Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 3; April-June, 2017, pp. 151-154
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Credit Card Fraud Detection with Accuracy-using Fuzzy Logic and Machine Learning Decision Tree Induction Algorithm

Devika Bajetha

M.tech-CSE (Mahrishi Dayanand University)
E-mail: devikakrk@gmail.com

Abstract—*Almost every one holds and uses credit card. With the increasing credit card users the fraud rates are also in peak. Because of fraudulent transactions credit card companies has to bear a huge loss. To control loss, credit card companies use many techniques and tools based on algorithms like genetic algorithm, HMM etc to detect fraudulent transaction. As the credit card users, companies providing online transaction facilities and fraudsters are increasing it becomes very difficult for credit card companies to mark the exact fraud transaction for every customer. Fraud detection involves monitoring the activities of populations of users in order to estimate, perceive or avoid undesirable behavior. This paper represents the use of fuzzy logic (to build fuzzy databases and information retrieval and fuzzy decision making) and machine learning decision tree induction algorithm with weights to detect the most appropriate fraudulent (doubtful) transaction.*

1. INTRODUCTION

Card fraud begins either with the theft of the physical card or with the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder, the merchant, or the issuer at least until the account is ultimately used for fraud.[1]. Card fraud can take place in many ways like Card not present transaction, Identity theft, Application fraud, Account takeover, Skimming, Checker, BIN attack, Phishing, Balance transfer checks. so, before a credit card user complaints fraudulent transaction, card issuer bank want to mark fraudulent transaction, to save from loss. There are many techniques involved in fraud detection like Decision tree, Genetic algorithms and a range of additional algorithms, Clustering techniques, Neural networks[2] **.** Credit card companies detect fraud by flagging several different kinds of transactions. Among them are large purchases made just after small ones, online purchases and purchases that don't fit a cardholder's profile.

They have incentive to do this: Credit card companies "lose approximately seven cents per every hundred dollars of transactions due to fraud," said Andrew Schrage, co-owner of the Money Crashers Personal Finance website. "For 2010, this translated into roughly $8.6 billion."

If the credit card company "notices a relatively small purchase — for example, gas, followed by a large one say, for a flat-screen TV — this is likely to tip them off," he said. "This is standard behavior for a criminal with a stolen card. They make one small purchase to see if the card is still active, and then make a major purchase."

The anonymity of the Internet makes it an ideal venue for credit card thieves, he added."A large number of online purchases in a short period of time is also likely to get a credit card account flagged," he said. Multiple purchases in rapid succession will also set off the credit card companies' alarm bells, whether they're made online or at a store.

Credit card companies also monitor cardholder transaction habits to establish individual customer profiles. These help issuers determine which purchases are standard operating procedure for the cardholder, and which ones deserve closer scrutiny.

According to Steve Weisman, author of "The Truth About Avoiding Scams," issuers become suspicious whenever a transaction occurs that falls outside of the parameters of a customer's profile. So if a cardholder usually only uses a credit card buys groceries and pay the dry cleaning bill but suddenly incurs a charge for five Louis Vuitton handbags, it's almost certainly a red flag.

Similarly, people who do most of their spending in the U.S. should notify card issuers before traveling overseas, as any charges they incur in a foreign country could be flagged.

The *ex post facto* nature of credit-card fraud detection may not offer much comfort to uneasy cardholders. However, they should be aware issuers spare no effort to crack down on these crimes, and not just because it's good for their customers.

So the next time the credit card company calls to let you know they've detected suspicious activity on your account, remember they have as much of a vested interest in stopping it as you do[3]

2. IMPLEMENTATION

By the use of fuzzy database, fuzzy information retrieval and fuzzy decision making, a credit card company can form a refined database having examples on which decision tree can be applied to find out the most appropriate transaction which can be marked fraudulent.

A. Fuzzy database:

A fuzzy database is a database which is able to deal with uncertain or incomplete information using fuzzy logic. There are many forms of adding flexibility in fuzzy databases. The simplest technique is to add a fuzzy membership degree to each record, that is, an attribute in the range [0,1]. However, there are other kinds of databases allowing fuzzy values to be stored in fuzzy attributes using fuzzy sets, possibility distributions, or fuzzy degrees associated to some attributes and with different meanings (membership degree, importance degree, fulfillment degree, etc.).

for example the relation MARKETS with the domains AREA, SIZE and POTENTIAL represented by the table

Table 1

RELATION:MARKETS		
AREA	SIZE	POTENTIAL
East	large	good
Mideast	(large,medium)	(moderate,good)
South	small	(good,excellent)

B. **Fuzzy information retrieval**:It refers to the methods of information retrieval that are based upon the theory of fuzzy sets

C. fuzzy decision making

A – set of alternatives or possible actions.

Θ– set of states (various conditions) of the environment in which decisions are taken.

€– set of consequences resulting from the choice of a particular alternative.

$\acute{K}$ – is a mapping A x Θ→€ specifying a consequence for each element of the environment. The space A x Θ defines the solution space.

D – decision function D : €→R . R Reflects the preference structure of the decision maker.

The decision function D incorporates the goals of the decision maker. It induces a preference ordering on the set of consequences € ; such that $\xi_i > \xi_j$ iff $D(\xi_i) > d(\xi_j)$ where ξ_i , ξ_j ε Θ, and > is the preference relation, i.e., ξ_i consequence is preferred to consequence ξ_j [6]

Consider that the states of the environment Θ are known to the decision maker.

In this case, the elements of Θ can be incorporated in the set A. Thus, $\acute{K}$ is a mapping $\acute{K}$: A→€

Best decision alternative a * for n decision criteria:

$a^* = \max_{a \varepsilon A} D(\acute{K}(a))$

$\acute{K}(a) = [\acute{K}_1(a), \ldots.., \acute{K}_n(a)]$

D. machine learning –decision tree induction

Machine learning is a type of artificial intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can change when exposed to new data.

Machine learning tasks are typically classified into three broad categories, depending on the nature of the learning "signal" or "feedback" available to a learning system. These are:

Supervised learning: The computer is presented with example inputs and their desired outputs, given by a "teacher", and the goal is to learn a general rule that maps inputs to outputs. Supervised algorithms can apply what has been learned in the past to new data.

Unsupervised learning: No labels are given to the learning algorithm, leaving it on its own to find structure in its input. Unsupervised learning can be a goal in itself (discovering hidden patterns in data) or a means towards an end (feature learning). Unsupervised algorithms can draw inferences from datasets.

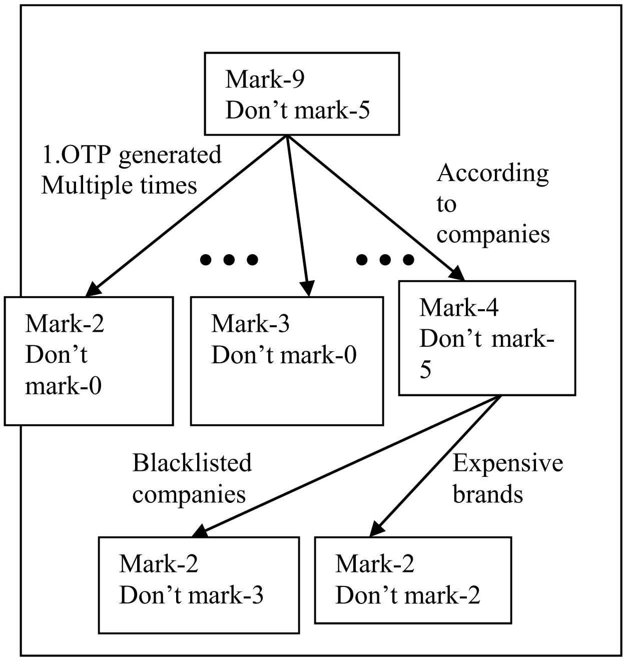

Fig. 1

Reinforcement learning: A computer program interacts with a dynamic environment in which it must perform a certain goal (such as driving a vehicle or playing a game against an opponent[4]:3). The program is provided feedback in terms of rewards and punishments as it navigates its problem space.[5]

Behind the scenes, the software is simply using statistical analysis and predictive analytics to identify patterns in the user's data and use to patterns to populate the News Feed.

Decision tree learning uses a decision tree as a predictive model, which maps observations about an item to conclusions about the item's target value (represented in the leaves).It is a predictive modeling approach used in statistics, data mining and machine learning. Tree models where the target variable can take a finite set.

Entropy: It measures the homogeneity of examples

Entropy(s)= $-p_{+}\log_{2}p_{+} - p_{-}\log_{2}p_{-}$

Where p_{+} = proportion of positive examples
p_{-} = proportion of negative examples

The entropy is a measure in the information theory, which illustrates the impurity of an arbitrary collection of examples.

For e.g. if training data has 14 instances with 9 positive and 5 negative instances, the entropy is calculated as

Entropy ([9+, 5-]) = $-(9/14)\log_2(9/14) - (5/14)\log_2(5/14)$ = 0.940

Entropy =0 if all member of S belongs to same class

Entropy = 1 if equal examples are considered

A key point to reminder here is that the more uniform is the probability distribution, the greater is its entropy

3. RESULT

Decision tree building procedure require two things: appropriate training data sets build with fuzzy database, fuzzy information retrieval and fuzzy decision making techniques to choose which example data set is included as negative example and which one should be included as positive example, in database, and the second thing is applying decision tree for every elements to be considered as a group so that only one result of the question “whether it is fraudulent transaction” could be generated.

Table 2: Example shows a fuzzy database considered.

Company name	Transacted Amt	Card Type	Card issuer	Location of card usuage
DIOR	2,000$	VISA	ICICI	U.K EAST
PRADA	1,080$	VISA	HSBC	USA MID WEST
GUCCI	3,012$	VISA	SBI	CHINA SOUTH
PRADA	1,281$	VISA	PNB	BANGLORE

According to the area of usage of card,credit card issuer can be more alert. Or it can mark the companies with whom the transactions are more prone to be fraud.

Table 3

S. no	OTP generated (Times)	Bill exceeding Limit set	Location of shop/ shopping brand	Last usage of card	fraud
1	3	yes	visited	20/4/17	N
2	1	no	no	12/3/17	Y
3	1	no	visited	23/4/17	N
4	2	no	no	24/4/17	Y
5	1	yes	No	24/4/17	N
6	1	no	visited	20/4/17	N
7	2	yes	No	1/2/17	Y

In the above table data we can also include weightage to every example type, like the examples which are more prone to fraud are given more weightage so that the incidence matching with highest weight example should be analysed prior to other incidences. Every data has four properties required to maintain information gain and build decision tree, the four properties are no. of times OTP generated, shopping bill is exceeding the limit set, the brand or shooping center is visited or not,,last date when the card used.

4. CONCLUSION

With the increasing risks of fraudulent transactions, credit card issuer banks are using many techniques to detect fraudulent transactions. To be more precise in detection I proposed the concept employing scientific approach. It increases the probability of detecting the fraudulent transaction.

5. ACKNOWLEDGEMENT

We acknowledge the effort and hard work by the experts who have contributed towards the development of Credit Card Fraud Detection System. We also acknowledge the reviewers of the journal for the suggestions and modifications to improve the quality of the paper.

REFERENCES

[1] YUAN, G. J. (2013). *FUZZY SETS AND FUZZY LOGIC.* DELHI: PHI Learning private ltd.

[2] https://en.wikipedia.org/wiki/Credit_card_fraud

[3] http://www.mydigitalshield.com/credit-card-fraud-detection-techniques/

[4] http://www.igi-global.com/dictionary/fuzzy-database/11718

[5] ftp://ftp.irisa.fr/local/caps/DEPOTS/BIBLIO2010/Harastani_Rima.pdf

[6] https://fenix.tecnico.ulisboa.pt/downloadFile/3779579218041/CDI_SI_Fuzzy_Decision_2012.pdf

[7] http://www.cnbc.com/id/46907307

[8] https://en.wikipedia.org/wiki/Machine_learning

[9] http://whatis.techtarget.com/definition/machine-learning

[10] https://fenix.tecnico.ulisboa.pt/downloadFile/3779579218041/CDI_SI_Fuzzy_Decision_2012.pdf

[11] V.Dheepa,Dr. R.Dhanapal“Analysis of Credit Card Fraud Detection Methods”. International Journal of RecentTrends in Engineering, Vol 2, No. 3, November 2009.

[12] Krishna Kumar Tripathi, Mahesh A. Pavaskar“ Survey on Credit Card Fraud Detection Methods”. International Journal of Emerging Technology and Advanced Engineering,Volume 2, Issue 11, November 2012.