FINANCIAL FRAUD DETECTION BASED ON HUMAN BEHAVIOR ANALYSIS

P.Muthyalu
Associate Professor, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India 524101 ,muthyalu.pindi@gmail.com
U. Sai jyothi, P.Nithya , V.Grace mary , V.Rohini

saijyothisdss@gmail.com ,nithyanithu561@gmail.com , ,vandalagracemary@gmail.com,

rohiniveguru814@gmail.com

UG Student, Department of Computer Science Engineering , Narayana Engineering College, Gudur, AP, India

524101

Abstract –Financial fraud is commonlyrepresented by the use of illegal practices wherethey can intervene from senior managers until payroll employees, becoming a crime punishable by law. There are many techniques developed to analyze, detect and prevent this behavior, being the most important the fraud triangle theory associated with the classic financial audit model. In order to perform this research, a survey of the related works in the existing literature was carried out, with the purpose of establishing our own framework. In this context, this paper presents Financial FraudDetection Scheme, a conceptual framework that allows to identify and outline a group of people inside an banking organization who commit fraud, supported by the fraud triangle theory. Financial Fraud Detection Scheme works in the approach of continuous audit that will be incharge of collecting information of agents installed in user's equipment. It is based on semantic techniques applied through the collection of phrases typed by the users under study for later being transferred to ar epository for later analysis. This proposal encourages to contribute with the field of cybersecurity, in the reduction of cases of financial fraud.

Index Terms- financial fraud, Cyber security,

NTRODUCTION

Fraud is a worldwide phenomenon that affects public and private organizations, covering a wide variety of illegal practices and acts that involve intentional deception ormisrepresentation. 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 unfairacts.

This paper presents Financial Fraud Detection Scheme, a conceptual framework that allows detecting and identifying potential criminalswho work in the banking field, in real time, based on the theory of the fraud triangle. For the design of the Financial Fraud Detection Scheme 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 offraud and the use of semantic techniques will allow finding possible bank delinquents with alower false positive rate.

II. LITERATURE SURVEY

This study aims to design an architecture modeladapted to the fraud triangle factors, complemented with the human factor and analyzing suspicious behavior to identify possible cases of fraud. For a future work to carry out its implementation. In this context, several studies were found in the literature, which contribute to this topic.

Most of the documents address the issue of financial fraud and the different circumstances surrounding it. Nevertheless, identifying people who might be involved in fraudulent activities is a determining factor. The incursion into the behavioral analysis is quoted to [6], whose authors introduce an automatic text mining process by e-mail for the detection of different types of patterns in messages. While in [7] a generic architectural model is proposed that supports the factors of the fraud triangle. Inaddition, it performs the classic quantitativeanalysis of commercial transactions that arealready applied as part of the fraud detection audit. The identification and classification of possible fraud by suspicious individuals is a central element of the internal threat predictionmodel [8]. A key aspect is to classify individuals by focusing on reducing the internalrisk of fraud through a descriptive mining strategy [9].

Besides, the experience of auditors plays an important role in the fight against financial fraud. Some work is proposed which points to the creation of new frameworks that provide systematic processes to help auditors to discover financial fraud within an organizationby analyzing existing information and data mining techniques using their own experience and skills [10].

Accordingly, another proposal creates generic frameworks for the detection of financial fraudFFD, to evaluate the different characteristics of FFD algorithms according to a variety of evaluation criteria [11]. New approaches detectatypical values by studying and modifying clustering algorithms such as K-Means, with the purpose of improving the performance andaccuracy in the detection of unusual values in adata set [12][13][14].

PROPOSED WORK

The proposed framework operates in the continuous auditing approach to discover financial fraud within an organization belonging to the banking sector which will be our main study environment and also focused on the fraud triangle theory with the human factor considered as an essential element. Financial Fraud Detection Scheme is proposed with the objective of analyzing large amounts of data from different sources of information for later processing and registration, using the ELK stack. ELK is a scalable open sourceplatform used for real-time data analysis composed by ElasticSearch, Logstashand Kibana applications, which will be explained below. 1) ElasticSearch is an open source search engine developed in Java, which is a distributed, scalable document warehouse and works in real time. Designed mainly to organize data in order to be easily accessible. 2)Logstash is an open source tool used for event management, by centralizing and analyzing a large number of structured and unstructureddata types. 3) The Kibana web interface is an adjustable board that can be altered andchanged to suit our environment. It allows the creation of tables and diagrams, in addition to complex representations

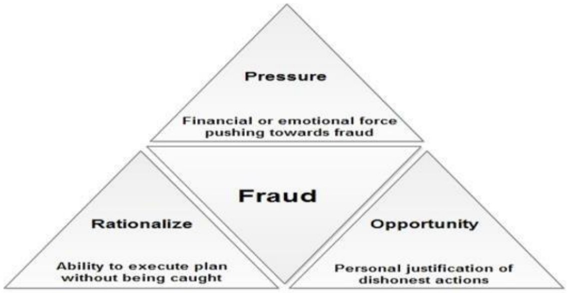
Pressure
Financial or emotional force pushing towards fraud
Fraud
Rationalize
Ability to execute plan without being caught
Opportunity
Personal justification of dishonest actions

Figure 1. Triangle of Fraud

In Figure 2 we can observe the different modules that compose the framework: Agent, QoS, Collect & Transform, Search & Analyze;and View & Manage.

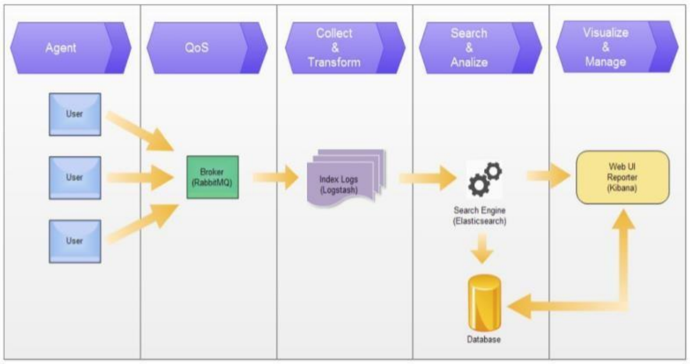

Figure 2. Financial Fraud Detection SchemeFramework

A. Agent

The agent is an application installed in the workstations of the users (endpoints), in orderto extract the data that they generate from the different sources of information that reside ontheir equipments.

B. QoS

The integration between several systems or components suggests the need to receive or send information, so these communications must be reliable, safe, fast and above all be permanently available. Due to that the volume of in formation generated by the agents is considerable and recurrent, this module will ensure its delivery in an orderly and reliable way to Logstash. Figure 3 shows the operationof RabbitMQ.

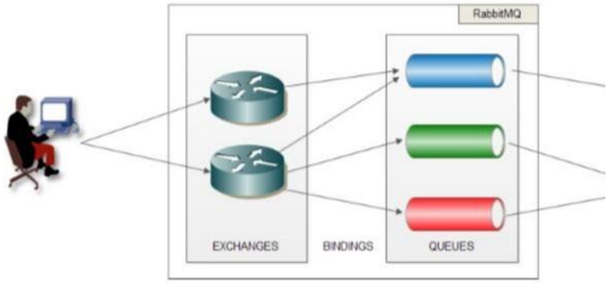

Figure 3. RabbitMQ

C. Collect and Transform

This module is responsible for processing the data sent by the agents. As seen in Figure 2, after ordering the input data of the agents in theQoS module, they are recorded in a temporary file that has raw information that Logstash doesnot understand and does not know how to handle it.The operation of Logstash is presented in Figure 4.

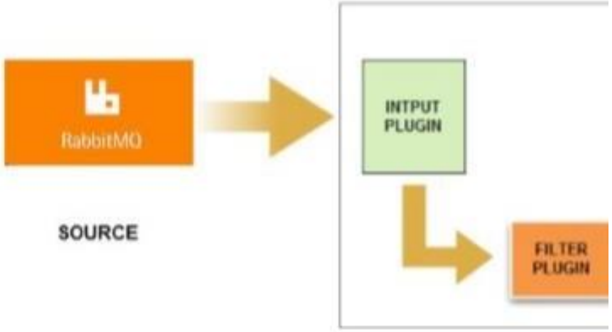

Figure 4. Logstash

D. Search and Analyze

This module has all the information processed by Logstash, which is stored immediately after it is received, being able to perform searches efficiently. ElasticSearch is a tool designed with the clustering approach, based on the premise of no fault tolerance hardware.Figure 5 shows the architecture of ElasticSearch and its components.

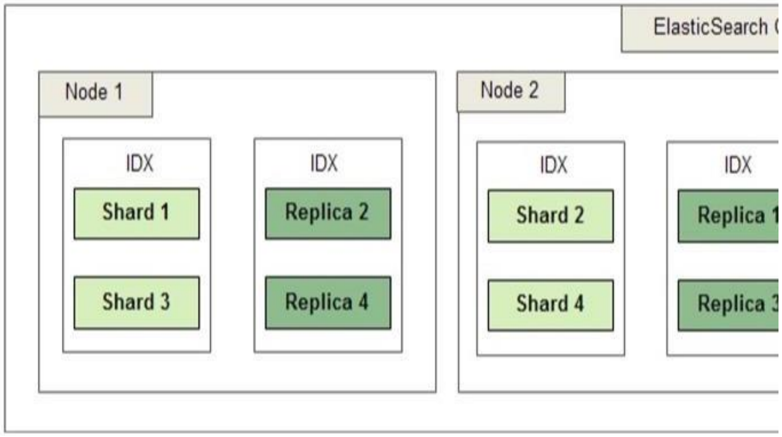

Figure 5. Elastic Search

E. Visualize and Manage

Finally, in this module the presentation of the data contained in Elasticsearch is performed, using for this purpose Kibana.

III. RESULTS

Performance analysis Financial Fraud Detection Scheme consists of the extraction of data from different sources of information through agents installed in workstations, whichcollect behavioral data and send these information in an organized way, reporting itsactivity to the central server. The typed words are sent to RabbitMQ, an application that manages message queues, which delivers fast, secure and reliable information to Logstash, a tool used to collect, analyze data from monitoring heterogeneous sources and finally to ElasticSearch that performs indexing. All this is aimed at ensuring the security in the transactions generated by the users trying to identify possible acts of fraud through the analysis of human behavior and the treatment of the results. Unusual behavior does not guarantee the intentionally of committing fraud, so it should take into consideration the analysis of risk factors associated with this behavior, which should be measurable and weighted in accordance with security policies in an organization.Technical analysis The ELK (ElasticSearch, Logstash and Kibana) platform provides versatile and functional records management when searching and analyzing information from a source. Centralized data logging can be useful for identifying unusual traffic patterns, allowing you to search for all stored records that quickly execute the necessary event correlation.Security analysis the possible violation of privacy is a factor that should be considered when implanting this solution within a company. Legal data protection regulationsshould be considered in a given region. The possible violation of privacy is a factor that must be considered when setting up to integratethis solution into a company. The legalregulations for data protection in a given regionshould be considered. The level of monitoring will depend on the internal policies in an organization and the laws that are governed in each country and should be determined taking into account the advice of the legal part of the institution or company.

CONCLUSIONS

The present work proposes Financial Fraud Detection Scheme, a conceptual framework to detect financial fraud supported by the fraud trianglefactorswhich,comparedtotheclassicaudi tanalysis, makes a significant contribution to the early detection of fraud within an organization. Taking into account human behavior factors, it is possible to detect unusualtransactions 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. Thecollected data is examinedusing data mining techniques to obtain patterns of suspicious behavior evidencing possible fraudulent behavior.

REFERENCES

[1]“ACFE Asociaci´on de Examinadores de Fraudes Certificados,” (Date last accessed 15-July-2014). [Online]. Available: http://www.acfe.com/uploadedfiles/acfewe bsite/ content/documents/rttn-2010.pdf

[2]“PwC,” (Date last accessed 15-July-2014). [Online].Available:https://www.pwc.com/gx/en/economic- crime-survey/ pdf/GlobalEconomicCrimeSurvey2016.pdf

[3] N. B. Omar and H. F. M. Din, “Fraud diamond risk indicator: An assessment of its importance and usage,” in 2010 International Conference on Science and Social Research (CSSR 2010). IEEE, dec 2010.

[4]“Lynx,” (Date last accessed 15-July-2014).[Online].vailable:http://www.iic.uam.es/soluciones/banca/lynx/

[5]“Ibm,” (Date last accessed 15-July-2014). [Online].available:https://www.ibm.com/developerworks/ssa/local/analytics/prevencionde-fraude/index.html

[6]C. Holton, “Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billiondollar problem,” Decision Support Systems,vol. 46, no. 4, pp. 853–864, mar 2009.

[7] S. Hoyer, H. Zakhariya, T. Sandner, and M.

H. Breitner, "Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit," in 2012 45th Hawaii International Conference on System Sciences. IEEE, jan 2012.

[8]M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model," in Trust, Privacy and Security in Digital Business. Springer Berlin Heidelberg, 2010, pp. 26–37.

[9]M. Jans, N. Lybaert, and K. Vanhoof, "Internal fraud risk reduction: Results of a data mining case study," International Journal of Accounting Information Systems,vol. 11, no. 1, pp. 17–41, mar 2010.

[10] P. K. Panigrahi, "A framework for discovering internal financial fraud using analytics," in 2011 International Conferenceon Communication Systems and Network Technologies, June 2011, pp. 323–327.

[11] D. Yue, X. Wu, Y. Wang, Y. Li, and C. H.Chu, "A review of data mining-basedfinancial fraud detection research," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Sept 2007, pp. 5519– 5522.

[12] M. Ahmed and A. N. Mahmood, "A novelapproach for outlier detection and clustering improvement," in 2013 IEEE 8th Conference on Industrial Electronics andApplications (ICIEA), June 2013, pp. 577–
582.

[13]. V Sucharita, S Jyothi, PV Rao,"Comparison of machine learning algorithms for classification of Penaeid prawn species 2016 3rd International Conference on Computing for sustainable global development pages, 1610-1613.

[14]. S. Jyothi, V. Sucharita, D.M. Mamatha " Survey on Computer Vision and Image Analysis based Techniques in Aquaculture", CIIT International Journal of Digital Image Processing, 2013

Castleman, K. (1993). Digital image processing