International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 6th Mar 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: **FRAUDFIND: A NEW APPROACH FOR IDENTIFYING FINANCIAL FRAUDS BY OBSERVING HUMAN CHARACTERS**

Volume 08, Issue 03, Pages: 62–66.

Paper Authors

MR. PRADEEP KUMAR, SK.NAGEENA
Vignan's Lara Institute of Technology & Science

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

FRAUDFIND: A NEW APPROACH FOR IDENTIFYING FINANCIAL FRAUDS BY OBSERVING HUMAN CHARACTERS

MR. PRADEEP KUMAR[1], SK.NAGEENA[2]
Assistant Professor[1], Department of M.C.A, Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A Vignan's Lara Institute of Technology & Science

Abstract:

Financial fraud is commonly represented by theuse of illegal practices where they can intervene from seniormanagers until payroll employees, becoming a crime punishableby law. There are many techniques developed to analyze,detect and prevent this behavior, being the most importantthe fraud triangle theory associated with the classic financialaudit model. In order to perform this research, a survey of therelated works in the existing literature was carried out, withthe purpose of establishing our own framework. In this context,this paper presents FraudFind, a conceptual framework thatallows to identify and outline a group of people inside anbanking organization who commit fraud, supported by thefraud triangle theory. FraudFind works in the approach ofcontinuous audit that will be in charge of collecting informationof agents installed in user's equipment. It is based on semantictechniques applied through the collection of phrases typed bythe users under study for later being transferred to a repositoryfor later analysis. This proposal encourages tocontribute withthe field of cybersecurity, in the reduction of cases of financialfraud.

Introduction

Fraud is a worldwide phenomenon that affects public and private organizations, covering a wide variety of illegal practices and acts that involve intentional deception or misrepresentation. According to the Association of Certified Fraud Examiners (ACFE) [1] fraud includes any intentional or deliberate act of depriving another of property or money by cunning, deception or other unfair acts. The 2016 PwC Global Economic Crime Survey report describes that more than a third of organizations worldwide have been victims of some kind of economic crime such as asset misappropriation, bribery, cybercrime, fraud and money laundering. Approximately 22% of respondents experienced losses of between one hundred thousand and one million, 14% suffered losses of more than one million and 1% of those surveyed suffered losses of one hundred million dollars. These high loss rates represent a rising trend in costs caused by fraud. In organizations, 56% of cases are related to internal fraud and 40% to external, this difference is since any individual related to accounting and financial activities is considered a potential risk factor for fraud [2]. When observing the behavior of people in the scope of business processes, it can be concluded that thehuman factor is closely linked and related to the fraud triangle theory of the Donald R. Cressey [3], where three basic concepts: pressure, opportunity and rationalization; are needed. Nowadays, there are different solutions in the commercial field [4], [5] as well as the the academic field, where some works in progress had been identified [6], [7] aimed at detecting financial fraud. In both cases, these solutions are focused on the use of different tools that perform statistical and parametric analysis, as well as behavioral analysis, based on data mining techniques and Big Data; but none of them solve the problem of detection financial fraud in real time. FraudFind, unlike other proposals, detects, reports and stores fraudulent activities in real time through the periodic analysis of the information generated by users for further analysis and treatment. This paper presents FraudFind, a conceptual framework that allows detecting and identifying potential criminals who work in the banking field, in real time, based on the theory of the fraud triangle. For the design of the FraudFind framework, some software components related to the processing of informtion were analyzed, among them, RabbitMQ, Logstash and ElasticSearch. In addition, the computerization of the triangle of fraud and the use of semantic techniques will allow finding possible bank delinquents with a lower false positive rate.

Existing system:

A key aspect is to classifyindividuals by focusing on reducing the internal risk of fraudthrough a descriptive mining strategy.Besides, the experience of auditors plays an importantrole in the fight against financial fraud. Some work isproposed which points to the creation of new frameworks that provide systematic processes to help auditors to discover financial fraud within an organization by analyzing existing information and data mining techniques using their own

experience and skills. Accordingly, another proposalcreates generic frameworks for the detection of financialfraud FFD, to evaluate the different characteristics of FFDalgorithms according to a variety of evaluation criteria.

Proposed system

The proposed framework operates in the continuous auditingapproach to discover financial fraud within an organizationbelonging to the banking sector which will beour main study environment and also focused on the fraudtriangle theory with the human factor considered as anessential element. FraudFind is proposed with the objectiveof analyzing large amounts of data from different sources ofinformation for later processing and registration. The agent is an application installed in the workstationsof the users (endpoints), in order to extract the data thatthey generate from the different sources of information thatreside on their equipment. This application is responsiblefor sending the data entered by the user forordering and classification. Later this organized informationis received by Logstash for its treatment.

Module Implementation

1. **Agent**

The agent is an application installed in the workstationsof the users (endpoints), in order to extract the data thatthey generate from the different sources of information thatreside on their equipment. This application is responsiblefor sending the data entered by the user forordering and classification.

2. **Behavior analysis**

If we are given a set of patterns or a set of feature vectors for some set of population then we would like to know if the data set has some relatively distinct subsets or not. In this context we can define cluster analysis as a classification technique for forming homogeneous groups within complex data sets. Typically, we do not know a priori the natural groupings or subtypes, and wewish to identify groups within a data set. We wish to form classifications, taxonomies, or typologies that represent different patterns in the data.

3. **Fraud detection**

Behavioral analytics solutions are designed to understand the normal behavior of each individual account holder, calculate the risk of each new activity and then choose intervention methods commensurate with the risk. The key characteristics that make behavioral analytics effective are automatically monitoring all activity for all account holders, not just devices or transactions; no requirement for prior knowledge of the specific fraud that the perpetrator is attempting; and providing detailed historical context for suspicious activity.

4. **Fraud category**

Periodically, a task that do the alert tracking, checks the information entered and compares it with a fraud triangle library to determine if there is a relation in order to generate an alert that will be stored in the database. The library of the fraud triangle is just a dictionary that contains three definitions: pressure, opportunity and justification. Under these parameters, the sentences and words associated with these behaviors are composed.

Algorithm

1. **K means clustering**

K-Means clustering intends to partition *n* objects into *k* clusters in which each object belongs to the cluster with the nearest mean. This method produces exactly *k* different clusters of greatest possible distinction. The best number of clusters *k* leading to the greatest separation (distance) is not known as a priori and must be computed from the data. The objective of K-Means clustering is to minimize total intra-cluster variance, or, the squared error function.

Conclusion:

The present work proposes Fraud Find, a conceptual framework to detect financial fraud supported by the fraud triangle factors which, compared to the classic audit analysis, makes a significant contribution to the early detection of fraud within an organization. Taking into account human behavior factors, it is possible to detect unusual transactions that would have not been considered using traditional audit methods. These patterns of behavior can be found in the information that users generate when using the different applications on a workstation. The collected data is examined using data mining techniques to obtain patterns of suspicious behavior evidencing possible fraudulent behavior. Nevertheless, the legal framework and the different regulations that are applied in public and private institutions of a particular region represent a high risk for the non-implementation of this architecture as an alternative solution. Future work will have as its main objective the implementation and evaluation of the framework as a tool for continuous auditing within an organization.

References

1. Sharing in MULTICS. In Proceedings of the Fourth Symposium on Operating System Principles, SOSP 1973, Thomas J. Watson, Research Center, Yorktown Heights, New York, USA, October 15-17, 1973.

2. Robert Morris and Ken Thompson. Password Security: A Case History, 1979. http://cs-www.cs.yale.edu/homes/arvind/cs422/doc/unix-sec.pdf.

3. Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In Dan Boneh, editor, Advances in Cryptology – CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 617–630. Springer, 2003.

4. Password Hashing Competition (PHC), 2014. https://password-hashing.net/index.html.

5. Donghoon Chang, Arpan Jati, Sweta Mishra, and Somitra Kumar Sanadhya. Rig: A simple, secure and flexible design for password hashing. In Dongdai Lin, Moti Yung, and Jianying Zhou, editors, Information Security and Cryptology - 10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers, volume 8957 of Lecture Notes in Computer Science, pages 361–381. Springer, 2014.

6. Ari Juels and Ronald L. Rivest. Honeywords: making passwordcracking detectable. In 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4- 8, 2013, 2013.

7. Fred Cohen. The Use of Deception Techniques: Honeypots and Decoys. http://all.net/journal/deception/Deception Techniques .pdf.

8. Lance Spitzner. Honeytokens: The Other Honeypot, 2003. http://www.symantec.com/connect/articles/honeytokens-other-honeypot.

9. Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. Kamouflage: Loss-resistant password management. In Computer Security - ESORICS 2010, 15th European Symposium on Research in Computer Security, Athens, Greece,

September 20-22, 2010. Proceedings, pages 286–302, 2010.

10. Wikipedia contributors. 2012 LinkedIn hack. Wikipedia, The Free Encyclopedia, Date retrieved: 29 May 2016. Available at: https://en.wikipedia.org/w/index.php?title=2012 LinkedIn hack&oldid=722095159.

11. Bruce Schneier. Cryptographic Blunders Revealed by Adobe's Password Leak. Schneier on Security, 2013. Available at: https://www.schneier.com/blog/archives/2013/11/ cryptographic b.html.

12. Swati Khandelwal. Hacking any eBay Account in just 1 minute, 2014. Available at: http://thehackernews.com/2014/09/ hacking-ebay-accounts.html.

13. Wikipedia contributors. Ashley Madison data breach. Wikipedia, The Free Encyclopedia, Date retrieved: 29 May 2016. Available at: https://en.wikipedia.org/w/index.php?title= Ashley Madison data breach&oldid=721001290.

14. Troy Hunt. Observations and thoughts on the LinkedIn data breach, 2015. Available at: https://www.troyhunt.com/ observations-and-thoughts-on-the-linkedin-data-breach/.

15. Michael Gilleland. Levenshtein Distance, in Three Flavors. Available at: http://people.cs.pitt.edu/_kirk/cs1501/assignments/editdistance/Levenshtein%20Distance .htm.

15. Bibliography

(1) Java Complete Reference by Herbert Shield

(2) Database Programming with JDBC and Java by George Reese

(3) Java and XML By Brett McLaughlin

(4) Wikipedia, URL: http://www.wikipedia.org.

(5) Answers.com, Online Dictionary, Encyclopedia and much more, URL: http://www.answers.com

(6) Google, URL: http://www.google.co.in

(7)Project Management URL: http://www.startwright.com/project.html