Deep Learning Techniques for Online Fraud Detection

Sheema Murugesh Babu

Based on the paper: A Survey of Deep Learning based Online Transactions Fraud Detection Systems

- **Online banking allows a user to conduct financial transactions via the Internet. Online banking is also known as Internet banking or web banking.**

- **Online banking offers customers almost every service traditionally available through a local branch including deposits, transfers, and online bill payments.**

- **However, with the growth of online transactions, internet fraudulent activities are also increasing. Customers and banks lose money due to these fraudulent activities.**

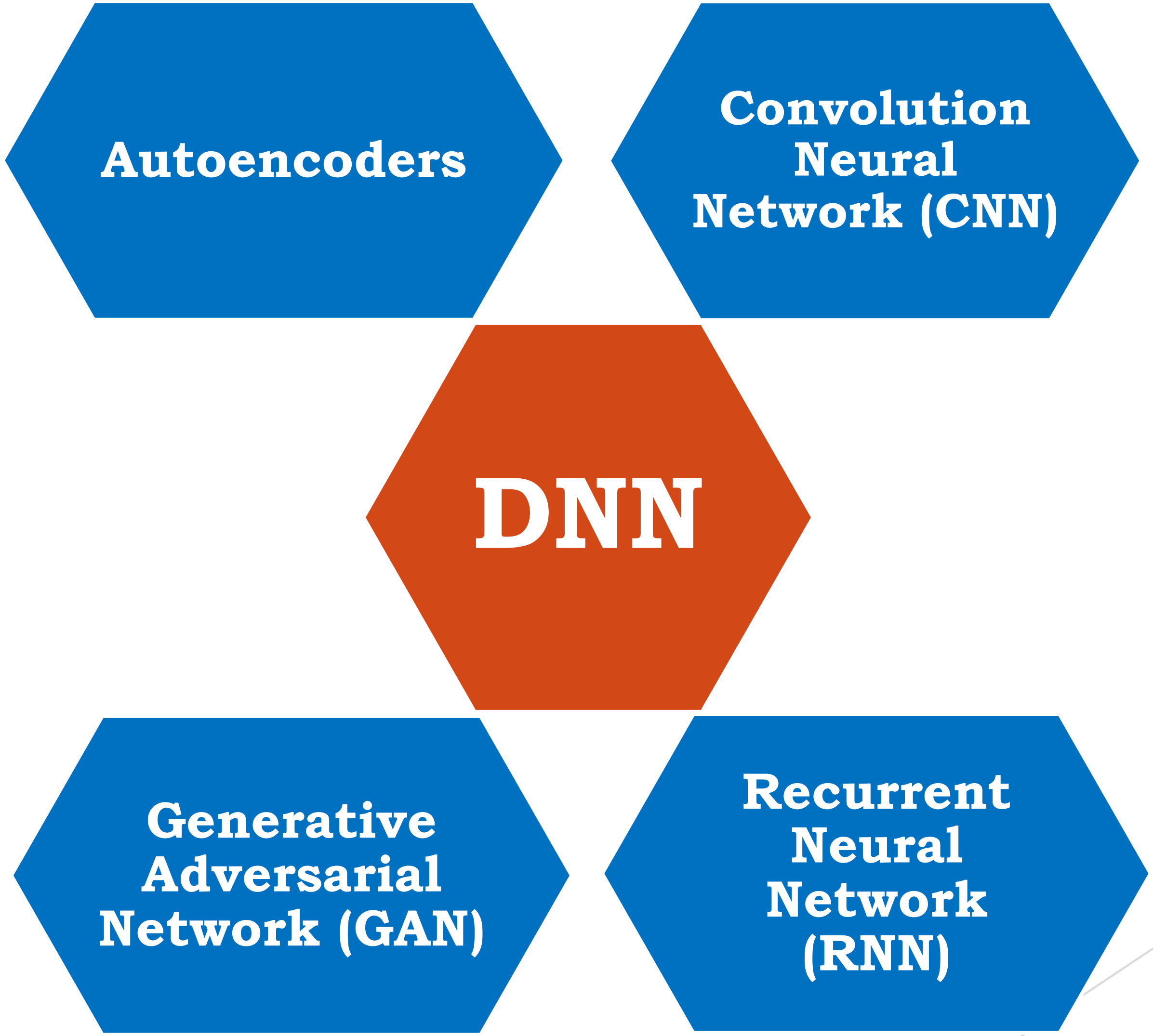
- **Although fraud prevention is difficult, sophisticated security protocols can be used to prevent access to unauthorized transactions.**

- Deep learning is one of the techniques which can be successfully applied for the detection of financial, e-payment frauds, and anti-money laundering.

- Deep learning is a class of machine learning algorithms that use a cascade of multiple layers of non-linear processing units for feature extraction and transformation.

- Its hidden layers have a high computational capability and are hence able to achieve high accuracy.

Huge number of transactions can be learned and classified into legitimate and fraudulent transactions by the DNN. Some of these are:



Autoencoders

Convolution Neural Network (CNN)

DNN

Generative Adversarial Network (GAN)

Recurrent Neural Network (RNN)

Deep Neural Networks

Deep Learning is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks.

DNNs for fraud detection have used Fisher's discriminant analysis which separates the fraudulent operations away from the normal operations.

Deep nets process data in complex ways by employing sophisticated math modeling.

The three classification methods i.e., neural networks, logistic regression, and decision tree to build the fraud detecting models can analyze the credit card history transaction and can detect any fraudulent and suspicious transaction.

Convolutional Neural Networks (CNNs)

A convolutional neural network (CNN) is a Deep Learning algorithm used in image recognition and processing that is specifically designed to process pixel data.

Several methods can be used to detect fraudulent activities based on CNNs. Some are based on a framework of mining fraud patterns in credit card transactions.

They can convert each transaction from the dataset into a feature matrix so that the intrinsic relations in time series can combine cost-based sampling method with the imbalanced sample datasets resulting in a better fraud detection process.

Convolutional neural networks (CNN) along with Long Short-Term Memory (LSTM) can be effectively used to solve stock market risky transactions, detection of fraudsters in mobile communications, and online transaction frauds.

Autoencoders

An autoencoder is a feed-forward multilayer neural network that reproduces the input data on the output layer and is a specific type of feedforward neural network where the input is the same as the output.

An autoencoder consists of 3 components: encoder, code, and decoder. The encoder compresses the input and produces the code, the decoder then reconstructs the input only using this code.

Some of the applications of autoencoders in fraud detection include Brazilian export systems, frauds in credit card transactions, unusual journal entries, etc.

Other applications of Auto-Encoder and Restricted Boltzman Machine are to detect fraudulent transactions in real-time in three datasets i.e., German, European, and Australian datasets.

Recurrent Neural Networks

A recurrent neural network (RNN) is a type of artificial neural network which uses sequential data or time-series data.

RNN is a better technique than the machine learning techniques like SVMs for learning a non-genuine user's activities.

Using RNN, suitable models can be created which model which uses the patterns in web access logs to detect fraudulent activities.

A novel deep learning-based model called CLUE which uses RNN can be used to detect fraud in e-commerce transactions of a real dataset. It can be effectively used to capture the click sequences and their sequence patterns as well.

Generative Adversarial Networks

Generative adversarial networks can be used for translating data from images and can be utilized for image-to-image translations, semantic image-to-photo translations, and text-to-image translations.

GANs are a clever way of training a generative model by framing the problem as a supervised learning problem with two sub-models: the generator model and the discriminator model.

GANs can be trained to obtain duplicate minority class transactions as output which were merged with the raw dataset to produce an extended network to output duplicate minority class transactions which were merged with the raw dataset to produce an extended training dataset.

GAN can be successfully applied to solve the problem of detecting fraudulent credit card transactions

Summary

Online fraudulent detections have not been fully explored using deep learning techniques. Very few researchers have worked in this area and the complete details about their datasets, features used, and results achieved by them have not been revealed. In addition, the datasets are mostly imbalanced and are not available in the public domains.

THANK YOU