International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

TELECOMMUNICATION FRAUD AND FRAMEWORK TO MITIGATE IT

Satya Brata Routray[1], Tripti Dhote[2]

[1,2] Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.
Email: [2]tdhote@sidtm.edu.in

Abstract

To highlight the pervasiveness of telecom fraud and how it affects the telecommunications network and its subscribers. In this paper, a framework will be developed for the understanding of telecom fraud. This framework can be then used to indicate the possible avenues for combating existing fraud. This paper draws on secondary sources of data and available literature on telecom fraud and financial crime. The study adopts the case study approach wherein various use cases of the telecom sector have been analyzed. This paper presents the big picture of the issue in the context of telecom fraud and the different challenges associated with it. The findings indicate that elements of fraud risk not only have an adverse effect on revenue of telco's but also affects the incident of telecom fraud.

Key words: Telecommunications network fraud; causes; prevention; fraud detection

Introduction

The word Fraud is as old as human civilization itself. Over time its representation has been a wide range of injustices that includes forgery of art, educational plagiarism, self-Preservation (e.g., perjury), and email frauds (e.g., famous Nigerian-email fraud). However, in recent years, advancements in technology have provided new methods in which fraudsters can commit fraud. Conventional methods of fraud such as money laundering have now become easier and accompanied by a new type of fraud such as telecom fraud and computer intrusion. PriceWaterhouseCoopers performed a worldwide survey of financial crime, showing that in spite of a significant increase in investment in compliance and being continuously monitored by the regulators during that time and forty-seven percent of respondents still have reported being victims of financial crime within the past twenty-four months. A total loss of US$42 billion was reported in the last 24 months due to fraud [1].In the 21st century, fraudulent crime grew within the space of transactional business, especially in the telecom and banking sectors, because of the large transaction volume of in these businesses, fraud can very easily go unnoticed, as it accounts for a little proportion of the entire business. We start by differentiating between the fraud prevention and fraud detection. Fraud prevention can be described as measures taken to prevent fraud from happening. It includes elaborate designs, watermarks, laminated metal strips and holographs on currency notes, (PIN) for bank cards, online security for internet transactions and password protection for computer systems. Of course, none of the mentioned methods are perfect. On the other hand, fraud detection is identifying and detecting fraud as quickly as possible once it has been committed. Once fraud prevention fails then fraud detection comes into play. In practice, fraud detection is a continuous process, as one will usually be unaware that fraud prevention has failed. We can try to avoid credit card fraud by safeguarding our cards continuously, nonetheless if in case our card details are misplaced or get stolen, then we should be able to detect it as soon as possible before fraud has been committed. Fraud detection is a constantly evolving discipline, as criminals are adopting different strategies and creating new ways to commit fraud. This means that the methods used earlier for detection need to be in place along with that new methods should be adopted to mitigate fraud. Communication service providers (CSP) have a very large number of multiple external touchpoints like subscribers, channel partners, service providers, and regulators. At each of these external touchpoints across this network of systems, service providers become more susceptible to fraudulent activities. At the same time, they need to address acute competition, increasing demand for rapid growth and also have to maintain a high customer satisfaction rate. In these circumstances, the telecom industry is exposed to a variety of fraud risks such as subscriber (identity) frauds, illegal use of the network, leakage of critical information, and challenges related to internal or external misconduct investigations.

Telecommunications fraud is usually considered to be victimless. Moreover, if a telco takes a considerable fraud hit then it's almost inevitably passed on to the customer in the long run.

Objective

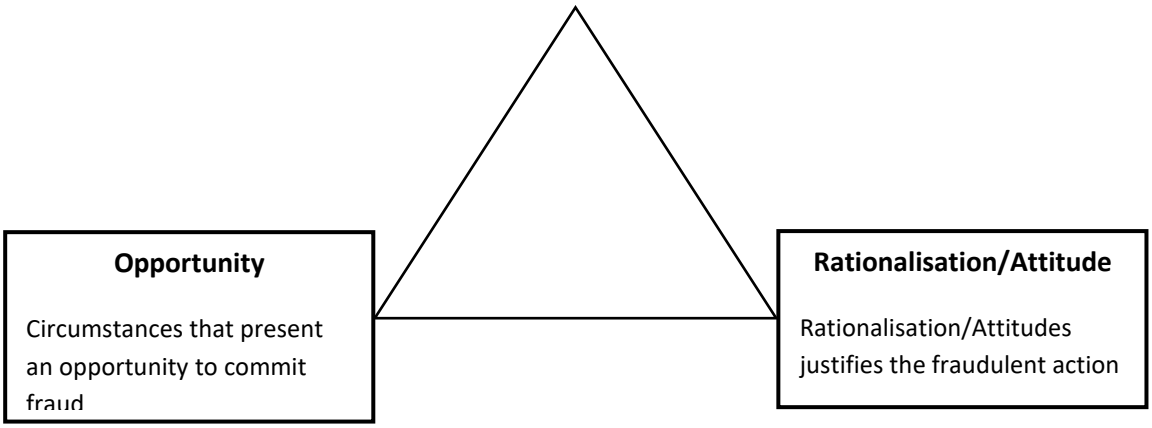
Over the last few years, the telecommunications industry has grown exponentially. With affordable and new technology available in the market the number of users has also increased dramatically and revenue losses due to fraud are also set to rise. Several estimates have been presented for revenue losses due to this fraud. For example, the figure given was equivalent to $1 billion a year [2]. There are various types of telecom fraud and these can occur at different levels of the telecommunication network [3]. The objective of the research is focused on telecommunication fraud and various possible avenues to mitigate fraud. The study will provide an in-depth understanding of telecommunication fraud and its impact on service providers also to devise a framework for mitigation telecommunication fraud.

Review Of Related Literature

The literature review conducted was thoroughly and systematically based on the guidance approach for the information system as suggested by Webster & Watson [4]. Napel suggests that for reducing the number of fraud cases, it is important to understand why people commit fraud in the first place [5]. In any case, detection of fraud is not a simple task as it requires intensive knowledge about the type of fraud and why it's committed? [6]. In the 1950s, Donald R. Cressey Criminologist by profession introduced a theory to clarify what causes perpetrators to commit fraud. He interviewed 250 criminal fraudsters whose conduct met specific criteria. Initially where the person was given a position of trust and faith and then violated that trust when compelled by financial related pressures [7]. Cressey identified the determinants that motivated individuals to commit fraud. He concluded that the presence of three determinants **pressure, opportunity, and rationalisation** is a must for a person to violate trust and commit fraud [8].The Pressure is that the incentive to commit fraud, while opportunity acts as an added advantage along with the intent for committing fraud and rationalisation will help fraudster to claim that fraudulent actions are just and right, correlated with the behavior [6]. The final hypothesis of Cressey's (1973) published in the book *Other People's Money: A Study in the Social Psychology of Embezzlement, was* [9]:

Trusted Persons grow to believe violators once they are sure of themselves as having a *financial problem which is non-shareable*, are aware that the predicament could be quietly re*solved by violating the position of financial trust*, and can apply to their own conduct in that situation *verbalizations which enable them to adjust their conceptions of themselves* as a trusted person with their notion about themselves as users entrusted funds or assets.

The segments italicized from the hypothesis (often abbreviated as pressure, opportunity, and rationalization) became the pillars of Cressey's research. Albrecht coined the term "Fraud Triangle" (Figure 1) which represented the three pillars of Cressey's hypothesis [10]. Over the years, this hypothesis was famously known as the "fraud triangle theory" [11].



Source: Adapted from Wells [30]

Figure 1. The fraud triangle

During the early days, the fraudsters were easily able to commit fraud. This resulted in significant losses on telecommunications companies, amounting to billions of dollars in uncollectable revenue. One of the telecommunications company AT&T, has played a major role in the detection of fraud. It was one of the first companies to automate communication systems thus making it a prime target for the fraudsters [12]. In 1957 a new culture was developed when an early telecommunications fraudster (known as phreakers) Joe Engressia, stumbled accidentally into fraud**.** He realized when whistled at specific frequencies, he was able to control the trunks responsible for automated call routing [13]. In the subsequent years, he mastered the craft of breaking and entering into AT&T's telephone network. Over time, these organizations have tried many methods to combat fraud. Few of them used methods such as whitelisting and blacklisting for the prevention of telecommunications fraud [14] [15] [16] [17]. While some of them used machine learning techniques for identifying fraudulent calls. Subudhi and Panigrahi published their findings on telecommunications fraud where they used the Quarter-Sphere Support Vector Machine algorithm to identify fraudulent calls [18]. The input to this algorithm were the features of telephony communication such as call duration, call type, call frequency, location, and time. The use of telecom services without any intention of paying for the services used is known as telecommunications fraud [19]. Revenue losses due to fraud results in an increase in operational costs for telecom operators. Although operators have taken steps to mitigate fraud and reduce revenue loss due to fraud, criminals still find new methods to abuse communications networks and services. Telecom fraud has increased exponentially over the years and is definitely expected to increase furthermore. Revenue loss due to fraud is not something that can be easily recovered upon detection, unlike revenue leakage which can be easily corrected once the leakage has been identified. Based on a survey conducted by the Communications Fraud Control Association (CFCA) the revenue loss due to fraud now amounts to 1.74 percent of annual revenue in the telecom industry. Compared to 2017 the total global fraud losses in 2019 as a percent of global telecom revenue grew by 37% to US$28.3bn or 1.74% of total revenues. Some commonly associated telecommunication frauds are Wangiri fraud, Telecom arbitrage fraud, Subscription fraud, PBX fraud, etc. One particular fraud known as 'Roaming fraud' is much more favored by fraudsters to commit fraud. Why does roaming appeal to fraudsters? The multiple locations that can be used. Fraudsters use these locations to camouflage fraud incidents as well as extend the length of fraud incidents by exploiting the time lag involved with the exchange of records between operators [20].Telecom fraud is a type of cross-border crime that not only features long-distance but also has no direct contact in the real world. The rising demand for internet and exponential growth of telecom technology provides opportunities for fraudulent activities and cross-border crimes. Hence this paper aims in finding an optimal framework solution for implementation by telco's, to avoid and detect fraud.

Research Methodology

The approach adopted for the research is a systematic review of the literature. The search of the literature was conducted on the following databases: Scopus, EBSCOhost, Emerald Insight, Jstor, Science Direct, Web of Science, Frost & Sullivan, and Google Scholar. Additionally, a reference list of articles deemed to be relevant was also scanned. It helped in covering most of the relevant articles. Here the approach adopted was a case study approach. According to Bromley and Smith, the case study approach will not only help in analyzing the actual context of the research but also help in realizing the real-world circumstances [21] [22]. Brewer and Miller also postulate that the case study approach provides very fascinating and intriguing research in the field of social science because it provides a very detailed and thorough understanding of the issues and problems faced [23]. Meanwhile, Ormrod and Leedy recommend that the case study approach is best suited for a better understanding of the poorly understood environment, which is not accessible via normal research and generally not available publicly [24]. It allows researchers to examine the case with the attention given to minute details [25]. Few of the previous research on malpractices and fraud also used a similar kind of approach [26][27][28][29]. Based on the above arguments, the case study approach is the most suitable method of researc

Fraud Detection Framework

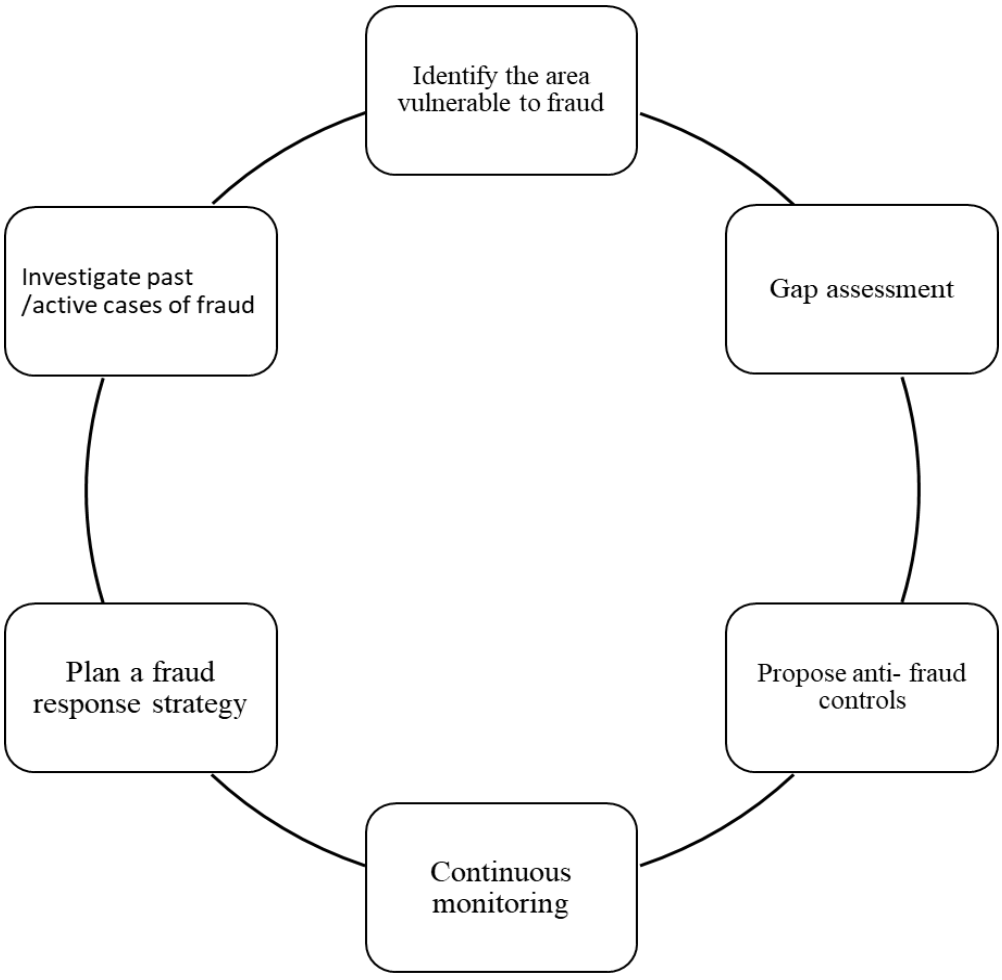


Figure 2-Proposed framework

Source-Author

Here a framework (Figure-2) is proposed for mitigating telecommunication fraud consisting of six fraud management activities. This framework will enable organisations to have controls that avoid fraud from happening, fraud detection and effectively respond to fraud whenever it happens. This framework requires clearly defined actions to mitigate fraud.

1. Identify the area vulnerable to fraud –
- Critically evaluate the current status and effectiveness of the service provider and identify the areas more susceptible to fraudulent activities.
- Conduct past data/transaction analysis for identifying red flags and then a root cause analysis should be performed on those flags to identify absence/overriding controls**.**
- Existing anti-fraud controls, policies should also be evaluated, this includes a critical assessment of culture, attitude, and awareness among the employee about their knowledge of response to any fraudulent activities or misconduct as they are foundations on which effective anti-fraud process are built.

2. Gap Assessment –
- Evaluation of existing anti-fraud control framework and identification of the potential gaps.
- Establish risk profiles by analyzing and ranking them (as high/medium/low) based on the existing framework.
- Carry out detailed for testing to check the effectiveness of existing control in the framework.

3. Propose anti-fraud controls –
- Enhancement of existing anti-fraud framework based on gaps identified.
- Implementing new processes and control to improve enterprise-wide to gain efficiencies and prevent fraud recurrences.
- Preparing a pathway for assigning the responsibilities after consulting the management of the organization.

4. Continuous monitoring –
- Continuously monitoring and periodic assessment of the anti-fraud control measures.
- Analysing transactional data at the process level to identify potentially fraudulent activities.
- Continuous monitoring will help in the early detection and prevention of fraud.

5. Plan a fraud response strategy –
- A fraud response plan should be in place which not only helps the organization to develop a fraud response strategy but also would help in minimizing the impact of fraud that occurs.
- The fraud response strategy should also include the capability to conduct sound investigations of active/past fraudulent cases.

6. Investigate past/active case of alleged fraud
- The framework should identify and fraud risk and schemes.
- Formulate past fraud scenarios and map the existing anti-fraud controls to the identified scenarios.

Telecom Fraud Cases

Case1 - Roaming fraud

Roaming fraud is one of the most common types of fraud committed by fraudsters. When a subscriber moves from home network to another network and uses the subscribed services thus making home network responsible for the charges. When a call is made, the visited public mobile network (VPMN) queries the home network about the services subscribed by the roaming user. The call detail records (CDRs) are sent to the billing system for the generation of invoices to subscribers. The visiting network sends CDR information to the home network, then the home network must settle accounts as per roaming agreement tariffs. When the home network is unable to charge the subscriber for the services and is obliged to pay the roaming network as per the agreement. This behavior results in significant revenue loss for the home network.

Solution

A proposed solution is adopting a proper framework and technology (Blockchain-based solution) that will help in combating fraudulent activities. It helps in authorization and settlement to be done on a real-time basis thereby completing mitigating fraudulent activities. With an improved solution, Telco's will not only be able to cut down on the revenue losses due to roaming fraud but also will have an improved fraud prevention system in place.

Additionally, the blockchain solution helps eliminate 3rd party data clearinghouses, resulting in additional savings.

CASE2 - Subscription Identity Fraud

Subscriber Identity theft takes place when a subscriber uses fake identification or other person's credentials to obtain services from communication service providers. The subscriber identity is essential for service providers to render services and to create an account for the subscriber in the database of service providers. The fraudsters can purchase the SIM cards with the fake ID proofs of another person and utilize the services. Subscriber Identity Module (SIM) consists of an International Mobile Subscriber Identity (IMSI) and Communication service providers use this number to verify the account of a subscriber. The existing solutions for this problem are not robust. There are also problems such as subscriber's identity being compromised by (email phishing, SIM cloning, etc.). Due to the various services provided by telecom operators, identity theft may result in compounded losses through access to several services under a stolen identity. The 2017 CFCA fraud loss survey indicates that the Subscription Identity Fraud losses were $15.6 billion or near about 50% of all fraud losses.

Solution

To solve the problem, Telco can subscribe to a centralized database where the subscriber's identity is verified and thereafter the services are resumed. Once the identity of the subscriber is verified, the telco can issue an eSIM that will help protect private information which is in an encrypted form. It will also eliminate the cost of manufacturing and distributing physical SIM. By using the above-suggested method telecos can mitigate subscription identity fraud to a huge extent.

Case 3 – IOT Connectivity

To deal with increased connectivity, current network operators manufactured Low Power Wide Area Networks (LPWAN) that consumed lower power and could efficiently manage higher traffic and bandwidth needs. It is used for connectivity across the device. For example, in manufacturing, plant machines will be able to communicate among themselves during the production process. The sensors in these devices usually carry and transmit sensitive information about the core network or critical information belonging to customers of the company thereby making data and network security an essential and costly pillar for IoT connectivity. These devices are subjected to fraudulent activities thereby making the entire ecosystem vulnerable. Without securing the underlying telecommunications technology IOT operation cannot be trusted as secured.

Solution

A possible solution would be to use a blockchain-based solution that uses a secure peer to peer self-managed network that uses multiple nodes. This network can be represented by a single IoT sensor verifying every transaction in the network. The verified transaction enables only the desired information to be passed on without exposing critical network elements.

Conclusion And Future Research Work

As we have seen fraud is a very complex phenomenon that not only involves the opportunity for committing fraud, but also rationalization and motivation thereof. In this paper, a framework has been proposed to detect

and mitigate telecommunication fraud. Telcom fraud cases are typical examples of misuse cases, as the actions impact revenue of the provider. When a new service is launched by telco's, it is very important to identify any fraudulent/unaccepted activities as early as possible, for minimizing the revenue losses. If information is already available from previous misuse cases then fraudulent activities can be detected and mitigated even before fraud happens.

Finally, the findings may not be full-proof as the technology advances fraudsters will come up new methods to commit fraudulent activities so the future research should consider all kinds of fraudulent activities and develop a framework that is not only generalized to Telco's but is also applicable to all kind of business, culture and work environment.

References

1. PriceWaterhouseCoopers (2020), "Global economic crime survey 2020 – Financial services industry insights." 2020. [Online].Available:https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf [Accessed: 01-Aug-2020].

2. Kenneth C. Cox, Stephen G. Eick, Graham J. Wills, Ed., Brief application description; visual data mining: Recognizing telephone calling fraud, vol. 1, no. 2. Data Mining and Knowledge Discovery, 1997. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.2088&rep=rep1&type=pdf [Accessed: 01-Aug-2020].

3. J. Shawe-Taylor et al., "Novel techniques for profiling and fraud detection in mobile telecommunications," in Progress in Neural Processing, world scientific, 2000, pp. 113–139. .[Online].Available: https://www.worldscientific.com/doi/abs/10.1142/9789812813312_0008 [Accessed: 04-Aug-2020].

4. B. J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," Njit.edu.[Online].Available:https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf. [Accessed: 04-Aug-2020].

5. K. Ten Napel, Risk factors of occupational fraud: a study of member institutions of the national association of independent colleges and universities. 2013 .[Online].Available:https://search.proquest.com/openview/1868cdc5054c3324fd670d4def5a1160/1 [Accessed: 04-Aug-2020].

6. S. Dellaportas, "Conversations with inmate accountants: Motivation, opportunity and the fraud triangle," Account. forum, vol. 37, no. 1, pp. 29–39, 2013. [Online].Available:https://www.sciencedirect.com/science/article/abs/pii/S0155998212000518 [Accessed: 04-Aug-2020].

7. H. H. Mustafa Bakri, N. Mohamed, and J. Said, "Mitigating asset misappropriation through integrity and fraud risk elements: Evidence emerging economies," J. Finance. Crime, vol. 24, no. 2, pp. 242–255, 2017. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/JFC-04-2016-0024/full/html . [Accessed: 04-Aug-2020].

8. D. R. Cressey, "The criminal violation of financial trust," Am. Sociol. Rev., vol. 15, no. 6, p. 738, 1950. [Online]. Available: https://www.jstor.org/stable/pdf/2086606.pdf. [Accessed: 04-Aug-2020].

9. M. B. Clinard and D. R. Cressey, "Other people's money: A study in the social psychology of embezzlement," Am. Sociol. Rev., vol. 19, no. 3, p. 362, 1973. [Online]. Available: https://psycnet.apa.org/record/1954-06293-000 . [Accessed: 04-Aug-2020].

10. W. S. Albrecht, Ed., Fraud in governmental entities: the perpetrators and the types of fraud, vol. 7, no. 6. 1991.

A. Higson & R. Kassem "The new fraud triangle model," Journal of emerging trends in economics and management sciences, pp. 191-195, 2012. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.885.5778&rep=rep1&type=pdf [Accessed: 05-Aug-2020].

11. R. A. Becker, C. Volinsky, and A. R. Wilks, "Fraud detection in telecommunications: History and lessons learned," Technometrics, vol. 52, no. 1, pp. 20–33, 2010. [Online]. Available: https://www.jstor.org/stable/pdf/40586677.pdf [Accessed: 05-Aug-2020].

12. W. by R. Rosenbaum, "Secrets of the Little Blue box," Spolearninglab.com.

13. [Online].Available:https://www.spolearninglab.com/curriculum/lessonPlans/hacking/resources/readings/rosenbaum71_bluebox.pdf. [Accessed: 04-Aug-2020].

14. N. Jiang et al., "Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis," in Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys '12, 2012. [Online]. Available:

15. https://d1wqtxts1xzle7.cloudfront.net/49049995/Isolating_and_analyzing_fraud_activities20160922-7917-e05404.pdf?1474596947=&response-content-disposition=inline%3B+filename%3DIsolating_and_analyzing_fraud_activities.pdfKey-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Accessed: 05-Aug-2020].

16. G. Zhang and S. Fischer-Hübner, "Detecting near-duplicate SPITs in voice mailboxes using hashes," in Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 152–167. [Online]. Available https://www.researchgate.net/profile/Ge_Zhang6/publication/220905133_Detecting_Near-Duplicate_SPITs_in_Voice_Mailboxes_Using_Hashes/links/0046353bbe2659b870000000.pdf. [Accessed: 05-Aug-2020].

17. P. Patankar, G. Nam, G. Kesidis, and C. R. Das, "Exploring anti-spam models in large scale VoIP systems," in 2008 The 28th International Conference on Distributed Computing Systems, 2008, pp. 85–92. [Online]. Available https://ieeexplore.ieee.org/abstract/document/4595872 [Accessed: 05-Aug-2020].

18. F. Wang, Y. Mo, and B. Huang, "P2P-AVS: P2P Based Cooperative VoIP Spam Filtering," in 2007 IEEE Wireless Communications and Networking Conference, 2007. [Online]. Available https://ieeexplore.ieee.org/abstract/document/4224895. [Accessed: 05-Aug-2020].

19. S. Subudhi and S. Panigrahi, "Quarter-sphere support vector machine for fraud detection in mobile telecommunication networks," Procedia Comput. Sci., vol. 48, pp. 353–359, 2015. [Online]. Available https://www.sciencedirect.com/science/article/pii/S1877050915007024 [Accessed: 05-Aug-2020].

20. Cfca.org.[Online].Available:https://cfca.org/sites/default/files/Fraud%20Loss%20Survey_2019_Press%20Release.pdf. [Accessed: 05-Aug-2020].

21. "Telecoms Fraud Management -Who is winning the Battle? A Praesidium Business Consultancy[WhitePaper],"2011.[Online].Available https://www.ciosummits.com/media/pdf/solution_spotlight/wedo_telecoms-fraud-management.pdf [Accessed: 05-Aug-2020].

22. M. Smith, Research Methods in Accounting, 4th ed. London, England: SAGE Publications,2017.[Online].Available

http://digilib.umpalopo.ac.id:8080/xmlui/bitstream/handle/123456789/399/%5BMalcolm_Smith%5D_Research_Methods_in_Accounting.pdf [Accessed: 05-Aug-2020].

23. D. B. Bromley, Case study method in psychology and related disciplines. Chichester, England: John Wiley & Sons, 1986.

24. D. R. L. Miller and D. J. D. D. Brewer, Eds., The A-Z of social research: A dictionary of key social science research concepts. Sage Publications, 2003.

25. P. D. Leedy and J. E. Ormrod, Practical research: Planning and design, global edition, 11th ed. London, England: Pearson Education, 2015.

26. W. G. Zikmund, J. C. Carr, and M. Griffin, Business research methods. South Melbourne, VIC,Australia:CengageLearning,2013.[Online].Available https://books.google.co.in/books?hl=en&lr=&id=ydcKAAAAQBAJ&oi=fnd&pg=PR6 [Accessed: 05-Aug-2020].

27. S. A. A. Rahim, A. Nawawi, and A. S. A. P. Salin, "Internal control weaknesses in a cooperative body: Malaysian experience," International Journal of Management Practice (IJMP)., vol. 10, no. 2, p. 131, 2017.[Online].Available

28. https://www.inderscienceonline.com/doi/pdf/10.1504/IJMP.2017.083082 [Accessed: 05-Aug-2020].

29. M. Omar, A. Nawawi, and A. S. A. Puteh Salin, "The causes, impact and prevention of employee fraud: A case study of an automotive company," J. Financ. Crime, vol. 23, no. 4, pp. 1012–1027,2016.[Online].Available https://www.emerald.com/insight/content/doi/10.1108/JFC-04-2015-0020/full/html [Accessed: 05-Aug-2020].

30. K. M. Zakaria, A. Nawawi, and A. S. A. P. Salin, "Internal controls and fraud – empirical evidence from oil and gas company," J. Financ. Crime, vol. 23, no. 4, pp. 1154–1168, 2016. [Online].Available https://www.emerald.com/insight/content/doi/10.1108/JFC-04-2016-0021/full/html [Accessed: 05-Aug-2020].

31. Archambeault, D.S., Webber, S. and Greenlee, J., Ed., Fraud and corruption in US Nonprofit entities:a summary of press reports 2008-2011,Non-profit and Voluntary Sector Quarterly,vol.44,no.6,pp.1195-1224,2015.[Online].Available https://journals.sagepub.com/doi/pdf/10.1177/0899764014555987 [Accessed: 05-Aug-2020].

32. J. T. Wells, Corporate fraud handbook: Prevention and detection, 5th ed. New York, NY: John Wiley & Sons, 2017. [Online].Available

33. https://books.google.co.in/books?hl=en&lr=&id=gLZpDgAAQBAJ&oi=fnd&pg=PR11 [Accessed: 05-Aug-2020].