International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Autoencoder-Driven insights into Credit Card Fraud: A Comprehensive Analysis

[1]Wani Bisen, [2]Hirkani Padwad, [3]Gunjan Keswani, [4]Yash Agrawal, [5]Rashmi Tiwari, [6]Vinit Tiwari

Submitted: 16/11/2023 **Revised:** 28/12/2023 **Accepted:** 08/01/2024

Abstract: Exponential growth of online transactions has posed a serious threat to security of individuals, institutions and for the broader economy. Credit card fraud remains a pervasive and costly issue in the financial industry, necessitating the development and implementation of effective fraud detection algorithms. This research paper provides a comparative analysis of three distinct algorithms, namely Random Forest, Autoencoder, and Logistic Regression, to evaluate their performance in identifying fraudulent transactions in credit card data. The study delves into the specifics of the data preprocessing and feature engineering steps crucial for preparing credit card transaction data, thus highlighting the significance of data quality in algorithm performance. Subsequently, the research paper scrutinizes the three selected algorithms. Random Forest, a powerful ensemble method, is known for its ability to handle complex, high-dimensional data. Autoencoder, a type of neural network, is explored for its ability to capture intricate patterns and anomalies in transaction data. Logistic Regression, a well-established linear classifier, is included for its simplicity and interpretability.

Keywords: *Credit Card Fraud Detection(CCFD), autoencoder, Machine Learning(ML), Deep learning(DL), Random forest, Logistic regression*

1. Introduction

In this digital era, it is very common for people to use online payment options as they offer convenience. But sometimes this convenience is overshadowed by malicious activities by fraudsters, hackers, criminals, etc. leading to financial loss to the individuals, organizations, etc. Apart from this, people face a lot of mental trouble seeing their hard-earned money go to scammers, organizations/ financial institutions incur substantial costs related to fraud investigations, customer reimbursements, and implementing security measures. Therefore, it is a pressing need to build robust fraud detection models to ensure privacy and security of people, helping them strongly establish their trust in online payment methods. This study explores comprehensive fraud detection methods, combining both supervised techniques such as Random Forest and logistic regression and unsupervised deep learning technique Autoencoders.

2. Related Work

The paper employs Genetic Algorithms to iteratively select and recombine features, mimicking natural selection to optimize the CCFD system's performance[1]. The paper employs anomaly detection algorithms, such as Local Outlier Factor and Isolation Forest, on PCA-transformed credit card transaction data, highlighting the significance of machine learning in addressing class imbalance and evolving transaction patterns over time for automated fraud detection[2]. The paper presents a novel fraud detection approach using machine learning, featuring cardholder grouping, classifier training, and a feedback mechanism. Logistic regression, decision tree, and random forest, along with SMOTE, enhance performance on an imbalanced dataset. The Matthews Correlation Coefficient is highlighted for evaluating model performance[3]. The author explores card payment fraud detection through a comprehensive survey of 45 research papers from 2009 to 2020, highlighting four common fraud types, and underscores the importance of adapting strategies to address evolving fraud tactics for a secure digital economy[4]. This research conducts a comparative analysis of ML techniques, including Random Forest, Artifcial Neural Network (ANN), Support Vector Machine (SVM), and K-Nearest Neighbour (KNN), for CCFD while addressing data confidentiality. The study proposes a hybrid solution utilizing ANN in a federated learning framework, ensuring both high accuracy in CCFD and privacy preservation using blockchain technology[5]. This work introduces a two-stage model for CCFD, employing an autoencoder to transform

[1]*Department of Computer Science and Engineering RCOEM Nagpur,India*
bisenwh@rknec
[2]*Department of Computer Science and Engineering RCOEM Nagpur, India*
padwadhs@rknec.edu
[3]*Department of Computer Science and Engineering RCOEM Nagpur,India*
keswanigv@rknec.edu
[4] *Department of Computer Science and Engineering RCOEM Nagpur,India*
agrawalys_2@rknec.edu
[5]*Department of Computer Science and Engineering RCOEM Nagpur, India*
tiwarirs@rknec.edu
[6]*Department of Computer Science and Engineering RCOEM Nagpur, India*
tiwarivv_3@rknec.edu

transaction attributes into a lower-dimensional feature vector attributes into a lower-dimensional feature vector. The proposed model demonstrates superior performance in terms of F1-measure compared to systems relying solely on classifiers or other autoencoder-based approaches[6]. The paper addresses CCFD, emphasizing the challenges of imbalanced and dynamic transaction data. It conducts comparative analyses using SVM, KNN, naïve Bayes(NB), and logistic regression techniques, focusing on feature selection and machine learning algorithms. The logistic regression algorithm is highlighted as the most accurate in detecting credit card fraud among the evaluated models, with potential future improvements suggested for larger datasets and advanced bias prevention methods [7]. The study addresses the vulnerabilities in the financial sector, particularly credit card transactions, proposing an automated model utilizing NB, Random Forest, Logistic Regression, and SVM machine learning algorithms for fraud detection. After applying these algorithms to a large dataset, Naive Bayes stands out with an impressive 80.4% accuracy and a 96.3% area under the curve[8]. This paper addresses the challenges of Credit Card Fraud (CCF), utilizing Genetic Algorithm (GA) as a feature selection technique with an emphasis on application level detection. The study employs NB, Random Forest, and (SVM) machine learning techniques on an imbalanced German credit card dataset. The GA feature selection is conducted in two phases, prioritizing eight attributes in each phase. The experimental results highlight the significance of the first priority features, with Random Forest outperforming NB and SVM with relation to precision, accuracy, and fraud detection rate [9]. This research delves into a number of methodologies, including genetic programming, machine learning, fuzzy logic, and sequence alignment. It also explicitly applies the KNN algorithm and outlier detection approaches to maximize fraud detection. The proposed approaches aim to minimize false alarm rates and increase fraud detection rates, offering potential solutions for enhancing CCFD systems in banks[10]. The research work focused on comparing machine learning algorithms for CCFD using random under-sampling (RUS) as a data balancing technique. Logistic Regression (LR) outperformed NB and KNN across different data proportions (50:50, 34:66, 25:75). LR exhibited higher accuracy, sensitivity, specificity, precision, F-measure, and area under the curve (AUC) compared to NB and KNN. The study emphasized the importance of data balancing techniques in dealing with imbalanced datasets in CCFD. Future work could explore other resampling methods and compare the results with additional machine learning techniques such as Random Forest, SVM, Decision Trees, Neural Networks, and Genetic Algorithms. Improvements in resampling methods could be investigated to address the limitations of information loss associated with random under-sampling. The finding of this research may lead to the development of more effective CCFD systems capable of handling skewed data and providing accurate assessments[11]. The study investigates CCFD with two random forest models using a B2C dataset. The paper emphasizes the need for continuous improvement in the models to address evolving fraud scenarios[12].Various techniques such as under-sampling, over-sampling, SMOTE, and AdaSyn are applied to balance data. Classifiers including Logistic Regression, Random Forest,

K-Nearest Neighbors, Decision Tree, and Naive Bayes are evaluated using metrics like accuracy, precision, recall, and F1-score[13]. The research proposes a novel cost-sensitive metaheuristic algorithm, CSFPA, combining flower pollination optimization, correlation-based feature selection, and a random forest classifier, to minimize misclassification costs in CCFD. CSFPA outperforms existing techniques on the Brazilian bank dataset, achieving superior metrics, including a low average cost of 0.037, high precision, recall, and accuracy, showcasing its effectiveness in handling class imbalance and improving fraud detection[14]. This paper addresses CCFD using machine learning algorithms, emphasizing the challenge of class imbalance. The proposed system employs Random Forest and Decision Tree classifiers, with Random Forest outperforming due to its ability to handle imbalanced data[15]. The paper treats credit card fraud detection as an anomaly detection problem, utilizing unsupervised attentional anomaly detection network (UAAD-FDNet) comprising a generator and a discriminator. The proposed model aims to effectively separate fraudulent transactions from normal ones through adversarial training, feature attention, and hybrid weighted loss functions[16]. It proposes a two-stage framework for fraud detection, combining a deep Autoencoder for representation learning with supervised deep learning techniques. Deep learning classifiers (DNN, RNN, RNN_CONV) are applied to both the original and transformed datasets obtained by the deep Autoencoder[17]. The presented work focuses on utilizing artificial neural networks (ANNs), specifically multilayer perceptron models and explores the impact of different configurations of hidden layers and neurons on the performance of the ANN models[18]. The proposed CCFD method utilizes a neural network ensemble, employing LSTM neural network as the base learner in the AdaBoost framework. The hybrid data resampling method combines SMOTE-ENN to address imbalanced datasets[19]. The paper introduces a customized model architecture for credit card fraud detection, potentially leveraging aspects of the 1D DenseNet and autoencoder for feature extraction[20].

3. Proposed Model

The depicted figure, Figure 1, showcases the blueprint of the proposed methodology in this paper, encompassing a series of steps, from dataset processing to the final assessment of the proposed model's accuracy.

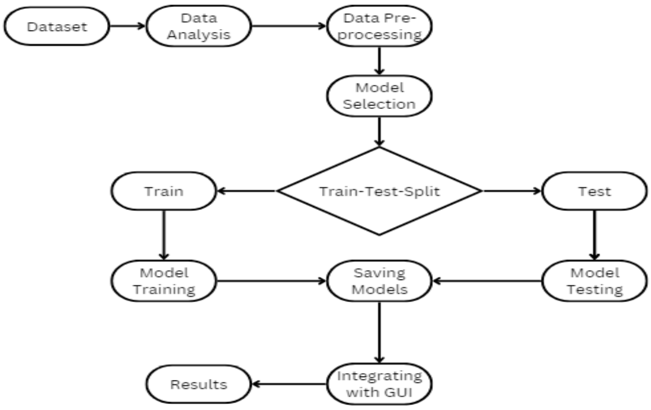


Fig.1 Architecture of proposed model

1 Dataset Analysis

This dataset is openly accessible and was obtained from the open-source website "Kaggle." This dataset is made up of simulated credit card transaction data from January 1, 2019, to December 31, 2020, including both valid and fraudulent transactions. It protects the credit cards of one thousand customers who deal with eight hundred retailers. Brandon Harris's Sparkov Data Generation | Github tool was used to generate this. The simulation was conducted from January 1, 2019, to December 31, 2020. After merging the files, they were formatted into a common format. This dataset has about 22 total features, including the target class "is_fraud." There are 1296675 total entries (rows) in this collection. Here, we plotted different graphs like Amount vs Fraudulent and Non-fraudulent transaction, Month, day, hour vs Fraudulent and Non-fraudulent transactions and many such. We created some useful columns like hour, days and month to analyze the trend and appended these columns in our dataset to increase accuracy. We found that features like Amount, City population, Day, Month, Category, Zip, latitude and longitude of sender and receiver , Age, state plays a key role and can help in distinguishing fraudulent transactions. Given below are the selected features.

Input features		
Category	State	Amount
Zip	Latitude	Longitude
City population	Merchant latitude	Marchant longitude
Age	Hour	Day
Month	Algorithm	

2 Data Preprocessing

Here we started by Data cleaning.We removed duplicates and handled missing values.Then, we created some useful columns like hour, days and month to analyze the trend and appended these columns in our dataset to increase accuracy. Finally, we concluded our EDA and took the following features into consideration : category, state , amount ,zip, latitude , longitude , city population , merch_latitude , merch longitude , age, hour, day, month, is_fraud. We incorporated SMOTE (synthetic minority oversampling) to balance our dataset.Using One-hot Encoder and Standard Scaler, we performed normalization.Then we splitted the dataset into training and test sets.

3 Model Training

For supervised algorithms, we first trained our models on preprocessed data. We used different models like Logistic regression, Random forest, SVC.Then we defined a pipeline in Python using scikit-learn's Pipeline class. Then we made predictions using the pipeline pipe1 and calculated the accuracy of those predictions.

In autoencoder, we preprocessed and applied SMOTE to balance our dataset.This step resulted in converting our 14 featured dataset to 73 featured dataset.Then we created 1 input layer, followed by 2 encoding and 2 decoding layer.The encoder layers reduce the dimensionality of the input data while capturing important features.

The encoder maps the input data from 73 dimensions to a hidden layer of 18 dimensions using the formula:

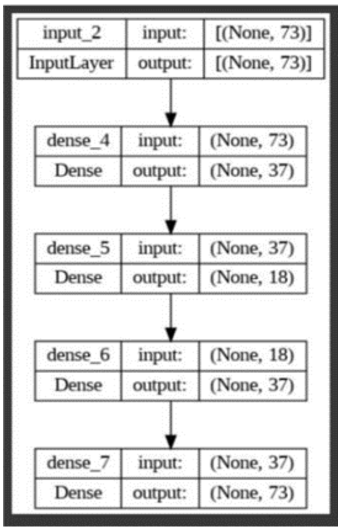
$Z = f E (W\varphi \times X + B\varphi)$

where X represents the input data, Wφ and Bφ represent the weights and biases for the encoder layer, fE is the encoder activation function, and Z is the hidden form of data.

The decoder works in a similar way; it transforms the 18 dimensions hidden layer into the original state of 73 dimensions using the formula:

$X' = f D(W\theta \times Z + B\theta)$

where fD is the decoder activation function and X′ represents the reconstruction of the original data.Wφ and Bφ represent the weights and biases for the decoder layer



input_2	input:	[(None, 73)]
InputLayer	output:	[(None, 73)]

dense_4	input:	(None, 73)
Dense	output:	(None, 37)

dense_5	input:	(None, 37)
Dense	output:	(None, 18)

dense_6	input:	(None, 18)
Dense	output:	(None, 37)

dense_7	input:	(None, 37)
Dense	output:	(None, 73)

Fig.2 Layers of Autoencoder model

The training process utilizes the RMSPROP optimizer and minimizes the mean squared error loss. The classification model for fraud detection is defined using the Keras sequential model. The model architecture consists of an initial layer, class_model, which probably works as a feature extractor.The model is compiled using the 'adam' optimizer and the mean squared error (MSE) loss function to enhance accuracy.

Layer(type)	Output Shape	Param #
input_2 (InputLayer)	[(None, 73)]	0
dense_4 (Dense)	(None, 37)	2738
dense_5 (Dense)	(None, 18)	684
dense_6 (Dense)	(None, 37)	703
dense_7 (Dense)	(None, 73)	2774

Fig. 3. Autoencoder layers with output shape

Total params: 6899 (26.95 KB)

Trainable params: 6899 (26.95 KB)

Non-trainable params: 0 (0.00 Byte)

4 Integration with GUI

The machine learning model was integrated with a user-friendly interface using Streamlit which involves creating a web application that provides an interface for users to interact with our model. Streamlit is a popular Python library for building web applications quickly and easily.

4. Result

In this digital era, detection of credit card fraud is very crucial for financial institutions and businesses. With the advent of sophisticated fraud techniques and the increasing number of digital transactions, the need for accurate and efficient fraud detection models has never been greater. In our study, we evaluated multiple models to address this critical issue and found promising results that can significantly contribute to enhancing fraud detection capabilities. The efficiency of several methods for detecting credit card fraud has been revealed through performance evaluation. The Autoencoder model is the highest performance among the models examined, with an astounding accuracy of 99.9%. A simpler but still strong model, Random Forest, obtained an accuracy of 99.7%.Logistic Regression got an accuracy of 96.4 while Support Vector Classifier (SVC) achieved a competitive accuracy of 96.6%, demonstrating its efficacy in capturing complicated decision boundaries. The Ensemble model designed exclusively for anomaly identification, obtained 96.15% accuracy. The model still holds a lot of potential and its accuracy can be increased using different models and optimizers.

Model	Random Forest	LR	SVC	AutoEncoders	Ensemble
Accuracy	99.77%	96.44	96.60%	99.93%	96.15%

Fig 4. Accuracy of models

5. Conclusion and Future Work

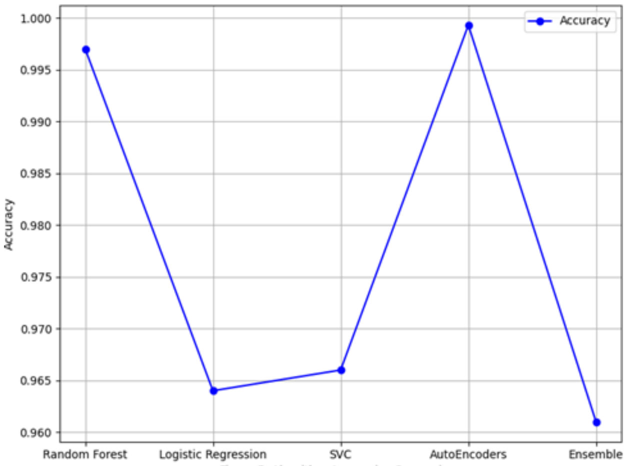


Figure 5. Algorithm Accuracies Comparison

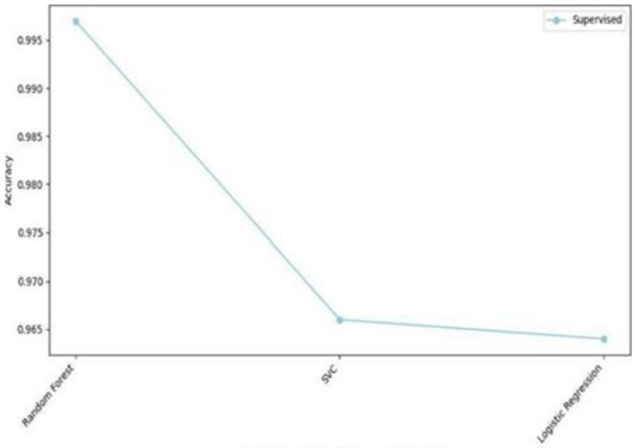


Figure 6 .Comparison of Supervised Algorithms

Credit card fraud is one of the biggest frauds that are happening right now around the globe. This paper has explained how credit card frauds have been happening and we studied these frauds using a dataset that consists of transactions made in the real world.

We saw how different machine learning algorithms are used to predict the fraud transactions on our dataset and we also addressed the class imbalance issue of our dataset and used SMOTE techniques to address this issue. Later, we trained different models and found that autoencoder and Random Forest give comparatively better results.

Future work in this domain should focus on staying ahead of these challenges and improving the overall effectiveness of fraud detection systems. Explore the use of more advanced machine learning and deep learning models, such as recurrent neural networks (RNNs), convolutional neural networks (CNNs). User notification systems can be built for cross verification and security purposes.

References

[1] Emmanuel Ileberi, Yanxia Sun ,Zenghui Wang, “A machine learning based credit card fraud detection using the GA algorithm for feature selection” 2022

[2] Maniraj SP, Saini A, Ahmed S, Sarkar D, “Credit card fraud detection using machine learning and data science”. Int J Eng Res 2019;8(09).

[3] Dornadula VN, Geetha S., “Credit card fraud detection using machine learning algorithms”. Procedia Computer Science 2019

[4] B. Wickramanayake, D. K. Geeganage, C. Ouyang, and Y.Xu, “A survey of online card payment fraud detection using data mining-based methods” , arXiv, [2020].

[5] Rejwan Bin Suleiman, Vitaly Schetinin and Paul Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection

[6] Sumit Misra, Soumyadeep Thakur, Manosij Ghosh, Sanjoy Kumar Saha, “An Autoencoder Based model for detecting fraudulent credit card transaction”

[7] Olawale Adepoju; Julius Wosowei; Shiwani lawte; Hemaint Jaiman, “Comparative Evaluation of Credit Card Fraud Detection using Machine Learning Techniques

[8] Amit Gupta, M.C. Lohani and Mahesh Manchanda, “Financial Fraud Detection using Naïve Bayes algorithm in highly imbalanced dataset”

[9] Yakub K. Saheed, Moshood A. Hambali, Micheal O. Arowolo and Yinusa A. Olasupo, “GA Feature selection on Naïve Bayes, Random Forest and SVM for Credit card fraud detection”

[10] N. Malini; M. Pushpa, “Analysis on Credit card fraud identification techniques based on KNN and outlier detection”

[11] Fayaz Itoo, Meenakshi and Satwinder Singh, “Comparison and analysis of logistic regression, Naïve bayes and KNN machine learning algorithms for credit card fraud detection

[12] Shiyang Xuan; Guanjun Liu; Zhenchuan Li; Lutao Zheng; Shuo Wang; Changjun Jiang, “Random Forest for credit card fraud detection”

[13] Hordri, Yuhaniz, Azmi and Shamsuddin, “Handling Class Imbalance in Credit Card Fraud using Resampling Methods”

[14] Fahimeh Ghobadi, Mohsen Rohani, “Cost sensitive modeling of credit card fraud using neural network strategy”

[15] Bora Mehar Sri Satya Teja1, BoomireddyMunendra2, Mr.S. Gokulkrishnan.[2022] A Research Paper on Credit Card Fraud Detection

[16] Shanshan Jaing, Ruiting Dong, Jie Wang and Min Xia, “Credit Card Fraud Detection Based in Unsupervised Attentional Anomaly Detection Network

[17] Hosein Fanai, Hossein Abbasimehr, “A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection[2023]

[18] Bassam Kasasbeh, Balqees Al-dabayah, Hadeel Ahmad, “Multilayer perceptron artificial neural networks-based model for credit card fraud detection”[2022]

[19] Ebenezer Esenogho, Domor Mienye, Theo Swart and Kehinde Aruleba, “A neural network ensemble with feature engineering for improved credit card fraud detection” [2022]

[20] Saleh Albali, Tahira Nazir, Awais Mehmood, Aun Irtaza, Ali Alkhalifah, Waleed Albattah , “AEI-DNET: A novel densenet model with an autoencoder for the stock market predictions using stock technical indicators[2022]