

MANAGEMENT & ACCOUNTING REVIEW

Volume 16 No. 2
December 2017

CONTENTS

- 1 Does Social Risk Management Matter? Influencing Factors and Their Link to Firms' Financial Performances
Tamoi Janggu, Yussri Sawani, Haslinda Yusoff, Faizah Darus and Mustaffa Mohamed Zain
- 17 Corporate Social Responsibility Practices among the Smes in Malaysia – A Preliminary Analysis
Norhafizah Norbit, Anuar Nawawi and Ahmad Saiful Azlin Puteh Salin
- 41 Ethical Values, Integrity and Internal Controls in Public Sector Organisations: A Developing Country Perspective
Philip Ayagre and Julius Aidoo-Buameh
- 59 A Review on Computer Technology Applications in Fraud Detection And Prevention
Rafidah Zainal, Ayub Md Som and Nafsiah Mohamed
- 73 Detecting Accounting Anomalies Using Benford's Law: Evidence from the Malaysian Public Sector
Nooraslinda Abdul Aris, Rohana Othman, Muhamad Anas Mohd Bukhori, Siti Maznah Mohd Arif and Mohamad Affendi Abdul Malek
- 101 Integrated Reporting and Financial Performance: Evidence from Malaysia
Luk Pui Wen and Angeline Yap Kiew Heong
- 131 The Role of Intra-Organizational Factors in Accounting Information System Effectiveness
Shamsudeen Ladan Shagari

- 157 Malaysian Code of Corporate Governance and Tax Compliance:
Evidence from Malaysia
*Mohd Taufik Mohd Suffian, Siti Marlia Shamsudin,
Zuraidah Mohd Sanusi and Ancella Anitawati Hermawan*
- 181 Sustainability and Accountability of Social Enterprise
*Nur Hayati Ab Samad, Roshayani Arshad,
Siti Haliza Asat and Nawal Kasim*
- 203 The Usefulness of Financial Statement Reporting by Charitable
Companies Limited by Guarantee in Malaysia
*Ahmad Saiful Azlin Puteh Salin, Muhammad Faiz Tumiran
and Anuar Nawawi*
- 231 Public Sector Accountability – Evidence from the Auditor General’s
Reports
*Juliana Shariman, Anuar Nawawi
and Ahmad Saiful Azlin Puteh Salin*
- 259 A Comparative Analysis of Intellectual Capital Disclosure Practices
between Malaysia and Indonesia
*Zuraida Mohamad Noor, Amrizah Kamaluddin
and Erlane K Ghani*

A Review on Computer Technology Applications in Fraud Detection and Prevention

Rafidah Zainal, Ayub Md Som
and Nafsiah Mohamed
Accounting Research Institute

ABSTRACT

Since the advancement in computer technology, fraud has become one of the high-risk crimes in the world which needs urgent detection and prevention at an early stage. Nowadays, various kinds of fraud exist in commercial areas namely; credit card, healthcare insurance, online reviews, telecommunications, automobile, etc. Fraud can also happen internally and externally in an organization. In internal fraud an employee commits it individually, whereas external fraud involves a wide range of schemes including a third party. Therefore, a detection and prevention mechanism in the form of a computer software is essential in preventing fraud to curb further financial losses. The aim of this paper is to critically review the use of computer technology to detect and prevent fraud in selected areas. Recent computer platforms used as a tool to develop fraud detection and prevention systems are namely; spreadsheets, big data, forensic analytics, text analytics and expert systems. Based on the review, expert systems have been found to be the best option used as a future tool to curb fraud. The opportunities from this review may allow others to explore more on the technology implemented to improve fraud detection and prevention in future.

Keywords: *fraud detection, fraud prevention, ACL, HADOOP, expert systems*

ARTICLE INFO

Article History:

Received: 14 August 2017

Accepted: 13 November 2017

Available online: 31 December 2017

INTRODUCTION

Financial crime is known as a crime against property. It involves unlawful conversion of the property which belongs to another owner for a personal benefit. This type of crime is very profit-driven as someone could gain access and control over any particular asset in which does not belong to them (Gottschalk, 2016). Fraud can be considered as one of the world's most famous financial crimes and it is now spreading like a virus since the advancement in computer technology. Fraud has grown tremendously since the introduction of electronic commerce in financial business transactions.

According to the Central Bank of Malaysia (Bank Negara Malaysia, BNM), fraud is defined as an intended act of deception which involves financial transactions solely for personal gain. The Association of Certified Fraud Examiners (ACFE) defines fraud as the use of occupation for personal enrichment through deliberate abuse of employing organization's resources or assets (Abdallah, Maarof, & Zainal, 2016).

Computer technology usage has been very favourable nowadays which leads to many activities involved in electronic commerce (E-commerce) systems. Though it is handy, E-commerce has opened tremendous opportunities for fraudsters to be involved with financial crimes. Most of the technological systems that involve money and services can be compromised by fraudulent acts; for instance, credit card, healthcare insurance, telecommunications, insurance, etc. (West & Bhattacharya, 2016).

Having looked at all the fraud crimes which emerge so dangerously, counter measures are needed to prevent fraud from becoming an outbreak. Therefore, a system or program is essential to detect and prevent fraud from spreading like an epidemic as well as matching with the advancement in computer technology. Fraud detection and fraud prevention are two important components that are needed to strategically fight fraud. Fraud detection is the ability to recognize or discover fraudulent activities, while fraud prevention refers to measures that can be taken to avoid or reduce fraud (Baesens, Vlasselaer & Verbeke 2015).

Traditional fraud audit techniques are complicated and time consuming which transact with various areas of knowledge like economics, finance,

law and business practices (Abdallah et al., 2016). Hence, more powerful tools are needed in order to raise the effectiveness of fraud detection. The original fraud detection systems which are now in existence use data mining and statistics to extract fraudulent information from available data. When fraud becomes more complex, these methods have become outdated which leads to the emergence of advanced detection mechanisms to improve its performance (Kavitha & Suriakala, 2015). There are plenty of tools used for fraud detection, each of which tries to retain maximum quality of service while keeping false alarm at a minimum rate.

According to Bănărescu, (2015), 65% of participants who took part in the study used spreadsheet tools as forensic data analysis, 26% used text analytics tools and forensic analytics software, and only 2% employed big data technologies. Another tool that can be used to detect fraud is expert systems. The limited use of expert systems towards fraud detection has either not been published due to lack of research or it has been referred to by other names, i.e. “data mining”. The development of expert systems was based on a network administrator’s expert knowledge and the application of data mining techniques on detailed user accounts (Hilas, 2009).

This paper reviews and discusses a few forensic analytics tools that are used in detecting fraud in selected areas. The review will be divided into five sections namely; spreadsheet, big data, forensic analytic, text analytics, and expert systems.

LITERATURE REVIEW

Data can be obtained from numerous and diverse sources such as contracts, customer interactions, phones, social media, call centers, emails, faxes and many more. The trend is to use these inputs for interest of the public or private entity so as to visualize strategies, identification of opportunities, goodwill development, preventing and detecting fraud, etc. (Bănărescu, 2015).

Even though there is a wide spectrum of specialized tools on the analytical market that can support and enhance anti-fraud activities, surveys carried out have shown that managers are not taking advantage of them.

This shows that managers are not using all the applications that have been created to detect and prevent fraud.

SPREADSHEET TOOL

When electronic spreadsheet was first introduced in the late 1970s and early 1980s to the business world, it became a nearly immediate success. The usefulness, adaptability and power of the spreadsheet has shown a strong draw and helped launch the broad-based adoption of personal computers in business. Spreadsheets can do calculations, conditional statements, linking and programming through acronyms which make them extremely adept at creating ad-hoc applications (White Paper Spreadsheets, 2017).

Varma & Khan, (2013) demonstrate how to use the Excel Spread Sheet to perform the Benford distribution statistical test as an effective tool for locating red flags in suspected data from decision-making data-set of supply chain network. The application of the Excel Spreadsheet as a decision supporting tool can lead to identifying abnormal mismatch or hidden pattern of data, and its depth analysis helps organisations to scientifically examine the feasibility of implementing one 'trust-but-verify' method. Based on their results, with the simple function from Excel, fraud detection can be as one of the proactive activities to help auditors or detecting agencies to identify abnormal transactions and can assist them in performing their tasks with flying colours in a short span of time.

However, using the spreadsheet tool as a tool for detecting fraud is not enough since it limits the detection through offline services. By the time fraud is detected, the perpetrator might have walked away. Dealing with fraud, the tools should be able to handle huge amount of data for analysis but spreadsheet tools can only handle a certain amount of data. Besides that, errors during coding can interrupt the process in detecting and preventing fraud. Moreover, an additional equipment to host a database application may be needed and it will be costly.

BIG DATA TECHNOLOGIES

Datasets that grow so large in which they become hard to work with using the traditional database management systems are called “Big Data”. The size of big data is beyond the ability of normally used software tools and storage systems to capture, store, manage, as well as process the data within a tolerable time. Hadoop is a framework for performing big data analytics which provides reliability, scalability, and manageability by providing an implementation for the MapReduce paradigm (Elgendy & Elragal, 2014).

Hadoop is a framework for running programs on cluster by using a computational paradigm named MapReduce which splits up the program into smaller parts and runs them on cluster nodes. Using Hadoop cluster, data will be stored in distributed manner in data nodes before being analyzed. Using a MapReduce technique, enables resilient, distributed processing of enormous unstructured data sets across commodity computer clusters in which each node of the cluster includes its own storage. The results are analyzed using a model evaluation which varies in supervised and unsupervised learning. Overall model diagnostics will focus on determining how capable the model is in dividing the input data into discrete sets of similar cases (Phulari, Lamture, Madage, & Bhandari, 2016).

According to Kavitha & Suriakala, (2015), the Negative Selection algorithm was parallelized in the Hadoop environment to determine accuracy. It used the basic format of determining the outliers using the Euclidean distance and compared it with the threshold. While the map function performs the distance calculation, the reduced function calculated the average distance and recorded the output. The map function also calculated the affinity threshold. Cost, False Negative Rate, detection rate and true positive rates were also considered as the measuring criterion.

Though it is a sophisticated program that can detect and preventing fraud, there is still the issue of vulnerability and security concern in order to develop a secure and not vulnerable to cyber-crime. If the program is easy to be hacked and exposed to cyber-crime, the program itself is not a suitable one to be used to detect fraud as it can be easily manipulated by hackers. Hence, it will become costly to develop and to be used by others.

FORENSIC ANALYTICS SOFTWARE

Nowadays, there are many audit software that can assist auditors to improve the overall audit process and shorten the time to process it. Some of the software are namely; Audit Command Language (ACL), Interactive Data Extraction and Analysis (IDEA), Statistical Analysis System (SAS), and Microsoft Data Analyser (Bagga & Singh, 2011). In this paper, the ACL tool is used as an example of a forensic analytics software.

The ACL is one of the most leading tools in the industry and delivers audit data analytics to customers who want to oversee activities within their organizations. It is a tool that can assist auditors to test an enormous amount of data sets. The ACL can be used as audit data analytics, monitoring and auditing of the company, investigating and detecting fraudulent activities certifying compliance within company policies and developing secure data access for all users (Aiken, 2016). The use of the ACL is demonstrated in the case study by the Austrian Ministry of Finance (2017) in which they are responsible for the management of taxation and customs programs all over Austria. The Ministry auditors must inspect enormous quantities of data from a wide variety of computer platforms, while operating under severe time pressures. In Austria, all companies and individuals must submit their tax data by electronic means, but they can do so in many formats. The ACL's flexible audit analytics software has been the key to the Ministry's ability to enhance the scope and effectiveness of its tax audits. In one major initiative, over a four-year period, the Electronic Data Processing (EDP) audit team has used powerful audit analytics to identify and then recover €85 million in missed tax revenues. They are also able to stop a fraud scheme that has been misused by the hospitality sector for years. The ACL gathers valuable information for decision-making purposes. The data will be checked manually to confirm whether all the required and adequate fields are provided or not. After confirming that the data are successfully imported into the ACL tool, the raw data will then be processed (Wadhawan & Mahajan, 2016).

The ACL is known for its processing data and handling large volume of data. Though the software itself is good, users need to pay large amount of money to acquire the license and also for the training session. Not only this will be costly, the trainees might not fully understand on how to use

the program. Moreover, if the trainees do not pass the knowledge to others before they changed their job, then it will be a waste to have a program that nobody can operate.

TEXT ANALYTICS TOOL

Most financial fraud detection researches are limited to numerical data in financial statements only. However, due to deliberate concealment and/or accounting mischief, fraudulent financial data could hardly be notable from authentic data. Considering most of data contents in the financial statements are textual explanation for numeric data, researches have begun to alert the value of the largely disregarded textual information to detect fraud (Dong, Liao, & Liang, 2014). For instance, when claim adjusters write long reports during investigations, clues of fraud are normally hidden in the reports which the adjuster would not have noticed. However, the computing system which is based on business rules can spot evidence of foul play. The most important point is to observe people, who usually commit fraud, will alter their story over time and fraud detection can spot these discrepancies (Verma & Mani, 2014).

In the Kumar & Ravi, (2016) review, text mining techniques extract the information from text documents that go through a process of two steps which are text preprocessing and knowledge extraction. The text preprocessing step will convert unstructured data into a document-term matrix, whereas knowledge extraction step involves with data mining. Preprocessing step involves tokenization, stop word removal, stemming, etc. followed by formulation of a document-term matrix (West & Bhattacharya, 2016). Preprocessing plays an essential role in text mining since a high-quality of preprocessing will always yield superior results.

Text analytics is very useful when it involves with large amount of textual data such as financial statements. However, to develop a classification method to detect fraud is hard since it involves reporting from a person. Each person will have a different type of reporting which then needs a modification on the method to analyze the data. Besides that, if the report format differs each time, it can be time consuming to detect fraud due to the reformatting that need to be done so that it can follow the program format.

EXPERT SYSTEMS

An expert system can be defined as a computer system that can represent and reasoning about some knowledge-rich domain with a view to solve problem and providing advice. Expert system detectors encode knowledge about IF-THEN-ELSE rules.

According to Hilas, (2009), expert system development was based on the network's administrators' expert knowledge and the application of data mining techniques on several detailed user accounts. User demographics data can be incorporated into the expert system to enhance its accuracy. The expert system was built to detect fraudulent activity in the telecommunications network of a big organization. Prior to the expert system's integration with the organization's database, calls made were examined manually. The expert design can adapt new data and is programmed to incorporate new rules. When a fraud case was detected or reported, all the data related to it are analyzed and the outcome is expressed in the form of new rules that are fed back to the system. Appropriate adjustment of existing rules also can be performed.

An expert system can also be used to detect fraud in automobile insurance fraud. Empirical evaluation has shown that automobile insurance fraud can be efficiently detected using the proposition and the most essential thing was a proper representation of data. The system allows the imputation of domain expert's knowledge; thus, it can be adopted to new types of fraud as soon as they are noticed. The approach can assist the domain investigator to detect and investigate fraud faster and more efficiently. Moreover, the employed framework is easy to implement and applicable for fraud detection in other relational domains (Subelj *et. al.*, 2011).

An expert system can have a user-friendly interface that makes it easier to be used and it can perform real-time tests whether on historical data or new data. Not only that, it can be incorporated into a database and provide decision making based on the preference provided by the user. This is an advantage to detect fraud as the scenario can be changed to follow the current trend of fraud occurrence.

Having mentioned all the forensic analytics tools, the advantages and disadvantages of each tool are listed in Table 1 to determine which tool is more suitable to be used for fraud detection and prevention.

Table 1: Advantages and Disadvantages of Forensic Analysis Tools

Analysis tool	Advantages	Disadvantages	References
Spreadsheet	<ul style="list-style-type: none"> - Easy to get Free software (Microsoft Excel) - Easy for access logs 	<ul style="list-style-type: none"> - Errors during coding - Data might change inadvertently - Not a user friendly interface - Costly if need to use other equipment to host database application 	<p>Varma & Khan (2013)</p> <p>White Paper Spreadsheets (2017)</p> <p>Lysis (2015)</p>
Big data technologies	<ul style="list-style-type: none"> - Time taken to analyze data is shorter - Can handle enormous amount of data - More efficient 	<ul style="list-style-type: none"> - There is security concern due to lack of encryption - Vulnerable to cyber-crime - Some software can be costly due to license and training - Performance can be unclear due to external factors (human) 	<p>5 Big Disadvantages of Hadoop for Big Data (2017)</p> <p>Bonchi, <i>et. al.</i> (2017)</p>
Forensic analytics software	<ul style="list-style-type: none"> - Faster in processing data - Can compare large database - Have complete set of pre-programmed analysis 	<ul style="list-style-type: none"> Require training Costly to obtain (license) 	<p>Aiken (2016) Using Computer-Assisted Auditing Techniques to Detect Fraud (2017)</p>
Text analytics	<ul style="list-style-type: none"> Very useful for fraud with large amounts of textual data (financial statement) 	<ul style="list-style-type: none"> - Need another classification method to perform actual fraud detection - Textual data hard to process because more subjective 	<p>West & Bhattacharya (2016)</p> <p>Verma & Mani, (2017)</p> <p>Ravi & Kumar (2016)</p>

Expert system	<ul style="list-style-type: none"> - Proposed combination of rules and profile extraction - Simple to implement - User friendly interface - Used decision-making technique - Can perform real-time tests and batch tests on historical data - Reliable - Increased output quality and productivity 	<ul style="list-style-type: none"> - Difficult to transfer human expert to the system since explanation can bring miscommunication - Have potential liability from use of expert systems 	Technology Guide 4: Intelligent System (2017)
---------------	---	--	---

It is shown that an expert system gives more advantages in detecting and preventing fraud as compared to other tools. Expert systems have the advantage of combining rules and profile extraction in the framework for fraud detection. These are considered good advantages for auditors since they can insert their own constraint to detect fraud. Besides its user-friendly interface, it is also a reliable system that can be operated in real-time or on historical data. This option would enable auditors to compare latest result with prior results, thus they can keep their performance at the top. The downturn of this software is that it is difficult to transfer human expertise into the system due to miscommunication and different understanding of a certain topic. Compared it to other tools, the spreadsheet tool is the least preferable tool because data might be changed inadvertently which will affect conclusive results. As for the forensic analytics software, despite being advantageous, the main problem with the software is the cost to obtain and for training. Big data technologies have security problems with their database because of its programming languages which are written in Java, thus it is vulnerable to cyber-crime attack.

CONCLUSION

The best computer technology application to detect and prevent fraud is the expert system because of its characteristics which is user friendly. Expert systems can combine rules and profile extraction in the framework for fraud detection. This is a good advantage for auditors since they can insert their own constraint to detect fraud. It is also a reliable system that can be operated in real-time or on historical data. This option enables auditors to compare the latest results with prior results, thus they can keep their performance at the top.

While this review focuses on fraud detection and prevention, a review on different types of financial crime can be done in future studies. This is due to the flexibility of each tool to detect and prevent different types of crime. Besides that, more reviews on the use of expert systems on fraud crime should be conducted since there is very limited research available in the literature.

ACKNOWLEDGMENT

The authors wish to extend their gratitude to the Malaysian Ministry of Higher Education for the financial support through 600-RMI/ARI_IRES 5/3 (0053/2016). The authors would also like to thank the Accounting Research Institute (ARI) and Faculty of Chemical Engineering, Universiti Teknologi MARA (UiTM), Shah Alam for the support given.

REFERENCES

- 5 Big Disadvantages of Hadoop for Big Data. (2017, February 28). Retrieved from Big Data Companies: <http://www.bigdatacompanies.com/5-big-disadvantages-of-hadoop-for-big-data/>.
- Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90–113. <https://doi.org/10.1016/j.jnca.2016.04.007>.

- Aiken, K. (2016). Analyzing Proactive Fraud Detection Software Tools and the Push for Quicker Solutions. *Economic Crime Forensics Program*.
- Baesens, B., Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive and Social Network Techniques*. North Carolina.
- Bagga, S., & Singh, G. N. (2011). Comparison of Data Mining and Auditing Tools. *International Journal of Computer Science and Communication*, 275-277.
- Bănărescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, 32(15), 1827–1836. [https://doi.org/10.1016/S2212-5671\(15\)01485-9](https://doi.org/10.1016/S2212-5671(15)01485-9).
- Bonchi, F., Castillo, C., Gionis, A., & Jaimes, A. (2017, February 28). *Social Network Analysis and Mining for Business Applications*. Retrieved from Citeseerx Web Site: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.225.9932&rep=rep1&type=pdf>.
- Dong, W., Liao, S., & Liang, L. (2014). Financial Statement Fraud Detection Using Text Mining: A Systemic Functional Linguistics Theory Perspective.
- Elgendy, N., & Elragal, A. (2014). Big Data Analytics: A Literature Review Paper. *Springer International Publishing Switzerland*, 214-227.
- Gottschalk, P. (2016). Investigating Fraud and Corruption : Characteristics of White-Collar Criminals. *Journal Of Forensic Sciences & Criminal Investigation*, 1(2).
- Hilas, C. S. (2009). Designing an expert system for fraud detection in private telecommunications networks. *Expert Systems with Applications*, 36(9), 11559–11569. <https://doi.org/10.1016/j.eswa.2009.03.031>.
- Lysis. (2015, March 31). *The Disadvantages of a Microsoft SQL Server*. Retrieved from Techwalla Web Site: <https://www.techwalla.com/articles/the-disadvantages-of-a-microsoft-sql-server>.

- Kavitha, M., & Suriakala. (2015). Fraud Detection in Current Scenario, Sophistications and Directions: A Comprehensive Survey, *III(5)*, 35–40.
- Kumar, B. S., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems, 114*, 128–147. <https://doi.org/10.1016/j.knosys.2016.10.003>.
- Phulari, S. V, Lamture, U. S., Madage, S. V., & Bhandari, K. T. (2016). Pattern Analysis and Fraud Detection Using Hadoop Framework, *5(1)*, 92–100.
- Subelj, L., Furlan, S., & Bajec, M. (2011, April 21). An Expert System for Detecting Automobile Insurance Fraud Using Social Network Analysis. *Journal Of Expert Systems with Applications*.
- Technology Guide 4: Intelligent System*. (2017, 28 February). Retrieved from Auburn.edu Web Site: www.auburn.edu/~fordfn1/r14tg4.ppt.
- Using Computer-Assisted Auditing Techniques to Detect Fraud*. (2017, February 28). Retrieved from Optimize Our Inventory: <http://www.optimizeourinventory.com/download/ExamplesProfitLeakingFraud/CAATS%20and%20Fraud%20-%20June%2014>
- Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems, 75*, 38–48. <https://doi.org/10.1016/j.dss.2015.04.013>.
- Varma, T. N., & Khan, D. A. (2013). Fraud Detection in Supply Chain using Excel Sheet. *International Journal of Computer Applications, 80(October)*, 975–8887.
- Verma, R., & Mani, S. R. (2014). Using analytics for insurance a new opportunity for fraud detection? *Infosys FINSights*.

Wadhawan, A., & Mahajan, R. (2016). Detecting and Managing Operational, Transactional and Auditing Risk using Data Analytics. *5th International Conference on Reliability, Infocom Technologies and Optimization*.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security*, 57, 47–66. <https://doi.org/10.1016/j.cose.2015.09.005>.

White Paper Spreadsheets. (2017, February 25). Retrieved from ACL website: https://www.acl.com/pdfs/White_Paper_Spreadsheets.pdf.