Credit Card Fraud Detection using FPGA with K-NN Clustering

Pooja Bainsla[1] Ms. Pooja Yadav[2]
[2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]SRCEM, India

Abstract— Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud. In simple terms, Credit Card Fraud is defined as: "When an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made." Credit card frauds are committed in the following ways: An act of criminal deception (mislead with intent) by use of unauthorized account and/or personal information

- Illegal or unauthorized use of account for personal gain
- Misrepresentation of account information to obtain goods and/or services.

Contrary to popular belief, merchants are far more at risk from credit card fraud than the cardholders. While consumers may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed. Increasingly, the card not present scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the 'physical world' checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 12 to 15 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario.

Keywords: Credit Card Fraud, CVV, FPGA

I. INTRODUCTION

A. Fraud Detection System

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions will be developed, then fraud detection system will start to work. By using this observation, determine users spending profile. The purchase amount will be checked with spending profile of user. By transition probabilistic calculation based on HMM, it concludes whether the transaction is real or fraud. If transaction may be concluded as fraudulent transaction then user must enter security information. This information is related with credit card (like account number, security question and answer which are provided at the time of registration). If transaction will not be fraudulent then it will direct to give permission for transaction. If the detected transaction is fraudulent then the Security information form will arise. It has a set of question where the user has to answer them correctly to do the transaction. These forms have information such as personal, professional, address; dates of birth, etc are available in the database. If user entered information will be matched with database information, then transaction will be done securely. And else user transaction will be terminated and transferred to online shopping website. The flowchart of proposed module is shown in Figure 1.

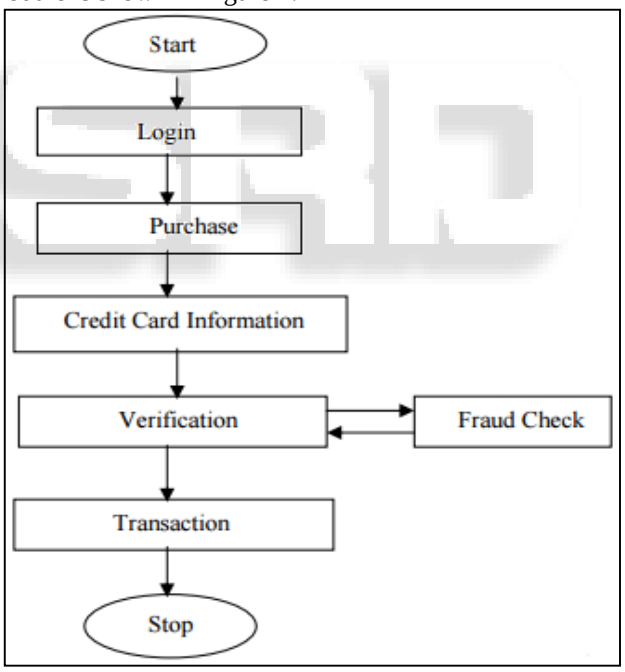

Fig. 1.1: Flowchart of HMM module for credit card fraudulent detection

B. Different Type of Fraud Techniques

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, i.e., traditional card related frauds, merchant related frauds and Internet frauds. The different types of methods for committing credit card frauds are described below.

1) Merchant Related Frauds

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

a) Merchant Collusion:

This type of fraud occurs when merchant owners or their employees conspire to commit fraud using the cardholder accounts or by using the personal information. They pass on the information about cardholders to fraudsters.

b) Triangulation:

Triangulation is a type of fraud which is done and operates from a web site. The products or goods are offered at heavily discounted rates and are also shipped before payment. The customer while browse the site and if he likes the product he place the online information such as name, address and valid credit card details to the site. When the fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudsters then by using the credit card information purchase the products.

2) Internet Related Frauds

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers from most countries around the world. The below described are most commonly used techniques in Internet fraud.

a) Site Cloning

Site cloning is where fraudsters close an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned site will receive these details and send the customer a receipt of the transaction through the email just as the real company would do. The consumer suspects nothing, while the fraudsters have all the details they need to commit credit card fraud.

b) False Merchant Sites:

Some sites often offer a cheap service for the customers. That site requests the customer to fill his complete details such as name and address to access the webpage where the customer gets his required products. Many of these sites claim to be free, but require a valid credit card number to verify an individual s age. These kinds of sites in this way collect as many as credit card details. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

c) Credit Card Generators:

These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. This makes the user to allow to illegally generating as many numbers as he desires, in the form of any of the credit card formats.

II. Application Areas

- Data mining application for credit-card fraud detection, the anomaly detection algorithm is implemented for cyber credit-card fraud detection process.
- Once the data to be analyzed is selected, the anomaly detection algorithms will be applied to perform a data mining process for matching the behavior of the current transaction if it differs in behavior with the owner's past transactions on its credit-card.
- If the behavioral pattern in the current transaction differs with the learned pattern of the original credit-card owner, the system will continue to match the pattern of the current transaction if it's similar with past cyber credit-card fraud transactions.
- If the system returns false (of mismatch patterns between the current transaction and past fraud transactions) then the system classifies the transaction as suspicious fraud but if true, then the system will classify the transaction as illegal fraud transaction.

III. Motivation of the Work

Data mining is about finding insights which are statistically reliable, unknown previously, and actionable from data (Elkan, 2001). This data must be available, relevant, adequate, and clean. Also, the data mining problem must be well-defined, cannot be solved by query and reporting tools, and guided by a data mining process model (Lavrac et al, 2004). The term fraud here refers to the abuse of a profit organisation's system without necessarily leading to direct legal consequences. In a competitive environment, fraud can become a business critical problem if it is very prevalent and if the prevention procedures are not fail-safe. Fraud detection, being part of the overall fraud control, automates and helps reduce the manual parts of a screening/checking process. This area has become one of the most established industry/government data mining applications. It is impossible to be absolutely certain about the legitimacy of and intention behind an application or transaction. Given the reality, the best cost effective option is to tease out possible evidences of fraud from the available data using mathematical algorithms. Evolved from numerous research communities, especially those from developed countries, the analytical engine within these solutions and software are driven by artificial immune systems, artificial intelligence, auditing, database, distributed and parallel computing, econometrics, expert systems, fuzzy logic, genetic algorithms, machine learning, neural networks, pattern recognition, statistics, visualisation and others. There are plenty of specialized fraud detection solutions and software1 which protect businesses such as credit card, e-commerce, insurance, retail, telecommunications industries. There are often two main criticisms of data mining-based fraud detection research: the dearth of publicly available real data to perform experiments on; and the lack of published well researched methods and techniques. To counter both of them, this paper garners all related literature for categorization and comparison, selects some innovative methods and techniques for discussion; and points toward other data sources as possible alternatives.

IV. SCOPE

In the faceless world of the Internet, online fraud is one of the greatest reasons of loss for web merchants. Advanced solutions are needed to protect e-businesses from the constant problems of fraud. Many popular fraud detection algorithms require supervised training, which needs human intervention to prepare training cases. Since it is quite often for an online transaction database to have Terabyte-level storage, human investigation to identify fraudulent transactions is very costly. The expected outcome describes the automatic design of user profiling method for the purpose of fraud detection. We use a FP (Frequent Pattern) Tree rule-learning algorithm to adaptively profile legitimate customer behavior in a transaction database. Then the incoming transactions are compared against the user profile to uncover the anomalies. The anomaly outputs are used as input to an accumulation system for combining evidence to generate high-confidence fraud alert value.

V. ORGANIZATION OF DISSERTATION

In chapter 2, we have a look at the basics of fraud detection systems. First, we discuss the history and the literature survey and then we look at one of the algorithms used in credit card fraud detection systems We analyses this algorithm discussing all the steps that are involved in unauthorized detection.

In chapter 3 we discuss the features of typefaces which are designed specifically for fraud detection systems. We discuss the need of a specially designed typeface for fraud detection and perform an in-depth analysis of one of the most commonly used typeface for fraud detection system.

In chapter 4, we give an overview of the chapter. We discuss the chapter principle and architecture.

In chapter 5, we discuss the method that need to be taken.

In chapter 6, we show the outcome of the fraud detection systems. We discuss each character in detail and how the features of the work are designed for improved performance in Fraud detection systems.

In chapter 7, we will give information about Thesis conclusion and future enhancement.

VI. CHAPTER SUMMARY

This Chapter has provided an overview of the research study by explaining the historical facts of the research area, the motivation behind the study, and the research technique that are going to be answered and its relevance. Research contributions from this study are also overviewed in this Chapter, and finally the outline of the thesis document is clearly explained.

Because of the research problem, the topic area and the purpose, previous research literature is reviewed in order to define a theoretical framework to use for the study and to understand what others have done in the same areas. Therefore, to achieve good research results a literature review of the research area is carried out in the next section, Chapter two.

REFERENCES

[1] Credit Card Security and E-payment, Enquiry into credit card fraud in E-Payment, JithendraDara, Luleå University of Technology, 2006 .
[2] Unawed by fraud: new techniques and technologies have been enlisted in the fight against online fraud, by Micci-Barreca, Daniele, Security Management, Electronic Commerce, Sept, 2003.
[3] S Alfuraih, "Location of Trusted Email for Detection of Credit Card Fraud in Soft Products E-Commerce", 2004.
[4] Saleh I. Alfuraih, Nie n T. Sui and Dennis McLeod, "Using Trusted Email to Detect Credit Card Frauds in Multimedia Products", 2002
[5] Sunil S Mhamane and L.M.R.J Lobo "Use of Hidden Markov Model as Internet Banking Fraud Detection" International Journal of Computer Applications (0975 – 8887) Volume 45– No.21, May 2012
[6] PankajRichhariya et al "A Survey on Financial Fraud Detection Methodologies" BITS,Bhopal," International Journal of Computer Applications (0975 – 8887) Volume 45 No.22, May 2012.
[7] Srivastava, Abhinav, Kundu, Amlan, Sural, Shamik and Majumdar, Arun K., (2008) "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 1, pp. 37-48..
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection," Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., pp. 220-226, 1997.
[14] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[15] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67-74, 1999.
[16] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.
[17] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e-Service, pp. 177-181, 2004.
[18] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," http:// www.bsys.monash.edu.au/people/cphua/, Mar. 2007.
[19] S. Stolfo and A.L. Prodromidis, "Agent-Based Distributed Learning Applied to Fraud Detection," Technical Report CUCS-014-99, Columbia Univ., 1999.
[20] C. Phua, D. Alahakoon, and V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.
[21] V. 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.
[22] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection," ACM Trans. Information and System Security, vol. 3, no. 3, pp. 186-205, 2000.
[23] "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection. E. Aleskerov, B. Freisleben, and B. Rao. 1997, pp. 220-226.
[24] Minority Report in Fraud Detection: Classification of Skewed Data. C. Phua, D. Alahakoon, and V. Lee. 2004.
[25] Distributed Data Mining in Credit Card Fraud Detection. W. Fan, A.L. Prodromidis, and S.J. Stolfo. 1999.
[26] A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Tsai, C. Chiu and C. 2004.
[27] Association rules applied to credit card fraud detection. D. Sa´nchez, M.A. Vila, L. Cerda , J.M. Serrano. 2009.

