Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Instant Awareness of Fraud and Risk

Katende Nicholas*, Kibe Ann, Kubwimana David
Computing & JKUAT,
Rwanda

Abstract--Internet-based fraud is when the internet is used to steal information and resources for financial gain. Simple fraud scams can seek money or personal details, while others seek personal information that will be misused to obtain money, resources or information by deceptive means. 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. The strategic method of fraud is an effective way to detect and describe both known and unknown frauds. When used proactively to detect unknown fraud, it provides laser-like accuracy that allows for much more efficient investigation than the traditional shotgun approaches that have been used in the past. A firewall is a piece of software or hardware that secures your computer by limiting who can send you information; some firewalls even help to prevent hackers from using your computer to launch attacks on other computers. Heighten the intelligence of your existing security infrastructure to find hidden patterns and relationships suggesting malicious activity. Make better business decisions about your cyber risks.

Keywords--fraud, fraud detection, cyber security, proactive, adaptive, risk, firewall

I. INTRODUCTION

Internet-based fraud is when the internet is used to steal information and resources for financial gain. Simple fraud scams can seek money or personal details, while others seek personal information that will be misused to obtain money, resources or information by deceptive means.

Fraud can occur in many ways—from somebody using credit card details illegally to shop online, to having a person's identity assumed by another to open bank accounts, take out loans and do business illegally, under that name. Sophisticated information gathering tools such as malware and spyware enable fraudsters to gather personal information about the person they target. Phishing is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

II. FRAUD DETECTION MECHANISMS

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 behavior 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 behavior 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

Fraud-fighting activities can be grouped into three primary categories: prevention, detection, and investigation.

Fraud prevention includes such activities as designing corporate fraud policies, creating internal audit departments, implementing internal controls, whistle-blower systems, and publicizing fraud occurrences. Investigation involves steps taken to answer the questions of who, how, when, and why once fraud is suspected or "fraud predication" is present. Fraud detection includes both proactive and reactive activities targeted at finding the first indication that fraud might be occurring or undertaken to develop a "predication of fraud". Most traditional fraud detection methods are reactive in nature---that is, they are initiated by tips or complaints, control overrides, or other indicators that someone observes or hears.

Proactive fraud detection involves aggressively targeting specific types of fraud and searching for their indicators, symptoms, or red flags. Early fraud detection is critical because the sizes of most frauds increase geometrically over time as perpetuators gain confidence that their schemes are not being detected.[12]

Fraud detection can be categorized into technology-base and non-technology-based methods. Further categorizes technology-related methods into the following two categories: (1) Computerized traditional methods and (2) strategic methods. Strategic methods can be subdivided into those that (2a) focus on people, and (2b) focus on transactions and reports. Focusing on people includes methods such as using artificial intelligence techniques and fuzzy logic to score personnel profiles or matching individuals against known `bad guy' lists. Focusing on transactions involves searching records and databases for fraud symptoms relating to sales, purchasing, payment, receipt, borrowing, or other types of transactions.

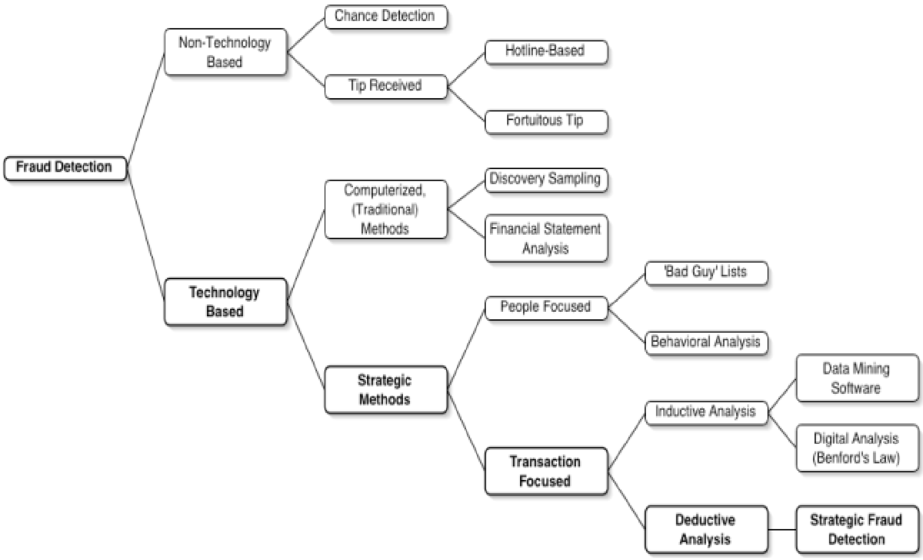


Figure 1 Fraud detection categories

Source: David J. Hand Imperial College London (2007)

III. THE STRATEGIC METHOD OF FRAUD DETECTION

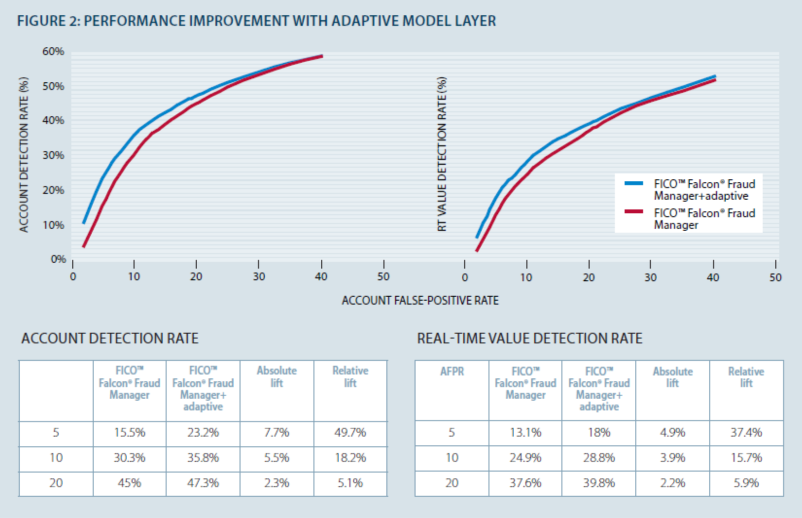
This approach can be viewed as an inductive method: it begins with anomalies brought to someone's attention and continues by researching additional events and data until it is determined that fraud may be causing the indicators

The strategic method of fraud is an effective way to detect and describe both known and unknown frauds. When used proactively to detect unknown fraud, it provides laser-like accuracy that allows for much more efficient investigation than the traditional shotgun approaches that have been used in the past. Disadvantages of the strategic method are (1) that it is more expensive to implement than reactive and inductive fraud detection methods and (2) it requires significantly more effort and expertise from team members. With repeated applications, however, economies of scale can be gained and fraud detection approaches can be automated. It is most suited to entities that have large, digital data stores and the ability to support this larger effort.

IV. ADAPTIVE MODELS

Adaptive models deployed in a cascade architecture strengthen conventional fraud detection by providing an additional method of refining the prediction of future normal and fraudulent behavior. Detection based on historical customer transactional behavior is complemented by detection based on the current behaviors observed in the operational environment.

The cascade architecture combines this deep analytic strength, based on masses of historical data, with the agility of the adaptive model. At the same time, it keeps the technologies separate, which is advantageous both for detection and operations. [5]



ACCOUNT DETECTION RATE

	FICO™ Falcon® Fraud Manager	FICO™ Falcon® Fraud Manager+ adaptive	Absolute lift	Relative lift
5	15.5%	23.2%	7.7%	49.7%
10	30.3%	35.8%	5.5%	18.2%
20	45%	47.3%	2.3%	5.1%

REAL-TIME VALUE DETECTION RATE

AFPR	FICO™ Falcon® Fraud Manager	FICO™ Falcon® Fraud Manager+ adaptive	Absolute lift	Relative lift
5	13.1%	18%	4.9%	37.4%
10	24.9%	28.8%	3.9%	15.7%
20	37.6%	39.8%	2.2%	5.9%

Figure 2

Source: fico 2010, 6

Benefits of adaptive models

General benefits

Higher fraud detection performance, particularly at low levels of false positives.

Performance rises not only because a second layer of analytics is being applied to high-scoring transactions, but because the adaptive model is scoring these transactions based on analyst fraud/no-fraud feedback on similar recent cases. Moreover, by increasing the proportion of fraud in referred transactions, the cascade enables analysts to work more fraud cases, subsequently feeding more fraud examples back into the adaptive model's fraud table. [3]

Shorter time to detect and intercept new fraud.

The adaptive cascade enables the overall fraud solution to adjust to the operational environment as captured in analyst dispositions of suspicious cases. Fraud detection is thereby able to leverage new variable relationships and fraud behaviors that were absent from or not sufficiently represented in the historical data used to train the base model. New fraud types receive higher scores much sooner than they would without the adaptive layer. Alerted to rising threats, companies can also move faster to implement new fraud rules and other policy/program changes necessary to increase protections and mitigate losses.

Flexibility to increase analytic scrutiny on certain fraud types.

Companies can put more focus on rising fraud types without reducing the effectiveness with which their base model detects all other fraud or otherwise skewing it in undesirable ways.

Reduced risk when deploying new detection approaches.

Supervised fraud models are highly refined analytics that undergo rigorous and exacting retraining procedures based on previous years' data. The use of an adaptive analytics layer provides a low-risk, more forgiving means of trying approaches not fully supported by historical data. Companies can leverage variable candidates in the adaptive model's superset (even variables suggested by observation or hunches), knowing that the variable's ultimate selection and weighting will be performed by the model itself through a completely data-driven process in the production environment.

Additional benefits for companies using custom fraud models

Decreased rate of degradation.

After deployment of a custom model, as fraud behavior changes, the effectiveness of the model gradually diminishes, particularly when the model sees fraud behavior that had not existed in the bank's historical data prior to model retraining. Degradation will occur much more slowly, however, when there is an adaptive layer absorbing current fraud case data and adjusting scores based on new fraud behaviors and patterns.

More effective extension of existing fraud detection to acquired portfolios.

Financial institutions that acquire additional portfolios can now consider protecting these new accounts with their existing fraud detection solution. While the characteristics of the acquired portfolio will differ from those used to train the supervised fraud model (based on the original portfolio of historical data), the adaptive layer will adjust variables and weights in real time to the new production environment and the behaviors in the acquired portfolio.

Additional benefits for companies using consortium fraud models

Broad fraud-type detection with tighter portfolio fit.

Companies that use consortium models are able to detect a broad range of fraud types, thanks to the vast amount of data from many different financial institutions used to build the models. With an adaptive layer, they can enjoy this benefit while making fraud detection more responsive to the specific characteristics of their own portfolio.

Retraining that goes wide and deep.

With each retraining, consortium models are refreshed with data about fraudulent and normal behaviors experienced across multiple institutions and markets over the past year. Companies that use a cascade architecture benefit from continuous retraining of their adaptive model as it self-adjusts to current fraud/no-fraud cases. Users may also choose to perform a deeper adjustment annually, perhaps adding to the superset of variable candidates based on their own portfolio's fraud experience.

V. THE THREAT AND RISK CYCLE

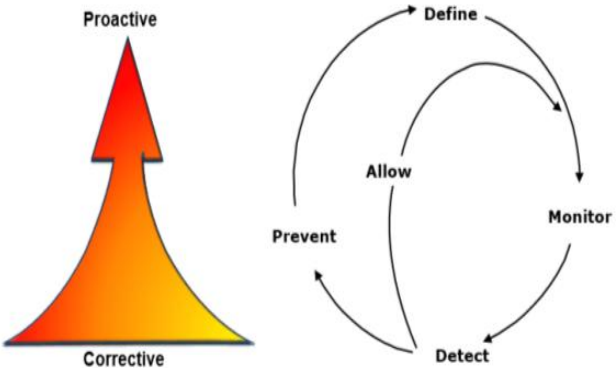


Figure 3 Threat and Risk Cycle

Source: D Dhillon - IEEE Security & Privacy, 2011 - computer.org

Define - what are the parameters, the company policy against threat, what we have learnt from the past and what do we need to take into account

Monitor - this is where we start monitoring the different types of data, using of tracking tools that are available to us, monitoring allows us to extend and include wide data sources

Detect – using predictive analytics and looking at fact based real-time data we are able to proactive detect suspicious behavior whether that's at a people or data level. Once an activity has been detected we have a choice to make **allow** the activity because it falls within the acceptable bounds or is actually a risk worth taking with advantages

Once a suspicious activity detected and it´s something that´s not acceptable this is where we take action to either prevent or put in place actions to minimize the risk and reduce our exposure.. This action could be putting more police into the field, plugging an information leak or declining a fraudulent claim

By including predictive analytics into the mix we are able to be proactive, we can prevent this activity from happening again as we run the cycle we are creating more accuracy and we´re widen our framework to include risks that might need to be considered further.

Access to fact-driven predictive insights in real-time, and driven by business needs, is key to ensuring an optimal balance between preventative and corrective actions.

Predictive Analytics enables organizations to

- monitor your environment by including a wide variety of data across multiple sources
- detect suspicious behavior to identify threats, information breaches, crime fraud
- And then control outcomes to deliver the best response to reduce exposure or loss and maximize the impact of any action taken

Predictive risk and threat management is about using analytics proactively to reduce exposure and minimize negative impact

VI. FIREWALLS

Connecting to the Internet is safer when you install and use a firewall

One of the most important things you can do if you want to stay safe online is to protect where your computer connects to the Internet. Both incoming and outgoing Internet traffic can be exploited by cyber criminals to install malicious code, destroy files, cause malfunctions or even cause an online virus to proliferate. A correctly installed and configured firewall puts up a barrier between your private computer or network and a variety of these Internet threats. A firewall is a piece of software or hardware that secures your computer by limiting who can send you information; some firewalls even help to prevent hackers from using your computer to launch attacks on other computers. While firewall protection is essential, it is also important to understand what a firewall can and cannot do so you can take the steps you need to be cyber secure. [15]

Firewall Basics

When you access the Internet, information reaches your computer through various ports opened to receive specific types of data, such as from normal Web browsing, instant messaging or checking your e-mail. A firewall determines if a source address trying to connect to your computer through an open port is one you have decided to trust and denies access to any unauthorized traffic. By dividing your communications into two distinct groups—incoming and outgoing—a firewall acts like a gatekeeper at a private club. Only those on the guest list can come into your computer and any abnormal behavior won't be allowed to leave your computer and cause harm to others. Using a firewall as part of your overall strategy for cyber security is important no matter how you connect to the Internet. While it won't guarantee the safety of your computer, not having a firewall is taking a big risk. Sooner or later, there's a good chance a hacker will discover an open port and gain access to all your information. Remember, too, that if the firewall on your computer is disabled, turned off, or has too many open ports, it can't protect you at all.

As part of an overall strategy for cyber security, firewalls play an important role in establishing the first line of defense against cyber threats. Combined with anti-spyware, anti-virus and anti-spam software, strong passwords and safe online practices, a firewall adds a layer of protection that increases your chance of staying safe online.

VII. DETECT ATTACKERS' RECONNAISSANCE ACTIVITIES IN REAL TIME

Heighten the intelligence of your existing security infrastructure to find hidden patterns and relationships suggesting malicious activity. Make better business decisions about your cyber risks. Cybersecurity arms you with an essential layer of business-relevant cyber analytics that enhances your existing security defenses. [6]

Benefits

Inject intelligence at scale.

Identify possible threats and prevent attackers from finding your organization's sensitive information. Cybersecurity finds complex links in all your network and enterprise data to give you immediate and continuous cybersecurity risk insight. By recognizing potential threats sooner, you can take action faster to neutralize their impact.

Gain true situational awareness.

Understand the meaning behind each cyber risk to develop the most effective mitigation strategy. Cybersecurity uses real-time behavioral analytics on correlated data to understand normal versus abnormal activity. With this knowledge, you can find hidden patterns that may indicate suspicious activity.

Improve SOC efficiency with analytic-driven triage.

Focus security operations center (SOC) investigations, and rescue security analysts drowning in data, false positives and duplicate alerts. Enable security analysts to manage an accurate, prioritized short list of critical risks. Cybersecurity helps security analysts do what they do best, without requiring them to become data scientists.

Stay abreast of trends and adversaries.

Attackers are getting smarter when it comes to breaching security measures, but Cybersecurity helps you stay a step ahead of the game. Behavioral analytics automatically evolves cyber analytic models based on new events, new data and new contexts. So when attackers get more sophisticated, so do your detection methods.

VIII. CONCLUSIONS

Fraud is a universal problem for businesses around the globe. Although some slight regional variations could be noted in methods used both by fraudsters to commit their crimes and by organizations to prevent and detect fraud schemes, the overall trends in our data are quite consistent, both across borders and over time. This consistency underscores the nature and pervasiveness of fraud’s threat to all organizations.

The longer frauds last, the more financial damage they cause. Passive detection methods (confession, notification by law enforcement, external audit and by accident) tend to take longer to bring fraud to management’s attention, which allows the related loss to grow. Consequently, proactive detection measures — such as hotlines, management review procedures, internal audits and employee monitoring mechanisms — are vital in catching frauds early and limiting their losses.

Hence using predictive risk and threat management in business analytics proactively will reduce exposure and minimize negative impact.

REFERENCES

[1] European Journal of Accounting Auditing and Fiancé Research Vol.1, No.4, pp.129-138, August 9, 2015

[2] Credit Scoring and Credit Control X, Edinburgh 2007

[3] How can fraud models combat new tricks (2010, January) retrieved from www.fico.com, Accessed on 8/8/2015

[4] Denning, D. (2000) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy http://www.nautilus.org/info-policy/workshop/papers/denning.html, Accessed on 8/8/2015.

[5] Fair Isaac Corporation (2010)insights» how Can Fraud Models Combat new tricks? http://www.fico.com/en/wp-content/secure_upload/Insights_Adaptive_Models_2489WP.pdf, Accessed on 8/8/2015.

[6] SAS, The essential layer for cyberdefensehttp://www.sas.com/en_us/software/fraud-security-intelligence/cybersecurity-solutions.html, Accessed on 8/8/2015.

[7] Australian Government, Protecting personal informationhttps://esafety.gov.au/esafety-information/esafety-issues/protecting-personal-information, Accessed on 8/8/2015.

[8] Albrecht, C. C., W. S. Albrecht, et. al. 2001a. "Can Auditors Detect Fraud: A Review of the Research Evidence." The Journal of Forensic Accounting**I:** (January-June) 1-12.

[9] Albrecht, C. C., W. S. Albrecht, et al. 2001b. "Conducting a Pro-Active Fraud Audit: A Case Study." The Journal of Forensic Accounting**II**: (June-December) 203-218.

[10] Albrecht, W. S. 2003. Fraud Examination. Mason, Ohio, South-Western.

[11] Nieschwietz, R. J., J. Joseph J. Schultz, et al. 2000. "Empirical Research on External Auditors' Detection of Financial Statement Fraud." Journal of Accounting Literature**19**: 190-246.

[12] David J. Hand Imperial College London (2007) Statistical techniques for fraud detection, prevention, and evaluation. http://langtech.jrc.ec.europa.eu/mmdss2007/htdocs/Presentations/Docs/MMDSS_Hand_PUBLIC.pdf, Accessed on 8/8/2015.

[13] PricewaterhouseCoopers LLP (2009). "2009 Global Economic Crime Survey". Retrieved August 9, 2015.

[14] Estevez, P., C. Held, and C. Perez (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. Expert Systems with Applications 31, 337–344

[15] The University of Texas at Austin (2010), Cyber Security Awareness,http://www.utexas.edu/its/secure/articles/firewalls.php, Accessed on 8/8/2015.