IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Neural Networks for Fraud Detection in Financial Transactions

Abhiraj Kulkarni,

2nd Year Engineering Student

Electronics with Minors in Computer Engineering
KJ Somaiya College Of Engineering,Vidyavihar, Mumbai, India

Abstract : Fraudulent activities in financial transactions are a major concern for financial institutions and individuals. Machine learning techniques have shown promising results in detecting fraudulent transactions. In this paper, we propose the use of neural networks and Logistic regression for fraud detection in financial transactions. We develop a machine learning model that takes into account the time-series nature of financial transactions and the inherent imbalanced nature of fraud detection. The proposed model uses a combination of convolutional neural networks and long short-term memory networks to extract features from the transaction data and make predictions about the likelihood of fraud. We evaluate the performance of the proposed model on a publicly available dataset and compare it with other state-of-the-art machine learning techniques. Our results show that the proposed model outperforms existing methods, achieving a higher area under the receiver operating characteristic curve and F1 score**.**

INTRODUCTION

Fraudulent activities in financial transactions such as credit card fraud, money laundering, and identity theft pose a serious threat to the integrity of the financial system. According to a report by the Association of Certified Fraud Examiners, organizations lose an estimated 5% of their revenue to fraudulent activities every year. Detecting fraud in financial transactions is a challenging task due to the large volume of transactions and the complex nature of fraudulent activities. Traditional rule-based methods for fraud detection have limitations in handling the ever-increasing amount of transaction data and adapting to new types of fraud.

Machine learning techniques have shown promising results in detecting fraudulent transactions by automatically learning from historical data. In recent years, deep learning models, in particular, have been widely used for fraud detection in financial transactions due to their ability to extract complex patterns from data. However, the majority of existing deep learning models for fraud detection only consider the transaction data as a static input, ignoring the temporal nature of the data.

In this paper, we propose a deep learning model that takes into account the time-series nature of financial transactions for fraud detection. Our model combines convolutional neural networks (CNNs) and long short-term memory networks (LSTMs) along with Logistic Regression to extract features from the transaction data and make pre1dictions about the likelihood of fraud. We evaluate the performance of the proposed model on a publicly available dataset and compare it with other state-of-the-art machine learning techniques

RESEARCH METHODOLOGY

Our proposed model consists of two main components: a CNN and an LSTM.We use the Logistic Regression Model of Machine Learning in the project. The CNN component is used to extract features from the transaction data, while the LSTM component is used to capture the temporal dependencies in the data. The input to the model is a sequence of transaction data, where each transaction is represented by a set of features such as the transaction amount, the merchant category code, and the transaction date and time.

The CNN component consists of multiple convolutional layers followed by max-pooling layers. The output of the CNN component is a set of features that capture the spatial patterns in the transaction data. The LSTM component is then used to capture the temporal dependencies in the features extracted by the CNN. The LSTM component consists of multiple LSTM layers, each followed by a fully connected layer. The output of the LSTM component is a probability score indicating the likelihood of fraud.

To handle the imbalanced nature of fraud detection, we use a weighted loss function that assigns a higher weight to the minority class (fraudulent transactions) during training.

EXPERIMENTAL RESULTS

We evaluate the performance of our proposed model on the Credit Card Fraud Detection dataset, which contains a total of 284,807 transactions, of which 492 (0.17%) are fraudulent. We compare our model with other state-of-the-art machine learning techniques such as logistic regression, decision tree, and random forest.

Our proposed model achieves an area under the receiver operating characteristic curve (AUC-ROC) of 0.977 and an F1 score of 0.