Fraud Detection using Neural Networks

CREDIT CARD

Today, as the majority of us use credit cards as a form of payment more regularly, credit card fraud is a typical occurrence. This is a result of technological advancements and a growth in online transactions, which have led to frauds that have resulted in enormous financial loss. Consequently, there is a need for efficient ways to lessen the loss. Additionally, scammers find ways to obtain a user's credit card information through calling and sending phoney SMS, as well as by phishing, impersonating, and other attacks.

In all types of businesses, including banks, the automobile and appliance industries, credit card theft occurs. Many methods, including data mining and machine learning algorithmic approaches, are used to spot fraud in credit card transactions, however the results are generally insufficient. Consequently, it is necessary to build effective and efficient algorithms that work considerably. By employing an artificial neural network method and comparing it to a few other machine learning algorithms, we attempt to stop a fraudster from using our credit card before the transaction is approved.

The user or consumer submits the required information to complete any transaction using a credit card, and the transaction should only be approved after being examined for any signs of fraud. This is how credit card fraud is detected. To make this happen, we must first send the transaction data to the verification module, where they are divided into groups for fraud and non-fraud. Any transaction classified as fraud is deemed invalid. If not, the transaction is authorised.

Classifications of credit card frauds

1 **Application fraud** is when a fraudster takes control of the application, steals the customer's login information, creates a phoney account, and then conducts transactions.

2 **Electronic or manual card imprints**: In this type of fraud, the perpetrator steals data from the card's magnetic strip, then uses the credentials to carry out fraudulent transactions.

3 **Card not present**: This is a kind of credit card where the actual card is not present while the transaction is being completed.

4 **Counterfeit card fraud**: This sort of fraud involves copying all of the data from the magnetic strip onto a real card so that it resembles the original card and only functions as the original card. Fraudulent usage of this card.
5 **Lost or stolen card**: This sort of fraud occurs when the cardholder either misplaces or has their card stolen.

6 Card id theft is a sort of fraud in which the cardholder's identity is taken and fraud is committed.

7 **Fraudulent mail delivery of credit cards**: As part of the credit card issuance process, the recipient will get a letter; this is where phishing or fraudulent postal delivery of credit cards can happen.

8 **Account Takeover:** In this scenario, the fraudster will seize total authority over the account holder in order to commit fraud.

9 A malicious code would be introduced by the fraudster to the website to carry out their fake scam.

Here we use the Artificial Neural Network to find the fraud in the credit card transactions. Performance is measured and accuracy is calculated based on prediction. And also classification algorithms such as Support vector machine and k-Nearest Neighbor are used to build a credit card fraud detection model. We compare all the three algorithms used in the experiment and made a decision that artificial neural networks predicts well than system developed using support vector machine and k-nearest neighbor algorithms. The dataset used in the experiment consist of 31 attributes out of which 30 attributes consist of information related to name, age, account information and so on and last attribute give the outcome of the transaction in either 0 or 1.

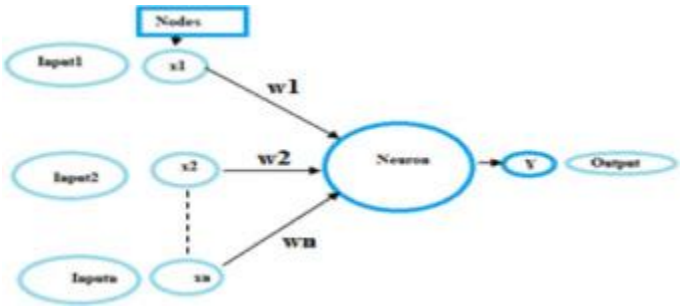

Figure 1: Architecture of Artificial neural network ANN is biologically inspired by human brain. The neurons are interconnected in the human brain like the same nodes are interconnected in artificial neural network.
Figure 1 depicts the structure of ANN with input, output and hidden layers. Inputs are x1, x2…Xn and output is y. w1…wn are the weights associated with inputs x1…xn respectively. There are 15 hidden layers used in this neural network. The activation Asha_Sureshkumar/ Procedia Manufacturing 00 (2019) 000–000 3 function used in our credit card fraud detection model is RELU.

Neural networks are used to match and analyse expenditure patterns, as shown in figure 2. wherein we use a model of a multilayer perceptron neural network, one of the most comprehensive models of an artificial neural system. It is a neuronal mechanism that supports forward movement.
The multilayer perceptron can transmit outputs with more than two classes and features a hidden layer. Planning the hidden layer, i.e., the hidden layers should have enough neurons to understand the information provided and produce two unique classes of output, is one of the most important aspects of a multilayer perceptron. The output will be better if there are fewer neurons in the buried layer.
Using Neuroph Java framework, the Multilayer Perceptron [14] Neural Network is implemented.

The procedures below can be used to deploy a neural network model using Neuroph, which is a fairly simple process.
1. Open Neuroph Studio and import the sample data or historical data.
2. Construct a neural network by selecting one of the numerous models provided by Neuroph (which includes specifying input and output, hidden layer neurons, and transfer functions; we chose sigmoid transfer function and weighted sum).
3. By feeding the model the sample transaction data that has previously been gathered, train it with the proper momentum, learning value, and set an upper limit for network error.
4. Create Java code to test the model and deploy it.
Since the system verifies the user and examines the transaction's nature, it can be used in real time.

Credit card use has become a more common method of payment because to advancements in e-commerce and communication technology, and transaction fraud is also on the rise, according to Altab Althar Taha and Sareef Jameel Malbery.
They employed the optimised light gradient boosting machine, which combines Bayesian-based hyper-parameter optimization with light gradient boosting machine parameter tuning (LightGBM). In this method, two sets of real-world, publicly available datasets, including both fraudulent and non-fraudulent transactions, were employed. Their proposed approach outperformed other techniques in terms of accuracy when compared. Accuracy of 98.40%, area

under the receiver operating characteristics curve (AUC) of 92.88%, Precision of 97.34%, and F1-score of 56.95% are the results of the suggested system [1].
To assess the precision of fraud detection, Debachudamani Prusti and Santhnu Kumar Rath created an application using machine learning techniques such decision trees, the k-nearest neighbour algorithm, extreme learning machines, multilayer perceptrons, and support vector machines. They put up a model by fusing the DT, SVM, and kNN approaches. For effective data interchange across numerous heterogeneous systems, they employed two web-based protocols called Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Based on an accuracy parameter, the results of five machine learning algorithms were compared. SVM outperformed previous algorithms by 81.63%, while their proposed hybrid system had a higher accuracy rate of 82.58% [7].

Weather Forcasting using Neural Networks

Due to chaotic nature of the atmosphere, the massive computational power is required to solve the equations that describe the atmosphere, error involved in measuring the initial conditions, and an incomplete understanding of atmospheric processes. This means that forecasts become less accurate as the difference in current time and the time for which the forecast is being made (the range of the forecast) increases. The use of ensembles and model helps narrow the error and pick the most likely outcome. Several steps to predict the temperature are · Data collection(atmospheric pressure, temperature, wind speed and direction, humidity, precipitation), · Data assimilation and analysis, · Numerical weather prediction, · Model output post processing. A neural network is a powerful data modeling tool that is able to capture and represent complex input /output relationships. The motivation for the development of neural network technology stemmed from the desire to implement an artificial system that could perform intelligent tasks similar to those performed by the human brain. Neural network resemble the human brain in the following two ways: 1) A neural network acquires knowledge through learning. 2) A neural network‟s knowledge is stored within inter-neuron connection strengths known as synaptic weights The true power and advantages of neural networks lies in the ability to represent both linear and non linear relationships directly from the data being modeled. Traditional linear models are simply inadequate when it comes for true modeling data that contains non linear

characteristics. A neural network model is a structure that can be adjusted to produce a mapping from a given set of data to features of or relationships among the data. The model is adjusted, or trained, using a collection of data from a given source as input, typically referred to as the training set. After successful training, the neural network will be capable to perform classification, estimation, prediction, or simulation on new data from the same or similar sources. An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the new structure of the information processing system. It is composed of a huge number of highly interconnected processing elements (neurons) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a particular application, such as pattern recognition or data classification, through a learning process. Learning in biological systems adds adjustments to the synaptic connections that exist between the neurons.

A back propagation network consists of at least three layers (multi layer perception): an input layer, at least one intermediate hidden layer, and an output layer. In contrast to the Interactive Activation and Competition (IAC) neural networks (IAC) and Hop-field networks, connection weights in a back propagation network are one way. Typically, input units are connected in a feed-forward fashion with input units fully connected to units in the hidden layer and hidden units fully connected to units in the output layer. An input pattern is propagated forward to the output units all the way through the intervening input-to-hidden and hidden-to output weights when a Back Propagation network is cycled. As the algorithm's name gives a meaning, the errors (and therefore the learning) propagate backwards from the output nodes to the inner nodes. So technically it can be explained, back propagation is used to calculate the gradient of the error of the network with respect to the network's modifiable weights. This gradient is always used in a simple stochastic gradient descent algorithm to find weights that minimize the error. Frequently the term "back propagation" is used in a more general sense, to refer to the entire procedure encompassing both the calculation of the gradient and its use in stochastic gradient descent. Back propagation regularly allows quick convergence on satisfactory local minima for error in the kind of networks to which it is suited. The proposed Temperature Prediction System using BPN Neural Network is tested using the dataset. The results are compared with practical temperature prediction results. This system helps the meteorologist to predict the future weather easily and accurately.