Deep Learning Techniques for Online Fraud Detection

Sheema Murugesh Babu

Introduction

Online banking allows a user to conduct financial transactions via the Internet. Online banking is also known as Internet banking or web banking. Internet usage is increasing day-by-day in online transactions. Transfer of money has become extremely easy these days through internet banking as internet banking simplifies the transactions and prevents the customers from physically visiting the bank for such transactions. They can do all of this at their convenience, wherever they want-at home, at work, or on the go. In addition, Online banking offers customers almost every service traditionally available through a local branch including deposits, transfers, and online bill payments. Cashless transactions have become the order of the day even in small shops and business firms opting for wallet transfers. However, with the growth of online transactions, internet fraudulent activities are also increasing. Customers and banks lose money in these fraudulent activities. It is, in fact very difficult to detect these fraudulent transactions both by customers and banking system (Aisha Abdallah 2016). Although fraud prevention is difficult, sophisticated security protocols can be used to prevent access to unauthorized transactions. Present advanced systems are not fully-proof and fail from time to time as fraudsters can manipulate the security systems.

Advanced online fraud detection

Online fraud detection and prevention solutions should be designed to stop different types of fraud before any harm occurs. The system should be able to check the previous transactions of the customers and compare them to check whether there are any fraudulent transactions. Numerous challenges are faced by the developers to develop advanced online fraudulent detection systems, one of them being the privacy issue for financial organizations as they cannot reveal secret data to their customers.

Deep Learning Online Fraud Detection System

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. Deep learning constitutes different types based on the type of data and the methodology used. Its hidden layers have a high computational capability and are hence able to achieve high accuracy. A huge amount of data is involved in online transactions, but this huge data cannot be handled by ordinary machine learning algorithms. In addition, the performance of deep learning continues to increase even when data size is increased. Hence, this huge number of transactions can be learned and classified into legitimate and fraudulent transactions by the DNN. Some of these are Deep Neural Network (DNN), Autoencoders, Convolution Neural Network (CNN), Generative Adversarial Network (GAN), and Recurrent Neural Network (RNN).

(i) Deep Neural Networks (DNN):

Deep Learning is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks. It is a neural network with some level of complexity, usually, at least two layers qualify as a deep neural network (DNN), or deep net for short. Deep nets process data in complex ways by employing sophisticated math modeling. Some of the earlier research works carried out on the use of DNNs for fraud detection have used Fisher's discriminant analysis which separates the fraudulent operations away from the normal operations. Some were based on three classification methods i.e., neural networks, logistic regression, and decision tree to build the fraud detecting models. These methods can analyze the credit card history transaction and can detect any fraudulent and suspicious transaction. Other researchers have used DNNs to detect the fraud score in credit card payments and have concentrated on data imbalance, processing, and evaluation to achieve better performance, speed, and accuracy compared to optimized models.

(ii) 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. This can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image and be able to differentiate one from the other. However, it can be used for applying textual data since it is highly adaptable. 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 and 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 (Fu et al, 2016).

(iii) Autoencoders:

An autoencoder is a feed-forward multilayer neural network that reproduces the input data on the output layer. In other words, they are 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 **(Figure 1).**

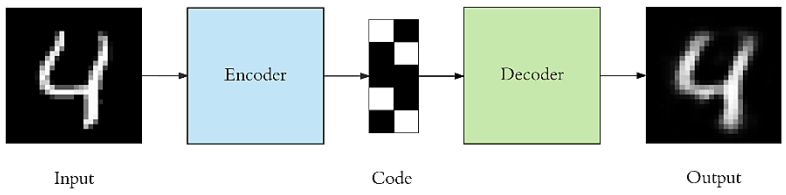

Figure 1 Components of an autoencoder

Some of the applications of autoencoders in fraud detection include Brazilian export systems, frauds in credit card transactions, unusual journal entries, etc. Other applications are Auto-Encoder and Restricted Boltzman Machine to detect fraudulent transactions in real-time in three datasets i.e., German, European, and Australian datasets.

(iv) Recurrent Neural Networks

A recurrent neural network (RNN) is a type of artificial neural network which uses sequential data or time-series data. These deep learning algorithms are commonly used for ordinal or temporal problems, such as language translation, natural language processing (NLP), speech recognition, and image captioning; they are incorporated into popular applications such as Siri, voice search, and Google Translate. Like feedforward and convolutional neural networks (CNNs), recurrent neural networks utilize training data to learn. The RNN is promising in the context of deep learning. RNNs are used for modeling sequential data, such as natural language, speech, and handwritten characters. Using RNN, suitable models can be created which model which uses the patterns in web access logs to detect fraudulent activities. They have applied and evaluated RNN models can be applied and evaluated to recognize fraudulent activities. It is demonstrated that RNN is a better technique than the machine learning techniques like SVMs for learning a non-genuine user's 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 (Yoshihiro Ando et al, 2016).

(v) Generative Adversarial Networks

Generative adversarial networks can be used for translating data from images. GANs 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 that we train to generate new examples, and the discriminator model that tries to classify examples as either real (from the domain) or fake (generated). The two models are trained together in a zero-sum game, adversarial, until the discriminator model is fooled about half the time, meaning the generator model is generating plausible examples. 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 applied to solve the problem of detecting fraudulent credit card transactions (Lebichot et al, 2020).

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.

References

Aisha Abdallah, Mohd Aizaini Maarof and Anazida Zainal. 2016. Fraud detection system: A survey, *Journal of Network and Computer Applications,* 68: 90-113.

Fu K., Cheng D., Tu Y., Zhang L. 2016. Credit Card Fraud Detection Using Convolutional Neural Networks. In: Hirose A., Ozawa S., Doya K., Ikeda K., Lee M., Liu D. (eds) *Neural Information Processing*. *ICONIP 2016. Lecture Notes in Computer Science*, Vol 9949. Springer, Cham. https://doi.org/10.1007/978-3-319-46675-0_53

Lebichot B., Le Borgne YA., He-Guelton L., Oblé F., Bontempi G. 2020. Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection. In: Oneto L., Navarin N., Sperduti A., Anguita D. (eds) *Recent Advances in Big Data and Deep Learning*. INNSBDDL 2019. *Proceedings of the International Neural Networks Society, Vol 1. Springer, Cham.* https://doi.org/10.1007/978-3-030-16841-4_8

Yoshihiro Ando, Hidehito Gomi, Hidehiko Tanaka, Detecting Fraudulent Behavior Using Recurrent Neural Networks, 2016. *Computer Security Symposium 2016*, 11 - 13 October 2016, 805-810.