Credit card fraud detection using neural network and geolocation

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042039 doi:10.1088/1757-899X/263/4/042039

Credit card fraud detection using neural network and geolocation

Aman Gulati, Prakash Dubey, MdFuzailC, Jasmine Norman and Mangayarkarasi R

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: jasmine@vit.ac.in

Abstract. The most acknowledged payment mode is credit card for both disconnected and online mediums in today's day and age. It facilitates cashless shopping everywhere in the world. It is the most widespread and reasonable approach with regards to web based shopping, paying bills, what's more, performing other related errands. Thus danger of fraud exchanges utilizing credit card has likewise been expanding. In the Current Fraud Detection framework, false exchange is recognized after the transaction is completed. As opposed to the current system, the proposed system presents a methodology which facilitates the detection of fraudulent exchanges while they are being processed, this is achieved by means of Behaviour and Locational Analysis(Neural Logic) which considers a cardholder's way of managing money and spending pattern. A deviation from such a pattern will then lead to the system classifying it as suspicious transaction and will then be handled accordingly.

1.Introduction

1. Credit card fraud is a sort of burglary or unapproved action to make instalment utilizing Visa as a part of an electronic instalment framework. The motivation behind credit card fraud is to get cash or make instalment without proprietor consent. It includes illicit utilization of card or card data without the proprietor consent however it is a criminal trickiness and banned by laws. In light of the technology innovation and software's, clients can shroud their personality and areas while submitting any exchange over the web, which expands the misrepresentation over the web.This paper gives the knowledge about various sorts of techniques used by the frauds and proposes a method to overcome it.

2. The various frauds are carried out as stolen cards, application misbehaviour, taking over accounts, Magnetic strip manipulation, fake cards and so on. The trend of these kinds of frauds is ever increasing. In the research filed, some techniques have been proposed to identify the frauds. Most of the methods are based on artificial intelligence and machine learning. The survey and analysis of credit card fraud detection can be found in [1-3]. The hidden markov model implementation could be found in [4-6]. In [7-9] authors have used neural network and Bayesian learning to detect credit card frauds. Evolutionary techniques and genetic algorithm is used in [10-12] for the same. This paper

addresses stages required in building artificial neural networkstructure for the problem. It is a challenge to perfectly predict the online transaction fraud, as no method can exactly suspect that the present transaction is fraudulent and is being carried out by an impostor. An impressive Fraud detection system should be able to do the following:

3. 1. Should distinguish the illegitimate transactions quickly.

4. 2. Should not consider legitimate customer as an impostor.
Most of the work related to credit card fraud detection is done after the crime is committed. In this paper a method to detect the fraud during transaction is proposed. The implementation results show 80% accuracy. Since it is based on consumer's behaviour, the system suggests a fraud when the consumer deviates from his regular pattern.

2. Classification of Credit Card Frauds

There are three classes of frauds in particular: card related, dealer related and web related. Some of them are recorded underneath

2.1.Card Related Frauds

1. Application Frauds: This sort of extortion happens when the fraudster controls the application by picking up someone else's sensitive data opens a fake account in his name.
2. Stolen Card: This sort of extortion happens when the impostor essentially takes a client's card. For this situation, the client may feel he has lost his card, all things considered his card may have been procured by an impostor.

2.2. Dealer Related Frauds

1. **Merchant Collusion**: This sort is done when a Dealer deliberately passes on his client's sensitive data to fraudsters.
2. **Triangulation**: In such fraud cases the fraudster poses as a dealer and indices the customer with deals and offers that are sure to get their attention, once the customers get interested and buy something all the payment details are then recorded by the fraudster and is then used to perform illegal transactions.

2.3 Web Frauds

1. **False Merchant Sites**: This can more or less be defined as a phishing attack where the fraudster makes a fake Webpage usually similar to that of Numerous known websites in a certain country and then offers various discounts in order to get the customer to buy products once the customers buy a given product on the website all the transaction information is collected and the fraudster then uses this information to perform ill-conceived exchanges.
A portion of the most recent sorts of credit card cheats are as takes after:

1. **Keystroke Loggers**: "Keystroke logger" is a spyware which corrupts a client's PC observes every single keystroke made by the user. This spyware tracks every one of the points of interest wrote by the client and gives this data to the fraudster.

2. **Cell Phone Camera Scam**: When a client is paying his bills, a fraudster might wander some place close to him. The client might be under the supposition that the aggressor is occupied with talking on

his smartphone, in any case he is taking pictures of the client's subtle elements, for example, card number, expiry date, and so forth. This is conceivable on account of cameras utilized nowadays

3. System Model

The proposed system does a job of classifying the transactions into one of the two types:
1. Suspicious Transaction
2. Non-Suspicious Transaction
The classification of transaction is done using the following algorithm as depicted in figure 1.
The system checks the location and the pattern of spending as the major parameters to decide a spurious transaction. If there is a mismatch in the location or the pattern, the system marks it as suspicious and subjects the transaction through a verification process. The verification could be any process such as alerting the user, calling the user or subject the user to go through another round of clearance such as OTP. If the transaction is valid, then the details are updated for the user. After verification if the system fails to identify the user, the transaction is declined. Since the accuracy depends on location and pattern, it is possible to get false alarms and a valid user may be subjected through verification process. It is also possible that the system could decline a valid transaction.

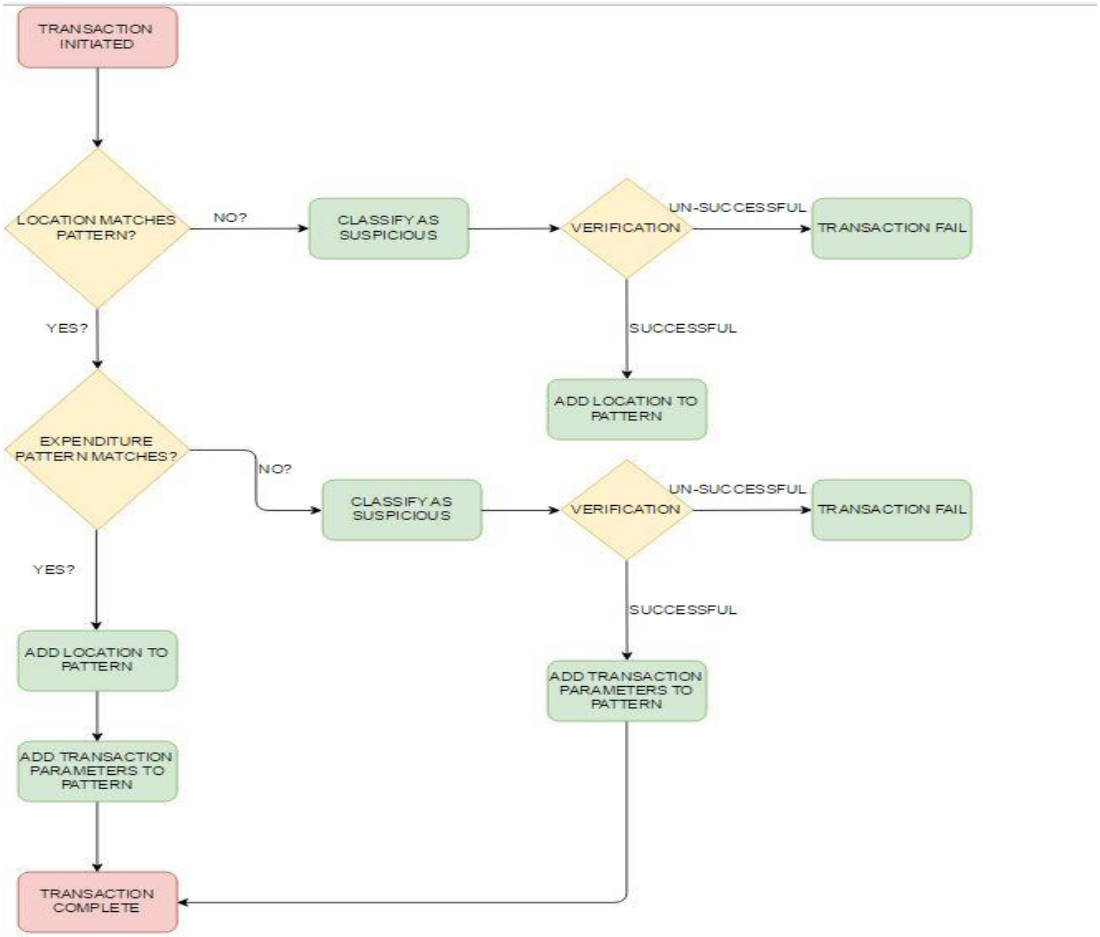

Figure. 1 System Model

4. Results

The location analysis uses a public ip lookup api to verify the location of the targeted user initiating the transaction and if the location is not found in the user pattern the transaction is then classified as suspicious and passed on to bank for appropriate handling and verification. In case the verification turns out to be successful the new location is then incorporated in the pattern so that the next time the customer initiates a transaction from the same place it passes of as a non-suspicious transaction.
The Geo-location analysis is achieved using the W3C'S standard[13] geo-location API from Erukaapi (GEO-LOCATOR) services/ipinfo.io/freegioip.net.

The api syntax is freegeoip.net/{format}/{IP_or_hostname}

The Expenditure pattern matching and analysis is done and achieved used neural networks as in figure 2. where in, we employ the Multilayer perceptron neural network model, which is a standout amongst the hugest models of artificial neural systems. It is a bolster forward directed kind of neural system. The multilayer perceptron has a concealed layer and can convey outputs with more than two classes. A standout amongst the most vital parts of multilayer perceptron is planning the concealed layer i.e. the hidden layers should contain adequate neurons to comprehend the information included and create two distinct classes of output. Lesser the number of neurons in the hidden layer, better the output will be.
The Multilayer perceptron [14] neural network is implemented using Neuroph java framework. Neuroph is lightweight Java neural system structure to create regular neural system designs. It contains all around planned, open source Java library with a number of fundamental classes which relate to essential Neural Network ideas. In this work the data is taken from Uci Machine Learning Repository and the sample data used is presented below in table 1.Figure 3 gives the output model.

Procedure:
Deploying a neural network model using Neuroph is fairly easy and can be achieved in the following steps:
1. Import the historical data or the sample data in Neuroph Studio
2. Create a Neural Network by choosing from the many models given in Neuroph(includes Specifying input and output and hidden layer neurons and transfer functions, we chose sigmoid transfer function and weighted sum)
3. Train the model with the appropriate momentum, learning value and set an upper limit for network error by feeding it the sample transaction data already collected.
4. Test the model and Deploy by generating JAVA CODE.

The system can be implemented in real time as its checks the nature of transaction and validates the user. It is possible for the system to raise false alarms based on location and different expenditure pattern. Also when a new user uses the card, the system will fail as it predicts based on the past behaviour.

CustomerID	Service Area	Account Description	Creditor	Transaction Date	JV Reference	JV Date	JV Value
11034	Childrens Services	Equipment and Materials Purcha	BQ	29-04-2014	358	20-05-2014	2.48
11034	Childrens Services	Equipment and Materials Purcha	HOMEBASE LTD 8	23-04-2014	151	20-05-2014	3.58
11034	Deputy Chief Operating Officer	Equipment and Materials Purcha	KAGI 1-51-42-5858	25-04-2014	155	20-05-2014	31.66
11034	ChildrensServices	Food Costs	MCDONALDS REST	22-04-2014	188	20-05-2014	9.38

11034	Childrens Services	Food Costs	ASDA HOME DELIVERY	17-06-2014	972	16-07-2014	209.1
11034	Childrens Services	Building Repairs & Maintenance	HOMEBASE LTD 24	16-06-2014	1243	16-07-2014	9.67
11034	Childrens Services	Travelling Expenses	LUL TICKET OFFICE.	01-07-2014	1071	16-07-2014	10
11034	Childrens Services	Consumable Catering Supplies	REYNARDS UK LTD	20-06-2014	955	16-07-2014	387.79
11034	Childrens Services	Equipment and Materials Purcha	SAINSBURYS S/MKTS	19-06-2014	1174	16-07-2014	6
11034	Childrens Services	Equipment and Materials Purcha	TECHNO-VISION SYSTE	16-06-2014	1110	16-07-2014	72
11034	Childrens Services	Other Services	MCDONALDS REST	01-08-2014	1447	19-08-2014	9.34

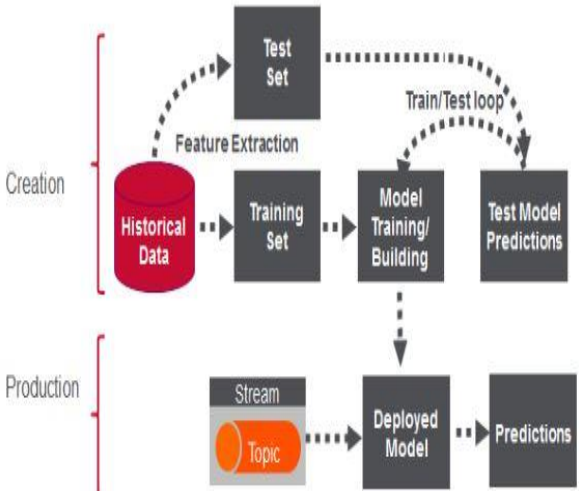

Figure 2: Neural Network Model

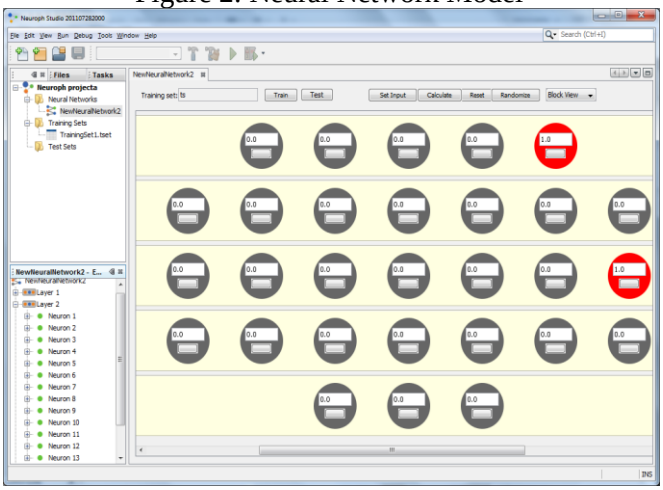

Figure 3: The output model

5. Conclusion

In this paper, we present a credit card fraud detection system which works on neural networks seem to detect up to 80% accuracy with sample transaction data(real data results may vary by a little difference) but it also has a drawback i.e., the system will not be able to identify the fraud exchanges/transactions if the impostor is a new user in the bank because one of the pre-requisites for a neural network to work is having a lot of data to chew through since without the initial data input feed the neural networked cannot be trained or deployed.

References

[1] Linda Delamaire, Hussein Abdou and John Pointon 2009 Credit card fraud and detection techniques: a review *Banks and Bank Systems 4(2)*
[2] Benson Edwin Raj S and Annie Portia A 2011 Analysis on Credit Card Fraud Detection Method *Int. Conf. on Computer, Communication and Electrical Technology – ICCCET2011*
[3] Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick 2012 A review of Fraud Detection Techniques: Credit Card *Int.J. of Computer Applications* (0975 – 8887) **45**
[4] Abhinav Srivastava, AmlanKundu, Shamik Sural and Arun K. Majumdar 2008 Credit Card Fraud Detection using Hidden Markov Model. *IEEE Transactions on dependable and secure Computing* **5** 37-48
[5] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent Detection *Int. J. of Computer Applications* **20**
[6] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent Detection.*Int. J. of Computer Applications*. **20**
[7] AmlanKundu, SuvasiniPanigrahi, Shamik Sural and Arun K Majumdar 2009 Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning *Special Issue on Information Fusion in Computer Security* **10** 354- 363
[8] RaghavendraPatidar and Lokesh Sharma 2011 Credit Card Fraud Detection Using Neural Network, *International Journal of Soft Computing and Engineering*
[9] RamaKalyani K and UmaDevi D 2012 Fraud Detection of Credit Card Payment System by Genetic Algorithm *Int. J. of Scientific & Engineering Research* **3(7)**
[10] EkremDuman, and HamdiOzcelik M 2011 Detecting credit card fraud by genetic algorithm and scatter search *Elsevier, Expert Systems with Applications* 38
[11] Brabazon A, Cahill J, Keenan P and Walsh D 2010 Identifying Online Credit Card Fraud using Artificial Immune Systems *IEEE Congress on Evolutionary Computation (CEC).*
[12] Pejic, Bojan, AleksandarPejić and Zlatko Covic 2010 Uses of W3C's Geolocation API."Computational Intelligence and *Informatics (CINTI) International Symposium on IEEE*
[13] Gardner, Matt W., and S. R. Dorling 1998 Artificial neural networks (the multilayer perceptron)— a review of applications in the atmospheric sciences *Atmospheric environment* **32** 2627-2636