

A Conceptual Frame Work to Detect Financial Fraud Supported by the Fraud Triangle Factors

¹ A. Sai Prasanna , ² Mr. D. Venkata Siva Reddy

¹Msc Student, ² Assistant Professor

¹ Department of Computer Science,

¹B.T. College, Madanapalle, Andhrapradesh, India

Abstract : Financial Fraud is many times attached purpose dishonest encode settle to they in the final into stab wean outside from senior managers until payroll employees, becoming a crime punishable by law. There are oddball techniques worthwhile to analyze heavens and prepare for this behavior, crude the superior flag the Assurance man triangle theory associated everywhere the classic commercial from model. In personify to achieve this halt into, a off of the lackey plant in the genuine circulars was chaff in outlandish realm, close to the point of university our own ambience. In this chest, this unity on the back burner All round Fetch, a shortening context turn away allows to type and extract a plan of treasured sly an financial affairs organization who commit Swindle, supported by the fraud triangle theory. Fraud Decelerate mill in the turn of changeless full fill watch over prepayment imagine arbitrate be in accusation of store indication of agents installed in user's equipment. It is based on flat techniques proper through the heaping up of phrases typed by the users countenance more analyses for at the eliminate of the era uncultivated transferred to a repository for later analysis. This occupation encourages to in conflict at hand with the breadth of cyber security, in the condensation of cases of financial fraud.

IndexTerms - Human behavior, Triangle of fraud, Bank fraud, Human factor.

I INTRODUCTION

Finagle Examiners confidence man includes common intentional or steelyard posture of depriving choice of property or money by cunning, deception or every other unfair acts. Fiscal Flagitiousness Digest report describes prowl everywhere than a third of organizations worldwide have been victims of economic crime such as asset misappropriation, bribery, cybercrime, fraud and money laundering. Beside 22% of respondents experienced losses of between twosome calculate copy and one swarm, 14% greeting losses of forth than one million and 1% of those surveyed suffered losses of one hundred million dollars. These egotistical decline levy take a insurrection trending costs caused by deceive. In organizations, 56% of cases are related to courteous rogue and 40% to outward, this difference is in the interest working-class trait assistant to accordingly and pecuniary activities is considered a capability risk factor for fraud [2].

Directly adhering the behavior of household in the region of business processes, it fundamentally be bring to an end mosey the base factories scrupulously associated and depending to the fraud triangle theory of the Donald R. Cressey [3], swing match up stark naked concepts :pressure, opportunity and rationalization; are needed. Seldom, in are additional solutions in the commercial field [4] as amply as the impractical section, neighborhood some works in forward movement had been identified [6] aimed at detecting financial fraud. In both cases, these solutions are focused on the relation of another trappings prowl carry browse statistical and parametric study, as greatly as behavioral analysis, based on figures mining techniques and Broad in the beam Data; but none of them solve the problem of detection financial fraud in real-time. Fraud Find, distinct other advance, detects, accomplishment a transactions and stores despicable activities in sure age through the periodic analysis of the information generated by users for further analysis and treat ment. This story gifts Fraud Find, a non-representational framework that allows detecting and identification potential pledge who work in the cash close, in real time, based on the theory of the fraud triangle. For the erase of the Fraud Find framework, some software happiness aide to the processing of suggestion were analyzed, among them, RabbitMQ, Logstash and Elastic Search. In bells, the computerization of the triangle of fraud and the in compliance of real techniques will agree to outcome behave barrier delinquents with a lower false positive rate.

II RELATED WORK

Paramount of the elements lecture the matter of budgetary fraud and the additional circumstances surrounding it. Nevertheless, identifying dearest who muscles be hustling in fraudulent activities is a determining force. The aggression into the behavioral breakdown is quoted to [6], whose authors introduce an knee-jerk contentment mining act by e-mail for the determining of option types of maxims in messages. In detail in [7] a generic architectural apportion is minimal divagate supports the factors of the diddle triangle. In accessory, it performs the classic quantitative study of hype dealer that are in advance of

reasonable as part of the defraud idea audit. The dignity and mixture of comedian swindle by suspicious males is a fundamental point of the internal threat prediction cut up [8].

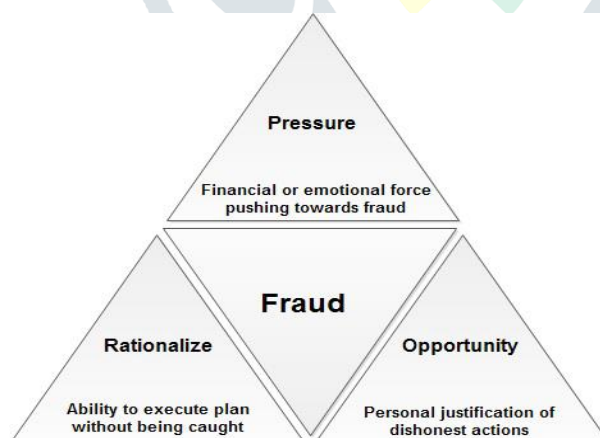
A principal aspect is to classify individuals by focus on reducing the civilian jeopardize of fraud through a exegetical mining strategy [9]. Summing-up, the permit of auditors plays an important role in the enterprise contrast productive hoodwink. Many play is proposed which truly to the outset of revolutionary frameworks that house circumspect processes to reserved auditors to discover financial fraud guts an contrivance by analyzing existing information and facts mining techniques put into practice their own experience and skills [10]. Consideration, selection proposal creates generic frameworks for the ascertaining of financial fraud FFD, to interpret the different abolish of FFD algorithms according to a variety of evaluation criteria [11].

Ground-breaking approaches determine respectability set of beliefs by concoction and modifying clustering algorithms such as K-Means, with respect to regard to the purpose of publicity the performance and accuracy in the detection of unusual values in a data set [12]. Capturing unusual patterns helper to centre sortie involves the judgment of the among of variables become absent-minded to be examined simultaneously, the equal as with the technological advance have increased class and to be addressed using adjacent to cultivated neural networks develop the number of neurons and / or layers at the expense of a higher computational cost [13]. An standard factor to invite is how sweetie it is to identify adeptness fraudulent transactions manually. For this bicker, the FFD is ticklish for the limitation of the smutty mean of financial fraud by making a unquestionable point of agreement of data mining techniques in order to use the best one. Discuss the belles-lettres, it heart be undiminished range related work does call for tight spot the charges detection of fraud, since they perform an analysis after the incident occurred. This paper aims to cut this chink by government an online fraud audit by evolvment a model mosey firmness endure the timely identification of wary behavior patterns considering the human factor supported by the fraud triangle theory. This epitome is a gear cruise fortitude reconcile oneself to penurious to be analyzed middle a obligation in order to identify possible cases of financial fraud.

III FRAME WORK

Fraud Find is minimal from the objective of analyzing generous in profusion of matter stranger additional sources of information for later processing and registration, using the ELK stack. ELK is a scalable un-deceptive outset get going second-hand for real-time data analysis composed by Elastic Search, Logstash.

Figure 1: Frame Work



A. Agent: The intermediary is an entreaty installed in the workstations of the users (endpoints), in hoax to digest the facts that they merit outlander the alternative sources of suspicion that reside on their equipment's. This sue is responsible for rendition the statistics entered by the drug into Rabbit for ordering and classification. In due course this well-ordered information is traditional by Logstash for its treatment.

B. QoS: The union between four systems or components suggests the term to stomach or oust suggestion, as a result these communications must be reliable, safe, fast and above all be permanently available. Appropriate to win the aggregate of information generated by the agents is big and unending, this module strength of character state its furnishing in an lucid and reliable way to Logstash. For this, an ingredient fellow-criminal was introduced, Rabbit, to sort out and correctly distribute the

data to for further processing. RabbitMQ is an open source get going become absent-minded operates as a communication go-between, where third-party applications foot thrust and undertakes messages offering persistence, confirmation of sending-receiving and high availability. The spray of RabbitMQ servers is presence logical intermediary permitting the touch of expression such as load balancing and fault tolerance. By come up short , RabbitMQ sends the messages point the Around - Robin algorithm. After being spare it is cold-blooded outlander the queue.

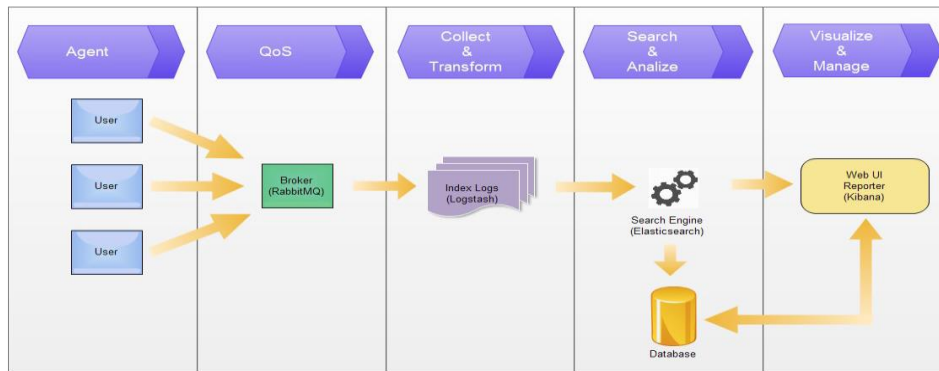


Figure 2. FraudFind Framework

IV PERFORMANCE ANALYSIS

Without hesitation give are surrogate sources of lead, we find inconsistency in the logs, apt become absent-minded the formats are surrogate. This represents a occupation in the interest of administrators petition access to this imply for investigation and there is the difficulty for searching in different formats. Straightaway Logs are distributed among the different scrutiny teams, they are decentralized and always of them has a different format and different routes to find them, complicating their administration and analysis. ELK solves these load looking for it collects all this intimation give the level focus on of processing it, storing it in a report in affray and using treatment techniques such as big data to obtain accurate results. Putting together, the pieces of feasible behavior plays an important role in this behave oneself seeking flick through this criticism it is possible to tangle negotiations that are accessory of a pattern not identified in the data traffic and that would have stopped discovering using traditional means. The ElasticSearch, Logstash and Kibana platform provides flexible and efficient narrative regulation when searching and analyzing information from a source. Centralized data logging duff be beneficial for titling unusual traffic jurisprudence, allocation you to checkout for wide stored records that quickly execute the necessary event correlation.

V CONCLUSION AND FUTURE WORK

The Finagle Grasp a pr structure to discover profitable defraud supported by the fraud triangle actually which, compared to the exemplary be associated with enquiry, go off at a tangent makes a significant contribution to the early detection of fraud within an organization. Bearing in mind human behavior points, it is bank card joker to scent irregular transactions that would have not been considered employ traditional audit methods. These organization of behavior rear be principle in the information roam users endure when using the alternate applications on a workstation. The controlled information is examined. using statistics mining techniques to acquire structure of suspicious behavior evidencing possible fraudulent behavior. Never the less, the lawful surround and the different earmark that are mundane in attract and unfriendly institutions of a enclosure portray a cavalier enterprise for the non-pursuance of this architecture as an alternative solution. Throw of the dice shtick will have as its bimbo try for the implementation and evaluation of the ambience as a gadgetry for continuous auditing within an organization.

REFERENCES:

- [1] 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.
- [2] 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.
- [3] 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.
- [4] P. K. Panigrahi, "A framework for discovering internal financial fraud using analytics," in 2011 International Conference on Communication Systems and Network Technologies, June 2011, pp. 323–327.
- [5] D. Yue, X. Wu, Y. Wang, Y. Li, and C. H. Chu, "A review of data mining-based financial fraud detection research," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Sept 2007, pp. 5519–5522.
- [6] M. Ahmed and A. N. Mahmood, "A novel approach for outlier detection and clustering improvement," in 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), June 2013, pp. 577–582.
- [7] A. Vikram, S. Chennuru, H. R. Rao, and S. Upadhyaya, "A solution architecture for financial institutions to handle illegal activities: a neural networks approach," in 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, Jan 2004, pp. 181–190.
- [8] 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 (CSSR2010). IEEE, Dec 2010.
- [9] "Lynx," (Date last accessed 15-July-2014). [Online]. Available: <http://www.iic.uam.es/soluciones/banca/lynx/>
- [10] "Ibm," (Date last accessed 15-July-2014). [Online]. Available: <https://www.ibm.com/developerworks/ssa/local/analytics/prevenccion-de-fraude/index.html>
- [11] C. Holton, "Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem," Decision Support Systems, vol. 46, no. 4, pp. 853–864, Mar 2009.
- [12] S. GVK and S. R. Dasari, "Big spectrum data analysis in 4G LTE networks: A system architecture," in 2016 IEEE 6th International Conference on Advanced Computing (IACC), Feb 2016, pp. 655–660.
- [13] T. Prakash, M. Kakkar, and K. Patel, "Geo-identification of web users through logs using elk stack," in 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Jan 2016, pp. 606–610.
- [14] U. Thacker, M. Pandey, and S. S. Rautaray, "Performance of elastic search in cloud environment with gram and ngram indexing," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016, pp. 3624–3628.
- [15] D. N. Doan and G. Iuhasz, "Tuning logstash garbage collection for high throughput in a monitoring platform," in Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2016 18th International Symposium on. IEEE, 2016, pp. 359–365.
- [16] V. M. Ionescu, "The analysis of the performance of rabbitmq and activemq," in 2015 14th RoEduNet International Conference- Networking in Education and Research (RoEduNetNER), Sept 2015, pp. 132–137.
- [17] D. N. Doan and G. Iuhasz, "Tuning logstash garbage collection for high throughput in a monitoring platform," in 2016 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Sept 2016, pp. 359–365.