Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning

Suvasini Panigrahi [a], Amlan Kundu [a], Shamik Sural [a,*], A.K. Majumdar [b]

[a] *School of Information Technology, Indian Institute of Technology, Kharagpur, India*
[b] *Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India*

ARTICLE INFO

Article history:
Received 30 November 2006
Received in revised form 19 July 2007
Accepted 14 April 2008
Available online 4 February 2009

Keywords:
FDS
Credit card
Dempster–Shafer theory
Bayesian learning
Suspicion score

ABSTRACT

We propose a novel approach for credit card fraud detection, which combines evidences from current as well as past behavior. The fraud detection system (FDS) consists of four components, namely, rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner. In the rule-based component, we determine the suspicion level of each incoming transaction based on the extent of its deviation from good pattern. Dempster–Shafer's theory is used to combine multiple such evidences and an initial belief is computed. The transaction is classified as normal, abnormal 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. Extensive simulation with stochastic models shows that fusion of different evidences has a very high positive impact on the performance of a credit card fraud detection system as compared to other methods.

1. Introduction

In today's electronic society, e-commerce has become an essential sales channel for global business. Due to rapid advancement of e-commerce, use of credit cards for purchases has dramatically increased. Unfortunately, fraudulent use of credit cards has also become an attractive source of revenue for criminals. Occurrence of credit card fraud is increasing dramatically due to the exposure of security weaknesses in traditional credit card processing systems resulting in loss of billions of dollars every year. Fraudsters now use sophisticated techniques to perpetrate credit card fraud. The fraudulent activities worldwide present unique challenges to banks and other financial institutions who issue credit cards. In case of bank cards (Visa and MasterCard) a study done by American Bankers Association in 1996 reveals that the estimated gross fraud loss was $790 million in 1995 [1]. The majority of the loss due to credit card fraud is suffered by the USA alone. This is not surprising since 71% of all credit cards are issued in the USA only. In 2005, the total fraud loss in the USA was reported to be $2.7 billion and it has gone up to $3.2 billion in 2007 [2]. Another survey of over 160 companies revealed that online fraud (committed over the Web or phone shopping) is 12 times higher than offline fraud (committed by using a stolen physical card) [3].

To address this problem, financial institutions employ various fraud prevention tools like real-time credit card authorization, address verification systems (AVS), card verification codes, rule-based detection, etc. But fraudsters are adaptive, and given time, they devise several ways to circumvent such protection mechanisms. Despite the best efforts of the financial institutions, law enforcement agencies and the government, credit card fraud continues to rise. In addition to significant financial losses, the main concern of the law enforcement agencies is that this money is also used to support other criminal activities worldwide. Thus, once fraud prevention measures have failed, there is a need for effective technologies to detect fraud in order to maintain the viability of the payment system. Fraudsters constitute a very inventive and fast moving fraternity. As preventive technology changes, so does the technology of criminals and the way they go about with their fraudulent activities.

The possibility of enhancing existing operations by introducing an effective FDS constitutes the objective of our work.

2. Related work

The approaches used in detecting credit card fraud mainly include neural network, data mining, meta-learning, game theory and support vector machine.

Artificial neural networks (ANN) have been considered for credit card fraud detection by Ghosh and Reilly [4], Aleskerov et al. [5] and Dorronsoro et al. [6]. Ghosh and Reilly [4] carried out a feasibility study for Mellon Bank to determine the effectiveness

* Corresponding author. Tel.: +91 3222 282330; fax: +91 3222 282206.
E-mail addresses: Suvasini.Panigrahi@sit.iitkgp.ernet.in (S. Panigrahi), kunduamlan@sit.iitkgp.ernet.in (A. Kundu), shamik@sit.iitkgp.ernet.in (S. Sural), akmj@cse.iitkgp.ernet.in (A.K. Majumdar).

1566-2535/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.inffus.2008.04.001

of neural network for credit card fraud detection. The authors concluded that it was possible to achieve a reduction of 20–40% in the total fraud losses. Aleskerov et al. [5] present CARDWATCH, a neural network based data mining system for credit card fraud detection. The system trains a neural network with the past data of a particular customer, which can then be used to analyze the current spending behavior of that customer and detect anomalies. They use three transaction features to represent a customer's spending pattern – category of purchase, transaction amount and time since last purchase of the same category. The system was tested with synthetically generated data. Dorronsoro et al. [6] describe the domain of fraud detection as having two particular characteristics – a very limited time span for decisions and a large number of credit card operations to be processed. They have used Fisher's discriminant analysis to separate the fraudulent operations from the normal ones.

More recently, Syeda et al. [7] have suggested the use of parallel granular neural networks for speeding up the data mining and knowledge discovery process. Maes et al. [8] have outlined an automated credit card fraud detection system by ANN as well as Bayesian belief networks (BBN). They show that BBN gives better results related to fraud detection and the training period is faster whereas the actual detection process is substantially faster with ANN. The neural network based methods are, in general, fast but not so accurate. Re-training the neural networks is also a major bottleneck since the training time is quite high.

Chen et al. [9] propose a novel method in which an online questionnaire is used to collect questionnaire-responded transaction (QRT) data of users. A support vector machine (SVM) is trained with this data and the QRT models are used to predict new transactions. Chen et al. [10] have recently presented a personalized approach for credit card fraud detection that employs both SVM and ANN. It tries to prevent fraud for users even without any transaction data. However, these systems are not fully automated and depend on the user's expertise level.

Some researchers have applied data mining for credit card fraud detection. Chan et al. [11] divide a large set of transactions into smaller subsets and then apply distributed data mining for building models of user behavior. The resultant base models are then combined to generate a meta-classifier for improving detection accuracy. Brause et al. [12] have explored the possibility of combining advanced data mining techniques and neural networks to obtain high fraud coverage along with a low false alarm rate. Use of data mining is also elaborated in the work by Chiu and Tsai [13]. They consider web services for data exchange among banks. A fraud pattern mining (FPM) algorithm has been developed for mining fraud association rules which give information regarding the features that exist in fraud transactions. Banks enhance their original fraud detection systems by using the new fraud patterns to prevent attacks. While data mining techniques are relatively accurate, they are inherently slow.

Meta-learning is a general strategy that provides a means for combining and integrating a number of separately learned classifiers or models. A meta-learning system allows financial institutions to share their models of fraudulent transactions by exchanging classifier agents. Stolfo et al. [14] suggest a meta-learning technique to learn patterns of fraudulent credit card transactions. They apply four base classifiers, namely, ID3, CART, Bayes and RIPPER and use the class-combiner strategy [15] to select the best classifier for meta-learning. It has been shown that meta-learning with Bayes gives good accuracy. Prodromidis and Stolfo [16] describe an artificial intelligence based approach that combines inductive learning algorithms and meta-learning methods to build accurate classification models for electronic fraud detection. The field of game theory has also been explored for credit card fraud detection. Liu and Li [17] suggest a game-theoretic approach for prediction of attacks on IDS protected systems and a specific prediction model for credit card fraud. Vatsa et al. [18] have modeled the interaction between an attacker and an FDS as a repeated game between two players, each trying to maximize its payoff. Such game-theoretic models make a number of assumptions, like availability of strategies, actions and payoffs to both the players, which are not often valid in practice. For example, it is quite unusual for a bank to advertise its strategies for fraud detection.

Some survey papers have been published which categorize, compare and summarize articles in the area of fraud detection. Phua et al. [19] did an extensive survey of data mining based FDSs and presented a comprehensive report. Kou et al. [20] have reviewed the various fraud detection techniques including credit card fraud, telecommunication fraud as well as computer intrusion detection. Bolton and Hand [21] describe the tools available for statistical fraud detection and areas in which fraud detection technologies are most commonly used.

Majority of the FDSs as described above show a lot of variation in their accuracy. The main challenge identified by most of them is that the bulk of the transactions flagged as fraudulent by the FDSs are in fact genuine. A substantial amount of time and money is spent by bankers in investigating a large number of legitimate cases. It also causes customer inconvenience and potential dissatisfaction. In credit card application, since occurrence of fraud is sparse, it involves detecting a relatively rare event from a very large collection of routine transactions. Axelsson [22] has pointed out that due to the base-rate fallacy problem, the factor limiting the performance of an intrusion detection system is not the ability to identify intrusive behavior correctly but its ability to minimize false alarms. While failure to detect a fraud causes direct loss to the company, follow up actions needed to pursue false alarms also tend to be costly. Any design choice that attempts to improve the rate of correct detection of fraud, usually causes a rise in the false alarms as well. One of the motivations of our current research is to address this challenge.

It is well known that every cardholder has a certain shopping behavior, which establishes an activity profile for him. Almost all the existing fraud detection techniques try to capture these behavioral patterns as rules and check for any violation in subsequent transactions. However, these rules are largely static in nature. As a result, they become ineffective when the cardholder develops new patterns of behavior that are not yet known to the FDS. The goal of a reliable detection system is to learn the behavior of users dynamically so as to minimize its own loss. Thus, systems that cannot evolve or "learn", may soon become outdated resulting in large number of false alarms. A fraudster can also attempt new types of attacks which should still get detected by the FDS. For example, a fraudster may aim at deriving maximum benefit either by making a few high value purchases or a large number of low value purchases in order to evade detection. Thus, there is a need for developing fraud detection systems which can integrate multiple evidences including patterns of genuine cardholders as well as that of fraudsters.

We propose a credit card fraud detection system that combines different types of evidences using Dempster–Shafer theory. The purpose of aggregation is to meaningfully summarize and simplify bulk data which might be coming from a single source or multiple sources. Familiar examples of aggregation techniques include arithmetic, geometric and harmonic averages, maximum and minimum functions, etc. [23]. Cremer et al. [24] have shown that sensor fusion improves detection rate and reduces false alarms over single sensor solutions. They use different sensor data fusion techniques, namely, Dempster–Shafer, Bayes and fuzzy logic for the detection of anti-personnel land mines. By testing on synthetic data set, they have shown that Dempster–Shafer and Bayes approach outperform the fuzzy technique. Comparing the