ISSN (Print) : 2320 – 9798
ISSN (Online) : 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Fraud Detection in Credit Card System Using Web Mining

Hetvi Modi[1], Shivangi Lakhani[2], Nimesh Patel[3], Vaishali Patel[4]

Student, Information Technology, Shri S'ad Vidhya Mandal Institute of Technology, Bharuch, India[1,2,3]
Lecturer, Information Technology, Shri S'ad Vidhya Mandal Institute of Technology, Bharuch, India[4]

Abstract: Now a day the usage of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. Various techniques like classification, clustering and apriori of web mining will be integrated to represent the sequence of operations in credit card transaction processing and show how it can be used for the detection of frauds. Initially, web mining techniques trained with the normal behaviour of a cardholder. If an incoming credit card transaction is not accepted by the web mining model with sufficiently high probability, it is considered to be fraudulent. At the same time, the system will try to ensure that genuine transactions will not be rejected. Using data from a credit card issuer, a web mining model based fraud detection system will be trained on a large sample of labelled credit card account transactions and tested on a holdout data set that consisted of all account activity. Web mining techniques can be trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, and mail-order fraud. The proposed system will be able to detect frauds by considering a cardholder's spending habit without its significance. Usually, the details of items purchased in individual transactions are not known to any Fraud Detection System. The proposed system will be an ideal choice for addressing this problem of current fraud detection system. Another important advantage of proposed system will be a drastic reduction in the number of False Positives transactions. FDS module of proposed system will receive the card details and the value of purchase to verify, whether the transaction is genuine or not. If the Fraud Detection System module will confirm the transaction to be of fraud, it will raise an alarm, and the transaction will be declined.

Keywords: Transaction, Technique, Fraud Detection, Verify

I. INTRODUCTION

Web mining is the use of data mining *techniques* to automatically discover and extract information from web documents and services. Web mining is the application of data mining techniques to discover patterns from the Web. Web mining can be divided into three different types, which are Web usage mining, Web content mining and Web structure mining.

Fraud is an intentional deception made for personal gain or to damage another user/individual is fraudulent. Legal definition varies by legal jurisdiction for fraud. Fraud is a civil law violation and also a crime. Defrauding people or entities of money is a common purpose of fraud.

Credit card is a medium of selling goods or services without having cash in hand. A credit card is a simple way of offering credit to a consumer automatically. Credit card carries an identifying number that helps in shopping *transactions* rapidity.

Credit card is a medium of selling goods or services without having cash in hand. A credit card is a simple way of offering credit to a consumer automatically [2].Credit card carries an identifying number that helps in shopping transactions rapidity. Credit card *fraud detection* is the process of identifying those transactions that are fraudulent into two classes of legitimate and fraudulent transactions. The credit card *fraud detection* system developed used four clusters of low, high, risky and high risk. Once the transaction is legitimate, it was processed but if any *transaction* falls into any of these clusters it was labelled as suspicious/fraudulent. The alert goes off and the reason is given. The fraudulent *transaction* will not be processed but will be committed to the database. Fraud is an intentional deception made for personal gain or to damage another user/individual is fraudulent. Legal definition varies by legal jurisdiction for fraud [1] [2]. Fraud is a civil law violation and also a crime. Defrauding people or entities of money is a common purpose of fraud.

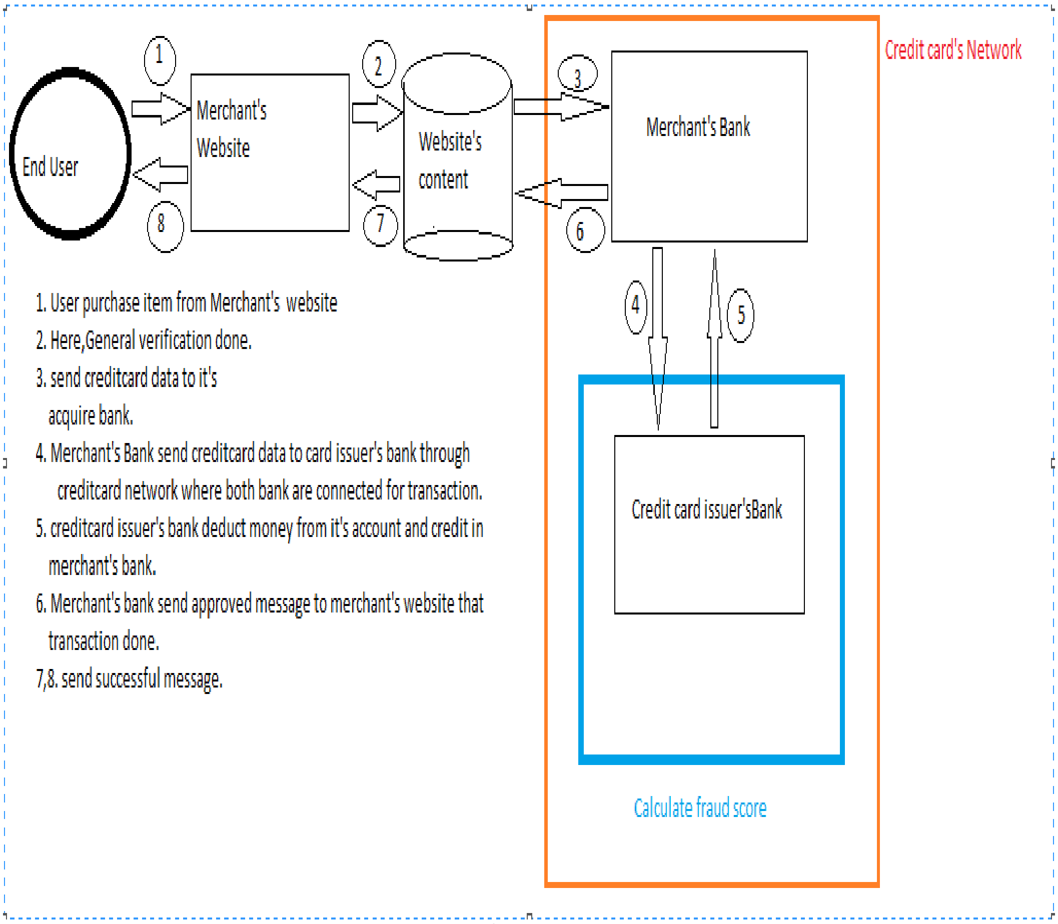
II. RELATED WORK

Various techniques like classification, clustering and association of web mining will be integrated to represent the sequence of operations in credit card transaction processing and show how it can be used for the detection of frauds. Initially, web mining techniques trained with the normal behaviour of a cardholder. If an incoming credit card transaction is not accepted by the web mining model with sufficiently high probability, it is considered to be fraudulent. At the same time, the system will try to ensure that genuine transactions will not be rejected. Web mining techniques can be trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, and mail-order fraud [6].

Using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labelled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (Non-Received Issue) fraud. The network detected significantly more fraud accounts with significantly fewer false positives over rule-based fraud detection procedures. There are several fraud detection technology exist based on Data mining, Knowledge Discovery and Expert System [6][7]. All these are not capable enough to detect the fraud at the time because there are many fraudulent transactions are in progress due to very less chance of a transaction being fraudulent.

III. PROPOSED TECHNOLOGY

There are many ways in which fraudsters execute a credit card fraud. As technology changes, so does the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. Frauds can be broadly classified into three categories traditional card related frauds, merchant related frauds and Internet frauds.



1. User purchase item from Merchant's website
2. Here,General verification done.
3. send creditcard data to it's acquire bank.
4. Merchant's Bank send creditcard data to card issuer's bank through creditcard network where both bank are connected for transaction.
5. creditcard issuer's bank deduct money from it's account and credit in merchant's bank.
6. Merchant's bank send approved message to merchant's website that transaction done.
7,8. send successful message.

Figure 1 Flow of Credit Card Transaction

There are many different kinds of neural networks and neural network algorithms. The most popular neural network algorithm is back propagation. In back propagation, Multilayer feed Forward Algorithm used to detect fraud in credit card system**.** The field of neural networks was originally kindled by psychologists and neurobiologists who sought to develop and test computational analogues of neurons. Back propagation is a common method of training artificial neural networks so as to minimize the objective function.

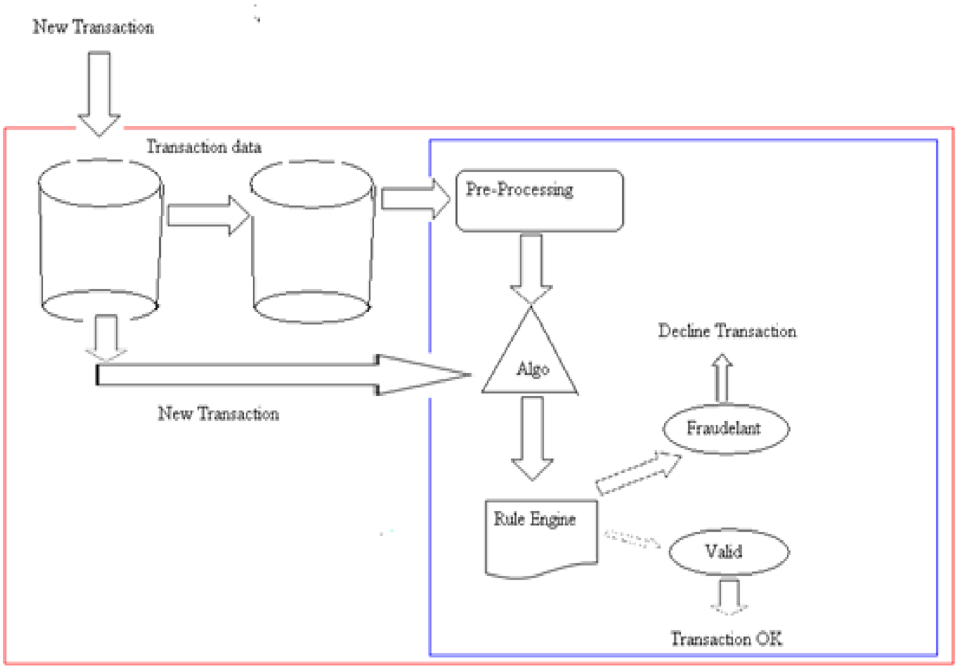


Figure 2 Fraud Detection Systems

IV. IMPLEMENTATION

The proposed work has been implemented in Net beans IDE 7.1.2. Some Patterns is given as the input. Once the errors are found reduction would be done based on Sigmoid. Used single layer feed forward algorithm using random patterns. Here, Inserted Random pattern for train network. For example inserted pattern are given in below table.

TABLE 4.1 Input Patterns

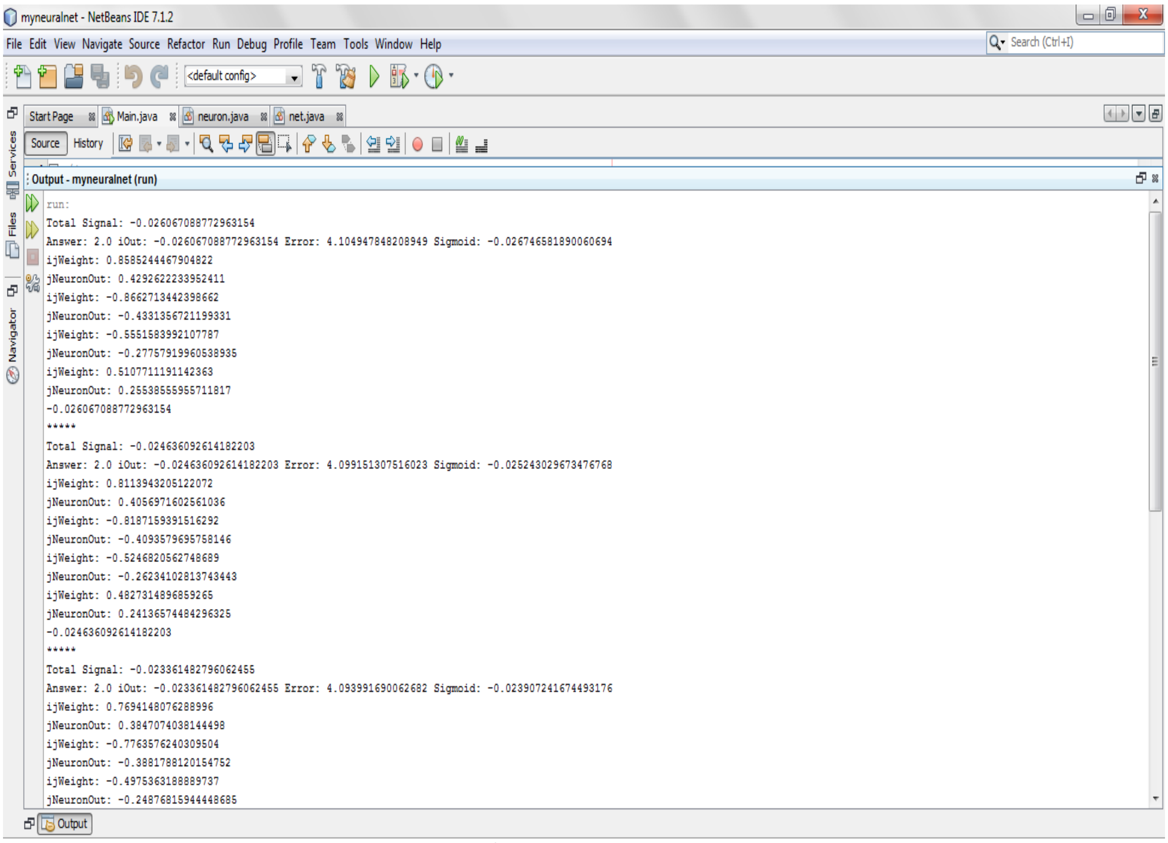
Patterns
10.0,11.0,24.0,23.0
24.0,34.0,23.0,13.0
11.0,61.0,24.0,28.0

Our system perform single layer feed forward neural network algorithm and predict the error. Assume & Consider any rth output neuron and for the training example we have calculated the output 'O' for which the target output 'T' Hence, the error norm in output for the rth output neuron is given by $E_r^1 = 1/2\ e_r^2 = 1/2\ (T\text{-}O)^2$ The Euclidean norm of error E^1 for the first training pattern is given by $E^{1\,=}\ 1/2 \sum (T_{or} – O_{or)})^2$. If we use the same technique for all the training patterns, we get E (V, W) = $\sum E^j$ (V, W, I) Where E is the error function depending on the m (1+n) weights of [W] and [V].

TABLE 4.2 Result Analysis

Patterns	10.0,11.0,24.0,23.0	24.0,34.0,23.0,13.0	11.0,61.0,24.0,28.0
Total signal	-0.026067088772963	-0.0246360926141822	-0.0233614827960624
Answer	2.0	2.0	2.0
Output	-0.026067088772963	-0.024636092614182	-0.023361482796062
Error	4.104947848208949	4.099151307516023	4.093991690062682
Sigmoid	-0.0267465818900606	-0.0252430296734767	-0.0239072416744931
Ijweight	0.8585244467904822	0.8113943205122072	0.7694148076288996
Jneuronoutput	0.4292622233952411	0.4056971602561036	0.3847074038144498
Ijweight	-0.8662713442398662	-0.8187159391516292	-0.7763576240309504
Jneuronoutput	-0.4331356721199331	-0.4093579695758146	-0.3881788120154752
Ijweight	-0.5551583992107787	-0.5246820562748689	-0.4975363188889737
Jneuronoutput	-0.2775791996053893	-0.262341028137434	-0.2487681594444868
Ijweight	0.5107711191142363	0.4827314896859265	0.4577561696988996
Jneuronoutput	0.25538555955711817	0.24136574484296325	0.2288780848494498
Final output If(error<tolerance)	-0.0260670887729631	-0.0246360926141822	-0.0233614827960624

The Screenshots of the implemented system


myneuralnet - NetBeans IDE 7.1.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
<default config>
Start Page
Main.java
neuron.java
net.java
Source
History
Services
Files
Navigator
Output - myneuralnet (run)
Output

```
run:
Total Signal: -0.026067088772963154
Answer: 2.0 iOut: -0.026067088772963154 Error: 4.104947848208949 Sigmoid: -0.026746581890060694
ijWeight: 0.8585244467904822
jNeuronOut: 0.4292622233952411
ijWeight: -0.8662713442398662
jNeuronOut: -0.4331356721199331
ijWeight: -0.5551583992107787
jNeuronOut: -0.27757919960538935
ijWeight: 0.5107711191142363
jNeuronOut: 0.25538555955711817
-0.026067088772963154
*****
Total Signal: -0.024636092614182203
Answer: 2.0 iOut: -0.024636092614182203 Error: 4.099151307516023 Sigmoid: -0.025243029673476768
ijWeight: 0.8113943205122072
jNeuronOut: 0.4056971602561036
ijWeight: -0.8187159391516292
jNeuronOut: -0.4093579695758146
ijWeight: -0.5246820562748689
jNeuronOut: -0.26234102813743443
ijWeight: 0.4827314896859265
jNeuronOut: 0.24136574484296325
-0.024636092614182203
*****
Total Signal: -0.023361482796062455
Answer: 2.0 iOut: -0.023361482796062455 Error: 4.093991690062682 Sigmoid: -0.023907241674493176
ijWeight: 0.7694148076288996
jNeuronOut: 0.3847074038144498
ijWeight: -0.7763576240309504
jNeuronOut: -0.3881788120154752
ijWeight: -0.4975363188889737
jNeuronOut: -0.24876815944448685
```

Figure 3 Output of Single Layer Feed Forward Algorithm

Effect of Learning Rate ‘η’

Learning rate coefficient determines the size of the weight adjustments made at each iteration and hence influences the rate of convergence. Poor choice of the coefficient can result in a failure in convergence. We should keep the coefficient constant through all the iterations for best results. If the learning rate coefficient is too large, the search path will oscillate and converges more slowly than a direct descent.

Table 4.3**:** Non-linear Activation function

Type	**Equation**
Linear	$O = gI, g=\tan\Phi$
Piece Wise Linear	1 if $mI>1$, $O = gI$ if $\lvert mI<1 \rvert$ -1 if $mI>-1$
Hard Limiter	$O = \mathrm{sgn}[I]$
Unipolar Sigmoid	$O = 1/(1+\exp^{(-\gamma I)})$
Bipolar Sigmoid	$O = \tanh[\gamma I]$
Unipolar Multimodal	$O=1/2[1+1/M\sum\tanh(g^m(I-W_o{}^m))]$
Radial Basis Function	$O = \exp(I)$

V. CONCLUSION AND FUTURE WORK

The detection of credit card fraud mechanism and examine the result based on the principles of this algorithm. Neural network's single layer feed forward neural network algorithm that are being used to execute credit card fraud how credit card fraud impact on financial institution as well as merchant and customer, fraud detection. Further work, to study in more detail about the neural network and their role in fraud detection and combine this approach with feature back propagation algorithms to smoothly handle data of different feature types and detect the errors in large amount of transaction of credit card system. If this algorithm is applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions by the banks. The advantages neural networks offer over other techniques is that these models are able to learn from the past and thus, improve results as time passes. They can also extract rules and predict future activity based on the current situation. By employing neural networks effectively, banks can detect fraudulent use of a card, faster and more efficiently. Fraud detected and fraud transactions are generated with the sample data set or patterns.

ACKNOWLEDGEMENT

Before penning a single word for the Paper, we take this opportunity to thank Mrs. Vaishali Patel bottom of our heart who guided us as much as possible and for giving us valuable information regarding the paper. This was our first professional step toward the high careers in IT field. It was a great experience of exposing as well as learning lot of new things in Information Technology. We are indebted to all those who provided reviews our tasks and we apologize to anyone if we may have failed to mention.

REFERENCES

[1]. D.J. Hand, G. Blunt, M.G. Kelly, and N.M. Adams, "Data Mining for Fun and Profit," Statistical Science, vol. 15, no. 2, pp. 111-131, 2000.

[2]. "Statistics for General and On-Line Card Fraud," http://www.epaynews.com/statistics/fraud.html, Mar. 2007.

[3]. S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems, vol. 3, pp. 621-630, 1994.

[4]. M. Syeda, Y.Q. Zhang, and Y. Pan, "Parallel Granular Networks for Fast Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Fuzzy Systems, pp. 572-577, 2002.

[5]. S.J. Stolfo, D.W. Fan, W. Lee, A.L. Prodromidis, and P.K. Chan, "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results," Proc. AAAI Workshop AI Methods in Fraud and Risk Management, pp. 83-90, 1997.

[6]. S.J. Stolfo, D.W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project," Proc. DARPA Information Survivability Conf. and Exposition, vol. 2, pp. 130-144, 2000.

[7]. Abdelhalim, A, and I Traore. "Identity Application Fraud Detection using Web". International Journal of Computer and Network Security 1, no. 1 (October 2009): 31-44.

[8]. Aha, David W., Dennis Kibler, and Marc K. Albert. "Instance-based learning algorithms."Machine Learning, 1991: 37-66.

[9]. Aleskerov, Emin, Bernd Freisleben, and Bharat Rao. "Card watch: A neural network based database mining system for credit card fraud detection." Computational Intelligence for Financial Engineering. Piscataway, NJ: IEEE, 1997. 220-226.

[10]. Ali, K., and M. Pazzani. "Error reduction through learning multiple descriptions." Machine Learning 24, no. 3 (1996): 173-202.

[11]. Basel Committee on Banking Supervision. "Basel Accords II." Basel, Switzerland: Bank for International Settlements Press & Communications, June 2006.

[12]. Bolton, R, and D Hand. "Unsupervised Profiling Methods for Fraud Detection." Credit Scoring and Credit Control VII, 2001.

[13]. Brause, R, T Langsdorf, and M Hepp. "Neural Data Mining for Credit Card Fraud Detection." Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence. Silver Spring: IEEE Computer Society Press, 1999. 103-106.

[14]. Vatsa, S. Sural, and A.K. Majumdar, "A Game-theoretic Approach to Credit Card Fraud Detection," Proc. First Int'l Conf.Information Systems Security, pp. 263-276, 2005.

[15]. X.D. Hoang, J. Hu, and P. Bertok, "A Multi-Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Proc. 11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.