available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A survey of signature based methods for financial fraud detection

*Michael Edward Edge**, *Pedro R. Falcone Sampaio*

Manchester Business School, University of Manchester, Booth Street East, Manchester M16 6PB, United Kingdom

ARTICLE INFO

Article history:
Received 30 October 2007
Received in revised form
23 January 2009
Accepted 2 February 2009

Keywords:
Fraud detection
Account signatures
Behaviour scoring
User profiling
Fraud management
Identity theft

ABSTRACT

Fraud detection mechanisms support the successful identification of fraudulent system transactions performed through security flaws within deployed technology frameworks while maintaining optimal levels of service delivery and a minimal numbers of false alarms. Knowledge discovery techniques have been widely applied in fraud detection for data analysis and training of supervised learning algorithms to support the extraction of fraudulent account behaviour within static data sets. Escalating costs associated with fraud however have continued to drive the migration towards increasingly proactive methods of fraud detection, to support the real-time screening of transactional data and detection of ambiguous user behaviour prior to transaction completion. This shift in data processing from post to pre data storage significantly reduces the available time within which to evaluate newly arriving system requests and produce an accurate fraud decision, demanding increasingly robust and intelligent user profiling technologies to support advanced fraud detection. This paper provides a comprehensive survey of existing research into account signatures, an innovative account profiling technology which maintains a statistical representation of normal account usage for rapid recalculation in real-time. Fraud detection architectures, processing models and applications to date are critically examined and evaluated with respect to their proactive capabilities for detection of fraud within streaming financial data. Discussion is also presented on challenges which remain within the proactive profiling of account behaviour and future research directions within the signature domain.

1. Introduction

Fraud detection is now a vital business function for minimising the effects of unauthorised transactions upon an organisations customer service delivery, bottom line expenditure and business reputation through deployment of innovative fraud technology frameworks. Knowledge discovery techniques have been widely applied for detection of fraudulent transactions within static data sets and training of neural network based learning algorithms to preclude the occurrence of previously experienced fraud cases within future business operations. Transactional instances which match established fraud activity patterns may therefore be alerted to fraud personnel for further manual investigation and initiation of any required preventive actions.

Data mining based methods however suffer from two distinct drawbacks in the detection and prevention of fraudulent account activity. Firstly, supervised techniques such as neural (Ghosh and Reilly, 1994; Aleskerov et al., 1997; Brause et al., 1999; Boukerche and Notare, 2000) and Bayesian learning algorithms (Maes et al., 1996; Viaene et al., 2005) require extensive training using labelled data sets for

* *Corresponding author*. Tel.: +44 (0)161 3063399.
E-mail addresses: michael.edge@postgrad.manchester.ac.uk (M.E. Edge), pedro.sampaio@manchester.ac.uk (P.R. Falcone Sampaio).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.02.001

formulation of evaluative models against which to assess newly arriving transactional instances. Adopted learning algorithms must therefore be continually retrained with labelled fraud data to support the extraction of emerging fraud threats resulting in a highly time consuming and costly business operation during which new fraud instances may go undetected. Secondly, fraud evaluation is undertaken using a reactive data processing model at scheduled intervals over the organisations associated transactional data store, requiring associated entries to be present within the account database prior to application of employed data analysis techniques. As a result, fraud analytics may only be undertaken following transaction completion, fraudulent exchange of associated goods/services and movement of the associated monetary value.

In response, institutions are now moving towards increasingly proactive methods of fraud detection for real-time screening of financial data, and triggering of a preventive response prior to transaction completion in order to minimise the potential fraud deficit (Falcon Fraud Manager, 2008; Entrust, 2008; StreamBase, 2008). While implementation of proactive methods increases the potential for early fraud alerting, real-time processing significantly reduces the available window within which to perform computational analysis and produce an accurate fraud decision in response to newly arriving system events. Policies based on global thresholds have limited capabilities due to their inability to learn and adapt to observed account behaviour commonly resulting in large volumes of false alerts to be resolved by a business analyst. Research has illustrated how such methods can be refined to produce account-specific thresholds, however such methods continue to rely on labelled training data and application of values to derived account segments (Fawcett and Provost, 1997). Existing research for monitoring of individual customer account behaviour therefore remains tuned to fraud detection within reactive data processing architectures through application of data mining based methods over static post-transactional data repositories (Phua et al., 2005).

Signatures are emerging as a key technology in response to the growing demand for real-time fraud analytics through maintenance of a statistical representation of user behaviour against which to evaluate new system transactions and their likelihood of representing a fraudulent transaction (Cahill et al., 2000; Cortes and Pregibon, 2001; Ferreira et al., 2006). Signatures may therefore be recalculated as part of proactive fraud policy evaluation and compared to previously held values for detection of sizable deviations from normal account behaviour which may be indicative of fraudulent account usage. While this may reflect a simple shift of data processing from 'post' to 'pre' data storage, emerging research illustrates the abundance of issues related to the implementation and maintenance of signature based models including data processing granularity, signature initialisation, calculation procedures and feature variable selection/weighting.

This paper provides a comprehensive survey of signature based architectures, models and fraud applications to date. In particular, existing research is critically evaluated with respect to its proactive capabilities for supporting sophisticated fraud detection over streaming financial data as detailed in Edge et al. (2007), and in which it is believed little published signature research currently exists. Discussion is presented upon issues which remain in the deployment of sophisticated profiling technologies and future research directions within the signature domain outlined towards supporting effective fraud detection within rapidly evolving ubiquitous financial service models.

The remainder of this paper is structured as follows: Section 2 presents a background on fraud within the financial services domain. Section 3 provides an overview of signature functionality, architectures and processing models. Section 4 details signature based models and processing solutions for fraud detection to date. Section 5 presents a discussion on challenges which exist within studied signature solutions. Section 6 analyses future research directions within the signature domain while Section 7 summarises the key aspects addressed in this paper.

2. Background: financial fraud management

The following section provides a background on financial fraud, fraud management architectures and customer profiling technologies for detection and prevention of fraudulent financial transactions.

2.1. *Financial fraud*

Financial institutions have now recognised that the application of isolated security mechanisms on individual delivery channels simply no longer enforces the necessary levels of protection against unauthorised account activity (Massey, 2005; Fair Isaac, 2005). Financial IT platforms are often easy fraud targets due to their potential for large scale monetary theft through the numerous authentication flaws and loopholes within deployed service platform security models. Weak authentication provided by signature, PIN, password and Card Security Code (CSC) mechanisms therefore continue to facilitate illegitimate financial transactions through development of innovative system attacks and methodologies by malicious third parties. Tables 1 and 2 present the total financial loss to UK banking institutions though plastic card, cheque and online banking services over the last four year period.

In 2004, financial institutions took an active step to reduce escalating card fraud statistics through migration from existing customer signature based methods to PIN based authorisation for all Point-of-Sale (POS) card present transactions (Chip and PIN consumer guide, 2006). Accordingly, fraud figures declined in the subsequent two year period as fraudsters existing techniques based upon the physical theft of cards and card details (skimming) were no longer successful due to the requirement of the customers associated PIN data for transaction completion. Following the initial decline however figures began to rise as fraudsters deployed innovative system attacks in response to new security protocols including false ATM fronts, pinhole cameras and false POS terminals enabling the capture of both card and pin details (BBC News, 2004, 2006; University of Cambridge, 2007). Furthermore, significant rises were seen in both Card-Not-Present (CNP) and overseas card transactions as fraudsters continued to explore additional opportunities within financial