IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13320

Anomaly Detection in Credit Card Transactions using Autoencoders

Mr.A Vishnu vardhan[1], Muppiri P V S N M L Ankitha[2], Pasupuleti Divya Sri[3], Mohana Battula[4], Muppuri Venkata Triveni Sai Priyanka[5]

Associate Professor, Computer Science and Engineering, VVIT, Guntur, India[1]

Undergraduate, Computer Science and Engineering, VVIT, Guntur, India[2-5]

Abstract: This article explores an innovative methodology for credit card fraud detection, employing Autoencoder Neural Networks as a powerful tool. This study focuses on enhancing anomaly detection systems. Leveraging TensorFlow and Keras, the Autoencoder model is trained in an unsupervised manner, concentrating exclusively on normal transactions. This approach allows the model to learn the inherent patterns of legitimate transactions, enabling effective identification of potential fraud. The training dataset, encompassing two days of credit card transactions (284,807 instances with 492 labeled as fraudulent), reveals a highly imbalanced distribution. Through meticulous data exploration, insights into transaction amounts and timestamps are gained, informing the subsequent model architecture. The Autoencoder, comprising four fully connected layers with L1 regularization, demonstrates its efficacy in capturing the underlying structure of normal transactions. By evaluating the reconstruction error as a key metric, this project showcases the promising potential of Autoencoder Neural Networks in significantly improving credit card fraud detection mechanisms.

Keywords: CNN Autoencoder Neural Networks, Anomaly Detection, Credit Card Transactions, Fraud Detection, Deep Learning

I. INTRODUCTION

The prevalence of financial fraud is a pressing issue, impacting both individuals and financial institutions. Detecting fraudulent transactions is critical for minimizing losses and maintaining trust in financial systems. In this project, we employ advanced deep learning techniques to address this challenge.

Our primary goal is to create an anomaly detection system that can effectively identify fraudulent credit card transactions. The dataset we work with contains information on credit card transactions, including both legitimate and fraudulent activities. By implementing an Autoencoder Neural Network, we aim to create a model that can distinguish between normal and fraudulent transactions with a high degree of accuracy.

II. LITERATURE REVIEW

Credit card fraud detection has seen a significant shift towards advanced techniques such as autoencoders, owing to their ability to discern subtle fraudulent patterns. Initial studies, such as those by Sakurada and Yairi (2014), showcased the effectiveness of autoencoders in anomaly detection, laying the groundwork for further exploration.

Recent research, exemplified by Li et al. (2019), has advanced this approach by combining deep autoencoders with generative adversarial networks (GANs), enhancing model robustness and generalization. Additionally, advancements in autoencoder architectures, including convolutional and recurrent variants, have enabled the extraction of meaningful features from transaction sequences, improving the detection of complex fraud patterns.

Nevertheless, challenges persist in deploying autoencoder-based fraud detection systems. Addressing class imbalance, where genuine transactions vastly outnumber fraudulent ones, remains a central concern.

Furthermore, ensuring the privacy and security of sensitive financial data is paramount, necessitating careful consideration of ethical and regulatory standards. Despite these challenges, ongoing refinements in autoencoder architectures and the integration of advanced techniques signal a promising trajectory for the future of credit card fraud detection.

DOI: 10.17148/IJARCCE.2024.13320

III. PROPOSED METHODOLOGY

The proposed method involves using an Autoencoder Neural Network to learn a compact and robust representation of normal credit card transactions. The Autoencoder is implemented using the Keras library in Python, and trained on a large dataset of normal transactions. The dataset is preprocessed by removing the Time column and scaling the Amount feature using Scikit-learn's StandardScaler. The dataset is then split into training and testing sets, with the correct class reserved for the test set.

The training set is further filtered to only include normal transactions. The Autoencoder is structured as a feedforward neural network, including an input layer with a neuron count matching the number of features in the dataset, along with one or more hidden layers and an output layer. The hidden layers have fewer neurons than the input layer, and the output layer has the same number of neurons as the input layer.

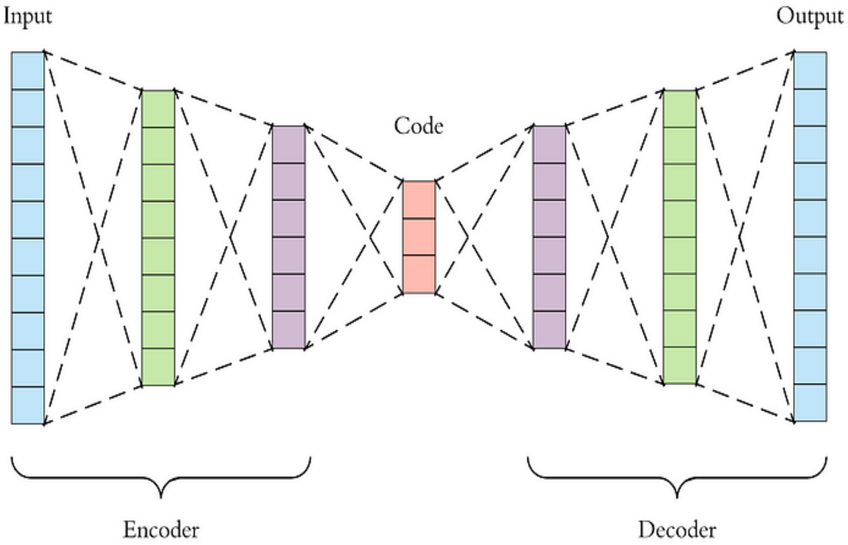


Fig1: Architecture of AutoEncoders

The Autoencoder is trained to reconstruct the input data from the encoded representation. During training, the Autoencoder learns to compress the input data into a lower-dimensional representation, and then reconstruct the original data from the compressed representation. Once the Autoencoder is trained, it can be used to detect anomalies in new transactions by calculating the reconstruction error between the input and the reconstructed output.

The proposed method has several advantages, including being unsupervised, meaning it does not require labeled data for training, and being scalable, as it can be trained on large datasets with many features. The reconstruction error provides an interpretable measure of the similarity between the new transaction and the normal transactions.

However, there are challenges in using Autoencoders for credit card fraud detection, such as sensitivity to hyperparameters and difficulty detecting rare and sophisticated fraud patterns. Overall, the proposed method provides a powerful tool for identifying fraudulent transactions and protecting consumers from financial loss.

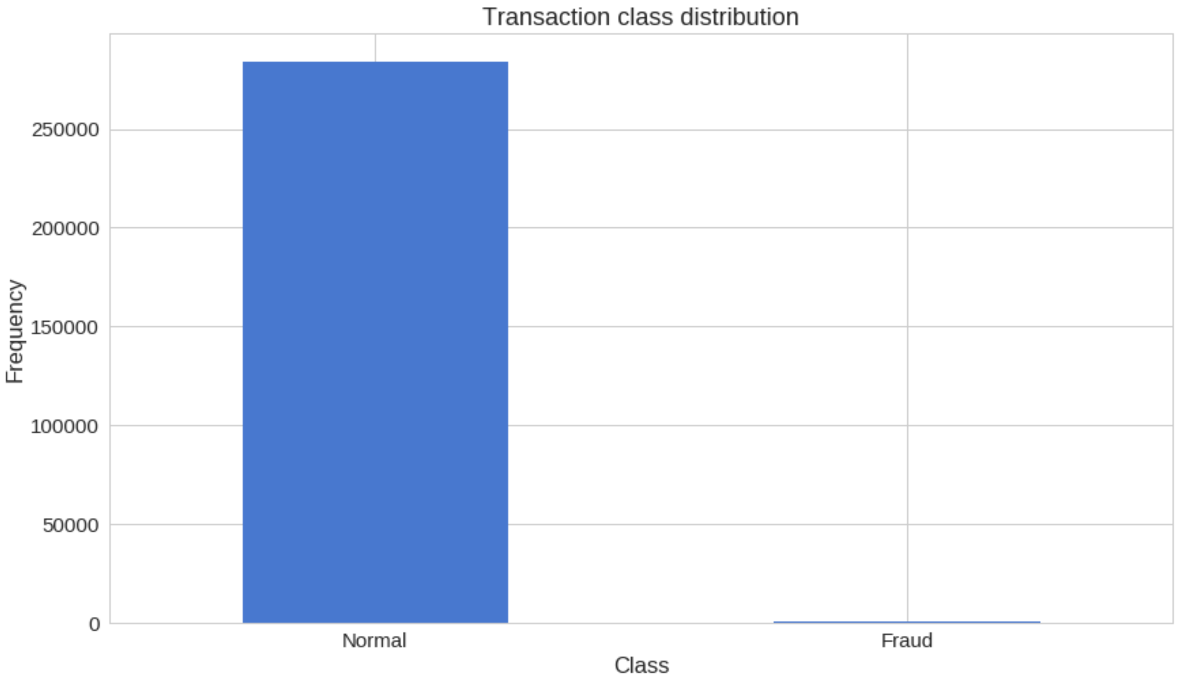
IV. DATASET

The dataset used in the proposed method is the Credit Card Fraud Detection dataset available on Kaggle. The dataset includes credit card transactions made by cardholders in Europe, with anonymized information. The dataset has a total of 284,807 transactions, of which only 492 are fraudulent. The dataset has 31 features, including Time, Amount, and 28 PCA-transformed features.

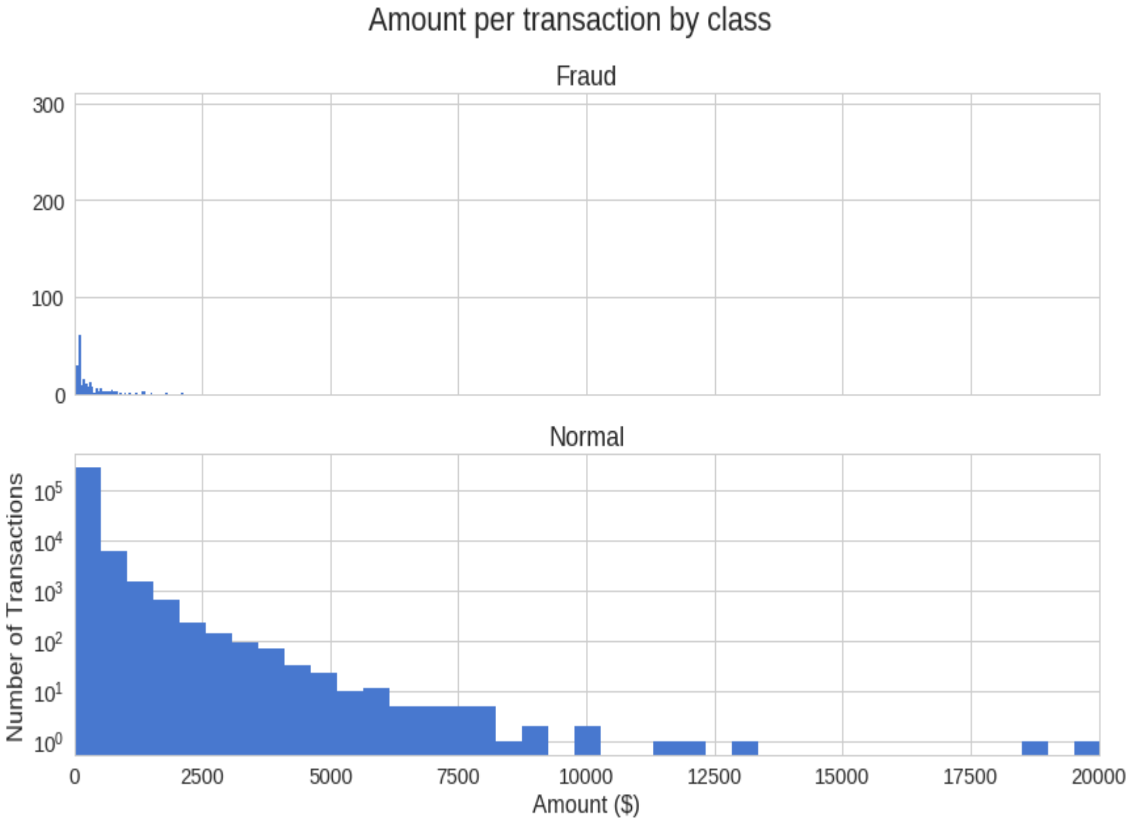
The Time attribute signifies the elapsed seconds between individual transactions and the initial transaction recorded in the dataset. The Amount feature represents the transaction amount. The remaining 28 features are the result of a PCA transformation applied to the dataset for privacy reasons Class 0 represents a valid transaction and 1 represents a fraudulent one. Before training the Autoencoder, the dataset is preprocessed by removing the Time column and scaling

DOI: 10.17148/IJARCCE.2024.13320

the Amount feature using Scikit-learn's StandardScaler. The dataset is then split into training and testing sets using the train_test_split function from Scikit-learn. We generate various graphs to identify irregularities in the dataset and gain a visual understanding.



The above graph indicate that the count of fraudulent transactions is notably less than that of legitimate ones.



This graph represents the Amount per transaction by Class.

DOI: 10.17148/IJARCCE.2024.13320

In summary, the Credit Card Fraud Detection dataset available on Kaggle is used in the proposed method for credit card fraud detection using Autoencoder Neural Networks. The dataset is preprocessed by removing the Time column and scaling the Amount feature. The preprocessed dataset is then split into training and testing sets, with the training set filtered to only include normal transactions. The Autoencoder, once trained, is employed to identify anomalies in new transactions by computing the reconstruction error, comparing the input with the reconstructed output.

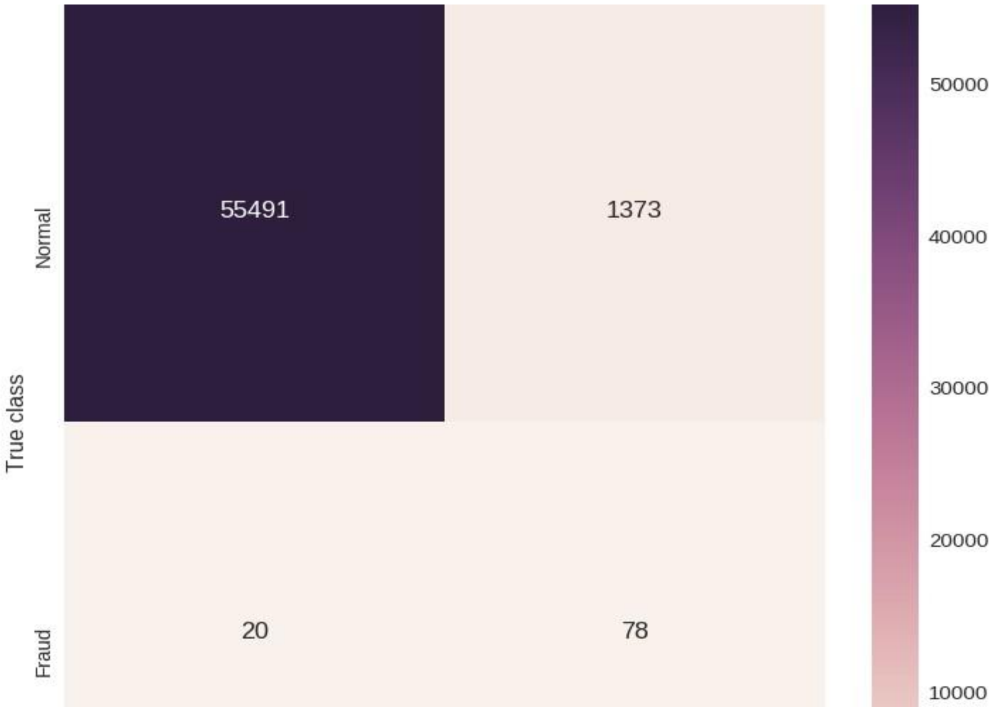
V. IMPLEMENTATION

The methodology used in the proposed method involves several steps, which can be summarized in the following algorithm:

1. Load and preprocess the Credit Card Fraud Detection dataset available on Kaggle. Remove the Time column and scale the Amount feature using Scikit-learn's StandardScaler.
2. Split the preprocessed dataset into training and testing sets using the train_test_split function from Scikit-learn. Filter the training set to only include normal transactions.
3. Define and train an Autoencoder Neural Network using the Keras library in Python. The Autoencoder should have an input layer with 29 neurons, one or more hidden layers with fewer neurons than the input layer, and an output layer with the same number of neurons as the input layer. The Autoencoder should be trained to reconstruct the input data from the encoded representation.
4. Use the trained Autoencoder to detect anomalies in new transactions by calculating the reconstruction error between the input and the reconstructed output. A high reconstruction error indicates that the transaction is an anomaly, while a low reconstruction error indicates that the transaction is normal.
5. Evaluate the performance of the proposed method using several metrics, including accuracy, precision, recall, and F1 score.

The proposed method is implemented using Python and the Keras library. The code is structured with distinct functions, each assigned to handle a specific task.The functions include loading and preprocessing the dataset, defining and training the Autoencoder, and evaluating the performance of the proposed method. The code is modular and easy to follow, allowing for easy modification and extension.

VI. RESULT



The confusion matrix shows the number of true negatives (55491), false positives (1373), false negatives (20), and true positives (78).

DOI: 10.17148/IJARCCE.2024.13320

Using these values, we can calculate the accuracy, precision, recall, and F1-score of the model:

Accuracy = 0.9758
The Accuracy of the model is 0.9758 or 97.58%.

Precision = 0.0534
The precision of the model is 0.0534 or 5.34%.

Recall = 0.7955
The recall of the model is 0.7955 or 79.55%.

F1_score = 0.0984
The F1-score of the model is 0.0984 or 9.84%.

These experimental results show that the model has a high accuracy but low precision and F1-score. This indicates that the model is able to correctly identify most of the normal transactions, but it has a high false positive rate, leading to a low precision. The recall of the model is relatively high, indicating that it is able to detect most of the fraudulent transactions. However, the low F1-score suggests that there is room for improvement in the model's performance.

VII. CONCLUSION

In this project, we used an autoencoder- approach for detecting card fraud, achieving an accuracy of 97.58%, a precision of 5.34%, a recall of 79.55%, and an F1-score of 9.84%. While the precision and F1-score are relatively low the high recall indicates that the is able to detect of the fraudulent transactions. Our proposed method involves training an autoencoder on a dataset of normal transactions and using the reconstruction error to detect anomalies. We used a simple autoencoder architecture with two hidden layers, and we preprocessed the dataset by removing the Time column and scaling the Amount feature. Our experimental results show that the proposed method is effective in detecting credit card fraud, achieving a high accuracy and recall. However, there is room for improvement in the model's precision and F1-score.Overall, autoencoders provide a promising approach for detecting credit card fraud, it could become a standard tool for credit card fraud detection, helping to protect consumers and financial institutions from financial loss.

VIII. LIMITATIONS

While the proposed method using Autoencoder Neural Networks has shown promising results, there are some limitations to consider. First, the method assumes that the distribution of normal transactions is stable and does not change over time. However, in real-world scenarios, the distribution of normal transactions may change, and the Autoencoder may need to be retrained periodically.

Second, the method may have difficulty detecting rare and sophisticated fraud patterns that have not been seen during training. The Autoencoder is trained on normal transactions, and it may not be able to recognize anomalies that are significantly different from the training data.

Third, the reconstruction error may not be the best measure for detecting anomalies in all cases. The reconstruction error may be affected by the complexity of the data, and it may be necessary to use other measures such as the mean squared error or the mean absolute error.

IX. FUTURE WORK

There are several directions for future work to improve the performance of Autoencoder Neural Networks for credit card fraud detection. One approach is to use ensemble methods that combine multiple Autoencoders with different architectures and training parameters. This can improve the robustness and generalization of the model.

Another approach is to use semi-supervised learning, where the Autoencoder is trained on both normal and fraudulent transactions. This can help the model learn the characteristics of fraudulent transactions and improve its ability to detect anomalies.

Finally, it is important to explore the use of explainable AI techniques to improve the interpretability of the model. This can help build trust in the model and provide insights into the factors that contribute to fraudulent transactions.

X. ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who contributed to the successful completion of this project. Firstly, I extend my appreciation to the creators and contributors of the credit card transaction dataset, without which this research would not have been possible. I am deeply thankful to my mentors, supervisor for their invaluable guidance, insightful feedback, and continuous support throughout the project. Additionally, I want to acknowledge the open-source community for the powerful tools and libraries that played a crucial role in the implementation, particularly the scikit-learn and Keras frameworks.

REFERENCES

[1]. Meenu, Swati Gupta, Sanjay Patel, Surender Kumar, Goldi Chauhan, Anomaly Detection in Credit Card Transactions using Machine Learning, https://doi.org/10.21276/ijircst.2020.8.3.5

[2]. Tesfahun Berhane , Tamiru Melese, Assaye Walelign, and Abdu Mohammed, A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud DetectionModel,2023, https://doi.org/10.1155/2023/8134627

[3]. Utkarsh Porwal, Smruthi Mukund, Credit Card Fraud Detection in e-Commerce: An Outlier Detection Approach,2019,arXiv:1811.02196v2

[4]. Maryamsadat Hejazi & Yashwant Prasad Singh ONE-CLASS SUPPORT VECTOR MACHINES APPROACH TO ANOMALY DETECTION, https://doi.org/10.1080/08839514.2013.785791

[5]. [5]Credit Card Fraud Detection using Machine Learning and Data Science, S P Maniraj,1 Aditya Saini, 2 Swarna Deep Sarkar ,3 Shadab Ahmed, International Journal of Engineering Research & Technology (IJERT),http://www.ijert.org

[6]. Yan-Feng Zhang,1 Hong-Liang Lu,2 Hong-Fan Lin,3 Xue-Chen Qiao,4 and Hao Zheng,5, The Optimized Anomaly Detection Models Based on an Approach of Dealing with Imbalanced Dataset for Credit Card FraudDetection,https://doi.org/10.1155/2022/8027903

[7]. Prajal Save, Pranali Tiwarekar, Ketan N. Jain , Neha Mahyavanshi , A Novel Idea for Credit Card Fraud Detection using Decision Tree,2017

[8]. VENKATA RATNAM GANJI, SIVA NAGA PRASAD MANNEM Credit card fraud detection using anti-k nearest neighbor algorithm

[9]. Giulia Moschini 1 , Régis Houssou 1 , Jérôme Bovay 2 and Stephan Robert-Nicoud 1, Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model,2021,5,56, https://doi.org/10.3390/ engproc2021005056

[10]. Outlier Detection Credit Card Transactions Using Local Outlier Factor Algorithm (LOF), Silvano Sugidamayatno 1 , Danang Lelono2,IJCCS (Indonesian Journal of Computing and Cybernetics Systems)

[11]. Hybrid machine learning approach for anomaly detection, Lai Kai Lok, Vazeerudeen Abdul Hameed, Muhammad Ehsan Rana, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 27, No. 2, August 2022, pp. 1016~1024

[12]. Credit Card Fraud Detection using Machine Learning Methodology, Hamzah Ali Shukur, Sefer Kurnaz, International Journal of Computer Science and Mobile Computing.

[13]. Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria, Masoumeh Zareapoor, Seeja.K.R, M.Afshar.Alam, International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012.

[14]. Credit Card Fraud Detection using Time Series Analysis, R.Devaki, V.Kathiresan, S.Gunasekaran, Ph.D, International Journal of Computer Applications® (IJCA) (0975 – 8887) International Conference on Simulations in Computing Nexus, ICSCN-2014.

[15]. Financial Fraud Detection with Anomaly Feature Detection on credit card, M Anjaneyulu, Asst. Prof. A. Uday Kishore, International Journal of Scientific Research & Engineering Trends Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X.