VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Credit Card Fraud Detection

Jay Anil Chamare, Henil Kundan Dandekar
(MCA, VIVA Institute of Technology / University of Mumbai, India)
(MCA, VIVA Institute of Technology / University of Mumbai, India)

Abstract: *The use of credit cards for online and regular purchases is growing exponentially with related fraud. A large number of fraudulent activities are performed on a daily basis. Various modern techniques such as Data Mining, Genetic Programming, etc. used in obtaining fraudulent sales. This paper uses a genetic algorithm that combines strategies to find the right solution to a problem and to produce a transparent result of counterfeiting. The main purpose is to detect fraudulent activity and to improve the production of test data. This algorithm is a heuristic method used to solve complex computer problems. It is a method of optimization and evolutionary search based on genetic and environmental selection. Implementing a fraud detection system is important for all credit card issuers and their customers to minimize their losses.*

Keywords - *Credit card, Electronic commerce, Fraud detection, Genetic algorithms.*

I. Introduction

Credit card is a thin plastic card that contains identification information such as a signed photo, and authorizes the person in it to charge for purchases or services in his or her account - a fee that will be charged from time to time. Today, the information on the card is read by automatic teller machines (ATMs), store students, the bank and is used in an online banking system. They have a unique card number that is very important. Its security depends on the physical security of the plastic card and the security of the credit card number.

There is a rapid growth in the number of credit card transactions that has led to a significant increase in fraudulent activities. Credit card fraud is a broad term for fraud and fraud committed using a credit card as a fraudulent source of funds for certain activities. In general, mathematical methods and many data mining algorithms are used to solve this problem detection problem. Most credit card fraud systems are based on artificial intelligence (AI), Meta learning and pattern matching.

Genetic algorithms are evolutionary algorithms aimed at finding the best solutions to eliminate fraud. High value is given to developing an efficient and secure electronic payment system to determine whether the transaction is fraudulent or not.

In this paper, we will focus on credit card fraud and ways to get it. Credit card fraud occurs when one person uses another person's card for personal use without the knowledge of the owner. If such a crime is committed by a fraud, it is used until all its available limits are exhausted.

Therefore, we need a solution that reduces the amount of limitations available on a credit card that is more prominent in fraud. Also, Genetic algorithm produces better solutions over time. Full emphasis is placed on establishing an effective and secure electronic payment system to detect fraudsters.

II. Headings

A proper and thorough literature survey concludes that there are various methods that can be used to detect credit card fraud detection. Some of these approaches are:

- Bayesian Network
- Artificial Neural Network
- Neural Network
- Hidden Markov Method

- Genetic Algorithm

In our research paper, as stated earlier, we will be emphasizing on the Genetic algorithm and how it is used in credit card fraud detection systems.

III. METHODOLOGY

Uncertainty

Uncertainty is common in many real-time events. Credit card fraud detection is a common uncertainty, where potential fraud cases must be detected in real time and marked before the transaction can be accepted or rejected. We are introducing extensions to IBM Proactive Technology Online (PROTON) open source tool to deal with uncertainty. The inclusion of uncertainties has an impact on all levels of architecture and the concept of event processing engine. Extensions used in PROTON include the addition of new built-in attributes and functions, support for new types of operands, and support for event processing patterns to address all of this. New skills are used as building blocks and basic basics in the language of event planning. This allows for the implementation of event-run applications with features of uncertainty from different domains in the normal way. The first application was designed on the basis of credit card fraud acquisition. Our initial results are encouraging, highlighting the potential benefits that come from combining the uncertainties in the background of credit card fraud.

GENETIC ALGORITHM

In this module the system must determine whether fraud has taken place in the sale or not. It should also show the user about the effect. It is calculated based on the following:

CC age per month can be calculated using CCage (from the database) as, CC years per month = CCage / 30
Total amount spent from the available limit (1 lakh _100000)

Bal = 100000 - avg BB Thus, the total amount spent can be obtained by, Tot = Age cc per month * Bal The amount spent per month can be calculated as, Ds = tot * cc years per month checks fraud status (i.e.) = Fraud status = (10 * DS) value spent today (AmtT on database)

If true, there may be a possibility of fraud using this property and its significant value is AmtT / (10 * DS)

If false, there is no fraud and the critical value is 0.01 It is to protect financial institutions from significant losses in the past and to reduce the risks associated with the electronic payment system. And this is proof that it is accurate in predicting fraudulent transactions. If this algorithm is used in a bank credit card fraud detection system, the chances of fraudulent fraud can be predicted after a credit card purchase by a financial institution.

A credit card fraud program needs a large amount of pre-existing data associated with the cardholder made when using a credit card when making a purchase, we should devise a specific system that can control credit card fraud before any real transaction can be made.

Genetic Algorithm is an efficient method that attempts to replicate evolutionary processes. A genetic group of people with a particular problem may have a better solution, or better solution. This is the basic concept behind the genetic algorithm. On the basis of genetic and evolutionary principles, the genetic algorithm repeatedly changes the number of artificial structures using startups, selections, crossings, and conversion operators. This was done in order to find an improved solution.

The synthetic genetic algorithm aims to improve problem solving. This improvement is done by maintaining the best combination of input variables. It develops the definition of a problem and also produces a function of purpose which is a way of determining which person produces the best outcome.

Initially, from a crowded sample space, the first number of people is randomly selected and the eligibility value is calculated and sorted. The competition method is used in the selection process and the chances of a single point are calculated from the crossover. In conversion, new interest rates change using the same rate of probability. The best solution is always selected and passed on to the next generation, each time new ones are produced.

Users of Genetic Algorithm are:

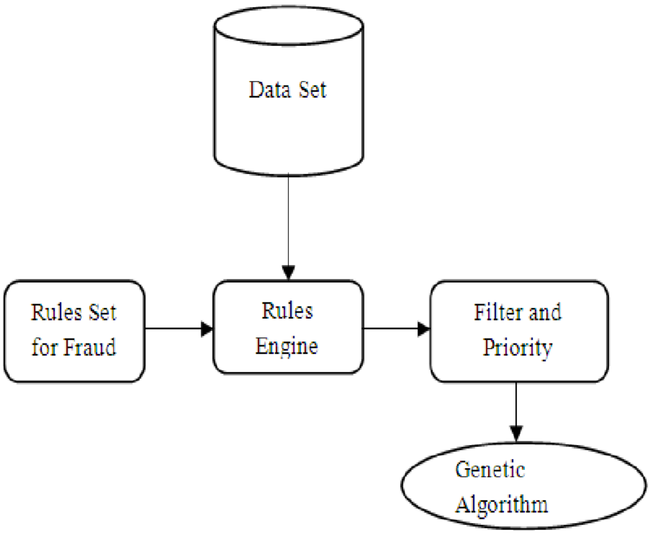
Choices - Survival of the fittest and favourites is always given to the best results.

• Genetic modification - Based on trying a random combination and evaluating the outcome (success or failure) of an outcome.
• Crossover- Made by combining components of good results with the hope of creating a better result.

A. 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.
```

B. System Design



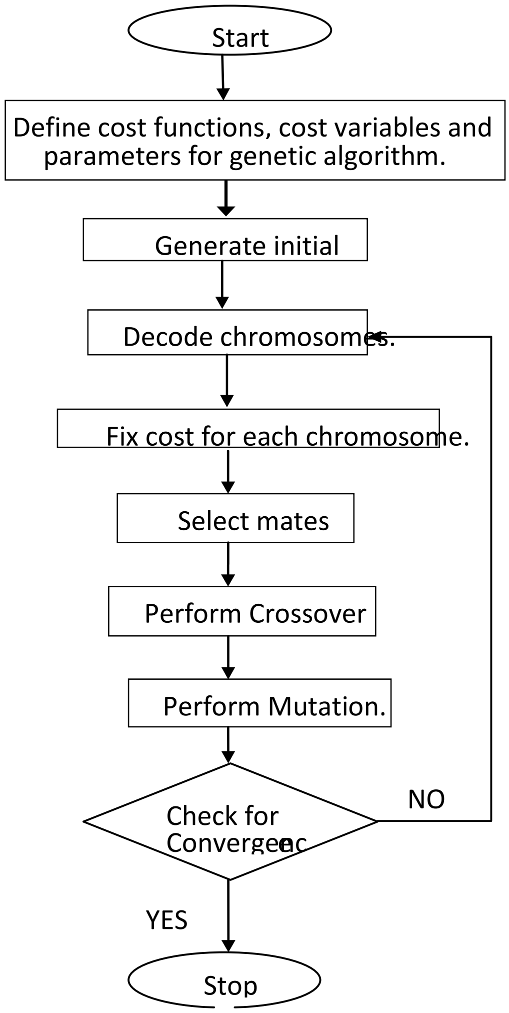
The above architectural design describes the work structure of the system:

- The data warehouse contains the customer data. This customer data is subjected to the rules engine and again, the rules engine comprises of the rules set.
- The filter and priority module sets the priority for the data and hence, plays a very important role in the system. Then the filtered data is sent to the Genetic Algorithm module which performs its functions and generates the output.

EXERIMENT PROCESS

Step1. Credit card activity data input, all transaction records have n attributes, and measure data, find sample at the end, which includes confidential information
for a card manager, save to the data set.
Step2. Calculate value, Calculate CC usage calculation, CC utility area, CC overdraft, current bank balance, average daily spending
Step3. Generate key values obtained after a limited number of
generations. Detected Sensitive Fraud, Detected Fraud Detected, Detected General Fraud etc. using the Genetic algorithm
Step4. Generate fraud using this algorithm.
This is an analysis of the feasibility of obtaining credit card fraud
based on operational strategies, mining acquisitions are based on priorities
prices on obtaining credit card fraud and suggesting these acquisition procedures and your process.

C. Process Flow of Genetic Algorithm



IV. Conclusion

This method proves to be accurate in detecting fraudulent sales and reducing the amount of false alarms. Genetic Algorithm is ideal for such types of program areas. The application of this rule of law to the credit card fraud detection system results in the detection or predict of fraud within a very short period of time after the purchase is made. This will ultimately prevent banks and customers from huge losses and will reduce risk.

This paper researched how to effectively develop a real-world credit card fraud detection system with data mining models. We have identified major challenges in this area: feature engineering, measurement, uneven data, conceptualization, performance measurements, and algorithm model selection. Research shows the area of improvement in the existing system and that one should invest first in feature engineering and tuning models. All data mining models performed better than the existing system, while the random forest did much better. We confirmed with great confidence the findings of the literature and found an exciting, weighty aspect of fraudulent discovery, which yields further research. We have developed appropriate model performance measurements — moderate accuracy and accuracy / memory measurement charts as we see this as a standard, not a binary split function. A carefully crafted set of integrated features, which can be viewed as a card / user profile, makes a difference, and the rules of the control engine containing valuable domain information should also be considered in its design. Regarding (below) the sample and the concept of erosion, we recommend using advanced upgrade solutions and not investing extra in custom solutions in this area, at least not initially. Our information is derived from the largest database representing credit card fraud, which involves interaction with domain experts. As a result, we believe that information is important and well-known in the same data sets of other credit card companies and related types of fraud.

Acknowledgements

We would like to express our sincere thanks to our guide Prof. Pragati Mestry for taking time from her busy schedule to provide us with a great deal of help, support and encourage us to work diligently at every aspect of our research paper. Her views have always been equitably providing a perfect balance between encouragement and constructive criticism. Her tips and suggestions helped us to decide the correct approach to the research paper. We attempted to find help from a variety of individuals at various stages of the research paper. We would like to thank everyone for their guidance.

REFERENCES

[1] S. H. Projects and W. Lovo, ―JMU Scholarly Commons Detecting credit card fraud : An analysis of fraud detection techniques,‖ 2020.
[2] S. G and J. R. R, ―A Study on Credit Card Fraud Detection using Data Mining Techniques,‖ Int. J. Data Min. Tech. Appl., vol. 7, no. 1, pp. 21–24, 2018, doi: 10.20894/ijdmta.102.007.001.004.
[3] ―Credit Card Definition.‖ https://www.investopedia.com/terms/c/creditcard.asp (accessed Apr. 03, 2021).
[4] K. J. Barker, J. D'Amato, and P. Sheridon, ―Credit card fraud: awareness and prevention,‖ J. Financ. Crime, vol. 15, no. 4, pp. 398–410, 2008, doi: 10.1108/13590790810907236.
[5] V. N. Dornadula and S. Geetha, ―Credit Card Fraud Detection using Machine Learning Algorithms,‖ Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.
[6] A. H. Alhazmi and N. Aljehane, ―A Survey of Credit Card Fraud Detection Use Machine Learning,‖ 2020 Int. Conf. Comput. Inf. Technol. ICCIT 2020, pp. 10–15, 2020, doi: 10.1109/ICCIT-144147971.2020.9213809.
[7] B. Wickramanayake, D. K. Geeganage, C. Ouyang, and Y. Xu, ―A survey of online card payment fraud detection using data mining-based methods,‖ arXiv, 2020.
[8] A. Agarwal, ―Survey of Various Techniques used for Credit Card Fraud Detection,‖ Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 7, pp. 1642–1646, 2020, doi: 10.22214/ijraset.2020.30614.
[9] C. Reviews, ―a Comparative Study : Credit Card Fraud,‖ vol. 7, no. 19, pp. 998–1011, 2020.
[10] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. Ramakoteswara Rao, ―Credit Card Fraud Detection Using Machine Learning,‖ Proc. Int. Conf. Intell. Comput. Control Syst. ICICCS 2020, no. Iciccs, pp. 1264–1270, 2020, doi: 10.1109/ICICCS48265.2020.9121114.
[11] I. Sadgali, N. Sael, and F. Benabbou, ―Detection and prevention of credit card fraud: State of art,‖ MCCSIS 2018 - Multi Conf. Comput. Sci. Inf. Syst. Proc. Int. Conf. Big Data Anal. Data Min. Comput. Intell. 2018, Theory Pract. Mod. Comput. 2018 Connect. Sma, no. March 2019, pp. 129–136, 2018.
[12] R. Goyal and A. K. Manjhvar, ―Review on Credit Card Fraud Detection using Data Mining Classification Techniques & Machine Learning Algorithms,‖ IJRAR-International J. Res. …, vol. 7, no. 1, pp. 972–975, 2020, [Online]. Available: http://www.ijrar.org/papers/IJRAR19K7539.pdf.
[13] Nitu Kumari, S. Kannan and A. Muthukumaravel, "Credit Card Fraud Detection Using Genetic-A Survey" published by Middle-East Journal of Scientific Research , IDOSI Publications, 2014
[14] Satvik Vats, Surya Kant Dubey, Naveen Kumar Pandey, "A Tool for Effective Detection of Fraud in Credit Card System", published in International Journal of Communication Network Security ISSN: 2231 – 1882, Volume-2, Issue-1, 2013.
[16] Rinky D. Patel and Dheeraj Kumar Singh, "Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm", published by International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
[17] M. Hamdi Ozcelik, Ekrem Duman, Mine Isik, Tugba Cevik, "Improving a credit card fraud detection system using genetic algorithm", published by International conference on Networking and information technology, 2010.
[18] Wen-Fang YU, Na Wang," Research on Credit Card Fraud Detection Model Based on Distance Sum", published by IEEE International Joint Conference on Artificial Intelligence, 2009. W.J. Book, "Modelling design and control of flexible manipulator arms: A tutorial review", *29th IEEE Conf. on Decision and Control*, San Francisco, CA, 1990, pp. 500-506