Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

A Survey on Digital Fraud Risk Control Management by Automatic Case Management System

Dr. Wang Haoxiang,
Director and lead executive faculty member,
GoPerception Laboratory,
NY, USA.
Email id: hw496@goperception.com

Dr. S. Smys,
Professor,
Department of CSE,
RVS Technical Campus,
Coimbatore, India.
Email id: smys375@gmail.com

Abstract: In this digital era, a huge amount of money had been laundered via digital frauds, which mainly occur in the timeframe of electronic payment transaction made by first-time credit/debit card users. Currently, Finance organizations are facing several fraud attempts and it likely happens due to the current infrastructure, which only has an older database.. The current infrastructure diminishes the working environment of any finance organization sector with frequent fraud attempts. In this perspective, the roposed research article provides an overview for the development of an automated prevention system for any finance organization to protect it from any fraudulent attacks. The proposed automated case management system is used to monitor the expenses of the behavior study of users by avoiding the undesirable contact. The proposed research work develops a new management procedure to prevent the occurrence of electronic fraud in any finance organization. The existing procedure can predict digital fraud with an old updated database. This creates disaster and destructive analysis of the finance segment in their procedure. The cyber fraud phenomenon prediction is used to predict the fraud attempt with content-based analysis. The lack of resources is one of the enormous challenges in the digital fraud identification domain. The proposed scheme addresses to integrate all safety techniques to safeguard the stakeholders and finance institutions from cyber-attacks.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

Keywords: *Digital fraud, risk control management*

1. INTRODUCTION

Generally, digital frauds are categorized into two types, namely direct and indirect frauds. It has been categorized based on their activities in the internet domain and type of robbery [1]. The debit/credit card fraud and money laundering activities will come under direct type. Website phishing, hacking, spreading virus, and malware will come under indirect types [2]. Besides, identity thieves are one of the types of e-fraud. They involve in credit/debit cards through an internet domain to carry out fraudulent activities [3]. It is an illegal usage of a credit/debit card to withdraw the money without intimation to the owner of the card [4]. There are many ways to steal someone's identity. Skimming involves stealing card information during the transaction period. Usually, this will happen in a business that uses digital transaction mode. Due to skimming devices, the fraudster can easily interfere with our records through magnetic strips [5]. Figure 1 shows the picture of some digital verification tools recently.

Figure 1 Digital verification tools

Digital fraud involves in hacking the card details by using sophisticated methods, when a digital transaction has been carried out by the user [6]. Unfortunately, in recent times these losses are increasing exponentially and there is no legal legislation to completely get rid of this crime [7]. Digital frauds involve designing the websites like similar real websites (phishing) of any financial sector, where the user will enter their data like username and date of birth, nickname,

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

debit/credit card details, and password without any hesitation [8]. Figure 2 shows the block diagram of the cybercrime activities procedure.

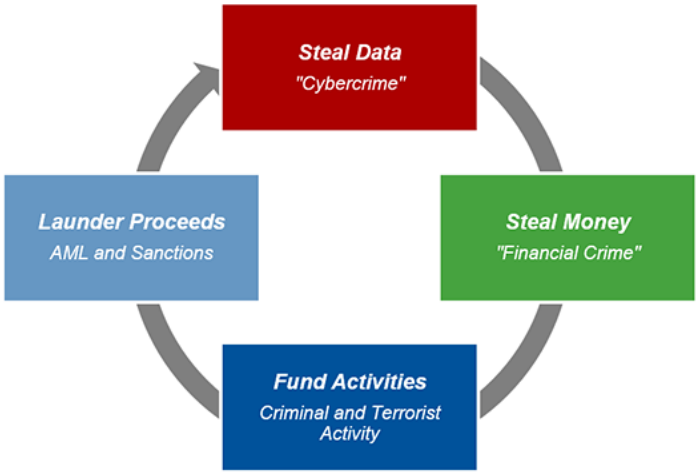

Figure 2 Cybercrime activities procedure

They often send emails to recipients, who requested for the disclosure of sensitive information. The main target of hackers will be on the corporates and big business merchants [9]. Many E-commerce merchant's websites are mostly unsecured and it does not have any protection. They are using websites as it is without introducing a secured protection. Traditionally, the financial institution will allow the trusted employees to retain the passwords with some simple key questions and answers [10]. It will increase the online access to retain the personal customer data. This is the way through which any employee can commit fraud [11]. In olden days, the employee internally commits fraud in any banking sector. Those days structured fraud risk control management was not available [12]. This construction varies year by year due to the attack level of digital frauds across the globe.

2. ORGANIZATION OF THE RESEARCH

The proposed research article includes different sections; related works are discussed in section 3. Section 4 provides a considerable management system for protecting the digital frauds, section 5 compares various management system contributions. Section 6 concludes the summary of the article and also includes the future possibilities of digital fraud.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

3. RELATED WORKS

Information Communication Technologies [ICT] are ubiquitous and it can help the trend to move towards digitization. This development contributes to many sectors particularly the finance and banking transactions [13]. Protection from fraudsters is very important during this rapid growth in any nation. Because of some negatively utilized perpetrators of fraud, all the banking systems should be protected during a transaction. Recently, many electronics gadgets are associated with information communication technology to provide more impact on a lot of constructive and destructive works. Here, these destructive works are categorized as electronic crime and are named as spamming, debit/credit card fraud, ATM fraud, phishing websites, and its host attacking etc. [14]. This transaction is further processed through the internet for any bank to create new opportunities for consumers as well as digital fraud [15]. Protection against digital fraudsters is very important and this helps for economic development. Michael Schindler et al discuss the difficulties during short transaction sequences, which will effect through the mystery from online games. This problem can be solved by applying some algorithm to protect the characteristic attributes present within the sequence of any mobile device. This awareness procedure should be used for accessing the internet financial sector for transactions [16].

In a precise manner, the introduction of the novel framework is to detect the fraud standing strategy. Many research articles concentrate on the banking sector from the customer point of view respectively. The exiting research work concentrates on credit card structure to withdraw the money from ATM. The focus on enormous capable research is working with the performance improving strategies [17].

The research article focuses on the credit card risk monitoring system and issues of the key tasks. The improved financial sector organization is protected based on the risk factor associated with the usage of credit card. The possibilities of digital fraud transactions can be monitored thoroughly with their system [18]. This appearance of digital fraud is spoiling the whole management system due to the older database system of anti-fraud strategy. Generally, this should be adopted to avoid the digital fraud in order to diminish the risks. There is a research gap to prevent the electronic fraud with the latest updated database of their fraudulent procedure.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

Therefore, this research article focuses on developing a procedure for the automated case management system (ACMS) for any digital fraud activities.

4. METHODOLOGY

Mostly, the recent advance in technology introduces high operational speeds for awareness. The financial institution will make legislation to handle any transaction process, which is easier to escape from detection. Many developing countries do not have any updated technical security protocol for protecting the digital frauds [19]. This lack of technology is virtuoso for digital frauds to attempt many times through the internet with a lot of chances. This will help to maintain a security level. This section is comprised of a discussion on the digital fraud risk management conditions [20]. This risk management consists of some workflow for the framework, which identifies risk and its analysis, plan implement action, measure, control, and monitor. It is shown in figure 3.

Figure 3 Simplified block diagram of Risk management

4.1 Risk Control Management

This program should be effective and it is very important for any organization, which has worked with the internet. The risk control management comprises of fraud risk governance (FRG), fraud risk assessment (FRA), fraud prevention (FP), and fraud detection (FD).

Fraud Risk Governance

This governance can serve as the substance of detection, prevention, and assessment. This ethical approach creates safety environment, which receives the treatment. This program

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

ensemble for right decision implicit of prohibits theft. The regulations are increased at the company level against criminal penalties involved in fraud schemes [21]. This settlement is given by many financial institutes of public property. Market capitalizations of many public companies have decreased the money control due to scandal. This expectation is very clear that, all the organization needs to maintain the board with entity-level control, which will include the FRM [22]. This senior management should be considered for digital fraud, which will control the entity level of the program. The constraint policies and job descriptions are related to the fraud risk management. Making documentation for this risk management should be reflected for any risk strategy with more reliability.

Fraud Risk Assessment

The risk assessment can be identified with a fraud attempt from the long-distance and a huge enterprise risk management system is applied. Those control activities should consider both fraud types and monitoring programs for the criminals of each method [23]. When it is programmed, the risk assessment is used to identify any type of digital frauds. The effective method involves these four phenomena named risk governance, assessment, detection, and prevention.

Fraud Prevention

“Prevention is better than cure” proverb is more suitable to overcome all the digital fraud attacks. The specific control program is used to mitigate the assessment process. This implementation of fraud risk prevention is continuously monitoring their process and operation [24]. An effective prevention method is required to incorporate the assessment and governance program to protect the digital fraud. This measure is designed and implemented for any digital crime control activities and it should be coordinated [25]. The address of identified risk and implementation of the control activities ensure the sufficiency to prevent the digital fraud risk.

Fraud Detection

Any financial institution should include a fraud detection control mechanism in place and it includes preventative measures. Generally, this management program provides evidence to identify the occurrence of fraud but this is not intended to protect the fraud. This approach

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

should always incorporate the preventative measures. The financial sector cannot minimize the risk of fraud attempts at any time [26]. Therefore, some people will get motivated to attempt fraud always. The incorporation of any detection techniques should be very flexible and reliable with various changes of any risk types [27]. The documentation of detailed descriptions of any type of digital fraud is very essential. Every organization should have awareness of the system with responsible factors as follows;

1. Constructing the digital fraud detection procedure.
2. The control mechanism of fraud detection design.
3. Implementation of easier detection methods.
4. Analysing many possible attacks of digital fraud activities.
5. Maintain the investigation reports.
6. Suspect and detect the fraudulent activities frequently.
7. Updating the database by periodically checking the used technology and procedures

Proposed Automated Case Management System

Generally, the flexible approach is an ensemble with an automated management system for finding any fraud detection. The financial institution requires updating regularly with a new updating database on any digital fraud attempts procedure. This flexible plan can be built strongly with easily take on new events. This can model and validate a new organized process after updating the database for an automated case management system (ACMS), which is responsible for preventing any digital frauds. Figure 4 shows the digital fraud scheme procedure for the proposed measures procedure.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

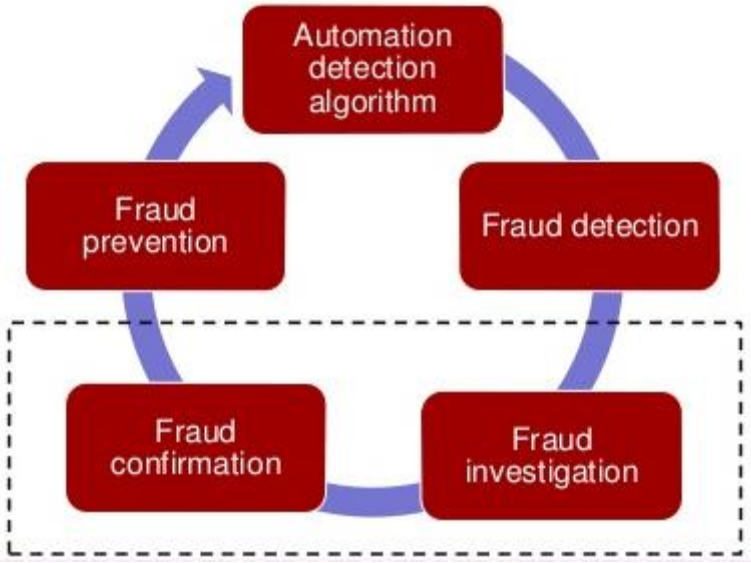

Figure 4 Consideration of Fraud Scheme Procedure

Therefore, this ACMS creates queue of monitoring control for many work policies with the current scheme and it issues the alerts, when it is necessary. This setup can give more reliable output to force the process efficiency, when compared to the old model of the risk management system.

5. RESULTS DISCUSSION

Every finance organization's risk control management should be established and improved for any kind of digital fraud. This measurement can be a categorized number of fraud schemes for an automated risk management system, which should be updating frequently [28] [29]. This updating factor can be favoured as

1. Collect the number of known / unknown fraud schemes against the organization.
2. Collect the status of digital fraud investigation.
3. Maintain the database for a number of a fraud inquiry.
4. Maintain the database with employees signed ethics statement records.
5. Database maintenance on global fraud survey incudes the digital fraud experience and their attempt loss.
6. Regular monitoring of internal fraud by internal auditors.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

These are all the considerations of ACMS and it maintains the updated database. The two cases are covering the transaction of digital money between the users.

Case 1:

Money flow through web link to anybody at the condition of digital scheme

Risk Control Management	Fraud risk Governance	Fraud Risk Assessment	Fraud Prevention	Fraud Detection
Detection Algorithm	Moderate	Moderate	High	High
ACMS	High	High	High	Very high

This lemma includes the four domain approach for risk control management system. The existing approach has provided moderate consideration for governance and assessment restriction. It gives a high profile for prevention and detection. During much iteration, those algorithms are a failure in the prevention of digital fraud due to the lack of database. But the proposed ACMS construct a strong boundary during many iteration attempts of digital fraud due to the updated database. Figure 5 shows a graph of the performance analysis chart of case 1.

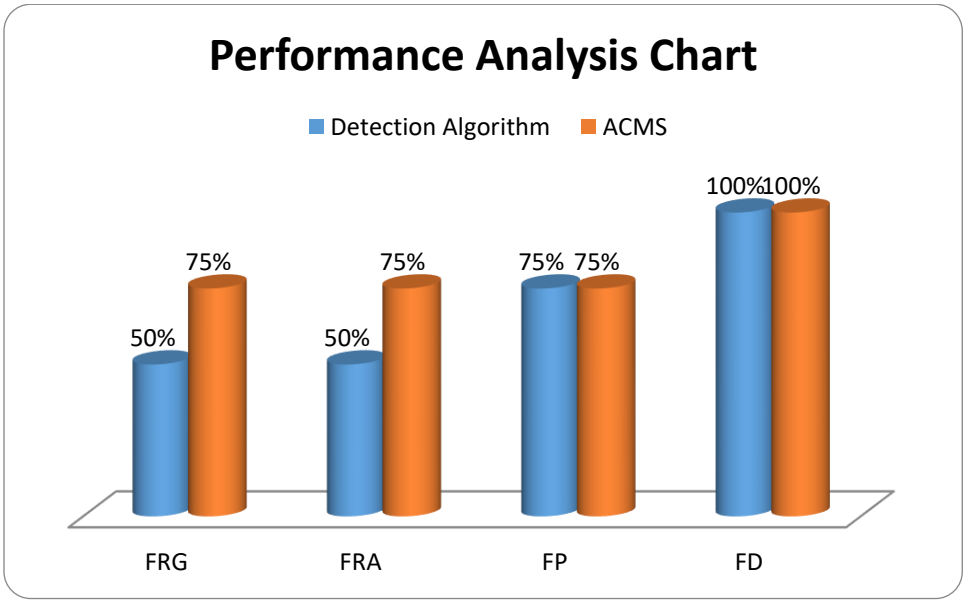

Figure 5 Performance analyses for CASE-1 study

Case 2:

All type of transaction through digital e-pay (gpay, phonePe etc) to the consumer

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

Risk Control Management	Fraud risk Governance	Fraud Risk Assessment	Fraud Prevention	Fraud Detection
Detection Algorithm	Low	Moderate	Moderate	High
ACMS	High	High	Very high	Very high

Case 2: lemma is constructed for the same four domain approach for any money risk control management system. The existing detection algorithms provide very low fraud risk governance due to the lack of sufficient details and consumer information. Also, the assessment procedure is very moderate during the fraud attempts. The detection is relatively high during the first iteration, when compared to the remaining iteration. But the proposed improved structure of risk control management system includes a strong boundary for any attackers or intruders with very high priority level in all management systems. Figure 6 shows the performance analysis of the case 2 study.

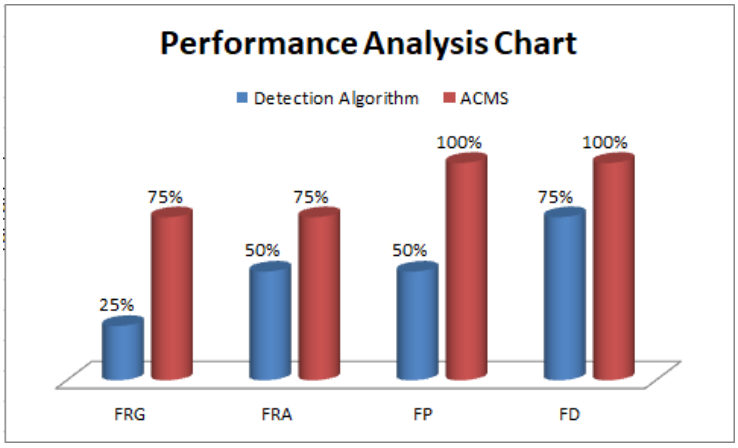

Figure 6 Performance Analysis for CASE-2 Study

6. CONCLUSION

Thus, the proposed ACMS can be configured in every preventive system of the finance organization and it provides good elimination results to overcome digital fraud in the current scenario. These basic procedures can frequently eliminate the digital fraud attempts in our digital server. This strong fraud prevention and detection coordinates in many attempts that risk over

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

money transaction, which can mitigate the fraudulent risks. The 100% achievable results are achieved for fraud prevention and it is not practical for future domain scenario. Initially, the fraud is not directly related to the money transaction and instead of it, they construct belief with any financial institution to steal the product or money in reality. This extend will go to some degree and the deal can be either positive or negative. But the proposed procedure is used to construct a strong boundary to establish a risk control and management system to overcome digital frauds with current scenarios. This is well recognized that, dynamic measurement of any finance organization of fraud possibilities help to respond the dynamic circumstances. Despite the hype, the proposed method will be less effective for future fraud possibilities such as spoofing etc. The digital fraud prevention procedures with location parameter analysis with the help of Google maps and location identifiers should be developed. The supply chain vulnerabilities should be designed with a very strong firewall, where the user exchanges their information. Finally, buyback, insurance settlement, and earlier settlement transactions can be controlled as a future research work.

REFERENCES

[1] D. Rahmawati, R. Sarno, C. Fatichah, and D. Sunaryono, ‘‘Fraud detection on event log of bank financial credit business process using hidden Markov model algorithm,’’ in Proc. 3rd Int. Conf. Sci. Inf. Technol. (ICSITech), Oct. 2017, pp. 35–40.

[2] H. A. Hartanto, R. Sarno, and N. F. Ariyani, ‘‘Linked warning criterion on ontology-based key performance indicators,’’ in Proc. Int. Seminar Appl. Technol. Inf. Commun. (ISemantic), Aug. 2016, pp. 211–216.

[3] W. M. P. van der Aalst, ‘‘Business process management: A comprehensive survey,’’ ISRN Softw. Eng., vol. 2013, pp. 1–37, Aug. 2013.

[4] R. Nisbet, G. Miner, and K. Yale, ‘‘Fraud detection,’’ in Handbook of Statistical Analysis and Data Mining Applications. Amsterdam, The Netherlands: Elsevier, 2018, pp. 289–302.

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

[5] A. Misra and V. Walden, ‘‘Proactive fraud analysis,’’ Intern. Audit., vol. 73, no. 2, pp. 33–37, 2016.

[6] T. Seyffarth, S. Kühnel, and S. Sackmann, ‘‘A taxonomy of compliance processes for business process compliance,’’ in Proc. BPM, vol. 297, 2017, pp. 71–87.

[7] G. D. Moyes, R. Young, and H. F. M. Din, ‘‘Malaysian internal and external auditor perceptions of the effectiveness of red flags for detecting fraud,’’ Int. J. Auditing Technol., vol. 1, no. 1, p. 91, 2013.

[8] R. Sarno and F. P. Sinaga, ‘‘Business process anomaly detection using ontology-based process modelling and multi-level class association rule learning,’’ in Proc. Int. Conf. Comput., Control, Informat. Appl. (ICINA), Oct. 2015, pp. 12–17.

[9] S. Huda, T. Ahmad, R. Sarno, and H. A. Santoso, ‘‘Identification of process-based fraud patterns in credit application,’’ in Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT), May 2014, pp. 84–89.

[10] R. Sarno, R. D. Dewandono, T. Ahmad, M. F. Naufal, and F. Sinaga, ‘‘Hybrid association rule learning and process mining for fraud detection,’’ IAENG Int. J. Comput. Sci., vol. 42, no. 2, pp. 59–72, Apr. 2015.

[11] N. Sandhu, ‘‘Behavioural red flags of Fraud—A qualitative assessment,’’ J. Hum. Values, vol. 22, no. 3, pp. 221–237, Sep. 2016.

[12] G. L. Gray and R. S. Debreceny, ‘‘A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits,’’ Int. J. Accounting Inf. Syst., vol. 15, no. 4, pp. 357–380, Dec. 2014.

[13] Gercke, M. (2011), Understanding Cybercrime: A Guide for Developing Countries.ICT Applications and Cybersecurity Division.Policies and Strategies Department.ITU Telecommunications Development Sector 2nd Edition, www.itu.int/ITUD/ cyb/cybersecurity/legislation.html

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

[14] Siddique, M.I. and Rehman, S. (2011), Impact of Electronic Crime in Indian Banking Sector – An Overview. International Journal of Business & Information Technology, Vol. 1 No. 2.

[15] Oracle (2012), Fraud Fight: Enterprise-wide Strategy Sets the Stage for Victory. Oracle Corporation, www.oracle.com.

[16] Cooper, D.R. and Schindler P.S. (2011), Business Research Methods, McGraw-Hill/Irwin Series

[17] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, ‘‘Learned lessons in credit card fraud detection from a practitioner perspective,’’ Expert Syst. Appl., vol. 41, no. 10, pp. 4915–4928, Aug. 2014

[18] A. Yang and U. Varshney, ‘‘A taxonomy for mobile health implementation and evaluation,’’ in Proc. 22nd Amer. Conf. Inf. Syst., 2016, pp. 1–10.

[19] K. Mule and M. Kulkarni, ‘‘Credit card fraud detection using hidden Markov model (HMM),’’ Int. J. Innov. Technol. Adapt. Manag., vol. 1, no. 6, p. 30, Aug. 2014.

[20] W. Wei, J. Li, L. Cao, Y. Ou, and J. Chen, ‘‘Effective detection of sophisticated online banking fraud on extremely imbalanced data,’’ World Wide Web, vol. 16, no. 4, pp. 449–475, Jul. 2013.

[21] S. Mardani and H. Shahriari, ‘‘Fraud detection in process-aware information systems using process mining,’’ in Proc. 21st Century, E-Syst. Theno, Dec. 2017, pp. 307–344.

[22] A. Dresch, D. P. Lacerda, and J. A. V. Antunes, Jr., Design Science Research. Cham, Switzerland: Springer, 2015.

[23] B. Wetzstein, KPI-Related Monitoring, Analysis, and Adaptation of Business Processes. Berlin, Germany: Stuttgart, 2016.

[24] D. Cotton, S. Johnigan, and L. Givarz, Fraud Risk Management Guide. New York, NY, USA: COSO, 2016. [Online]. Available: https://www.coso. org/Documents/COSO-Fraud-Risk-Management-Guide-ExecutiveSummary.pdf

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021

Journal of Electrical Engineering and Automation (EEA) (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2021.1.001

[25] A. Abdallah, M. A. Maarof, and A. Zainal, ‘‘Fraud detection system: A survey,’’ J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

[26] S. Huda, R. Sarno, and T. Ahmad, ‘‘Fuzzy MADM approach for rating of process-based fraud,’’ J. ICT Res. Appl., vol. 9, no. 2, pp. 111–128, Nov. 2015.

[27] S. Huda, R. Sarno, and T. Ahmad, ‘‘Increasing accuracy of process-based fraud detection using a behavior model,’’ Int. J. Softw. Eng. Appl., vol. 10, no. 5, pp. 175–188, May 2016.

[28] D. Al-Jumeily, A. Hussain, A. MacDermott, G. Seeckts, and J. Lunn, ‘‘Methods and techniques to support the development of fraud detection system,’’ in Proc. Int. Conf. Syst., Signals Image Process. (IWSSIP), Sep. 2015, pp. 224–227.

[29] Association of Certified Fraud Examiners. (Sep. 2016). 2016 ACFE Report to the Nations|Executive Summary. [Online]. Available: https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

ISSN: 2582-3051
Submitted:21.03.2021
Revised: 2.04.2021
Accepted: 28.04.2021
Published: 10.05.2021