Fraud Detection Using Analytics

Dr. Padmalatha N A

Assistant Professor, School of Commerce and Management Studies, Dayananda Sagar University. Shavige Malleshwara Hills, Kumaraswamy Layout, Bangalore, (Karnataka) India

Abstract

Business data is being stored in many organization by information technology systems. Experts predict online credit card fraud to increase to $32 billion by 2020. Because of which to detect and prevent frauds organization are going for automated systems. The business fraud can be generated by employees or from outside organizations. In this article an attempt has been made to find the technologies to address the fraud and steps of adopting the technology. The outcome of the research paper is to provide an understanding of how deep learning can be used for the fraud detection.

Key Words: Fraud detection, Data analytics, deep learning

1.0 Introduction

Fraud is intentional deception to secure unlawful gain to derive a victim of legal right. Although a company cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risks, limiting damages and protecting reputation. A well-knownmethod is a threat posed by frauds penetrated using technology can be countered with the help of technology only. It can be committed through any media including mail, Internet, kiosk etc.

Fraud can be committed by employee acting alone, or in collusion with another party (a second employee) or a third party. Because of the availability information any person can collate the information about the company, its employees and clients in a damaging manner. A recent EY study based on India Fraud survey 2012, indicates that with the ever-increasing use of technology in every business, is inadvertently leading to more sophisticated and complete frauds than before.

Through effective fraud detection methods, particularly with the use of technologies, losses can be reduced effectively. Today, a number of companies wanting to incorporate proactive fraud risk management in their companies as compared to a year ago. This indicates a good future for corporate governance in India.

Current Scenario

As per the RBI reports, of more than 1.1 million people who reported fraud,21% had lost more than $63 million dollar from 2016. According to RBI data, of the total 53,334 cases of frauds during 2008-09 and 2018-19 fiscal years, involving Rs 2.05 lakh crore, a highest of 6,811 were reported by ICICI bank involving Rs 5,033.8 crore.

2.0 Literature review

The article (Parr et al), mentions about the different ways small business owners can combat the theft, ways of identifying week links, types of controls, types of restriction

of activities were discussed. Even though author mentions that availability of tools for the specific requirement of business, the exact tools were not discussed. Machine learning as an important tool for solving business fraud is widely adopted. Automated fraud detection system is highly successful in solving the problem. Stages of machine learning and Models used were discussed in the article. (How machine learning facilitates fraud detection, 2019). The article (Detecting financial fraud using machine learning, 2018) discusses about how to handle imbalanced data in machine learning. Depending on the data, the author has mentioned the use of techniques such as SMOTE (Synthetic Minority Over-sampling Technique), Random Under Sampler or SMOTE+ENN (Edited Nearest Neighbour) technique.

3.0 Objectives of the research are

1. To identify the types of businesses frauds
2. To understand the technologies adopted to prevent fraud
3. To develop stages of adopting the technology
4. Adoption of automation in fraud detection

4.0 Research Finding

- The top few fraud risks that have the potential to pose threats to businesses in India are the following::
  - Data or information threat and IP infringement
  - Bribery and corruption
  - Fraud penetrated by Senior Management
  - Fraudulent disbursements (e.g. billing schemes, payroll schemes, expense disbursement schemes, check tampering)
  - Vendor fraud or kickbacks
  - Regulatory non-compliance
  - Theft or misuse of inventory
  - Misappropriation of assets(e.g. theft of cash or receipts)

Fraud detection tools in the industry are:

- Software for continuous monitoring of business transactions
- IT based tools for retrospective identification of fraudulent payments or other abusive activity
- Software for continuous monitoring of business communications
- IT based tools for identification of unethical behaviour based on social network analysis.

Technologies used to detect fraud

New and up-to-date technology is absolutely necessary to combat fraud effectively.

It involves procedures to collect data, quick evaluation of the collected data, identifying activities, formulating patterns of fraudulent activities. Risk assessment analyses must also be performed to identify where the week links are. .

Technological advancements in data analytics such as link analysis, data visualization, predictive modelling and other analytic testing are usual tests to identify the anomalies.

Some of the interesting observations are:

- Young Professionals are potential fraudster
- Small businesses with fewer than 100 employees are most susceptible to occupational fraud.

- Internet fraud is usually penetrated by employees
- Over 90% of online fraud detection platforms use transaction rules to detect suspicious transactions.

Fraud detection arises because of three causes. Pattern of Fraud as given by Association of certified Fraud examiner's Reports (ACEF),

1. **Employee generated :**This can be solved by background checks on employees when hiring, restrictions on employee activities, awareness in the organization
2. **Organization Generated**: This can be prevented by having policies and procedures for using the organization's funds, Safeguarding assets and documents, promoting appropriate workflow
3. **Third Party generated**: This can be prevented by safeguarding organization's data access, risk assessmenttechniques

Stages of adopting the fraud detection Technology

1. **Identification of fraud**: Data across different period of time need to be analysed for identifying anomalies. However, new suppliers or new customer involved with the suspicious transactions may not be in the Master data of the organization. Data analytics tools like SAP, CaseWare IDEA, etc. can be used to identify the anomalies.
2. **Identification of fraudster's relatives and close friends**: The mobile phones and social networking applications such as Facebook, Twitter, WeChat, Instagram ,WhatsApp provides an opportunity to observe interests, linking, lifestyle , characteristics etc. Social networking analysis tools , such as NodeXL, SVAT, Gephi, etc. could be deployed to achieve the same goal. Communicationrecords can also be used to identify the reasons behind the crime.
3. **Collect Evidence**: In a digital world, most all data are stored in cell phones, Servers, cloud systems. Forensic tools such as Encase or Helix can be the technological solutions for the same.
4. **Interpretation**: In order to represent the trends tools such as Qlik, or tableau can be deployed.

Adoption of integrated technology in Fraud detection

Data scientists can solve fraud problem using machine learning and predictive analytics. It uses various algorithms to facilitate the machines to respond to different situations for which they have not been programmed explicitly. Advanced machine learning tools can automatically update its models to reflect the trends. With increased data set, machine learning models can pick similarities and differences between multiple behaviours. The advantages of machines for the fraud detection are speed, scale and efficiency.

The stages for fraud detection involves

a. Getting historical data
b. Building models for predicting fraud
c. Using the model for prediction.

However, the machine learning requires significant number of cases or large datasets to give an accurate judgement. Other challenges in this approach are high infrastructural costs, strict regulations and risk of replacing existing technology.

5.0 Conclusion

In modern business, transactions takes place through a variety of payment channels such as credit /debit card, smartphones, kiosks, etc. At the same timefraudsters are becoming adept at finding weak links in the business transactions. Hence, detecting frauds is essential for any business. And, fraud detection is possible for banks and commercial industry with the advancement of technology. With the availability of increasing processing power, advancement in statistical modelling, ability to capture and store voluminous data organizations are adopting technology to detect fraud.

Bibliography:

- Arbinder Singh, EY, "Changing face of fraud in India,
- Kuo Ming Huang, Financier Worldwide Magazine, February 2017, Fraud prevention and detection- Focus on the technological Trend
- (n.d.), How machine learning facilitates fraud detection, Maruthi Techlabs, Pvt Ltd., 2019
- Cindy Parr, CFE, is a senior auditor with Whittaker Cooper Financial Group, Certified Public Accountants and Consultants. Contact her at (321) 723-3352 i4Business
- Rafael Piere, January 17,2018, Detecting financial fraud using machine learning: Winning the war against imbalanced data, Data Science