Credit Card Fraud Transaction Detection System Using Neural Network-Based Sequence Classification Technique

Kapil Kumar, Ambedkar Institute of Advanced Communication Technologies and Research, India

Shyla, Ambedkar Institute of Advanced Communication Technologies and Research, India

Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies and Research, India

ABSTRACT

The movement towards digital era introduces centralization of information, web services, applications, and devices. The fraudster keeps an eye over ongoing transaction and forges data by using different techniques as traffic monitoring, session hijacking, phishing, and network bottleneck. In this study, the authors design a framework using deep learning algorithm to suspect the fraudulence transaction and evaluate the performance of the proposed system by updating data repositories. The neural network-based sequence classification technique is used for fraud detection of credit card transactions by including threshold value to measure the deviation of transaction. The reconstruction error (MSE) and predefined threshold value of 4.9 is used for determination of fraudulent transactions.

KEYWORDS

Autoencoder, Deep Learning, Hidden Markov Model, Naïve Bayes, Random Forest, Support Vector Machine

1. INTRODUCTION

The continuous increase in online transactions leads to the issue of information security where fraud transactions through credit cards brings down customers financial condition regularly and will worst impact banking sector. The authors (Cheng et al., 2019) found that the need for electronic payment is increased due to extensive inclination of users towards internet to digitize the era. This introduces the need of secure transaction model for credit card system. The rigorous method of authentication and authorization needs more security which is achievable by conducting research. The implementation of research model under high-quality supervision restricts the financial losses through credit card transactions. The anticipation of loss due to credit card fraud transaction has become critical because statistical information is not available to users. The credit card fraud is classified into two categories as operational and rule-based fraud.

The operational fraud is implemented by manipulating information of authorization and authenticity, based on the approach followed by fraudster to gain unauthorized access. The users identity is obtained from the card issuer for violating cyber security. The rule-based credit card

DOI: 10.4018/IJOSSP.2021010102

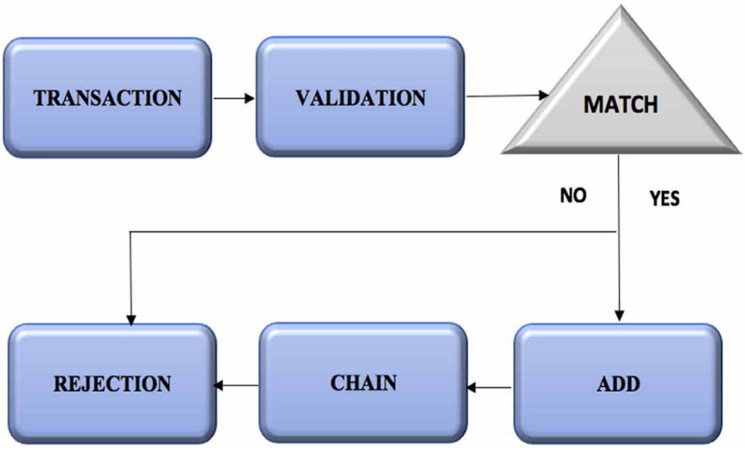
fraudulence occurs if the credit card is approved and is issued to fraudster for gaining unauthorized access to the credential and make the fake transaction for money of the actual card user. The example of rule-based fraud is behavior based fraud which acts according to the behavior of fraudsters by stealing the card or gaining access to lost card. The countered credit card fraud takes place by stealing fraudster information and behaves as a legitimate user to gain the access to mimic the identity of actual user. The transaction period of counterfeit is short. The another approach of fraud is by obtaining the information of credit card by calling an actual user.

The information technology is constantly evolving by providing ease and perfect security systems. The information security model is required to enhance information technology. In the case of credit card fraud system, there is requirement of standard security policies with a fraud detection model over neural network based deep learning approach. The companies and organizations always looks up to fraud detection system and will keep on seeking the evolution in the security field by conducting more research in this field for refining the prevailing system. The techniques used in the existing system is divided into two sections of machine learning as observed and unobserved learning where observed learning is used with labeled attributes for validation purpose, that include the decision tree and random forest, support vector machine and naive bayes.

The unsupervised learning do not include labeled data but include certain algorithms as clustering which is used to cluster data based on similarity and neural network based algorithm that includes the artificial neural network, convolution neural network, and recurrent neural network. In the context of artificial intelligence and data science, (Awoyemi et al., 2017) found that the generation of the effective model is needed to train on data but the generation of the model is not sufficient to optimize the result that cannot predict the future until the responsible factors are included as policy, infrastructure, platform and utility of the system. The most important aspect is the quality of data, where the quality of data does not mean collection of data from any sources meanwhile it depends on several factors as time used in a survey, the activity of the survey, manpower used in the survey, history of data, dimensions of data, and mutually related information. The model based on supervised and unsupervised machine learning techniques needs a susceptible score called fraudulence likelihood value to accept or reject the transaction and to detect the fraud.

The figure 1 illustrates the working of authentication system using a decentralization system, where the request of the credit card transaction is received, tested, validated, and is rejected and accepted on successful deployment in the existing chain of events. In the authentication system, a model contains a copy of transaction that comes for validation and verification.

Figure 1. Authentication system


TRANSACTION
VALIDATION
MATCH
NO
YES
REJECTION
CHAIN
ADD