Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit

Ganesh Kumar.Nune† and P.Vasanth Sena††

Jawaharlalnehru technological Univesity,Hydetrabad.

Summary

By the rise and rapid growth of E-Commerce, use of credit cards for online purchases has more increased and it caused an explosion in the credit card fraud. The most accepted payment mode is credit card for both online as well as regular purchase, pay bills etc. So frauds associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. Many modern mechanisms are developed such as CHIP & PIN the mechanism do not prevent the most common fraud type such as fraudulent credit card usages over virtual POS terminals through internet or mail orders. Finally fraud detection is the essential for stop such type of frauds. In this study, classification model based on Artificial Neural Networks (ANN) and Logistic Regression (LR) are developed and applied on credit card fraud detection problem.

Key words:

fraud; credit cards; fraud detection; Artificial Neural Networks, Sequence Alignment, Machine Learning; ANN;LR;

1. Introduction

The Credit Card Is A Small Plastic Card Issued To Users As A System Of Payment. It Allows Its Cardholder To Buy Goods And Services Based On The Cardholder's Promise To Pay For These Goods And Services. Credit Card Security Relies On The Physical Security Of The Plastic Card As Well As The Privacy Of The Credit Card Number. Globalization And Increased Use Of The Internet For Online Shopping Has Resulted In A Considerable Proliferation Of Credit Card Transactions Throughout The World. Thus A Rapid Growth In The Number Of Credit Card Transactions Has Led To A Substantial Rise In Fraudulent Activities. Credit Card Fraud Is A Wide-Ranging Term For Theft And Fraud Committed Using A Credit Card As A Fraudulent Source Of Funds In A Given Transaction. Credit Card Fraudsters Employ A Large Number Of Techniques To Commit Fraud. To Combat The Credit Card Fraud Effectively, It Is Important To First Understand The Mechanisms Of Identifying A Credit Card Fraud. Over The Years Credit Card Fraud Has Stabilized Much Due To Various Credit Card Fraud Detection And Prevention Mechanisms. Fraud can be defined as the undesired activities taking place in an operational system. Fraudulent activities are usually banned by laws and they are regarded as illegal. Correspondingly the normal activities can be named as legitimate. Fraud can appear in a variety of different domains including finance, telecommunications, health care and public services. During the last 10 years (1999-2009), 1361 articles on fraud were published according to the lSI Web of Knowledge data. Traditional detection methods mainly depend on database system and the education of customers, which usually are delayed, inaccurate and not in-time. After that, methods based on discriminate analysis and regression analysis are widely used [2], which can detect fraud by credit rate for cardholders and credit card transactions, however, with a shortcoming of a large amount of data. In recent years, the prevailing data mining concerns people with credit card fraud detection model based on data mining.

2. Related Works

Fraud detection involves monitoring the behavior of users in order to estimate, detect, or avoid undesirable behavior. To counter the credit card fraud effectively, it is necessary to understand the technologies involved in detecting credit card frauds and to identify various types of credit card frauds [20] [21] [22] . There are multiple algorithms for credit card fraud detection [21] [29]. They are artificial neural-network models which are based upon artificial intelligence and machine learning approach [5] [7] [9] [10] [16], distributed data mining systems [17] [19], sequence alignment algorithm which is based upon the spending profile of the cardholder [1] [6], intelligent decision engines which is based on artificial intelligence [23], Meta learning Agents and Fuzzy based systems [4]. The other technologies involved in credit card fraud detection are Web Services-Based Collaborative Scheme for Credit Card Fraud Detection in which participant banks can share the knowledge about fraud patterns in a heterogeneous and distributed environment to enhance their fraud detection capability and reduce financial loss [8] [13], Credit Card Fraud Detection with Artificial Immune System [13] [26],

Manuscript received September 5, 2015
Manuscript revised September 20, 2015

CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection [18] which is bases upon data mining approach [17] and neural network models, the Bayesian Belief Networks [25] which is based upon artificial intelligence and reasoning under uncertainty will counter frauds in credit cards and also used in intrusion detection [26], case-based reasoning for credit card fraud detection [29], Adaptive Fraud Detection which is based on Data Mining and Knowledge Discovery [27], Real-time credit card fraud using computational intelligence [28], and credit card fraud detection using self-organizing maps [30]. Most of the credit card fraud detection systems mentioned above are based on artificial intelligence, Meta learning and pattern matching.

3. Credit card fraud detection Algorithm Based on Outlier Mining

A fusion approach using Dempster–Shafer theory and Bayesian learningFDS of Dempster–Shafer theory and Bayesian learning Dempster–Shafer theory and Bayesian learning is a hybrid approach for credit card fraud detection [2][5][12][15] which combines evidences from current as well as past behavior.Every cardholder has a certain type of shopping behavior,which establishes an activity profile for them. This approach proposes a fraud detection system using information fusion and Bayesian learning of so as to counter credit card fraud.

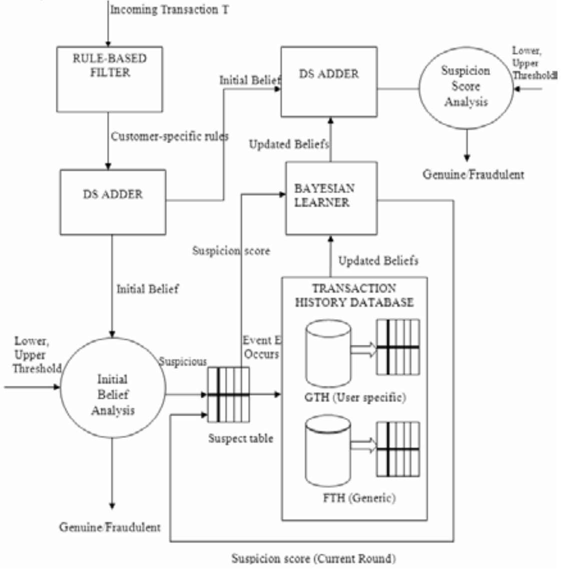


Figure 2. Block diagram of the proposed fraud detection system

The FDS system consists of four components, namely, rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner. In the rule-based component, the suspicion level of each incoming transaction based on the extent of its deviation from good pattern is determined. Dempster–Shafer's theory is used to combine multiple such evidences and an initial belief is computed. Then the initial belief values are combined to obtain an overall belief by applying Dempster–Shafer theory. The transaction is classified as suspicious or suspicious depending on this initial belief. Once a transaction is found to be suspicious, belief is further strengthened or weakened according to its similarity with fraudulent or genuine transaction history using Bayesian learning.It has high accuracy and high processing Speed. It improves detection rate and reduces false alarms and also it is applicable in E-Commerce. But it is highly expensive and its processing Speed is low.

A. BLAST-SSAHA Hybridization for Credit Card Fraud Detection

BLAST-SSAHA in credit card fraud detection The Hybridization of BLAST and SSAHA algorithm [1][6][14] is refereed as BLAH-FDS algorithm. Sequence alignment becomes an efficient technique for analyzing the spending behavior of customers. BLAST and SSAHA are the efficient sequent alignment algorithms used for credit card fraud detection. BLAH-FDS is a two-stage sequence alignment algorithm in which a profile analyzer (PA) determines the similarity of an incoming sequence of transactions on a given credit card with the genuine cardholder's past spending sequences. The unusual transactions traced by the profile analyzer are passed to a deviation analyzer (DA) for possible alignment with past fraudulent behavior. The final decision about the nature of a transaction is taken on the basis of the observations by these two analyzers. BLAST-SSAHA Hybridization When a transaction is carried out, the incoming sequence is merged into two sequences time-amount sequence TA. The TA is aligned with the sequences related to the credit card in CPD. This alignment process is done using BLAST.

SSAHA algorithm [9] is used to improve the speed of the alignment process. If TA contains genuine transaction, then it would align well with the sequences in CPD. If there is any fraudulent transactions in TP, mismatches can occur in the alignment process. This mismatch produces a deviated sequence D which is aligned with FHD. A high similarity between deviated sequence D and FHD confirms the presence of fraudulent transactions. PA evaluates a Profile score (PS) according to the similarity between TA and CPD. DA evaluates a deviation score (DS) according to the similarity between D and FHD. The FDM finally raises an alarm if the total score (PS - DS) is below the alarm threshold (AT). The performance of BLAHFDS is good and it results in high accuracy. At the same time, the processing speed is fast enough to enable on-line detection of credit card fraud.

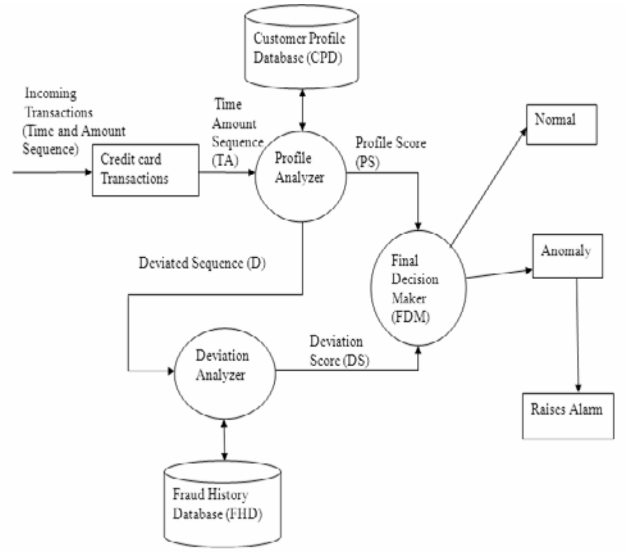

Customer Profile Database (CPD)
Incoming Transactions (Time and Amount Sequence)
Credit card Transactions
Time Amount Sequence (TA)
Profile Analyzer
Profile Score (PS)
Normal
Final Decision Maker (FDM)
Anomaly
Deviated Sequence (D)
Deviation Analyzer
Deviation Score (DS)
Raises Alarm
Fraud History Database (FHD)

Figure 3. Architecture of BLAST and SSAHA Fraud Detection System

It Counter frauds in telecommunication and banking fraud detection. But it does not detect cloning of credit cards

B. Credit Card Fraud Detection using Hidden Markov Model

Hidden Markov Model A Hidden Markov Model is a double embedded stochastic process with used to model much more complicated stochastic processes as compared to a traditional Markov model. If an incoming credit card transaction is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent transactions. Use Of HMM For Credit Card Fraud Detection

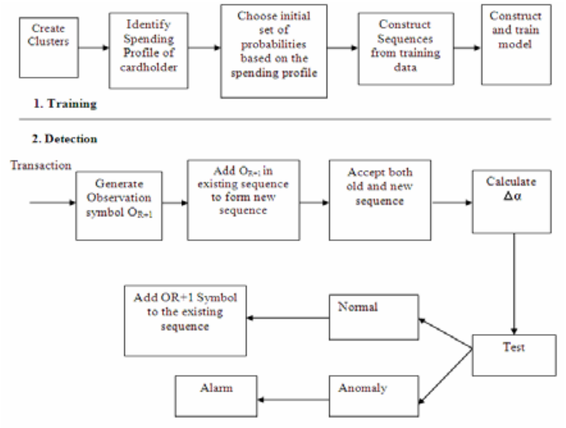

Create Clusters
Identify Spending Profile of cardholder
Choose initial set of probabilities based on the spending profile
Construct Sequences from training data
Construct and train model
1. Training
2. Detection
Transaction
Generate Observation symbol O_{R+1}
Add O_{R+1} in existing sequence to form new sequence
Accept both old and new sequence
Calculate $\Delta\alpha$
Add OR+1 Symbol to the existing sequence
Normal
Test
Alarm
Anomaly

Figure 4. Process Flow of the Proposed FDS

A Hidden Markov Model [3] is initially trained with the normal behavior of a cardholder. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. If the FDS confirms the transaction to be malicious, it raises an alarm and the issuing bank declines the transaction. The concerned cardholder may then be contacted and alerted about the possibility that the card is compromised. HMM never check the original user as it maintains a log. The log which is maintained will also be a proof for the bank for the transaction made. HMM reduces the tedious work of an employee in bank since it maintains a log. HMM produces high false alarm as well as high false positive.

C. Fuzzy Darwinian Detection of Credit Card Fraud

The Evolutionary-Fuzzy System Fuzzy Darwinian Detection system [4] uses genetic programming to evolve fuzzy logic rules capable of classifying credit card transactions into “suspicious” and “non-suspicious” classes. It describes the use of an evolutionary-fuzzy system capable of classifying suspicious and non-suspicious credit card transactions. The system comprises of a Genetic Programming (GP) search algorithm and a fuzzy expert system. Data is provided to the FDS system. The system first clusters the data into three groups namely low, medium and high. The GP The genotypes and phenotypes of the GP System consist of rules which match the incoming sequence with the past sequence. Genetic Programming is used to evolve a series of variable-length fuzzy rules which characterize the differences between classes of data held in a database. The system is being developed with the specific aim of insurance-fraud detection which involves the challenging task of classifying data into the categories: "safe" and "suspicious". When the customer’s payment is not overdue or the number of overdue payment is less than three months, the transaction is considered as “no suspicious”, otherwise it is considered as “suspicious”. The Fuzzy Darwinian detects suspicious and non -suspicious data and it easily detects stolen credit card Frauds.

The complete system is capable of attaining good accuracy and intelligibility levels for real data. It has very high accuracy and produces a low false alarm, but it is not applicable in online transactions and it is highly expensive. The processing speed of the system is low. E. Credit Card Fraud Detection Using Bayesian and Neural Networks. The credit card fraud detection using Bayesian and Neural Networks are automatic credit card fraud detection system by means of machine learning approach.

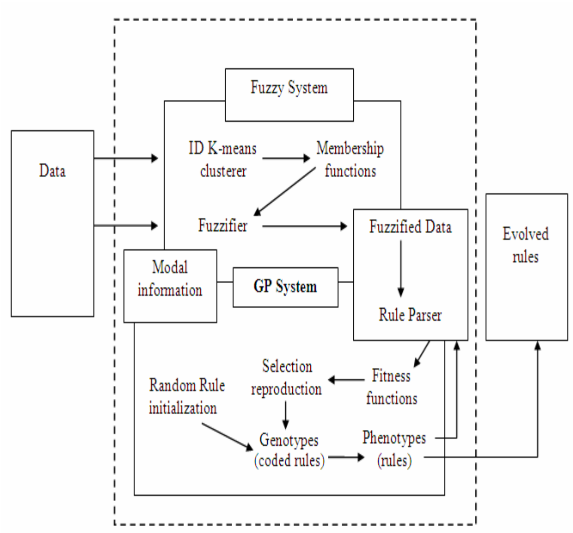


Figure 5. Block diagram of the Evolutionary-fuzzy system

These two machine learning approaches are appropriate for reasoning under uncertainty. An artificial neural network [5][7][9][10][16] consists of an interconnected group of artificial neurons and the commonly used neural networks for pattern classification is the feed forward network. It consist of three layers namely input, hidden and output layers. The incoming Sequence of transactions passes from input layer through hidden layer to the output layer. This is known as forward propagation. The ANN consists of training data which is compared with the incoming sequence of transactions. The neural network is initially trained with the normal behavior of a cardholder. The suspicious transactions are then propagated backwards through the neural network and classify the suspicious and nonsuspicious transactions. Bayesian networks are also known as belief networks and it is a type of artificial intelligence programming that uses a variety of methods, including machine learning algorithms and data mining, to create layers of data, or belief. By using supervised learning, Bayesian networks are able to process data as needed, without experimentation. Bayesian belief networks are very effective for modeling situations where some information is already known and incoming data is uncertain or partially unavailable. This information or belief is used for pattern identification and data classification. A neural network learns and does not need to be reprogrammed. Its processing speed is higher than BNN. Neural network needs high processing time for large neural networks. Bayesian networks are supervised algorithms and they provide a good accuracy, but it needs training of data to operate and requires a high processing speed.

GENETIC ALGORITHM

Genetic algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses. Since their first introduction by Holland, they have been successfully applied to many problem domains from astronomy to sports, from optimization to computer science, etc. They have also been used in data mining mainly for variable selection and are mostly coupled with other data mining algorithms. In this study, we try to solve our classification problem by using only a genetic algorithm solution.

Pseudo code of genetic algorithm

```
Initialize the population
            Evaluate initial population
            Repeat
 Perform competitive selection
Apply genetic operators to generate new solutions
Evaluate solutions in the population
Until some convergence criteria is satisfied.
```

Selection Process

Selection is used for choosing the best individuals, that is, for selecting those chromosomes with higher fitness values. The selection operation takes the current population and produces a ‘mating pool’ which contains the individuals which are going to reproduce. There are several selection methods, like biased selection, random selection, roulette heel selection, tournament selection. In this work the following selection mechanisms are used.

Tournament Selection

Tournament selection has been used in this as it selects optimal individuals from diverse groups. It selects t individuals from the current population uniformly at random, forms a tournament and the best individual of a group wins the tournament and is put into the mating pool for recombination. This process is repeated the number of times necessary to achieve the desired size of intermediate population. The tournament size controls the selection strength. The larger the tournament size, the stronger is the selection process.

Elitist Selection

In order to make sure that the best individuals of the solution are passed to further generations, and should not be lost in random selection, this selection operator is used. So we used a few best chromosomes from each generation, based on the higher fitness value and are passed to the next generation of population.

Reproduction

To generate a second generation population of solutions from those selected through genetic operators: crossover (also called recombination), and/or mutation.

For each new solution to be produced, a pair of "parent" solutions is selected for breeding from the pool selected previously. By producing a "child" solution using the above methods of crossover and mutation, a new solution is created which typically shares many of the characteristics of its "parents". New parents are selected for each new child, and the process continues until a new population of solutions of appropriate size is generated. Although reproduction methods that are based on the use of two parents are more "biology inspired", some research suggests more than two "parents" are better to be used to reproduce a good quality chromosome.These processes ultimately result in the next generation population of chromosomes that is different from he initial generation. Generally the average fitness will have increased by this procedure for the population, since only the best organisms from the first generation are selected for breeding, along with a small proportion of less fit solutions, for reasons already mentioned above.

Although Crossover and Mutation are known as the main genetic operators, it is possible to use other operators such as regrouping, colonization-extinction, or migration in genetic algorithms.

Termination

This generational process is repeated until a termination condition has been reached. Common terminating conditions are:

- A solution is found that satisfies minimum criteria
- Fixed number of generations reached
- Allocated budget (computation time/money) reached
- The highest ranking solution's fitness is reaching or has reached a plateau such that successive iterations no longer produce better results
- Manual inspection
- Combinations of the above

4. Experiment and Design

To Control the credit card fraud, During the credit card transaction, the fraud is detected and the number of false alert is being minimized by using genetic algorithm.

- ❖ **User GUI**

In this module, User Interface module is developed using Applet Viewer. This module is developed to user to identify the credit card fraud using genetic algorithm technique. So the user interface must be capable of providing the user to upload the dataset and make manipulations and finally must show the user whether fraud has been detected or not. Only final output will be in applet screen. All the generation details (crossover and mutation) will b in the console screen of eclipse.

***.Critical Value Identification**
Based on CC usage Frequency

```
Float                                                   …ccfreq
=Float.valueOf(temp[3])/Float.valueOf(temp[6]);
                    if(ccfreq>0.2)
                    {

          if(Float.valueOf(temp[7])>(5*ccfreq))
                              {
                                        res[0]=1;

          res[1]=(Float.valueOf(temp[7])*ccfreq);
                              }
                    }
                              if(res[0]<1)
                    {
                              res[1]=(float)ccfreq;
                    }
```

Ccfreq = Total number card used (CU) / CC age

If ccfreq is less than 0.2 , it means this property is not applicable for fraud and critical value =ccfreq

Otherwise, it check for condition of fraud (i.e) =

Fraud condition = number of time Card used Today (CUT) >(5 * ccfreq)

If true, there may chance for fraud using this property and its critical value is CUT*ccfreq

If false, no fraud occurrence and critical value =ccfreq

Based on CC usage Location

```
int loc=Integer.valueOf(temp[8]);
if((loc<=5)&& (Integer.valueOf(temp[9])>( 2 * loc)))
{
res[0]=1;
res[1]=(Float.valueOf(loc)/ Float.valueOf(temp[9]));
}
if(res[0]<1)
{
res[1]=(float)0.01;
}
```

Number of locations CC used so far (loc) obtained from dataset(loc)

If loc is less than 5, it means this property is not applicable for fraud and critical value =0.01

Otherwise, it check for condition of fraud (i.e) =

Fraud condition = number of locations Card used Today (CUT) >(5 * loc)

If true, there may chance for fraud using this property and its critical value is loc/CUT

If false, no fraud occurrence and critical value =0.01

Based on CC OverDraft

```
float od =Float.valueOf(temp[5])/Float.valueOf(temp[3]);
                    if(od<=0.2)
                    {
                              if(Float.valueOf(temp[10])>=1)
                              {
                                        res[0]=1;

          res[1]=(Float.valueOf(temp[10])*od);
                              }
                    }
                    if(res[0]<1)
                    {
                              res[1]=(float)od;
                    }
```

Number of times CC overdraft w.r.t CU occurred so far (od) can be found as,

Od w.r.t CU = OD/CU

If Od w.r.t CU is less than 0.02, it means this property is not applicable for fraud and critical value = Od w.r.t CU

Otherwise, it check for condition of fraud (i.e) =

Fraud condition = check whether overdraft condition occurred today from (ODT dataset)

If true, there may chance for fraud using this property and its critical value is ODT * Od w.r.t CU

If false, no fraud occurrence and critical value = Od w.r.t CU

Based on CC Book Balance

```
 Float bb =Float.valueOf(temp[2])/Float.valueOf(temp[4]);
                    if(bb<=0.25)
                    {     res[0]=1;

          res[1]=(Float.valueOf(2)*bb);
                    }
                    if(res[0]<1)
                    {
          res[1]=(float)bb;
                    }
```

Standard Book balance can be found as,

Bb = current BB / Avg. BB

If bb is less or equals than 0.25, it means this property is not applicable for fraud and critical value = bb

Otherwise, it check for condition of fraud (i.e) =

If true, there may chance for fraud using this property and its critical value is currBB * bb

If false, no fraud occurrence and critical value = bb

Based on CC Average Daily Spending

```
float mon= Float.valueOf(temp[6])/30;
                    float          bal=          100000          -
Float.valueOf(temp[4]);
                    float tot = mon*bal;
                    float ds =tot/Float.valueOf(temp[6]);
                    if((10*ds)<Float.valueOf(temp[11]))
                    {
                                        res[0]=1;

          if(Float.valueOf(temp[11])>0)

          res[1]=(Float.valueOf(temp[11])/ (10*ds));
                              else
                                        res[1]=(float) 0.0;
                              }
                    if(res[0]<1)
                    {
                              res[1]=(float)0.01;
                    }
```

❖ Fraud Detection using Genetic Algorithm

In this module the system must detect whether any fraud has been occurred in the transaction or not. It must also display the user about the result. It is calculated based on following:

Age of CC in months can be calculated using CCage (from dataset) by,

Age of cc by month = CCage/30

Total money being spent from the available limit (1 lakh _ 100000)

Bal = 100000 – avg BB

So, total money spent can be found as,

Tot = Age of cc by month * Bal

Total money spent on each month can be calculated as,

Ds=tot* Age of cc by month

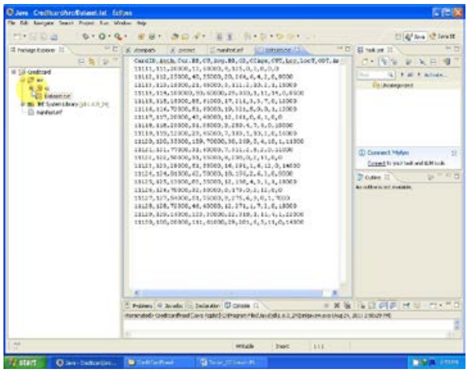
it check for condition of fraud (i.e) =

Fraud condition = (10 * ds) is amount spent today (AmtT in dataset)

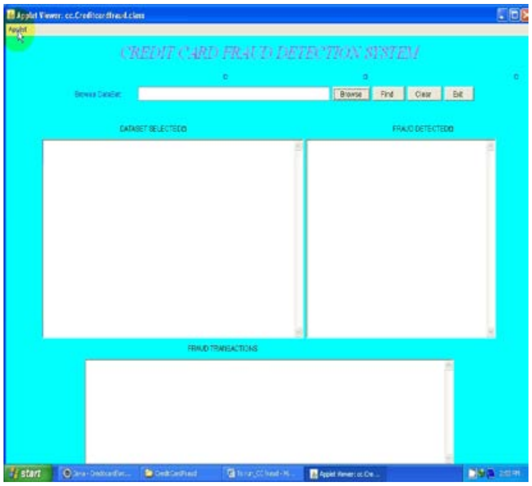
If true, there may chance for fraud using this property and its critical value is AmtT/(10*ds)

If false, no fraud occurrence and critical value 0.01

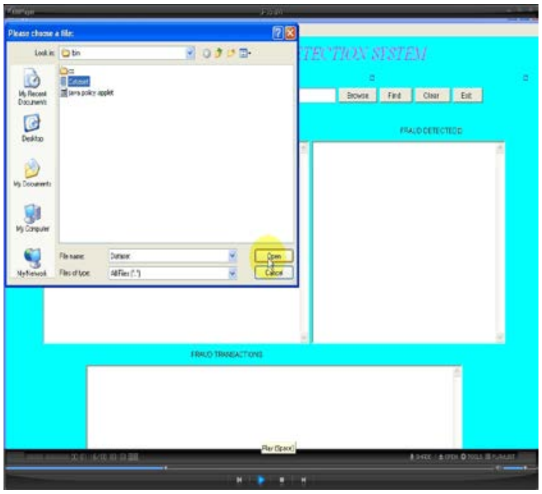
5. Analysis and screen shorts



Credit Card Dataset



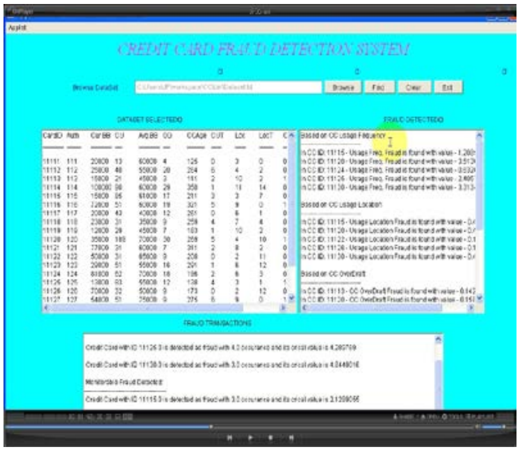
Credit Card Fraud Detection System



File name: Dataset

Files of type: All Files (*.*)

Placing Dataset in Fraud Detection System



CardID	Auth	CurBB	CU	AvgBB	OD	CCAge	OUT	Loc	LocT	C
11111	111	20000	13	60000	4	125	0	3	0	0
11112	112	25000	40	55000	20	264	6	4	2	0
11113	113	15000	21	45000	3	181	2	10	2	1
11114	114	100000	98	60000	29	358	1	11	14	0
11115	115	15000	05	61000	17	211	3	3	7	0
11116	116	22000	51	60000	19	321	5	9	0	1
11117	117	20000	43	40000	12	201	0	6	1	0
11118	118	23000	31	35000	9	259	4	7	4	0
11119	119	12000	29	45000	7	183	1	10	2	0
11120	120	35000	188	70000	30	259	5	4	10	1
11121	121	77000	31	60000	7	311	2	8	2	0
11122	122	50000	31	65000	9	208	0	2	11	0
11123	123	29000	51	55000	16	291	1	6	12	0
11124	124	81000	62	70000	18	186	2	6	3	0
11125	125	13000	93	95000	12	138	4	3	1	1
11126	126	70000	32	50000	9	173	0	2	12	0
11127	127	54000	51	25000	9	275	6	9	0	1

Based on CC Usage Frequency

In CC ID: 11115 - Usage Freq. Fraud is found with value - 1.200
In CC ID: 11120 - Usage Freq. Fraud is found with value - 3.513
In CC ID: 11124 - Usage Freq. Fraud is found with value - 0.632
In CC ID: 11126 - Usage Freq. Fraud is found with value - 2.806
In CC ID: 11130 - Usage Freq. Fraud is found with value - 3.313

Based on CC Usage Location

In CC ID: 11115 - Usage Location Fraud is found with value - 0.
In CC ID: 11120 - Usage Location Fraud is found with value - 0.
In CC ID: 11122 - Usage Location Fraud is found with value - 0.1
In CC ID: 11126 - Usage Location Fraud is found with value - 0.1
In CC ID: 11130 - Usage Location Fraud is found with value - 0.

Based on CC OverDraft

In CC ID: 11113 - CC OverDraft Fraud is found with value - 0.142
In CC ID: 11130 - CC OverDraft Fraud is found with value - 0.151

Credit Card with ID 11126.0 is detected as fraud with 4.0 occurance and its critical value is 4.289799

Credit Card with ID 11130.0 is detected as fraud with 3.0 occurance and its critical value is 4.0448016

Moderate Fraud Detected

Credit Card with ID 11115.0 is detected as fraud with 3.0 occurance and its critical value is 2.1209056

Screen Showing Fraud Detected

6. CONCLUSION

This method proves accurate in deducting fraudulent transaction and minimizing the number of false alert. Genetic algorithm is a novel one in this literature in terms of application domain. 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. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks.

The objective of the study was taken differently than the typical classification problems in that we had a variable misclassification cost. As the standard data mining algorithms does not fit well with this situation we decided to use multi population genetic algorithm to obtain an optimized parameter.

REFERENCES

[1] Wang Xi. Some Ideas about Credit Card Fraud Prediction China Trial. Apr. 2008, pp. 74-75.

[2] Liu Ren, Zhang Liping, Zhan Yinqiang. A Study on Construction of Analysis Based CRM System. Computer Applications and Software. Vol.21, Apr. 2004, pp. 46-47.

[3] S D Bay, M Schwabacher. Mining Distance-Based Outliers in Near Linear Time with Randomization and a Simple Pruning Rule[C]. In:SIGKDD 03, Washington.DC.USA, 2003.

[4] J.Laurikkala, M Juhola, E Kentala. Informal Identification of Outilers in Medical Data[C]. In:5th International Workshop on Intelligent Data Analysis in Medicine and Pharmacology,(IDAMAP-2000),2000.

[5] K Yamanishi, J Takeuchi. A Unifying Framework for Detectiong Outliers and Change Points from Nen-Stationary Time Series Data[C]. In:SIGKDD 02 Edmonton, Alberta, Canda, 2002

Ganesh Kumar. Nune Completed B.Tech Computer Science & Engineering Aizza College of Engineering (Jawaharlal Nehru University) Hyderabad, Pursuing M.Tech ComputerScience and Engineering in Sree Chaitanya College of Engineering (Jawaharlal Nehru University Hyderabad) Published Papers: Dynamic Behavior of T.P Mining Algorithm in 2011.