data. *Neurocomputing*, *275*, 330–340. https://doi.org/https://doi.org/10.1016/j.neucom.2017.08.035

Dasan, E., & Panneerselvam, I. (2021). Biomedical Signal Processing and Control A novel dimensionality reduction approach for ECG signal via convolutional denoising autoencoder with LSTM. *Biomedical Signal Processing and Control*, *63*(May 2020), 102225. https://doi.org/10.1016/j.bspc.2020.102225

de Sá, A. G. C., Pereira, A. C. M., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. *Engineering Applications of Artificial Intelligence*, *72*(October 2017), 21–29. https://doi.org/10.1016/j.engappai.2018.03.011

Ding, Y., Kang, W. E. I., Feng, J., Peng, B. O., & Yang, A. (2023). Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network. *IEEE Access*, *11*(July), 83680–83691. https://doi.org/10.1109/ACCESS.2023.3302339

Fanai, H., & Abbasimehr, H. (2023). A novel combined approach based on deep autoencoder and deep classifiers for credit card fraud detection. *Expert Systems With Applications*, *217*, 119562. https://doi.org/10.1016/j.eswa.2023.119562

Forough, J., & Momtazi, S. (2020). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing Journal*, *99*, 106883. https://doi.org/https://doi.org/10.1016/j.asoc.2020.106883

Ghrib, Z., Jaziri, R., & Romdhane, R. (2020). Hybrid approach for Anomaly Detection in Time Series Data. *International Joint Conference on Neural Networks (IJCNN)*, 1–7. https://doi.org/https://doi.org/10.1109/IJCNN48605.2020.9207013

Gianini, G., Ghemmogne, L., Mio, C., Caelen, O., Brunie, L., & Damiani, E. (2020). Managing a pool of rules for credit card fraud detection by a Game Theory based approach. *Future Generation Computer Systems*, *102*, 549–561. https://doi.org/10.1016/j.future.2019.08.028

IEEE-CIS Fraud Detection | Kaggle, https://www.kaggle.com/c/ieee-fraud-detection/data

Jiang, S., Dong, R., Wang, J., & Xia, M. (2023). Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network. *Systems*, *11*(6), 1–14. https://doi.org/https://doi.org/ 10.3390/systems11060305

Kang, J., Kim, C., Kang, J. W., & Gwak, J. (2021). applied sciences Anomaly Detection of the Brake Operating Unit on Metro Vehicles Using a One-Class LSTM Autoencoder. *Applied Sciences*, *11*(19), 9290. https://doi.org/https://doi.org/10.3390/app11199290

Li, Z., Huang, M., Liu, G., & Jiang, C. (2021). A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. *Expert Systems With Applications*, *175*(July 2020), 114750. https://doi.org/10.1016/j.eswa.2021.114750

Lin, T., & Jiang, J. (2021). Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest. *Mathematics*, *9*(2), 4–15. https://doi.org/https://doi.org/10.3390/math9212683

Malik, E. F., Khaw, K. W., Belaton, B., & Wong, W. P. (2022). *Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture*.

Mushtaq, E., Zameer, A., Umer, M., & Abbasi, A. A. (2022). A two-stage intrusion detection system with auto-encoder and LSTMs. *Applied Soft Computing*, *121*(May). https://doi.org/https://doi.org/10.1016/j.asoc.2022.108768

Oluwasanmi, A., Aftab, M. U., Baagyere, E., Qin, Z., Ahmad, M., & Mazzara, M. (2022). Attention Autoencoder for Generative Latent Representational Learning in Anomaly Detection. *Sensors*, *1*, 1–14. https://doi.org/https://doi.org/10.3390/s22010123

Prabha, D. P., & Priscilla, C. V. (2023). Probabilistic XGBoost Threshold Classification with Autoencoder for Credit Card Fraud Detection. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(8s), 528–537. https://doi.org/https://doi.org/10.17762/ijritcc.v11i8s.7234

Priscilla, C. V., & Prabha, D. P. (2020). Credit Card Fraud Detection: A Systematic Review. In *Springer, Cham* (pp. 290–303). https://doi.org/10.1007/978-3-030-38501-9_29

Priscilla, C. V., & Prabha, D. P. (2021). A two-phase feature selection technique using mutual information and XGB- RFE for credit card fraud detection. *International Journal of Advanced Technology and Engineering Exploration*, *8*(85). https://doi.org/https://doi.org/DOI:10.19101/IJATEE.2021.874615

Priscilla, D. P. P. and C. V. (2024). Estimation of optimal threshold shifting to handle class imbalance in credit card fraud detection using machine learning techniques □. *AIP Conference Proceedings*, *2802*(1). https://doi.org/https://doi.org/10.1063/5.0182386

Razaque, A., Ben, M., Frej, H., Bektemyssova, G., Amsaad, F., & Almiani, M. (2023). applied sciences Credit Card-Not-Present Fraud Detection and Prevention Using Big Data Analytics Algorithms. *Applied Sciences*, *13*(1), 57. https://doi.org/https://doi.org/ 10.3390/app13010057

Ruangsakorn, T., & Yu, S. (2021). A Study on Comparative Evaluation of Credit Card Fraud Detection Using Tree-Based. *In Advances in Internet, Data and Web Technologies*, *1*, 212–219.

Seeja, K. R., & Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining. *Scientific World Journal*, *2014*, 1–10. https://doi.org/10.1155/2014/252797

Siddharth, V. (2021). Application of Deep Reinforcement Learning to Payment Fraud. *ArXiv Preprint ArXiv:2112.04236.*, *1*(1).

Tayeh, T., Aburakhia, S., Myers, R., & Shami, A. (2022). An Attention-Based ConvLSTM Autoencoder with Dynamic Thresholding for Unsupervised Anomaly Detection in Multivariate Time Series. *Machine Learning and Knowledge Extraction*, *4*(2), 350–370. https://doi.org/https://doi.org/ 10.3390/make4020015

Trisanto, D. (2021). Modified Focal Loss in Imbalanced XGBoost for Credit Card Fraud Detection. *International Journal of Intelligent Engineering and Systems*, *14*(4), 350–358. https://doi.org/10.22266/ijies2021.0831.31

Wang, C., Deng, C., & Wang, S. (2020). Imbalance-XGBoost: leveraging weighted and focal losses for binary label-imbalanced classification with XGBoost. *Pattern Recognition Letters*, *136*, 190–197. https://doi.org/https://doi.org/10.1016/j.patrec.2020.05.035

Xiangwei Kong , Xueyi Li , Qingzhao Zhou, Zhiyong Hu, and C. S. (2021). Attention Recurrent Autoencoder Hybrid Model for Early Fault Diagnosis of Rotating Machinery. *IEEE Transactions on Instrumentation and Measurement*, *70*, 1–10. https://doi.org/https://doi.org/10.1109/TIM.2021.3051948

Zhao, Y., Zhang, X., Shang, Z., & Cao, Z. (2022). DA-LSTM-VAE: Dual-Stage Attention-Based LSTM-VAE for KPI Anomaly Detection. *Entropy*, *24*(11). https://doi.org/https://doi.org/10.3390/e24111613