Credit Card Fraud Detection Using Perceptron Training Algorithm and Prevention Using One Time Password

Prof. Gajanan Bherde[#1], Ashwin Telang[#2], Mehul Bhuva[#3], Harsh Gajra[#4], Ajit Patel[#5]

[#]*Computer Department, KJ Somaiya College of Engineering, Vidyavihar- Mumbai University*
KJ Somaiya College of Engineering, Vidyavihar, Mumbai, India

[1]gajananbherde@somaiya.edu
[2]ashwin.t@somaiya.edu
[3]mehul.bhuva@somaiya.edu
[4]harsh.gajra@somaiya.edu
[5]ajit.patel@somaiya.edu

Abstract— In today's world with evolving technologies and a new mode of shopping through online website, use of credit card has increased day by day. Since the credit card is more prone to fraud than debit card prevention of fraud is an important aspect. This paper will discuss about our approach in credit card fraud detection and its prevention using perceptron training algorithm as detection algorithm and one time password as the prevention of such fraud.

Keywords— *Neural Network, Perceptron, One Time Password, Transaction pattern, Attributes.*

*****

I. INTRODUCTION

In today's world due to increase in the use of credit card in online payment where the user of the credit card is not easily identified, credit card fraud detection becomes the primary goal. Credit card fraud is increasing day by day because of increasing online shopping and other online activities which include credit card as online payment option. There are various ways in which credit card fraud can take place of which most of the times the credit card fraud happens in online transaction. Since in online transaction the location of the fraud user can't be easily traced if the user changes the location by using any type of browser or any other tool, credit card fraud in online transaction is increasing day by day.

Considering this and its prevention technique we have developed a system which works on perceptron training algorithm and the desired output is given as fraud or not fraud on the basis of the transaction inputs which are called as transaction pattern.

Once fraud has been detected one time password is sent to the user and then user has to enter the password to proceed with the transaction. Once all the process gets over the entire transaction pattern is recorded along with the final result and stored in the database to improve our dataset. This paper will discuss the perceptron training algorithm and the one time password as the fraud prevention technique used in our application.

Abbreviations

OTP	One Time Password
SMTP	Simple Mail Transfer Protocol
DND	Do Not Disturb
API	Application Programming Interface

II. ARCHITECTURE OF FRAUD DETECTION SYSTEM

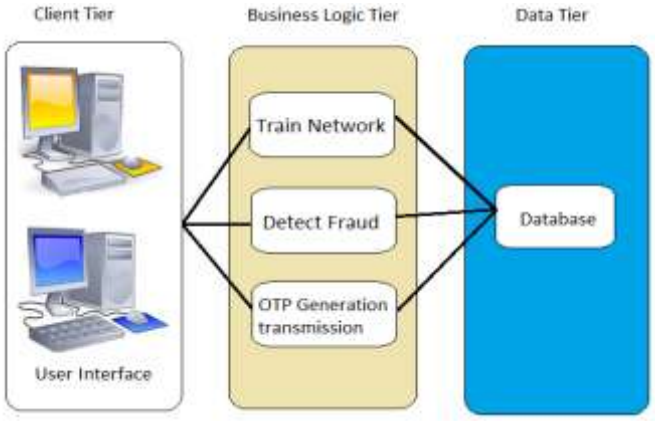

Fig. 1.0 Architecture of Fraud Detection System.

The Architecture of the system is Multitier/N-Tier which is client–server architecture. In this architecture presentation, application processing, and data management functions are physically separated. The Data Tier consists of databases which consist of data of registered users, the training dataset, OTP generated for users, etc. The Business Tier consists of training module, detection module and OTP Module which consist of all the business logic used to detect and prevent fraud. These modules are connected to the database for retrieving and updating the data during processing. We have used java swing as user interface implementation and the Client Tier consists of users who access the system.

A. Training a neuron.

For the dataset which we have considered, we would train our network according to the algorithm mentioned below so that our system can detect the fraud for new transactions

 ISSN: 2321-8169
2069 - 2071

pattern. In training of a neuron, the algorithm is applied to each dataset and weights are updated accordingly. Updated weights are then stored in the database so that they can be used in detection of fraud. Following algorithm was used in training a neuron:

1. *Perceptron Training Algorithm:*

Perceptron training algorithm is supervised training algorithm used to train the neuron in neural network. Being supervised algorithm it needs to be provided with the target output.

In perceptron training algorithm, neuron is provided with target output along with the input values. Once the actual output is calculated it has actual output and target output which are to be compared and trained the network accordingly. Each input is connected to the neuron with a link which has some weight. In training, we modify these weights so that the networks get trained.

Below is the example of a neuron with inputs as $x1$, $x2$, $x3$, weights as $w1$, $w2$, $w3$ target (destination) output Do and actual output Ao.

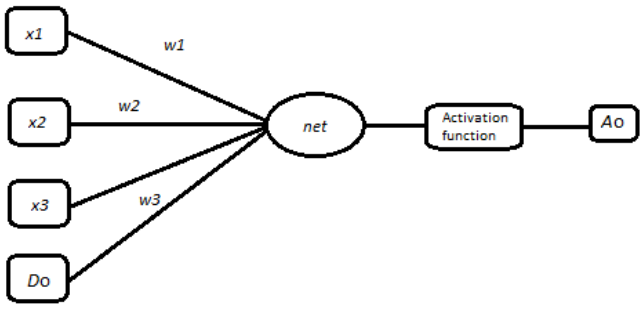

Fig. 1.1 Perceptron Network Consisting Of One Neuron.

For the above Perceptron network net is calculated in transfer function as:

$$net = x1 \times w1 + x2 \times w2 + x3 \times w3$$

Now inside the activation function we have used bipolar binary activation function to calculate actual output as below

If net < threshold Ao=-1 else Ao=1

Now if expected output i.e. Do==Ao no training is required else according to perceptron training algorithm the new weights are calculated as follows:

$w1 = w1 + \alpha \times (Ao - Do) \times x1$

$w2 = w2 + \alpha \times (Ao - Do) \times x2$

$w3 = w3 + \alpha \times (Ao - Do) \times x3$ where α is perceptron learning rate.

Now these weights are used as initial weights for next entry in dataset and similarly the training proceeds till the network is trained with all the entries in the dataset. Thus the entire network gets trained for all the values present in dataset and can be used for detection of fraud.

B. Detection of fraud.

Once the network gets trained it can be used to detect the fraud. During detection we have to just provide the network with the input values which are nothing but the transaction pattern which consist of various attributes such as amount transacted, card provider, bank type, site where the card is used for transaction employment status of the card holder, gender of the card holder, overdraft balance of the card holder. Once we provide the network with the input values the network will calculate the output as follows:

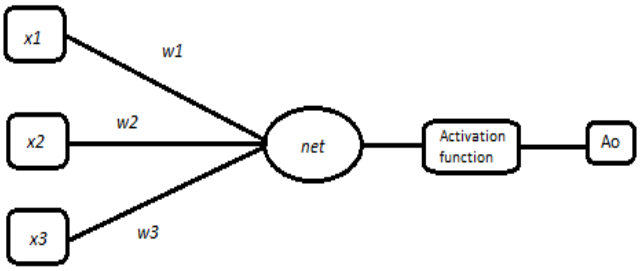

Fig. 2.0 Detection of fraud using Perceptron.

For the above network we calculate net using below formula and the weights of the link $w1$, $w2$, $w3$ are the final weights which were calculated in the training module after applying all entries of our dataset.

$$net = x1 \times w1 + x2 \times w2 + x3 \times w3$$

Now if net < threshold Ao=-1 else Ao=1 where Ao=-1 means that the transaction pattern was legitimate transaction pattern and Ao=1 means that the transaction pattern was fraudulent transaction pattern.

C. One Time Password.

One time password is a technique of detecting fraud users by giving the confirmation code or a password which is valid for short period of time and is sent to the user either to his registered mail or registered mobile number.

In our system we will use one time password technique to confirm whether the transaction pattern detected as fraud is really fraud or not. Sometime it may happen that the user might use a transaction pattern which seems to be fraudulent but is not. So we will use OTP confirmation and based on the result we would add the pattern as fraud or legitimate in our dataset.OTP is generated using industrial standards for OTP generations.

There are two options to send an OTP to the users:

1. OTP via SMS.

In OTP via SMS we will send the OTP to the user to its mobile number registered with us at the time of registration, as a SMS. Since people carry their mobile all the time it's the most convenient way to send the OTP. Use of SMS gateway is done while sending the SMS to the user.

2. OTP via Email.

In OTP via Email a mail will be sent to the user to its email id registered with us at the time of registration, which

contains the one time password. In this we have to setup a SMTP server then we have to get the session object. Session object is used for authentication of the username and password then using the session object we can compose a mail and send the mail to the user mail id.

Comparison of both the method

Details	OTP using SMS	OTP using Email
Transmission delay	Less, usually depends on SMS gateway	Depends on traffic at SMTP server.
Availability	Might fail if DND is activated.	It will reach to the user at any cost
Security	SMS will be sent to the registered number only.	Most secured as user should be logged in to view OTP

D. Workflow of the Fraud detection system

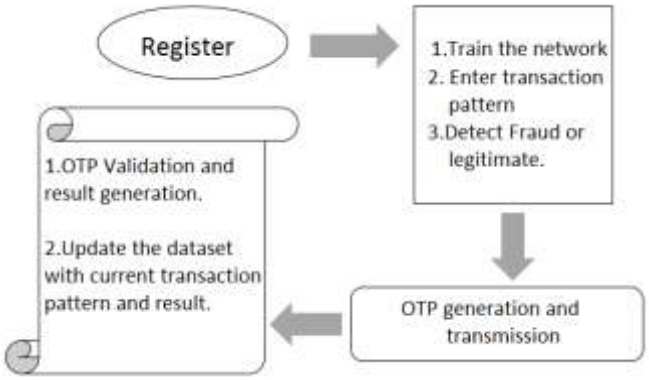

Fig. 3.1 Workflow diagram for fraud detection system.

As shown in above diagram workflow of our system will be as follows:
1. User logs in to the system.
2. User registers with the system if he is new user else proceeds to next step.
3. System undergoes training and weights are generated.
4. User enters the transaction pattern and the results are calculated according to the algorithm.
5. If the result is fraud then the OTP is sent to the user and then the OTP validation takes place.
6. If OTP is validated successfully the transaction is legitimate else the transaction is fraudulent.
7. Database is updated with the new transaction pattern and the result.

E. Experimental Results.
We have implemented the system for various dataset using netbeans8.0 on the computer with 2 GB ram 2.4 GHz processor and the following results were obtained:

1. Execution time: Registration module runs for 2 seconds. Training module runs for 30 seconds. Detection module runs for 5 seconds. OTP module runs for 75 seconds and maximum of 90 seconds if internet connectivity is weak.

2. Accuracy: Our system gives accuracy of up to 73.5% in many cases studied.

3. Availability: Due to use of both the OTP transmission system our system availability has increased because OTP transmission is done using both email and SMS.

III. Conclusions

The paper proposes the use of neural network's perceptron training algorithm in credit card fraud detection and prevention. We have detected the fraud transaction pattern on the basis of the users transactions input and also we have implemented the one time password as the prevention algorithm. On validation of the OTP the transaction will be distinguished as fraudulent or legitimate and similarly dataset will be updated.

Acknowledgment

This work is a part of B.E project on "Credit Card Fraud Detection and Prevention" under guidance of Professor Gajanan Bherde, Asst. Professor of K.J Somaiya College of Engineering-Computer Department, Vidyavihar-Mumbai.

References

[1] Payment Card Fraud: Challenges and Solutions Irina Sakharova The University of Texas at Dallas Richardson, Texas, USA 2012 IEEE Publications
[2] Profiling intelligent systems applications in fraud detection and prevention. Faculty of Economics & Business. University of Zagreb
Zagreb, Croatia 2010 IEEE Publications
[3] Detecting Credit Card Fraud by ANN and Logistic Regression By Y. Sahin Marmara University and E. Duman Dogus University 2011 IEEE Publications