Direct Research Journal of Engineering and Information Technology
Vol. 9, (1) Pp. 16-55, February 2022
ISSN 2354-4155
DOI: https://doi.org/10.26765/DRJEIT14035036
Article Number: DRJEIT14035036

http://directresearchpublisher.org/drjeit/

Review

A Plethoric Literature Survey on SIMBox Fraud Detection in Telecommunication Industry

Lateef Gbolahan Salaudeen[1,2*], Aliyu Rufai Yauri[2], Garba Muhammad[1], Hassan Umar Suru[1], Alimi, O. Al-Maru'f[1,3], Danlami Gabi[1], Suleiman Musa Argungun[1], and Muhammad Sirajo Aliyu[4]

[1]Department of Computer Science and Info-Tech, Faculty of Physical Science, Kebbi State University of Science and Technology, Aliero,P.M.B 1144 BirninKebbi, Kebbi State, Nigeria.
[2]Department of Information and Communication Technology, Faculty of Engineering, Kebbi State University of Science and Technology, Aliero, P.M.B 1144 BirninKebbi, Kebbi State, Nigeria.
[3]Department of Computer Science, Faculty of Computing Science, Al-Hikmah University, Ilorin, Kwara State, Nigeria.
[4]Department of Computer Science, College of Basic and Applied Science, Katsina State Polytechnic, Katsina, Katsina State, Nigeria.
Corresponding author E-mail: gbolahan_salaudeen@yahoo.co.uk, +234(0)7067442771, +234(0)8069499614

Received 5 January 2022; Accepted 28 January 2022; Published 5 February 2022

ABSTRACT: SIMBox or Interconnect Bypass Fraud is one of the most rapidly emerging frauds in today's telecommunications industry, costing the industry between $3 and $7 billion USD in annual revenue losses. This was spread as a result of calls made over the internet and routed to SIMboxes (machines that contain SIM cards) that redirect illegitimate VoIP traffic onto mobile networks. Fraudsters effectively avoid the inter-connect toll charging points by exploiting the difference between the high interconnect rates and the low retail price for on-network calls, thereby avoiding payment of an Operator's or MVNO's official call termination fee. This paper is a fact-finding type that investigates the impact of SIMBox fraud on the telecom industry and the economic development of nations. By disclosing the fraud detection approaches used for its abolition and identifying their flaws. For this study, a quantitative method was used. The study's literary material spans the years 1994 to 2021. Journals, white papers, M.Sc., and Ph.D. theses on the subject are examples.

Keywords: SIMBox fraud, fraud detection, fraud prevention, fraud analyst, ITR, LTR

INTRODUCTION

Due to an increase in illegal access to VoIP network or internet services and cybercrime mannerism, detecting and preventing unfavorable forms of fraud such as telecommunication fraud, e-commerce credit card transaction fraud, online banking fraud, insurance fraud, healthcare fraud, cyberspace transaction fraud, electronic cash machine fraud, money laundering and intrusion into computers and computer networks (Alraouji and Bramantoro, 2014; Chouiekh and EL haj, 2018), leading to multi-billion losses worldwide each year; has become important. This study focused it scope only to telecommunication fraud of SIMbox fraud ravaging the global telecom industry. While the study delves its prevention and detection modalities hypothesized and organized by scholars and anti-fraud vendors to checkmate its abrupt wrecks through its imprecation rendered upon the industry and nation's reputation which thus tarnished there transactional and developmental proceedings. Following the huge growth in telecommunication networks in the past years, which is so imperative in our lives and daily chores, the service providers and telecommunication industries,

faces a set of new big challenges (Marah, Elrajubi and Abouda, 2015). Fraud with terrifying degree (Becker, Volinsky and Wilks, 2010; Tawashi, 2010) which was fast spreading with millions of dollars feasibly engulf around the world.

Inherently, fraud in telecommunications networks can be characterized by fraud conditions, which basically describe how fraudster gained illegitimate access to telecom network (Ogwueleka, 2009) for suspicious and damaging purpose with motives for their intention instigation described in the work of (Alghawi, 2019; Alraouji and Ramantoro, 2014). The problem of fraudulent use of mobile phones or gadgets is now a days tolerable and has become a bane to communication service providers and telecom industry; this they have been subduing for decade and has enabled detrimental consequences as regards billions of dollars revenue losses penultimate annual at varying countries denominations together with horrific imprecations and threats (Kala, 2019; Sowe, 2018; Fayemiwo and Olasoji, 2014) on the victims of circumstance (Mobile operators, Telco organization, nations and service subscribers).

Gent (2017) in an article publicized comprehensive global survey of 150 telecommunications network operators man-hurting by two ensemble issues identified as the most significant threats to operators' revenues. One of which has already cost operators an average of 20% of their termination revenues this year. The other has been a risk for many years but continues to threaten revenues at 80% of the networks as surveyed. This Siemens' issues were labelled SIMbox fraud and Over-The-Top (OTT) network bypass fraud in association with some other harbored contemporaries. These contemporaries includes; Subscription Fraud, Superimposed/Surfing Fraud and Intrusion fraud, International Revenue share fraud (IRSF), Premier rate fraud, PBX fraud, Wangiri fraud, Slamming, Cramming, SIM Cloning, Call refiling and masking; False Answer Supervision, Social Engineering and phishing fraud with many other; most of which (Cataleya, 2016; Ighneiwa and Mohamed, 2017; Ayamga, 2018;Fayemiwo and Olasoji, 2014; Becker et al., 2010, Tawashi, 2010) extemporize and elucidated distinctly in their respective work.

Over decade ago, Becker et al. (2010) described "fraud "as an act of deceiving others for personal gain, and the act is affirmed to be as old as civilization itself". While the literary survey of (Alraouji and Bramantoro, 2014) presented numbers of definition about the fraud concept for intelligibility based on subscribers' point of view and fraudster's point of view.

Chouiekh and EL haj, (2018) refers to fraud in communication networks *"as an illegal access to telecom network and the use of its services with no intention to pay service charges or making money by using these services by proxy due to charges incentives"*. To deter these two key issues (SIMbox fraud and OTT) scenarios or combat myriad forms of fraud;fraud analyst needs to be able to differentiate between fraud prevention and detection approaches; likewise understanding telephony billing system concept with telephone ecosystem (Sahin and Antipolis, 2017). Wieland, (2004) refers to fraud as a biggest revenue leakage to the telecommunication industry and global economy. Alraouji and Bramantoro, (2014), Alghawi, (2019) differentiate between fraud and revenue leakage. A revenue leakage refers to as the loss of revenue due to operational or technical loopholes. For that losses, it can be probably being recovered when the causes are exposed, which is possible by applying new audits control or enhancing the build procedures. Fraud is usually characterized by evidence of intention; as it aid detrimental consequences (financial losses, causes danger, loss of services, loss of customer confidence, hurting reputation of network operators or nation, and as well threaten national security architecture of a country) any of these intention is best known to the culprits'. For fraud losses some cannot be recover and the causes of fraud can be detected through analysis of data by applying some rules over calling patterns.

However, the process of detecting fraudster or fraudulent activities and providing solution to its anomalous delinquent; similar scenery of fraud concept and techniques is germane for deployment across board. These of course should being tandem with other fraud detection criteria. Fraud prevention is describing as measures carved to stop fraud from occurring in the initial stage. Perhaps through elaborate designs, fluorescent fibers, multitone drawings, watermarks, laminated metal strips and holographs on banknotes, personal identification numbers for bankcards, Internet security systems for credit card transactions, Subscriber Identity Module (SIM) cards for mobile phones, and passwords on computer systems and telephone bank accounts (Adjaoute, 2006; Blatt and Kaufman, 2017). Of course, none of these methods is vouched to be 100 percent perfect and, in general, a compromise maybe struck between expense and inconvenience (e.g., to a customer) on the one hand, and effectiveness on the other. In contrast, fraud detection is referred as an approach organize to detect illegal usage of services on a communication network or link (Aranuwa, 2013) once fraudulent act is perpetrated as quickly as possible. Fraud prevention as earlier described precedes fraud detection. When fraud prevention approaches fail; fraud detections swing into action and it involves a continuous process in deterring the dubious and conspicuous activities.

SIMBox fraud and OTT hijack are retails and wholesales forms of telecom fraud affecting global telecommunication industry and has become one of encumbrance for telecommunication operator which is growing dramatically (David-admin, 2017; Alraouji and Bramantoro, 2014). This has befallen a serious international problem for GSM, VoIP, CDMA and PSTN network service providers. As it has undoubtedly become a significant source of revenue losses and bad debts to the telecommunication industry; and with the expected continuing growth in revenue it can be deduced that fraud will have increased proportionally (Alraouji and Bramantoro, 2014). SIMBox fraud, which is one of the most prevalent of telecom fraud; consist of

diverting international calls on the VoIP network and terminating them as local calls on cellular network using an off-the-self-device, referred to as SIMBox (Murynet et al., 2014).

In many countries, the international termination rate (ITR) is considerably higher than the local (retail) termination rate (LTR) within the country (e.g., up to 2.8-28 times of difference in developing countries like Nigerian, Ghana, Cameroon etc. (Kouam et al., 2021; NCC, 2015)). This makes it profitable for fraudsters to bypass the regular interconnect operator when terminating calls in the country as they can pay the lower local rate instead of the ITR. SIMBox fraud is a major problem in developing countries (e.g. about 78% of African countries and 60% of Middle Eastern countries are fraud destinations (Goantifraud,n.d; Sallehuddin et al., 2015). Besides, in some of these countries, as much as 70% of incoming international call traffic is terminated fraudulently (Revector, n.d; David-admin, 2017). This difference has led to severe financial repercussions, costing operators almost $6 billion in 2015, according to the CFCA report cited (Al-Atassi, 2016). However, in same 2015 a presented loss record of about$39.9m USD dollars as an incurred by Cameroon (African, 2015).Recently, in Kenya, it was estimated that operators and government agencies were losing approximately $440,000 per month as a result of this fraud. Whereas Governments are even losing more, since many countries impose taxes on international mobile services. In Ghana, for example, the government reported that SIM-Box fraud recently cost between $5.8-$9.8m in loss taxes (Nyarko-Yirenkyi, 2020; Al-Atassi, 2016). In Nigeria telecom industry, it is estimated to be costing the industry $3bn USD dollars of revenue losses (Comms week, 2020). While African continents and nations engulf $150m dollar annual loss due to interconnected fraud (GNA, 2016). This practice is thus illegal in most countries especially in developing countries (Sallehuddin et al., 2015).

The simplest way of committing bypass fraud involves setting up a SIMBox (VoIP GSM gateway). This is a standard device that can be easily acquired via the internet and equipped with a bundle of SIM cards. The calls are typically routed via an internet flow (VoIP) to the SIMBox residing in the terminating country. The SIMBox then converts the VoIP call into a local mobile call to the receiving party on the local cellular network. SIMBox fraud is a significant problem for telecommunication operators and tax authorities of the affected countries, as international traffic taxes cannot be collected. Beyond direct revenue loss, bypass fraud also leads to poor customer experience. Examples of such call quality experience degradation are low voice quality due to latency issues, highly-compressed IP connections, longer call set up time, or still, missing or incorrect Calling Line Identifier (CLI). In particular, this latter results in many call rejections by the called party, while missed calls are not returned. Such degradation impacts the customer experience, which has a direct effect on loyalty, lifetime value, and revenue (Kouam et al., 2021).

To prevent this illegal accesses and services arrogation over the mobility networks via SIMboxes savors by fraudster. Telecom industry and mobile operators spend around $51m a year on bypass fraud management solutions, with operators frequently identifying and blocking large numbers of SIMBoxes SIM cards, yet the problem seems persistently unresolved across the world (Fayza, 2019). For further deterrence on fraud crusade not only Test Call Generation (TCG), Traditional fraud Management System (FMS), Rule based techniques, CDR analysis and many others have suggestively been applied and proven insufficient with identifiable drawbacks that cost grievously (Tesfaye, 2020; Fayemiwo and Olasoji, 2014; Hagos, 2018; Sahin, 2017; Ando et al., 2016); as surmised by some vendors providing cellular anti-fraud services and researchers (Papernaia, 2021; Moulton, 2015; Murynets, Zabarankin, Jover and Panagia, 2014). But in recent times, data science fields encompassing data mining (DM), big data analytics (BDA), machine learning (ML) and evolving deep learning (DL) techniques have become a shifted focus research area deployed for curtailment of the abruptly heinous act of fraud by researchers (Mola, 2017; Hagos, 2018; Chouiekh and EL Haj, 2018; Airn, 2018) and fraud analyst. Due to ample of information springing from various sources in quintillion daily via cellular traffic and the number of connected mobile devices. These makes detection of SIMBox fraud extremely challenging and also otherwise easy in some instance. Adhesively, if the traffic data could be gathered and make available for research entrenchment.

Moreover, traffic patterns and characteristics of fraudulent SIMBoxes are very similar to those of certain legitimate devices, such as cellular network analyses. So detecting fraudulent SIMboxes resembles searching for a new needle in a huge haystack full of small objects that look like needles. However, Telecommunication operators of the intermediate and destination networks have high financial incentives to understand the problem of fraud, but do not have the data to analyze the international calls that are gone (Murynets et al., 2014). To this regard, the absence of publicly available SIMBox fraud related dataset is a major obstacle for emerging of comprehensive studies on bypassing fraud analysis and detection (Elmi, Ibrahim, and Sallehuddin, 2013). These data set could have been a bail eve through which insight could be delve from records related to subscribers of services to assist in decision making of organization and that of fraud analyst inquest. The records of whose accessibility and availability is minimal for probing in this research aspect of fraud detection due to confidentiality nature attached (Sallehuddin et al., 2015). Another problem also is any fraud detection article published on the subject whose approached for the detection is duly extemporize can be utilized by fraudster to evade detection and maximize their illicit actions. In the field of security such as malware, credit card fraud, telecom fraud and intrusion detection those techniques in (Sahin, 2017) work were explore for bail

eve and divulge on behavioral pattern via classification approaches to detect subscribers of services that are suspicious of illegal service usage across board.

However, there are few studies targeting the behavioral patterns of malicious SIMboxers engaged in fraudulent act on the VoIP services. In this paper, only literary survey about SIMBox fraud detection and techniques applied to address the inhumaneness were discussed. This paper can be categorized as an exploratory type which delve the terminology plethora. The rest of the paper is arranged as follows section 2: delve SIMbox fraud across board and its entanglement in Nigerian telecom sector Section 3: presented literature survey on earlier stages and transient modalities adopted for SIMbox fraud curtailment over the mobility network. Section 4: General theoretical concepts on SIMbox fraud; how it happens and approached are looked into Section 5: Discussed method used to combat SIMbox fraud. Section 6: Elucidated on the fraud detection evasion methods by fraudsters. Section 7: Delves the impact of SIMbox fraud on Stakeholders involves in Telecom industry and suggested solutions with recommendation while Section 8: Surmise the scope of the paper subject matter.

PLETHORA OF TELECOMMUNICATION FRAUD OF SIMBOX FRAUD ACROSS BOARD AND ITS ENTANGLEMENT IN NIGERIAN TELECOM SECTOR

In recent time, Telecommunications have become an inevitability worldwide due to technological advancement and viabilities of Telecommunication Industry that has rendered a meritorious prowess; these were duly encapsulated in the report of (Afrinvest, 2020; Umaru, 2019). Telecommunication industry and network infrastructure have undergone developmental transformation which were akin to the goals for enhancing share-ability of networks and services in order to eliminate the barricade of communication, ill application utilization (e.g. social media app, transaction apps) and thus aid commerce over a long distance at the ease and comfy of both service providers and subscribers adoring the services. This in turns is improving productivity and profitability (Adeoye and Adelowo, 2015).

Arguably, user's addictiveness and assertiveness to the usage of the modern technological facilities in prosecution of daily tasks without any hindrances have makes the network infrastructure satisfactorily acceptable by all as its both rewarding and fulfilling. An advantages of which (Ez Talks, 2021; Proshare, 2020) elucidated. As most users attest to the technology prowess for the role plays in reduction of stress of travelling as it saves time and cost, as well as improves efficiency in communication, enhances performance in collaborators work, boosts customer relations and services, makes missive (e-mail, Short Messages Service (SMS)) to be automatically dispatch and as well advances productivity and profitability (Ez Talk 2021; Adeoye and Adelowo, 2015). But these have become a motive for fraudsters who are making lot of money out of illegal accesses to the communication setup and using it to make huge profits, by selling services at much lower prices than their original prices (Airn, 2018).

In recent years, fraud modelling and detection of Subscriber Identity Module Box (SIMBox) fraud otherwise known by variant names voice traffic termination fraud, interconnected or international gateway or bypass fraud, Grey call fraud etc. has become a trending research aspect in both academic and telecom industry pursuit (Ighneiwa and Mohamed, 2017; Bolton and Hands, 2002; Telenor, n.d, Airn, 2018).Owing to it atrocious and socio-economic detrimental implications (Sowe, 2018; Murynets et al, 2014) which is as well accompanied by eminent national security threats and vulnerabilities with government of varied countries e.g. UK, India, Ghana, Nigeria etc. (Papernaia, 2021; Kala, 2019) thus ravaging the development and transactional proceedings of national, multinational telecommunication industry and telecom infrastructure of hosting countries of the third world or developing countries or continents (Sallehuddin et al., 2015; Alsadi and Abuhamoud, 2020). Apparently, causing cellular network operator losses between 3 to 5 percent of their annual revenue due to fraudulent and illegal services embedment. Juniper Research estimated that the total loss from the underground mobile network industry is at $58bn in 2011 (Yelland, 2013; Windsor, n.d, Murynets et al., 2014; Alsadi and Abuhamoud, 2020). As the recent published report by Neural Technologies in 2016, unleash the average loss of telecom industry in estimation at about $249bn dollars USD due to fraud activities. While the survey conducted by the center for strategic and international studies presented a high figure of $375bn as a global yearly loss incurs due to cybercrime mannerism (Losses, 2014; Ando, Gomi and Tanaka, 2016; Chouiekh and EL haj, 2018); the survey includes indirect cost such as the leakages of personal information and intellectual property theft. While (Danny,2012) had earlier quotes The Association of Certified Fraud Examiners (ACFE) reports to affirmed that organizations actually loses an average of 5% of their total annual revenue, amounting about $3.5 trillion USD dollars globally as a result of fraud.

However, for clarification this paper narrowed it scope to extenuate only those losses caused by telecom fraud and SIMBox fraud. According to a survey conducted by the Communication Fraud Control Association (CFCA), the mobile telecom industry lost $ 29.2 Billion (USD) in 2015 alone due to telecom fraud. Besides those huge losses, telecom fraud causes other indirect losses to mobile operators, like: decrease in quality of service, denial of service and network congestion, Customer Churn, Customer dissatisfaction are major challenges that arise due to telecom fraud. Also, in same survey conducted by (CFCA, 2015; Papernaia, 2021) it was established that bypass fraud cost telecom companies between $3, $6 and $7bn USD dollars annually. And it is presently ranked as the 2nd amongst the top 3 or 5 fraud types man-hurting the global mobile

Figure 1: CFCA 2015 Survey, Top 3 fraud losses globally (Source: Ighneiwa and Mohamed, 2016).

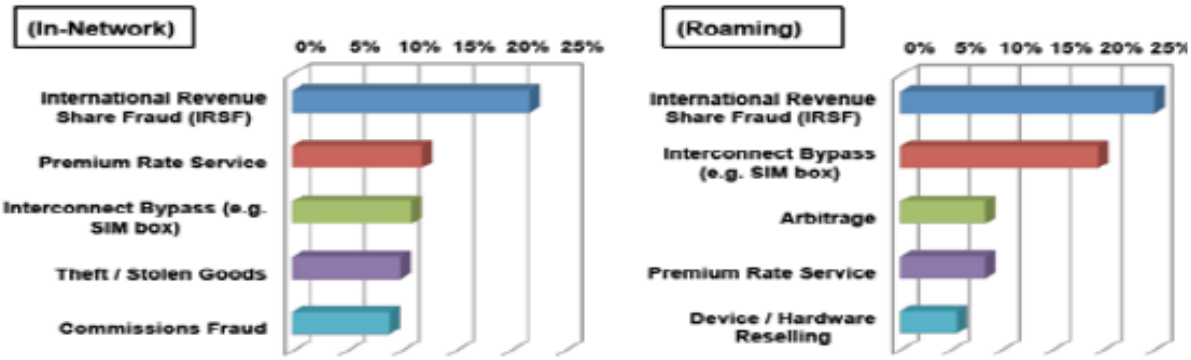

Figure 2: Percentage comparison of SIMbox fraud in network vs. roaming. (Source: Kala, 2019).

telecommunication industry (Ighneiwa and Mohamed, 2017) (Figure 1).

Figures 2 and 3 also show the top 5 fraud types with their annual percentage losses in network and roaming. The statistics depicted are huge. In an article (Subcable News, 2020) presented the list of major mobile operators owned by either state, public or private stakeholders, the revenue obtained by these bodies could help nations or telecom sectors grow economically and anything that affects it would degrade the country's GDP. It is believed that the revenue losses or incurs momentarily due to illegality of subscribers delving mobile operator and telecom services providers have limited this growth, and degrade the hosting country's GDP, overhauling industrial underperformance and deterred the government tax payment levy (revenue). SubexInc (n.d) however exclaimed that telecommunication operators globally have experiences significant amount of revenue losses due to bypass fraud otherwise called Subscriber Identity Module Box (SIM-Box) fraud unendingly. The author refers back to 2009, where an estimated loss of about $2 billion was recorded, which then increased by over 44% in 2011 to $2.8 billion base on figure presented by (Communications Fraud Control Association (CFCA) Fraud Survey, 2011). Koi-Akrofi *et al.,* (2019) respectively extenuates on the impact of cyber fraud/ telecom fraud severances in some country than the others; as (Reuter, n.d) publicized raids in countries like Mauritius, Haiti, and El Salvador in Brazil where fraudulent activities are rampant and causing lots of economic instability. SIMBox is one of major retail fraud that globally shares 10-19% of total losses determined by all frauds in telecommunication industry in network and roaming (Figure 2). With that percentage and amount of loss pictorially depicted in (Figure 1) from the work of Ighneiwa and Mohamed, (2017). SIMBox fraud is seen ranked second with $6bn USD loss after the whole sale fraud of IRSF engulfing loss of $11bn USD been the most dreadful and lastly premier rate fraud of $3bn. Papernaia, (2021) alleged that global cost of SIMBox fraud to telecom industry is massive in last year, while revealing the RAG RAFM survey estimating operators' loss of almost $7bn USD dollars to bypass fraudsters.

Unfortunately, more than 80 percent of mobile operators have already experienced SIMbox fraud. Africa seems to be the hub for mobile network fraud with cost implication (Tables 1, 2, 3, 4, and 5), as mobile operators there getting hit hard when SIMboxes are used fraudulently. SIM box fraud is leading telecom providers around the world to charging telecom industry momentarily to secure and protect their networks against its catastrophes.

Ali, Azad, Centeno et al., (2019) and McAfee (2018) collates the presented Table 1 to depict the recent cost implication effect of cyber fraud on the global technological compliance society or digital divides

Table1: Regional Distribution of E-Fraud for the Year 2017 (Ali et al, 2019; Mcafee, 2018).

S/N	Region (World Bank)	Region GDP (USD, Trillions)	Cyber fraud Cost (USD, Billions	Cyber fraud Loss (% GDP)
1	North America	20.2	140 to 175	0.69 to 0.87%
2	Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
3	East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
4	South Asia	2.9	7 to 15	0.24 to 0.52%
5	Latin American & the Caribbean	5.3	15 to 30	0.28 to 0.57%
6	Sub- Sahara Africa	1.5	1 to 3	0.07 to 0.20%
7	MENA	3.1	2 to 5	0.06 to 0.16%
WORLD TOTAL GDP (TRILLION USD)		$75.8	$445 to $ 608	0.59 to 0.80%

Table 2: Selected African Countries Population and their GDP.

AFRICAN COUNTRY	POPULATION (MILLIONS) & PENETRATION %					GDP(USD BILLION DOLLARS $)				
	2016	2017	2018	2019	2020	2016	2017	2018	2019	2020
NIGERIA	185,989,640	190,886,311	195,875,237 (50%)	200,962,417	206.049,597	$404.7	$376	$398.16	$448.12	$442.98
KENYA	46,790,758	49,699,862	50,950,879 (85%)	52,214,791	53,478,703	$63.398	$70.5	$77.61	$95.5	$101.048
TANZANIA	55,572,201	57,310,019	59,091,392 (39%)	60,913,557	62,694,930	$44.895	$47	$50	$63.18	$62.224
GHANA	28,206,728	28,833,629	29,463,643 (34%)	30,096,970	30,726,984	$37.86	$43	$48.14	$66.98	$50
UGANDA	41,487,965	42,862,958	44,270,563 (43%)	45,711,874	47,119,479	$26.369	$24	$26.369	$35.17	$36.484
NAMIBIA	2,479,713	2,533,794	2,587,801 (31%)	2,641,996	2,696,003	$9.23	$11	$13.3	$12.37	$10.30
BOTSWANA	2,250,260	2,291,661	2,333,201 (40%)	2,374636	2,416,176	$12.56	$15.6	$17.12	$18.34	$17.00
LESOTHO	2,203,821	2,233,339	2,26310 (28%)	2,294,024	2,323,785	$2.3M	$2.5M	$2.576M	$2.376	$1.91
MAURITIUS	1,262,132	1,265,138	1,268,315 (63%)	1,271,368	1,274,545	$26.69	$28.23	$30.01	$31.59	$29.63
AFRICA	1,185,529,58	1,256,268,03	1,300,000,000 (35%)	1,307,038,716B	1,345,200000 B	$2.78T	$3T	$3.5 T	$2.6T	$4T

region such as North America, Europe and Central Asia, East Asia and the Pacific, South Asia, Latin American and the Caribbean, Sub- Sahara Africa and MENA.As is SIMbox fraud is committed over the VoIP gateway or internet network.

Table1 revealed that the total GDP of the world is $75.8trn in 2017; where it established that North America, Europe and central Asia and East Asia and the pacific, are the most affected by the nefarious act of cybernetic fraud with cost behavior in approximation between 1 to 2 percentage losses. From which the cost of global cyber fraud has increased from $445Billion in 2014 to $608Billion in 2017 (McAfee, 2018). Table 1 provides an avenue to compare and contrast regional GDP with the percentage of losses in order to be wary of cyber fraud. Also, it is deduced from (Table 1) that the higher the regional GDP, the greater are the losses associated with the cyber fraud. Ali *et al.,* (2019) further explains that hi-tech-thieves use numerous techniques to defraud the consumers of technological services; by using stolen personal information to apply for debit, credit and store cards. They obtain such information via social engineering and phishing attacks using telephone and web (email, social networks).

A recent report published by Symantec revealed that 978 million people in 20 countries were affected by cyber fraud in 2017 (Norton cyber security report, 2018). These frauds resulted in a loss of $172 billion (an average of $142 per victim) to the consumers. Additionally, the report also revealed that consumers spend nearly 24 hours on average dealing with the consequences. Imperatively, fraud does not only bring financial loss but also leave the psychological and social effects on the well-being of the victims (Kaakinen et al., 2017). Most common type of cyber fraud experienced by consumers these days includes debit/credit card fraud, hacking of an email or a social media account, electronic commerce frauds and disclosing private information to fraudsters via the telephone call or clicking on phishing emails (Norton cyber security report, 2018, Ali et al, 2019). The others include cyber bulling, malware, rasomware and SIM box fraud as the recent inclusion (African Cyber Security Report, 2017; Kouam et al., 2021).

Table 3: Numbers of Internet Users & Estimated Cost of Cyber Fraud Losses Annually (Source https://www.statista.com).

COUNTRY/ CONTINENT	NUMBERS OF INTERNET USERS/ SUBSCRIBERS IN MILLIONS						ESTIMATED COST OF CYBER FRAUD LOSS (MILLIONS DOLLARS ($))				
	2016	2017	2018	2019	2020	2021	2016	2017	2018	2019	2020
NIGERIA	51.57	61.43	72.3	184.7	185.05	185.27	$550	$649	$800M	$748(N224B)	$700 (N350B)
KENYA	15.57	16.20	18.9	19.66 (+16%)	22.86	24.15	$175	$210	$230	$240	$245
TANZANIA	11.67	12.60	13.9	14.69 (+3.0%)	14.72	16.2	$85	$99	$113	$115	$117
GHANA	5.9	7.96	10.11	10.32	14.76	15.7	$50	$54	$58	$105	$9.8m
UGANDA	5.7	6.90	7.89	8.90	10.16 (+14%)	12.16	$35	$67	$99	$102	$107
NAMIBIA								--	-		
BOTSWANA	-	0.79	0.92	1	1.09	1.12		--	-		
LESOTHO								--	-		
MAURITIUS								--	-		
AFRICA							$2B	$3.5B	$4B	$4.5	$5.7B

Table 4: Selected estimated numbers of cyber fraud professionals.

COUNTRIES/ CONTINENT	Estimated No. of Certified Professionals				
	2016	2017	2018	2019	2020
NIGERIA	1500	1,800	2100	2400	2700
KENYA	1400	1600	1800	2000	2200
TANZANIA	250	300	350	400	450
GHANA	460	500	540	580	620
UGANDA	300	350	400	450	500
NAMIBIA	50	75	100	125	150
BOTSWANA	45	60	75	100	125
LESOTHO	25	30	35	40	45
MAURITIUS	100	125	150	175	200
AFRICA	6,892	10,000	13100	16200	19300

Table 5: Statistical Survey of Nigeria on Effect of Cyber Fraud (2006 - 2020).

Years	Population	Internet users/ mobile subscribers	GDP (n' (naira) trillions)	GDP (USD $) billion dollars	Estimated cost of loss to cyber fraud (million ($) and conversion in (naira)	Estimated no. of certified professionals
2006	140,431,790	50,000,250	39,995.50	236.10	$15m	125
2007	144,998,281	53,000,124	42,922.41	275.63	$20m	150
2008	149,713,264	60,000,100	46,012.52	337.04	$25m	200
2009	154,581,566	62,008,345	49,856.10	291.88	$30m	250
2010	158,578,261	63,245,123	54,612.26	363.36	$35m	300
2011	164,798,232	65,123,458	57,511.04	410.33	$36m	450
2012	170,157,060	70,000,678	59,929.89	459.38	$40m	650
2013	175,690,143	72,034,345	63,218.72	514.97	$46.3m	780
2014	181,403,148	80,789,456	67,152.,790	568.5	$50.8m	900
2015	183,301,926	97,210,000	69,023.930	481.1	$450M (N89.7B)	1200
2016	185,989,640	98,810,000	67,931.240	404.7	$550M (N127 B)	1500
2017	190,886,311	99,100,200	68,490.980	375.75	$649M (N197-250B)	1800
2018	195,875,237	92,300,000	132,120,000	448.12	$800M (N288B)	2100
2019	200,962,417	119,506,430	180,000.000	398.16	$748 (N224 B)	2400
2020	206,139,589	125,567,200	212,630,400	442.98	$ 700 (N350B)	2700

Explicitly, in the United Kingdom, it is estimated that the UK economy is suffering from the loss of around £27 billion per annum due to these cyber frauds (The cost of cybercrime, 2016). Through this, UK businesses are affected as they lost a cost of around £21Billion, followed by the government and citizens, with damage of around £3Billion respectively. The Internet Crime Complaint Center has received around 11,000 complaints in 2017, resulting in a loss of around $15Million, 90% higher than the losses reported in 2016 (How to spot tech support scams, 2016, Ali et al., 2019).

Furthermore, Microsoft also saw a substantial increase in the tech scam i.e. a 24% increase in tech scams reported by customers in 2017 over the previous year (Microsoft, 2018) with the average loss of $200 to $400 each. Fraud over financial systems such as ransomware, card payment, and Crime as a Service

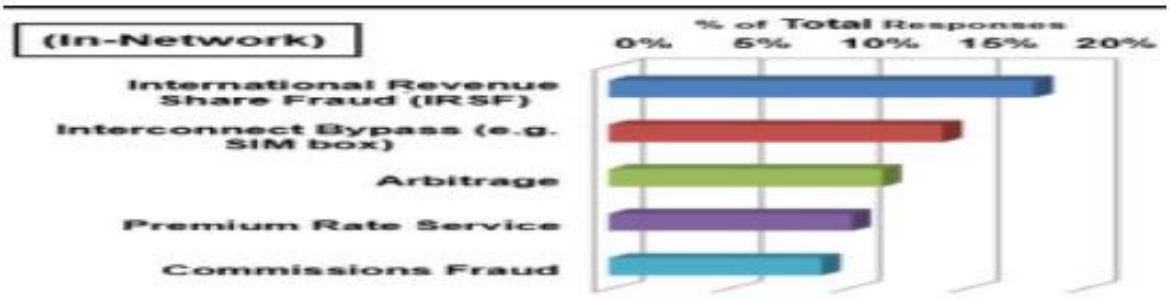

Figure 3: Fraud Responses as per CFCA Report (Source: Airn, 2018;Okumbor and Ateli, 2019).

(CaaS) is found to be some of the established and professionalized ways to commit fraud (Ali et al., 2019; Yaqoob, Ahmed, Rehman, Al-garadi, Imran, and Guizani, 2017).

In most cases, cybercriminals make use of customer facing platforms to target victims and practice cyber frauds (Ali et al., 2019; Xu et al., 2018; Yaqoob, Hashem, Ahmed, Kazmi and Hong, 2019; Modi and Dayma, 2017). Some of the highly targeted customer-facing platforms include but are not limited to: payment systems, where cybercriminals take control of the target victim's payment account, mobile platforms where a victim's mobile phone is targeted to get control over payment applications; and telecommunication systems where illegitimate acts are performed by targeting a victim through their telephony network. With the evolution in cyber systems, cybercriminals have also improved in their methods of targeting cyber systems and there is a strong need to characterize the most used mechanisms of cybercrimes in order to protect organizations and consumers from cybercriminals.

To this detail, we propose an exploration on the effect of cyber fraud in Sub-Sahara Africa region with least regional GDP of $1.5trn and revenue losses between 0.1 and 0.2 % as depicted in the (Table 1) to which Nigeria as a country is inclusive.

Nigeria is a country identified as one of the fastest moving economy and one of the most advanced ICT market sector in the Africa with largest population (Adeoye and Adetowo, 2015) making it attractive, lucrative and big markets for foreign investors to hump into for commerce. This as well as entices cybercriminal to re-strategies and to fishes on the deficiency of their victims through abruptly use of modern technologies to perpetrate the heinous act via it economic industrialized sector (e.g. Telecommunication industry, Banking and Financial Institution) to satisfy their selfish, cruel and detrimental purposes.

The comprehensive (Tables 2, 3 and 4) were combined to showcases records of cyber fraud in Sub-Sahara African region starting from 2016 till 2020. This paper improvises for 2018, 2019 and 2020 where nine (9) countries is enlisted and a total of 54 Africa nation details. The tables were constructed based on the datasets gathered from the (Africa Cyber Security Report, 2016 and 2017) that was conjointly prepared by Serianu, United States International University-Africa, Demadiur and (worldometer, 2019; world fact, n.d) with an updates for improvement.

From the analysis done, it was discovered that most African country losses gruesome percentages of their annually generated GDP (nominal, real, actual and potential) to cybernetic frauds trait despite haven varying magnitude of resources at their respective disposal for curtailment and/ or fight cybercrime.

In this, Nigeria bears the major brunt of fraudulent demoralization on its persons (citizens), economy and industries. A reason been that it is the most populated country in Africa continent with largest internet user's base and greater GDP and largest mobile market on Africa continent followed by South Africa (Afrinvest, 2020). Annually, Nigeria accrues a staggering revenue losses running into billions of naira due to cybernetic fraud (Tables 2, 3, and 5) for clarifications. As the work of (Frank and Odunayo, 2013) delve the approach to cyber security issues in Nigeria: challenges and solution. Where the concept of cybernetic fraud or cybercrime was literary described.

From the (Tables 2, 3 and 4) analysis was performed on the selected African countries by diving the GDP per year with the estimated loss cost to e-fraud to determine the percentage of revenue loss by these countries (i.e. GDP/cost of e-fraud loss*100 to determine = percentage of loss). To presents the actually incurred GDP losses due to cyber fraud mannerism in the last six (6) years by the countries in the tabulated tables.

In 2016, Nigeria incurs a loss of 74% of the GDP to Cyber fraud. An estimation which contradicts the earlier presented 43% by (Umoru, 2017); as the author only based the calculation on Nigerian banking industry. However, Kenya recorded 36.23% loss from their GDP to cybercrime, Tanzania 52.82%, Ghana 75.73%, and Uganda 75.34%. While Namibia, Botswana, Lesotho, and Mauritius details were anonymous as the GDP generated is lesser compared to their counterparts with much population growth rates, internet subscribers and GDP prospects. In African continent the percentage rate of fraud cases is 139%

In 2017, there were measurable decline in the loss as Nigeria recorded 57.90% of GDP loss to Cyber fraud with decrease of (12%) subjected to the anti-fraud

crusade reshuffles of President Muhammad Buhari against corruption and cybercrime during his first democratized tenure; Kenya recorded 33.57% in GDP loss with a fluctuating reduce of (2%), Tanzania recorded 47.5% GDP loss and a reduced (5%), Ghana GDP lose rise to 79.63% as it increases by (4%), While Uganda brazes up and kicked against cyber fraud to have experience drastic reduce of (35.94%) that leaves them with 35.82% GDP loss to cyber fraud. In African continent the percentage rate of fraud cases drops to 94.3%.

In 2018, Nigeria recorded a down trending loss of 56% to cyber fraud mannerism due to activeness in the anti-fraud war (Proshare, 2020), as Kenya recorded few drop in it GDP loss to have 33.74%, Tanzania recorded a reduction of 42.25% loss, as Ghana percentage lose rise to 82% and GDP loss of $105million dollars was recorded due to cybercrime (Nyarko-Yirenki, 2020), Uganda GDP percentage loss to cybercrime decrease to 26.64%.

In 2019, the GDP in dollar dropped due to reduction in exchange rate, and international crude oil crash market (OECD Policy Responses to Coronavirus (COVID-19), 2020). Due to these, couple of international economy suffers; as the global community were at the second quarter of that year begins to battling with the ravaging corona virus pandemics and on course to salvage wellbeing of humanity. In that period, Nigeria recorded a GDP loss of 53.23% despite continuous anti-fraud war shortly after the re-election success of President Muhammadu Buhari GCFR. During COVID-19 pandemic lockdown, fraudster advance their scheme by devising a new technique (phishing of credit card fraud, social engineering fraud etc.) to dupe their spry desperate for the government relieved fund and palliatives in which the majority of the populous could not accessed as it was siphon and diverted elsewhere for political motivated course. Meanwhile, Kenya recorded 39.79% GDP loss increase, Tanzania also recorded an increase in loss of 54.94% and Ghana percentage of lose to fraud sprang up to 111.6% and yet recorded a decline of $9.8m loss to cybercrime against the previous year (Nyarko-Yirenkyi, 2020). Uganda percentage GDP loss to cybercrime increase to 34.48%. As other countries detail still remain anonymous. The increased in GDP loss recorded across African continent in this period were worrisome, these was believed to have been necessitated due to statistics of poverty level in the continent and global socio-economic factors that craving for economy viability and sustainability.

In 2020, Nigeria recorded down trended loss of 46.83% to cyber fraud with 9 percentage decrease as a result of continuous fight against fraud and money laundering by E.F.C.C (Economic and Financial Crime Commission) and ICPC rejigs. Kenya recorded an increase of about 41.24%, Tanzania recorded a decrease in loss to 53.18%. Ghana dealt a great blow on cyber fraud to record a GDP lost shoot-down to 78.13% with (13% decrease). Uganda keep waging stronger in their anti-cybercrime crusade to witness a decrease in revenue loss by little drop to recorded 34.06% as result of government policy (Amanfu, 2018). Namibia, Botswana, Lesotho, and Mauritius details were still remains anonymous to us while trenching this research. In African continent the percentage rate of fraud cases is drop at 90%.

Observably, Ghana is the most affected with cybernetic fraud (SIMBox Fraud) problem (Laary, 2015; Amafu, 2018) in term of revenue losses annually, despite their lesser population strength, internet user and annual GDP generated and cyber professional at their possession compared to Uganda, Kenya, Tanzania and Nigeria. Nigeria follows in ascending lines as regards GDP loss to cyber fraud with over 1800 certified professional of cyber security experts. The country bears the highest population rate, generated staggering GDP and yet perceived as the most inflicted with cyber fraud losses. Reason, is due to the increase in numbers of internet subscriber that abruptly utilized the internet facility (technologies) as a results of poverty level in the country. Some decades back, when there was no much internet subscribers due to fixed line communication utilization against the cellular (GSM) obtainable now, crime over the cyberspace was minimal as must people were not ICT compliance, now that the populous are digitally aware and ICT literate everyone is susceptible to fraudulent witticism. From the analysis it can be deduces that the revenue lost by those country to cyber fraud is on increase years in and out without reduction. Proportionally, as the world and nation's population increases, so we have more internet users and Telco subscribers and inversely increases in rate of cybernetic fraud.

Analysis of Nigeria losses to cyber fraud (2006-2020)

From (Table 5) statistical detail of Nigeria was detractively stated between (2006- 2020). Where it's glaring that Nigeria population is on increases year in and out, as the number of internet users increases and the cost estimate losses to cyber fraud is also on rise except for the decline of internet users in 2018 which does not stop the amount losses instead its trodden. Nigeria has the highest numbers of cyber fraud professionals on the continent of Africa but could not get its axes together to fight cyber fraud to the barest minimum. From the economic loss recorded it is believed that the ICT sector (Telecommunication industry) and banking and financial sector were the most affected by the fraud activities of SIM box fraud, call masking and refilling, social engineering, phishing and many others (Adepetun, 2019; Mordi, 2019). This were note worthily established in Nigerian local and online magazines (e.g. Vanguard, Daily Sun etc.) and NCC reports that Nigerian Information and Communication Technology (ICT) sector housing the telecom industry and telephony users are currently being marred with challenges of cybernetic fraud attacks such as SIM-Box fraud, call masking, call refilling, SIM swap problem, slamming, cramming,

Phishing, SIM cloning, Signaling System No. 7 (SS7) (NAN, 2020; Ogunfuwa, 2020); affecting the country economic prospects; by subjugating it to revenue losses of gruesome amount ranging from N89.55billion (Ugoeze, 2016; Umoru, 2017), N127billion (Vanguard, 2017; Editorial Board, 2017), N141.1bn (Ogunfuwa, 2020), N197billions (Leadership, 2019), and more progressively per annum (Nwanchukwu, 2020, Daily Sun 2019; The Nation 2018; IT News Africa, 2017; Allafrica.com).

This the Chief Strategy Officer, Deloitte West Africa, Mr. Tope Aladenusi, confirmed and stated that Nigeria as a country had lost a staggering amount of about ₦5.5 trillion to fraud and cybercrimes in the last 10 years (Aliogo, 2021). When these figures were rehearsed; it was discovered to have form the basis for the country dwindling prospects in line with socioeconomic challenges (Kalau, 2021); giving an impression of causing its industrial sectors underperformances, leading to their residual degradation, investor's relocation of businesses to another country or possibly liquidations of most establishments, that furiously prone to the mass retrenchments of staff across organization's momentarily (Ahiuma-Young, 2016; Fadoju, 2017). In 2013, Nexus registered disconcert on why cellular merchant (operators) were the most affected in incurring the greatest fraud losses, as the cost of revenue lost is disgruntling, while accusing finger was pointed towards SIM-Box fraud unchecked in telecommunication industry by NCC Vice Chairman Prof. Umar Garba Danbatta (Nwogbo, 2018).

HISTORY OF SIM-BOX FRAUD AT THE GLOBAL SCALE AND IN NIGERIA TELECOM SECTOR

The article of (David Morrow 2017) titled "Telco Corruption Fuels SIM-box Frauds" reveal the genesis of SIM box frauds and facts about the first perpetrator of the act. The author shared his ordeal with a SIMboxer or more precisely, a former SIMboxer. He said: he had been aware of SIMboxing since 2002, and was involved in legal proceedings with one major SIMbox enterprise from 2003 to 2013, when their final appeal was thrown out by the European Court of Justice. The author disclose that he may be criticized by operators who think his publication will educate SIMboxers; as the author surmise that fraudsters already understand SIMboxing while charging the telecom sector to learn more about the scenario.

According to the Executive Vice Chairman, Nigerian Communications Commission (NCC), Professor Umaru Danbatta, "SIM boxing or Interconnect Bypass Fraud (IBF) is one of the most prevalent frauds in the telecom industry today and it is estimated to be costing the Nigerian Telecom industry $3 billion in revenue lost." (Umeh, 2018).

Prof. Danbatta described call masking as a phenomenon whereby an international call is masked to appear as a local call on any GSM network in Nigeria while SIM Boxing on the other hand refers to electronic boxes or devices with multiple SIMs that have the capacity to terminate calls at local interconnect rates.

SIM cloning involves the theft of identifying information of a SIM card belonging to a legitimate Subscriber in order to fraudulently provide calls on a telecom network at the expense of the legitimate subscriber (Blatt and Kaufman, 2017). A SIM card is a small memory module that contains, among other pieces of information, a unique serial number (ICCID) identifying that SIM card and an international mobile subscriber identity (ISMI) identifying a subscriber. These details are then input in new SIM cards to form SIM clones. A call made from a phone using a cloned SIM card may then be billed to the legitimate subscriber.

Prof. Danbatta said SIM Boxing was observed to have started in September 2016 in Nigeria at the time the Commission decided to review international termination rates from N 3.90/ min. to N24.40/ min. for international inbound traffic which provided an opportunity for technology manipulators to terminate calls at N 3. 90/ min. and cart away the difference thereby cutting the revenue meant for the Operators and by implication the government (Ogunfuwa, 2020; Adepetun, 2019). A SIM box has capacity to receive and transmit calls undetected. "However, the challenge is that these SIMboxes are never type-approved by the Commission, a clear indication that they are being used illegally in the country", the NCC boss stated (Ajanaku, 2020).

To drive home, the point; the Commission was serious about flushing the twin evils out of the industry, Professor Danbatta quickly vide a letter with Ref: TSNI/GEN/VOL.4/115 dated July 19, 2017 directed relevant licensees to ensure the cessation of call masking or refiling activity on their respective networks. The deadline for compliance was July 28, 2017. Furthermore, on August 3, 2017, at a stakeholders meeting organized by the Commission in which the affected companies participated, it was resolved that a comprehensive investigation would be carried out by the NCC to determine the companies/licenses involved in the illegal act.

All the licenses were warned to desist from this practice. It was also agreed that identified culprits would be sanctioned as part of measures to forestall the negative impact of this incidence on national security. After months of thorough investigation, the telecom regulator in a letter dated January 12, 2018 signed by Yetunde Akinloye, head, legal and regulatory services and EfosaIdehen, head, compliance monitoring and enforcement on behalf of the executive vice chairman/CEO, NCC, issued the Notice of Intention to Suspend license pursuant to Section 45 (1) and (3) of the Nigerian Communications Act of some culprits found wanting. NCC gave notice of its intention to suspend the interconnect exchange licenses granted to six telecommunications clearinghouses over the unethical practice of allowing call masking and call refilling emanate from their facilities. The companies Medallion Communications Limited, Interconnect

Clearinghouse Nigeria Limited, Niconnx Communication Limited, Breeze Micro Limited, Solid Interconnectivity and Exchange Telecommunications Limited and they were given p to January 31, 2018 to state reasons why the regulator should not suspend their licenses. According to the NCC's letter, ""having carefully analyses all the relevant data collected in the course of its investigation activities, the Commission has established a direct and indirect evidence against your company in the illegal and unwholesome activity of call masking and refiling. "Consequently, the Commission, pursuant to Section 45 (1 and (3) of the Nigerian Communications Act, 2003 hereby gives you Notice of its Intention to suspend Interconnect Exchange License granted to your company due to your involvement in call masking and refiling and your failure to rectify the breach, despite repeated interventions by the Commission. You are therefore required to state reasons why the Commission should not suspend the said license. We expected to receive your response on or before January 31, 2018" the letter read. Nearly a month later, NCC handed various levels of sanctions to telecom clearing houses and network providers implicated in the high incidence of call-masking, call-refiling and SIM-Boxing. NCC conducted a painstaking investigation process which included collaboration with the Office of the National Security Adviser (NSA) and the Department of State Services.

Among the various ranges of sanctions were the suspension of the Interconnect Clearing House License issued to Medallion Communications Limited for a period of 90 days, in the first instance; Issuance of a strong warning to Interconnect Clearinghouse Nigeria Limited; disconnection of Information Connectivity Solutions Limited (ICSL) and Solid Interconnectivity Services Limited from all networks, until they regularize their operations. Others were: Issuance of letters to Exchange Telecoms Limited, NiconnX Limited and Breeze Micro Limited, cautioning them against engaging in the fraudulent practice; and barring of over 750,000 numbers assigned to several Private Network Links (PNL) and Local Exchange Operator (LEO) licensees, which number ranges were found to have been utilized for the practice.

The Commission said the sanctioned entities were found to be directly and indirectly complicit in several infractions, including, covertly allowing organizations with expired licenses to transit calls, failure to undertake due diligence on parties seeking to interconnect, deliberately turning a blind eye to masking infractions by interconnect partners, and using a license issued to another organization to bring-in and terminate international calls which were masked as local calls to other operators.

During their further investigation, it was found that over 750,000 individual numbers across the nation made up of about 31 number ranges were used for the fraud. NCC barred those numbers which belonged to Vezeti Communications Services Limited, Voix Networks Limited, Mobitel Limited, Peace Global Satellite Communications Limited, ABG Communications Limited, Vodacom Business Africa (Nigeria) Limited, Swift Telephone Networks Limited, QVODA Telecoms Limited, Wireless Telecoms Limited and Emcatel Networks Limited. The Commission found that some of them were terminating millions of minutes, whereas they only have very few active customers. Following that, NCC began the second stage of investigation which focused on the Mobile Network Operators and other persons involved in SIM-Boxing. The aim of the Commission was to completely stamp out the fraudulent practice in the overall interest of all Nigerians. To this end, NCC in 2018 introduced a new technology which partially nipped in the bud, menace of call masking and call refiling (Comms Week. 2020).

The blaspheme of grievances ascribe to these telecom fraud (SIM-Box, call masking and call refilling) were seen as the causes of big and indirect losses to mobile operators, as it constituted the challenges of decrease in quality of service, denial of service and network congestion, Customer Churn and Customer dissatisfaction (Airn, 2018).

In March 2018, NCC proclaimed to wielded it hammer on the regulation of industry to fall on those licenses allegedly accused of call masking, call refilling and SIM-Box fraud (ITRealms, 2018) as the organization writes about new dawn in the fight against "telecom corruption" and sued for shunning of political motivated regulations in the telecom sector. The (Nwogbo, 2018) publication made disclosure on the effort of Mr. EfoseIdehen, a Compliance Monitoring and Enforcement officer of NCC, whom earlier said in Lagos that his team are currently monitoring incessant call masking upsurge after sanctions and warning had been issued on perceived culprits of interconnect clearing houses did not yield result. They identify SIM-Box operators as being responsible for call masking recently man-hunting the Nigeria telecom industry.

In respect to that, the NCC Boss Vice Chairman Prof Umar Garba Danbatta propose to deploy high technology for tracking and unmasking fraudster involved in SIM box frauds as a result of incessant fraudulent cost implication (Leadership.ng, 2018). The Executive Vice Chairman, Prof Umar Danbatta, said operators sparingly complained that they lost about 2.5million minutes per day to the fraudulent activities, while speaking at the 85th edition of the Telecom Consumer Parliament in Lagos last year (Ogunfuwa, 2020). According to him, some arrests were made in Lagos and it was discovered that perpetrators of the SIM boxing had over 100 SIM cards registered with fictitious names and used to divert international calls, thereby siphoning millions of revenues. In 2015, Nigeria recorded a loss of $450 million; an equivalent of ₦89.55b, as annual direct loses to cyber fraud (SIM-box fraud) at the CBN exchange rate of N199 to $1 (Ugoeze, 2016; Umoru 2017) revert to (Table 5) for summary of Nigeria economic losses to cyber fraud. If the amount is to be re-calculated at the current exchange rate of ₦500 to $1 we will have ₦225b of the exact loss. In (Allafrica.com, 2000) it was explained that Nigeria Telecom fraud losses is worth $22billion a year. And the rising waves of the cyber frauds is putting her embattled economy at risk (Allafrica.com, 2018).

Verily, the country through it commission stakeholders said telecom industry has been projecting to tighten its noose on the fraudulent activities (Nigeria Communication week, 2017) but to no achievable heading.

In 2019, Isaac reported for a magazine that quote the Vice President Prof. Yemi Osinbajo whom said Nigeria have losses over ₦197billion annually to the atrocious activities of cybercriminals who uses the digital sector to negatively perpetuate various financial crimes (Leadership, 2019). Emmanuel (2019) in another publication quotes the NCC Boss Prof. Umar Danbatta to reiterate that Nigeria have incurred losses in billions of dollars due to telecom related fraud of SIM-Box due to the introduction of Smartphone into the country and the mobile market; which necessitated the gulf up loss of ₦12.5billions of financial crime linked to the telecom industry.

In 2018, Nigeria and four other African countries (Kenya, Ghana, Uganda and Tanzania) shared an incurred loss worth estimated amount of $3.5b to the same deceptive act of cyber fraud (Webmaster, 2018). Therein, Nigeria is discovered, incurring the highest lost adjudging by the level of commitment; a reason of it been the central commercial hub of Africa economy.

In November 6th 2017, the erstwhile 8th Senate President of the Nigerian National Assembly, Dr. Bukola Saraki, said Nigeria have incurred a loss of about ₦127bn to cybercrime; a fact that was relinquished at Nigeria's first Legislative Stakeholders Conference on ICT and Cyber security on Monday in Abuja (Editorial board, 2017). While Ogunfuwa, (2020) in recent publication extenuated that Nigeria telecom industry was at the verge of losing another N141.1bn to fraud. Coherently, the Nigeria editorial board and Daily Sun magazine muttered over the Nigeria loses to the gruesome amount due to internet fraud; saying it's not news but the figure of over ₦127bn as annual losses presented by the former Senate President (Sen. Bukola Saraki) via his representative at the gathering; and former Minister of Communications Adebayo Shittu and the Director, e-Government Regulatory Department of National Information Technology Development Agency (NITDA) Dr. Vincent Olatunji also at different stakeholders' workshops or gathering is staggering unsettling. Judging by (Ugoeze, 2016) loss of ₦89.55b and the re-estimation to the current ₦225b lost and that of the erstwhile senate president affirmation loss of ₦127b in (Editorial board, 2017); a difference between (₦98b- ₦ 135.5b) loss was deduce with growth rate of 42% annually.

Osuagwu and Umeh (2018) gave key findings of the 2017 cyber security reports that the cost of cybercrime in Nigeria is $649millions (approximately ₦197.9billion) as (Proshare, 2020) presented a contrary figure of ₦ 250billion; with the banking sector serving as the most targeted industry followed by telecom industry in the country.

Reports by Nigeria Communications Week depicts that electronic payment transaction fraud rose by 82 percent in 2016 with an estimated ₦2.19billion ($6.9 million) loss to cyber criminals (Nigeria Electronic Fraud Forum (NeFF) annual report, 2016). IT News Africa, (2017) report shows that counter transaction amount to ₦571.07m ($ 1.6million of losses), followed by Automated Teller Machine transaction with ₦464.5 ($1.4million), internet banking ₦320.66m ($1million), point-of-sales transaction ₦243.32 ($765 thousand). A further breakdown also showed that mobile banking saw ₦235.1 million ($742 thousand) fraud, e-commerce ₦132.2 million ($416 thousand), web fraud ₦190.9 million ($60 thousand), Kiosk ₦10.1 million ($31 thousand), Cheque₦4.5 million ($14 thousand) and ₦190.9 million ($60.1 thousand) through other platform not categorized.

Nigeria Deposit Insurance Corporation (NDIC) released report of 2012 to presented statement of accounts which shows that banks in the Nigeria reported 3,380 cases of frauds involving ₦17.97 billion lost incurred by the industry. The reported cases of frauds represent a 43.7 per cent rise compared to 2,352 cases in 2011 while the expected/contingent loss rose by ₦455 million (10.9 per cent) from ₦4.072 billion reported in 2011. The expected/contingent loss in 2011 however fell by 36.4 per cent from ₦28.40 billion in 2011, to ₦18.04 billion to it prior year (i.e. 2010).

According to the CBN Governor, Mr. Godwin Emefiele, who unveiled the Nigeria Electronic Fraud Forum annual report in Abuja on Tuesday; disclosed Gistreel report of 19,531 fraud cases for banks in 2016 as against 10,743 recorded in 2015 (IT News Africa, 2017). The truth is that cyber fraud in entirety has been increasing in the country but most of it is not publicly reported. However, in the banking system, such crimes are reported by banks to the Central Bank of Nigeria (CBN) and the Nigeria Deposit Insurance Corporation (NDIC) their regulatory and supervisory bodies (Editorial Board, 2017). The reports from the banking sector more than corroborate the fact that internet frauds are alarmingly on the rise. The NDIC reported that the number of web-based (internet) banking frauds rose from 316 in 2013 to 1,271 and 1,471 in 2014 and 2015, respectively (a phenomenal increase of about 365.5% between 2013 and 2015). By all means, this increase brings about serious concerns to operators, regulators and other stakeholders including the government. But the actual amount lost to internet fraudsters, according to NDIC, declined significantly to ₦0.857 billion in 2015 from ₦1.683 billion in 2013, showcasing that efforts were made by the banks to mitigate losses from internet fraud attacks.

Imperatively, the concerns being expressed over internet-based frauds is therefore suggested (Editorial Board, 2017) to be extended to card-based frauds that have also been reported to be on rampage which the scope of this thesis did not cover.

In recent time, the banking sectors regulatory bodies unanimously agreed to induce quick steps into a cashless economy to maybe act as key economy driver. As reported by NDIC, presented number of frauds being perpetrated with the use of Automated Teller Machines (ATMs) cards and other card-related financial settlement modes rose from 1,739 in 2013 to 7,181 and 8,039 in 2014 and 2015, respectively. This is

a growth rate of about 362.27% between 2013 and 2015. Like their internet counterparts, the actual amount lost declined, presumably as a result of actions taken by banks to tackle the problem.

In June 2014, report by the USA Center for Strategic and International Studies and information security firm McAfee, a subsidiary of Intel, titled "Net Losses: Estimating the Global Cost of cybercrime; Economic impact of cybercrime II" revels that 0.80% of Nigeria's GDP, equivalent to their Cement sector, is lost to cybercrime. Nigeria's GDP in 2014 was $568.51billion.
Arguably, statistics of figure presented are devastating, and it was assumed to have constituted a negative impact on Nigeria economic prospects, which thus lead to the undermining of the country industrial sector's performance, causing retrenchment of workers and leads to organization degradations and their perpetual liquidation.

Kaspersky Lab also established that 45.3% of the Nigeria internet users suffered from internet fraud attack in the third quarter of 2015. "By implication, either you or the next person to you was hacked in some way" (IT News Africa, 2017). This kind of internet threat (social engineering, identity theft, SIM box fraud and many others) is still prevalent today.

The recently concluded eighth (8^{th}) senate affirmed the loss of the $450 million to cybercrime (Umoru, 2017) citing 3,500 cases of cyber-attacks on ICT infrastructure across Nigeria economy sectors.
Prof Danbatta (Vice Chairman of NCC) revealed that 750,000 SIM cards numbers assigned to 13 operators from the national network had been barred and six indicted interconnect exchange licensees suspended in February due to their involvement in telecom fraud (call masking, call refilling and SIM-Box fraud) activities (Ramoni, 2018).

As (Comms Week, 2020) published effort made by NCC to stopped $3bn call masking revenue fraud in Nigeria. Against this backdrop, the Nigerian Internet Registration Association (NiRA) and managers of Nigeria's domain name (.ng) for a numbers of times convenes meeting with representation of law enforcement agencies and other relevant stakeholders to foster a synergy and cooperation to arrest the internet fraudsters. As a result of these; the Bi-camera legislative arm of the government, concerned commission stakeholders and security agencies that now comprises (The Cybercrime Advisors Council) in the county; also have conduct headlock meeting and took measures on promulgated policies formulation and regulation, against offender to curtail the illegal act of cyber fraud and protect national network infrastructure. The outcome of these decisions is what gave birth to the formulation of the (Cybercrime Prohibition and prevention Act, 2015) to seek redresses on the hullaballoo of cybernetic fraud in the country. In recent time, an effort has also been made on telecom subscriber's proliferation which also gave birth to the present NIMC registration of network service subscriber to checkmate irregularity in the telecom industry and to help fight other social crime. However, as it is there is no promulgated law in the country establishing SIMbox fraud as crime punishable under the Nigerian law. Even though, efforts were continuously tried by the security personnel to nib the cyber offenders and safeguarded the network infrastructure, less was achieved as fraudulent activities lingers or persisted over the mobility network. Sequel to that the economy prospects envisage for leveraging infrastructural development and gratification keeps derailing. To this regards, based on survey carried out it seen that the implication of SIM-box fraud is more peculiar to the telecom industry and financial sector. This calls for a fraud detection approaches that could help deterred the negative inferences of SIMBox fraud and contemporaries have sparingly man-hurting the telecom sectors across board.

LITERATURE SURVEY ON EARLIER STAGE / TRANSIENT MODALITIES ADOPTED FOR SIMBOX FRAUD AND ITS CONTEMPORARIES CURTAILMENTS IN MOBILITY NETWORK

Earlier enough, conventional approaches have been embraced for detecting telecom fraud of SIMboxes and its contemporaries. These involve manually analyzing individual subscriber accounts in order to establish fraudulent use of telecom services (Blatt and Kaufman, 2017); the approach which is very costly, prone to spontaneous fraud analyst or human error (technical and operational) and time consuming. For example, if a Subscriber who notices fraudulent charges on a bill may notify a telecom service provider of the charges. In response, an investigator with the telecom service provider examines calls associated with the charges to determine the type of fraud being perpetrated against the subscriber. The investigator may then study a larger pool of calls made using the telecom services to determine a source of that fraud. Unfortunately, there are some deficiencies in the above-described conventional approaches (Blatt and Kaufman, 2017). Telecom networks stream a huge amount of data (~4TB of signaling data per hour). Manual analysis of individual calls through such a volume of data is unlikely to identify perpetrators of fraud within a reasonable amount of time. In contrast with the above-described conventional approach, which is reactive and slow to detect fraud, an improved techniques of detecting telecom fraud involve applying a combination of real-time data analysis and risk models to be typically used in authentication applications to phone call metadata that is streamed to a database server on a continual basis to derive phone usage patterns as the database server receives the phone usage data. The stated process is tediously bogus, costly and time consuming as well prone to yielding a lesser satisfactory result that resources inclined.

Therefore, mobile operators, though, face several challenges with SIM-Box fraud detection. One of the biggest involves most common methods deployed in the fraud detection crusade by telecom operators includes Test Call Generation (TCG), monitoring calling patterns and profiles through fraud management

systems (FMS), Customer Detail Records (CDRs) analysis and many others but they have drawbacks. The TCG involves a process in which operators set up test numbers on their networks and make calls to those test numbers from many different countries, through many different interconnect voice routes around the world. In this way, they can find out where “grey routes” are originating and the paths they use to reach SIM boxes in a particular country. The test-call generation method, however, has been weakened by new technologies that fraudsters can use to analyze voice call traffic coming to their SIM boxes. Based on usage patterns, these technologies can be used by fraudsters to determine which calls are real subscriber calls and which calls are originating from a test system, and fraudsters can then block or reroute test calls to legitimate routes to avoid detection.

In the last couple of years, however, new methods have been developed that offer more accurate, coverage, flexibility, and sophisticated detection of fraudsters and frauds (Hagos, 2018, Chouiek et al., 2018; Sahin, 2017; Reaves et al., 2015; Marah et al., 2015). In particular, one major advancement is the development of analytics-based methods are the one that uses call detail records (CDRs) to create statistical usage-based profiles and detection algorithms that can identify SIM card use illegally (Airn, 2018, Marah et al., 2015). These methods offer a number of advantages over test-call generation, including a more scientifically-based approach based on statistical data, a wider coverage area and more thorough search process, and near-real-time detection of SIM box activity.

In 1994, Wasserman and Faust in their work titled “Social Network Analysis: Methods and Application” used link analysis that relates known fraudsters to other individuals using record linkage and social network method. A case study, in telecommunications networks, security investigators have found that fraudsters frequently work in isolation from each other. In addition, after an account has been disconnected for fraud, the fraudster will often call the same numbers from another account. Telephone calls from an account can then being linked to fraudulent accounts to indicate intrusion. A similar approach has been taken in money laundering (Goldberg and Senator, 1995, 1998). Where unsupervised methods are used when there are no prior sets of legitimate and fraudulent observations. Techniques employed here are usually a combination of profiling and outlier detection methods. A model of base-line distribution is represented for normal behaviour and then attempt to detect observations that show the greatest departure from this norm. There are similarities to author identification in text analysis. Digit analysis using Benford's law is an example of such a method. Benford's law (Hill, 1995) says that the distribution of the first significant digits of numbers drawn from a wide variety of random distributions will have (asymptotically) a certain form. Until recently, this law was regarded as merely a mathematical curiosity with no apparent useful application. However, Nigrini and Mittermaier (1997) and Nigrini (1999) showed that Benford's law can be used to detect fraud in accounting data. The premise behind fraud detection using tools such as Benford's law is that fabricating data, which conform to Benford’s law, is difficult. The work of (Tawashi, 2010) presented an extensive literature on the earlier and transient stage of fraud detection approaches in tabulated and descriptive format across boards these are germane for the study but these are not exploring to avert repetition and scope contravention.

Barson et al. (1996) in their work titled “The detection of fraud in mobile phone network” deployed supervised feed-forward neural network (NN) to detect the anomalous use of subscribers. The recent and historic activity profile were constructed and it is found that the empirical results of the system show that Neural Network can accurately classify 92.5% of the subscribers.

Cox et al. (1997) in the work titled “Visual data mining: Recognizing telephone calling fraud” deployed a visualization method developed for mining very large data sets, and been developed for use in telecom fraud detection. Here human pattern recognition skills interact with graphical computer display of quantities of calls between different subscribers in various geographical locations. A possible future scenario was suggested to use code into software for humans’ pattern detect.

Hollmen and Jaakko, (2000) deployed user profiling and classification techniques, neural networks and probabilistic models are employed in learning usage patterns from call data for fraud detection in mobile communication network.

Estevez (2006) introduced a system to prevent subscription fraud using fuzzy rules and Neural Networks. The system has classification and prediction modules. Prediction modules were able to identify 56.2% of the true fraudsters, screening only 3.5% of all subscribers.

In 2009, Rosas et al., work proposed an approach based on the profiling and KDD (Knowledge Discovery in Data) techniques, supported in MAS (Multi-agent System). While, Hilas (2009) designed an expert system for fraud detection. The system worked on eight years of data for CDRs, having them aggregated on a weekly and daily basis (as shown in Figure 4 and Figure 5 respectively) for each subscriber and then applied the established rules and decision trees, which ended up with 90% as true positive and 25% as false negative.

Krenker *et al. (2009)* works proves that using bi-directional Neural Network (bi-ANN) in predicting generic mobile phone fraud in real time gave high percentage of accuracy. Bi-ANN is used in prediction the time series of call duration attribute of subscribers in order to identify any unusual behaviour. The results show that bi-ANN is capable of predicting these time series, resulting 90% success rate in optimal network configuration. However, call duration is the only parameter used, therefore, other relevant parameters are missing to accurately predict customer behaviour.

In 2011, Farvaresh and Seperi in their work applied decision tree (DT), Neural Network and SVM in order to identify customer with residential subscription of wire

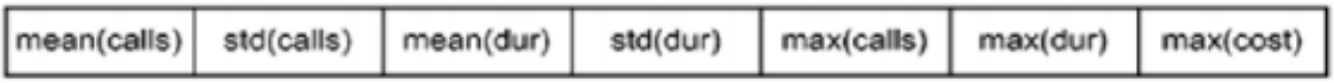

Figure 4: The basic vector for the weekly user behavior (Hilas, 2009).

Figure 5: The basic vector for the daily user behavior (Hilas, 2009).

line telephone service but used it for commercial purposes to get lower tariffs which is classified as subscription fraud. They also employed data mining approach consists of pre-processing, clustering and classification phases. Combination of SOM and K-Means were used in the clustering phase and decision tree (C4.5), Neural Network, SVM as single classifiers were examined in the classification phase. The results are evaluated in terms of confusion matrix. DT, NN and SVM as single classifiers were able to correctly classify 88.1%, 84.9% and 88.2% respectively. Therefore, SVM has shown the best performance among all the classifiers. The limitation might be the computational aspects if implement in real applications.

In 2012, Vodafone Teknoloji in the article titled "PADLOCK-SIMBOX Fraud Detection" elucidated on SIM box fraud and gave analogy on SIM box fraud case in country like Turkey. Where padlock is the first and the most effective patent pending SIMBOX Fraud detection using Big Data Analysis, padlock is on live since June 15th 2015 at Vodafone Turkey. It gives round the clock hours (7* 24hrs) daily outputs as near real-time, with success ratio of Padlock more than 99.5%. Usages before detection are reducing to nearly 100 minutes for fraud. Also, padlock gives 8-10 times early detection capability comparison. It is an independent solution. It detects all kind of telecom fraud. Padlock is easy to implements by Mobile or Fixed Line Operators in whose deployment is on an existing Big Data platform. Operator set up phase to provide efficient results on their own networks. While Bolton and Hand, (2012) in their work describes the tools available for statistical fraud detection and the areas in which fraud detection technologies are mostly used. They suggested that statistics and machine learning provide effective technologies for fraud detection and have been applied successfully to detect activities such as money laundering, e-commerce, credit card fraud, telecommunications fraud and computer intrusion, and many others.

Elmi et al.(2013) work titled "Detecting SIM Box fraud using Neural Network" deployed supervised learning methods on Artificial Neural Network (Multi-layer perception method) to detect fraudulent SIMboxes based on nine (9) voice call communication features (Total Calls, Total Numbers Called, Total Minutes, Total Night Calls, Total Numbers Called at Night, Total Minutes at Night, Total Incoming Calls, Called Numbers to Total Calls Ratio and Average Minutes) extracted from CDR of 6415 subscribers collected from telecom company from which Cell ID of (234,324 calls made in total) for two months were analysed. The dataset consisted of 2126 fraud subscribers and 4289 normal subscribers which are equivalent to one third of SIMboxes. The authors used the extracted features to train an Artificial Neural Network (ANN) classifier, where three architecture of neural network were considered and three hidden layers; 5, 9 and 18 hidden nodes in each layer. They discovered that the best architecture was when two hidden layers were used, each having five neurons; with a learning rate of 0.6 and a momentum term of 0.3. This method detects SIMboxes with 98.71% accuracy with just 20 accounts been wrongly classified as false positive. While, Yeshinegus, (2013) in M.Sc. thesis titled "Predictive Modelling for Fraud Detection in Telecommunications: The Case of ethio telecom" predict fraudulent calls made using SIM-boxes to terminate international calls. A classification methods of data mining are applied using J48, PART and multilayer perceptron algorithms on data collected from ethio telecom company. WEKA data mining tool was used to come up with a model for predicting fraudulent activities. For this study pre-paid sampled voice CDR data has been used along with SMS, GPRS and other data such as pre-paid wallet recharge log from OCS and CCB data warehouse in ethio-telecom. The experimentation result showed that the model from the PART algorithm exhibited 100% accuracy level followed by J48 algorithm with 99.98%. The rules generated from PART and J48 algorithms enable telecom operators in general and ethio telecom in particular to locate the whereabouts of SIM-boxes as well as other critical information. However, an effort has been made to show the impact of SIM-boxes on telecom operator's revenue.

Nuno and João , (n.d) in the article titled "Dispersion Estimates for Telecommunications Fraud" the author considers the problem of estimating the call destination dispersion on telecommunications usage to use in fraud detection. The problem is that such detection needs to be performed for each individual customer and kept up to date at all times. The use of fast and small footprint algorithms is critical due to the huge number of events and customers to verify and since approximate answers is enough in most situations. The paper presents telecommunications customer behaviour to justify the

use of approximate estimators and then presents multiple options of algorithms to solve the problem. These algorithms present a novel approach to the moving window dispersion problem by the use of a probabilistic time decay mechanism.

In 2014, Murynets *et al.,* (2014) in their work titled "Analysis and Detection of SIMbox Fraud in Mobility Networks" the research contravenes (Elmi et al., 2013; Sallehuddin et al., 2015) work to analyses the fraudulent traffic of SIMBoxes operating with a large number of SIM cards. It processes hundreds of millions of anonymized voice call detail records (CDRs) from one of the main cellular operators in the United States. The dataset contains CDRs of 500 IMEIs of fraudulent SIMboxes and of about 93,000 legitimate accounts. The author uses 48features information of CDR that includes Time, Duration, Origination number, Terminating country, Terminating country code, IMEI (International Module Equipment Identifier), IMSI (International Module Subscriber Identifier), LAC-CID, Account age, Customer Segment and others. Based on stated features in the work, they proposed four classifiers of fraudulent SIMboxes in mobility networks: Alternating decision tree, Functional tree, Random forest and Classification rules. The random forest and functional decision tree provide the lowest false positive and the lowest false negative, respectively. The false positive of the alternating decision tree is lower than that of the functional tree, and its false negative is lower than that of the random forest. The predictions of the four classifiers have been linearly combined into a classification rule, where classifiers' weight coefficients have been found from minimization of the total classification. The author presents a novel algorithm for SIMbox detection in mobility networks. Using the IMSI per IMEX, they are able to identified call traffic patterns distinguishing fraudulent SIMboxes from legitimate devices. Those patterns include high number of IMSIs per IMEI, large number of international phone calls, imbalance between MO and MT traffic (international and domestic) and static physical location. The accuracy of the classification rule is 99.95%. For large data sets, the scalability of the algorithm can be improved by filtering out accounts with less than 10 IMSIs (99.98% of all active subscribers). The operator's fraud department has confirmed that the proposed algorithm detects new fraudulent SIMBoxes with a low false positive error on the training dataset. The random forest has the largest weight coefficient followed by that of the alternating decision tree. In the work, ten CDR features were used. While, Fayemiwo and Olasoji (2014) in a paper titled "fraud detection in Mobile Telecommunication", the author developed a model that detects frauds in telecommunication sector in which random rough subspace based neural network ensemble method was employed in the development of the model to detect subscription fraud in mobile telecoms. In addition to that, the author presented the development of patterns that illustrate the customer's subscriptions behavior focusing on the identification of non-payment events. This information interrelated with other features produces the rules that lead to the prediction as earlier as possible to prevent the revenue loss for the company by deployment of the appropriate actions.

Sallehuddin et al. (2015) work titled "Detecting SIMBOX fraud Using Support Vector Machine and Artificial Neural Network" deploy Machine learning approaches to detect SIM Box fraud. The work is an improvement on previous work of (Elmi et al., 2013). Classification was done on the development of ANN and SVM to determine the model that gives the best performance from the experiments. It is discovered that SVM model gives higher accuracy than ANN by giving the classification accuracy of 99.06% compared with ANN model, 98.71% accuracy. Besides, better accuracy performance, SVM also requires less computational time compared to ANN since it takes lesser amount of time in model building and training. While (Subudhi, 2015) showed a prediction model based on a Quarter-Sphere Support Vector Machine and compared it to a Support Vector Machine-based model as shown in (Figure 6). Using a Quarter-Sphere Support Vector Machine showed better results and accuracy: higher true positive and lower false positive as show below.

Also, Reaves et al. (2015) in another work, presented a passive detection technique for combating SIMboxes at a cellular base station. The systems rely on the raw voice data received by the tower during a call to distinguish error in GSM transmission from the distinct audio artefacts caused by delivering the call over a VOIP link. The experiment carried out shows that the approach is highly effective and can detect 87% of real SIMBOX calls in only 30 seconds of audio with no false positive. SIMbox devices have little probability change to evade this detection mechanism. In the paper, they also present Ammit tool, a system for detecting SIMboxing was designed and deployed unto cellular network. Their solution relies on the fact that audio transmitted over the internet before being delivered to the GSM network are degraded in measurable, distinctive ways. They developed novel techniques that were built on mechanisms from the Pindrop call fingerprinting system of (Balasubramaniya et al., 2010) to measure these degradations by applying a number of lightweight signal processing methods to the received call audio and examining the results for distinguishing characteristics. These techniques rapidly and automatically identify SIMboxe calls and the SIMs used to make such connections, thereby allowing them to quickly shutdown those rogue accounts. In so doing, their approach makes these attacks far less likely to be successful and stable, thereby largely closing those illegal entrances to provider networks. In same year, (Marah et al., 2015) deployed user profiling approach which depends on analysing the subscriber's (SIMs) activity and behaviour based on detection patterns, while using fuzzy logic (FL) in decision making process. A technique that been designed and implemented in a program. Based on the fuzzy logic results the author decide that certain SIM card is suspicious one. In the works, a sample of real call detail record (CDR) from Almadar Aljadid Company, a mobile operator in

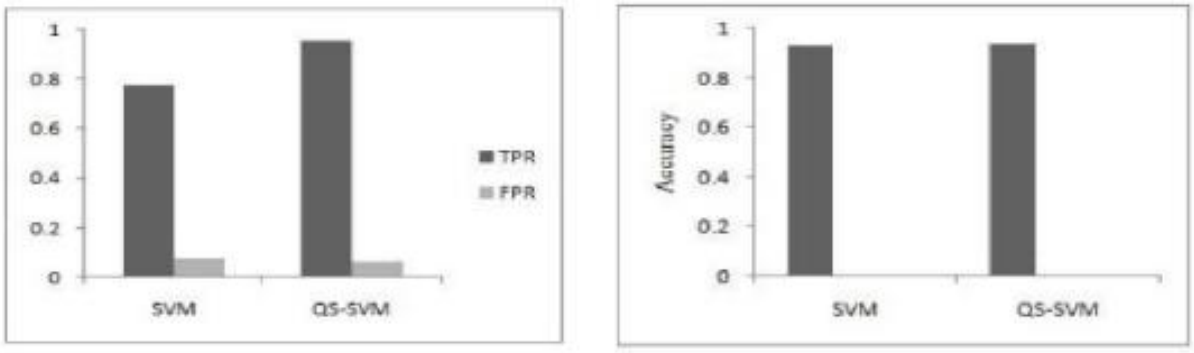

Figure 6: Comparison of the result between SVM and QS-SVM (Subudhi, 2015).

Libya was obtained and analysed. The CDR contains approximately 65 fields, out of which only 11 fields were used in the detection process, and five detection patterns (No or low mobility, Ratio of incoming to outgoing calls, Use only voice service, Suspicious activity in close proximity, and Calls during irregular hours, unusual night long calls) were extracted from the sample of CDR; by using structured query language (SQL) queries, the authors then found the (Max, Min) values for each detection pattern, the (Max, Min) values and used it for designing the membership function and fuzzy rules by using membership function equation. These are used to know if this SIM card perhaps as a suspicious case of fraud or not based on value of membership function for all patterns (fraud score), all these processes was implemented and processed in program. The results of the program depend on input database (CDR), is it contains fraud or not. The result of fuzzy logic membership function (MF) of patterns depends on extracted values from CDR for each detection pattern (Max, Min). The authors had used the program and got some results (fraud score) for SIMs cards which can be considered as fraud, but lack fraud data that can be used to test the results of the program, as they were unable to test or verify the results by the company's fraud department by using test call or other verification method to confirm the fraud happening in those SIMs. By using profiling with fuzzy logic in this technique can be more flexible and reliable in dealing with huge amount of input data (CDR). The profiling process can be updated every now and then, and the values of pattern (Max, Min) can be changed depending on input data (CDR) and accuracy and efficiency of the program's results. For their future work the author charge to add more detection patterns (features) and giving weights for each of them based on its importance and effectiveness for improving the performance and accuracy of the technique. Chen *et al.* (2015) in their work titled "Big data based fraud risk management at Alibaba" serves as a new trend in payment commercialized business. In the paper, they outline the fraud risk management and frameworks where CTU (Counter terrorism Unit) is built for monitoring system on real- time big data processing and risk models at Alibaba and a big data based fraud prevention product called Ant-Bucker. It captures signal directly from huge amount of data of user behaviours and network, analyses them in real-time. Ant-Buckler aims to identify and prevent all flavors of malicious behaviours with flexibility and intelligent for online merchants and banks. By combining large amount of Alibaba and customer's, Ant-Bukler uses the RAIN score engines to quantify risk levels of users or transaction for fraud detection. It also has a user-friendly visualization UI with risk scores, top reasons and fraud connections. The models and product built were safer and has a feature of a cleaner payment environment. In this same period, (Purnamasari and Amaliah, 2015) in their work titled "Fraud prevention: relevance to religiosity and spirituality in the workplace" carried out research on fraud prevention with religious and spiritual values in the working environment. In which research in the area is rare. This research is important considering the high cost of disclosing a fraud action case. Analysing measurement used is Moderated Regression Analysis (MRA) using 30 investigating auditors from Development Financial Controller (BPKP) as research respondents. The results indicate that there is positive and significant influence between religiosity and spirituality on fraud prevention. It is proven to give a positive and significant effect as a variable that strengthens the relationship between religiosity and fraud prevention. (Shikha Agrawal and Jitendra Agrawal 2015) in the research titled "Survey on Anomaly Detection using Data Mining Techniques" The paper reviews various data mining techniques for anomaly detection to provide better understanding among the existing techniques that may help interested researchers to work future in this direction. The author elucidates on Basic Methodology of anomaly detection technique (Parameterization, Training stage, and detection stage) and Anomaly Detection Using Data Mining Techniques. In this paper review of different approaches of anomaly detection focuses on the broad classification of existing data mining techniques. Data mining consists of four classes of task; they are association rule learning, clustering, classification and regression. In the subsection presents anomaly detection techniques under these four classes of task: Clustering based Anomaly

Detection techniques (k-Means, k-Medoid, EM Clustering Outlier Detection Algorithms). Classification based anomaly detection that uses M.L approaches (Classification Tree, Fuzzy Logic, Naïve bayes network, Genetic Algorithm, Neural Networks, and Support Vector Machine etc. Hybrid approaches (Cascading supervised techniques and Combining supervised and unsupervised techniques). Argyledata (2015) in the article "Real-Time Fraud Detection and Analytics using Hadoop and Machine Learning. Argyle Data // Technology Solution Brief" in the work, Argyle Data uses a real-time fraud analytics application built from the ground up on Hadoop using the latest Big Data, machine learning and anomaly detection technology. Argyle Data is able to ingest packet data extracted by Gigamon in real-time and perform Deep Packet Inspection (DPI). As packet data is stored machine learning algorithms identify fraud and send alerts to a fraud analyst dashboard. Applied graph theory allows sophisticated visualization and centrality calculations allow deeper investigation of criminal rings. The fraud analyst is able to query petabytes of data and get interactive response times using an industry standard SQL framework. Nwanga et al, (2015) work discussed the impact big data analytics can make on customer services and revenue generation of mobile phone industry.

Ighneiwa and Mohamed (2017), in a paper titled "Bypass fraud Detection: Artificial Intelligence Approach" This research basically focused on increasing awareness on SIM-box fraud and prevent the company's revenue losses as well as denial of service, reduction of service quality and communications network congestion. The authors used CDR data for their experiment and two supervised algorithms used SVM and Decision trees (Random Forest), accuracy and precision are used as model's performance evaluation matrices. Prajakta and Nitin, (2016) in another work titled "Solving Cyber Security Challenges using Big Data". In the paper, the authors embellished that Cyber security has become a Big Data problem as the size and complexity of security related data has grown too big to be handled by traditional security tools. In this paper, the authors have described the categories of cyber security threats (Advanced Persistent Threats (APT), Insider Data Theft, Distributed Denial of Service (DDoS), Trojan Attacks, Phishing, External Software Introduction including Malware, SQL Injection, Zero-day Attacks and URL Redirection or Parameter Tampering and challenges posed by them. They also analysed how big data tools and concepts are being used to solve these challenges, detect, and prevent attacks in real-time. In same year, Cataleya, (2016) in a work titled "Fighting Voice fraud with Big Data Analytics" investigates the full impact of voice fraud as evolving threat; where it's established that fraud can damage a service providers' reputation and long term trust in the industry. He listed top 10 (ten) countries for which fraudulent calls are originating and eventual spreads across developed and developing markets in Asia, Europe, Africa and Americans. Criminals that commit fraudulent acts are clever enough to use variety of destination and not rely on one place of origin. Fraud calls are terminated in a similar random set of countries like Cuba, Latvia, Nigeria, Taiwan, the United Kingdom and Somalia. He further elucidated on the common types of frauds and suggested new intelligence foe effective fraud mitigation solutions that can deliver the return on investments. Yuanzhu *et al. (*2016) in the work titled "Unlocking the power of big data in new product development" introduce a customer involvement approach as a new means of coming up with customer-centered new product development. In addition, this study investigates the approaches for utilizing big data in new product development. An in-depth case study is presented on the use of big data to improve customer involvement by STE, a young but Innovative high-tech company, to draw lessons for the effective use of big data to improve customer involvement in NPD. Findings reveal that big data can offer customer involvement to provide valuable input for developing new products. Studying the literature, we have identified three phases that big data can be used to support in NPD: generation of ideas and concepts; design and engineering; and test and launch. Findings include how to use big data analytics to determine customer profile, identify information source, to improve customer involvement in product design, to enable customer access and participation, for research and practices with all their implications. While, in (Tata Tete Business Service, 2018) work titled "Big Data and the Telecom Industry: The potential of big insights through deep data analysis" gives an insight on telecom customer experience, Network optimization, operational Analysis, Data monetization and ROI (Return On Investment) on big data. AlBougha (2016) in M.Sc. thesis titled "Comparing data mining classification Algorithm in Detection of SIMbox Fraud"; conducts comparisons among four major algorithms: Boosted Trees Classifier, Support Vector Machines, Logistic Classifier, and Neural Networks. Using about 1.2 million CDR event collected for over a week. The CDR employed for this analysis contains 6 fields' features that includes Caller Phone Number, Date Time Start, Date Time End, Event, and Event Type for 120 subscribers; of which almost 72,000 subscribers are SIMbox fraud cases. Results of the work show that Boosted Trees and Logistic Classifiers performed the best among the four algorithms with a false-positive ratio less than 1%. Support Vector Machines performed almost like Boosted Trees and Logistic Classifier, but with a higher false-positive ratio of 8%. Neural Networks had an accuracy rate of 60% with a false positive ratio of 40%. The conclusion is that Boosted Trees and Support Vector Machines classifiers are among the better algorithms to be used in the SIMbox fraud detections because of their high accuracy and low false-positive ratios.

Kun Niu et al. (2016) focused on fraud detection which is algorithm based namely United Intelligent Scoring (UIS) algorithm. Kun Niu et al. (2016) believes commonly used fraud detection approaches such as a rule-based, outlier detector and classifiers have a

problem with high computational cost while processing mass data in terms of accuracy. Therefore, telecom companies need to have a real-time solution to reduce fraudulent impacts. In order to achieve that, the authors propose a new algorithm which is called United Intelligent Scoring (UIS). UIS algorithm has less computational complexity in classification time and updates a real-time score in addition to that UIS could have the chance to detect new fraud patterns effectively.

In 2017, Wise-Anthena in their white paper titled "Eliminating Telco fraud with Self Learning Machines" uses cognitive analytics, smart visualization and Machine learning to bring a new solution to the telecom sector and fraud (SIM box) detection and protection. The author deployed Saas model to integrate, as it requires no end user maintenance and delivers a ROI measurable in days. Their technology maps the essential behaviours of network data to identify anomalies. It brings celerity and accuracy to fraud detection. SIMbox fraud is neutralized and no longer profitable for illicit operators. With as little as seventeen minutes of fraudulent calls, false positives are reduced with an accuracy 10,000 times greater than the traditional methods (from 1% to 0.001 %.). There 24x7 platform returns results in one minute, so SIMbox fraud can be seen happening in near real time. This is provided as a service (SaaS), one benefit from their responsiveness. Economies of scale and agility provide results at a tenth of the cost, and a sixth of the time compared to other providers. Reaves, (2017) in his Ph.D. thesis work titled "Authentication Techniques for Heterogeneous Telephone Networks" examine the poor state of authentication in telephone networks and provide new mechanisms to authenticate callers to each other. They began by examining how the telephone network specifically, text messaging is being used to bolster claims of identity and authentication in Internet systems, finding that public gateways negate many of the supposed advantages of these techniques. He then turns attention to interconnect bypass fraud, showing that while telephone networks cannot electively determine the true origin of a phone call, he can provide mechanisms based on in-call audio measurements to detect so-called "SIM boxing fraud. In the paper, they develop two new systems. In total, his thesis provides mechanisms to prevent robocalling, phone phishing, interconnect bypass fraud, preventing billions of dollars in fraud and restoring trust and confidence in the phone network. Sahin, (2017) also in Ph.D. theses titled "Understanding Telephony fraud as an Essential Step to Better Fight it", the researcher started with the Over-The-Top (OTT) bypass fraud and International Revenue Share Fraud (IRSF), which are the recent form of interconnected bypass fraud. In the paper, a possible technique to detect and measure SIMBox fraud and evaluate its real impact on a small European country, with more than 15,000 test calls and a large-scale user were done. Using a collected data, the author proposes a set of features for the sources and destination numbers of a call, which are used in detection of IRSF. In the work the author switched his focus to the consumer-side telephony fraud, mainly voice spam. In that regard, a recent counter-measure against unwanted phone calls, which involves connecting the spammer with a phone bot ("robocalle") that mimic a real personnel were built. Lenny is a bot (a computer program) which plays a set of pre-recorded voice messages to interact with the spammers. In the theses work, they try to understudy the effectiveness of the chatbot, by analyzing the recorded conversations of lenny with various types of spammers. The author presented a broad view of telephony fraud, the work finding reveals its complex nature and the key challenges in fighting fraud; of which it's been proposes to simulate research in this area, in particular, leveraging interdisciplinary approaches to study the diverse effect of telephony fraud.

Mouton (2017) in the article titled "Stealth Test Calls: A powerful New Weapon in the fight to Block SIMBOX Bypass" discussed about the two major telecom fraud of International Revenue Shared Fraud (IRSF) and SIM box bypass. In the paper, the author combines test calls and CDR (Customer Detail Records) profiling in one platform. The author uses an automated solution to detect the refilling of CLIs. Terminator and Stealth Test calls are the major contributions in the fight against interconnected fraud. Mola, (2017) in MSc. Thesis titled "Analysis and Detection Mechanisms of SIM Box Fraud in The Case of Ethio Telecom" for this research CDR's was obtained from ethio telecom industry in order to develop models to classified normal and fraudulent number behavior by deploying data mining techniques using WEKA tool. For the purpose of conducting this research the CRISP-DM process model is selected. The model includes six phases that address the main issues in data mining. The six phases include business understanding, data understanding, Data preparation, modeling, evaluation and deployment. Therein, four classification algorithms namely decision trees, rule based induction, neural network and hybrid algorithms are used. The author first performed data analysis on the data set and for classification, nine selected features of data extracted from CDR were used. The experimentation result enabled to understand the problem of SIM box fraud in the case of ethio telecom and clarifying the behavior of fraudulent and legitimate calls. The result from experiment shows that PART rule based and hybrid (J48 and PART) algorithms performed the best among the four algorithms. PART rule based induction classification algorithm had a better performance with an accuracy rate of 99.4906% with true positive and 0.5094 % false positive ratio and followed by hybrid of J48 and PART algorithm with accuracy rate 99.4795% with true positive and 0.5205% false positive ratios. For the study confusion matrix is the performance evaluate metrics adopted. In a trending manner, (Kehelwala, 2017) in M.Sc. thesis titled "Real-Time Fraud Detection in Telecommunication Network Using Call Pattern Analysis" the focus of this research is to detect fraud scenarios in telecom network in near real-time by using call patterns reflected in CDR stream. The author deployed new approach by proposing Complex Event

Processing (CEP) based solution for the real-time identification of fraudulent and extreme usage subscriber patterns. The author identified a rich set of features and set of call patterns, and then combined batch analytics with real-time analytics to increase the detection accuracy. The author demonstrated the utility of the proposed solution using a real dataset from a service provider. The proposed solution achieved an accuracy of 99.9% with average latency of 16 call attempts per detection at input event rate of 230 events per second with modest hardware.

Blatt and Kaufman, (2017) in the research work titled "Big Data Analysis for Telecom Fraud Detection" elucidates on the techniques for telecom fraud. These involves applying a combination of real-time data analysis and risk model that were typically used in authentication application to phone call metadata that are streamed to a database server on a continual basis to derive phone usage patterns as the data server receives the phone usage data. The data server then compares the derived phone usage patterns to patterns of fraudulent phone usage in order to detect SIMbox or SIM cloning frauds in the streamed data. A comparison result that indicates the likelihood of such fraud in a vast set of phone calls may take the form of a risk score derived using risk models typically found in the authentication application. This paper presented a pictorial figure to extenuate the concept. While Kassimi et al. (2017) in the paper titled" Design and Implementation of New approach using Multi-Agent System for security in Big Data" the authors proposed a new architecture based agent for Big Data security and safety. The novelty of the proposed architecture gives to it many advantages compared to the related works: a mobile and virtual router agent to protect the data paths, a scanning agent to detect malicious programmers, and authentication and integrity agent to be sure that the stored big data is conform to the original sent data. in the paper, they used pentaho platform to deploy hadoop clusters to manage the big data base and to deploy the multi agent system. Lastly, they plan to resolve the problem of hired party trust especially when it is deployed in cloud platform to ensure Big Data integrity and confidentiality.

In 2018, Hagos in a research titled "SIM-Box Fraud Detection Using Data Mining Techniques: The case of ethio telecom" suggested the major methods used in battling SIM box fraud mannerism these days to includes TCG (Test call generation), rule based FMS (Fraud Management system) and controlling distribution of SIM cards. However, in this work, the author developed models to classify Call Detail Records (CDRs) by proposing a model that differentiate fraudulent from legitimate subscribers with better performance. Three classification techniques, Random Forest (RF), Artificial Neural Network (ANN) and Support Vector Machine (SVM), and three users profiling datasets, 4 hours, and daily and monthly aggregated were proposed. These three algorithms along with the three datasets were applied in building the models. Results of the work show that Random Forest performed better among the three algorithms with accuracy of 95.99% and a lesser false positive on the 4 hour aggregated dataset. Confusion Matrix was deployed as performance evaluation matrix. Emsaieb et al. (2018) in their work titled "Analysis of Call Detail Records for Understanding User Behaviours and Anomaly Detection Using Neo4J" proposes an approach that makes use of Neo4J for automatic analysis of CDRs; where Call Detail Records (CDRs) is define as valuable source of information that opens new opportunities for mobile operator industries and maximize their revenue as well as helps the community to raise its standard of living in many different ways. In the paper, they analyses CDRs in order to extract its big values and detect abnormal customer behaviors to help companies to develop their plan. The analyses of CDRs are a very complex process, because it involves huge volume of data sets. To achieve their objective, the author transformed the CDR data into neo4J and used cyper query language for performing an automatic analysis. A real case study was used to evaluate the proposed approaches. In work of (Airn, 2018) in entitled "Analysis and detection of SIMBox" analyses the fraudulent termination of international traffic or calls by using a statistical, conventional, modern approaches for SIMbox fraud detection while processes hundreds of millions of anonymized voice call detail records (CDRs). The output of the author models is optimally fused to increases the detection rate of SIMbox. These was by the operators in the fraud department that the algorithms succeed in detecting new fraudulent SIMbox. While Chouiekh and El Haj, (2018) in the paper titled "CovNets for fraud detection Analysis" uses deep learning techniques. The first of publication on deep learning approach. It is an effective method to detect fraudsters in mobile communication. Fraud analysis were carried out from the CDR (Customer Details Records) datasets of a real mobile communication carrier deploy and learning features were extracted and classified to fraudulent and non-fraudulent event activity. Different experiment was carried out to evaluate the performance of their proposed model. The research finding shows that Deep Convolution Neural Networks (DCNN) techniques outperformed other traditional machine learning algorithms (Support Vector Machine, Random Forest and Gradient Boosting classifier in terms of accuracy (82%) and training duration. The use of their model reduces the cost related to illegal use of services without payment. In same period (Wu, Li and Zhou, 2018), published a paper titled "Application of Adaboost Algorithm and Immune Algorithm in Telecommunication Fraud Detection" therein, the authors proposed an adaptive improvement algorithm to solve the problem of low accuracy of the general algorithm. In the study, common algorithms are combined and enhanced, and these greatly improves the accuracy of the detection results. Also, the authors took the artificial immune algorithm as an example. The main application is combining machine learning and immune algorithm to apply to telecommunication fraud detection. The combination of the two is more conducive to pushing research on telecommunication fraud to a new stage

for the future telecommunication industry.

In 2019, Kashir and Bashir in a paper titled “Machine Learning Techniques for SIM box fraud Detection” The author proposed a similar Neural Network architecture with (Elmi et al., 2013) but the sign function as an activation function. The author selected 25 attributes for its input layer and built its model on the basis of a dataset with 8695 normal subscribers and 50 fraudulent subscribers divided into 3 groups: training, testing and validation. They tested 5 variants of NN by varying the optimization algorithms of the model and obtained very good performance: an accuracy of 99.87% with the Bayesian regulation algorithm and RMSE of 0.01654. In same vein, the author tested out 5 SVM kernels compared by classification and regression. Then, the author reported a poor performance compared to their previous work above based on ANN. This is in contradiction with (Sallehuddin et al., 2015), questioning the validity of these work.

In 2020, Alsadi and Abuhamoud published paper titled “Study to use NEO4J to analysis and detection SIM-Box fraud”, therein, the authors analyses and compare three known methods of SIMBox fraud detection such as alternating decision tree, Neural networks, and test call generation (TCG), explaining the advantages and defects of each method and proposed a new method. In terms of their detection rate. The TCG have the best results from all others, but it's made big load on the networks and taking BTS to rush houre in all the time. The neural networks are considered as “black boxes” due to their nonlinear behavior and complexity than other methods. The output is not easily understood by the user compared to other methods or when the output is seen by decision tree tool. Therefore, it is difficult to identify the important characteristics that lead to a successful classification and yet they are applicable in a variety of business applications and save their users time and money in the process.

In the paper, the author proposed new model, depending on use data mining technology (Neo4j) to analysis CDR for decrease total of phone numbers in the networks to short list, consist from SIM-cards that could be used in the SIMBox, then running TCG to examinant all routes and numbers. The author claim that this way they increase efficiency from 67% to 99.9 %. As the approach system relies on analyses of CDR files using data mining technology (Neo4j), and then use known method TCG (test call generation) to increase efficiency and to be more sure to results. This is an improvement over their previous paper jointly written (Emsaieb et al., 2018). In same period, (Tesfaye, 2020), In the thesis work, titled “Near-Real Time SIM-box Fraud Detection using Machine Learning in the case of ethio telecom” employ Sliding Window (SW) aggregation mode to provide a relevant dataset instance and reduce detection delay of SIM box fraud to one hour by using supervised Machine Learning (ML) algorithm. Here, three supervised ML classifier algorithms were used: Random Forest (RF), Artificial Neural Network (ANN), and Support Vector Machine (SVM) with the two validation techniques 10-fold cross-validation and supplied test. Call Detail Record (CDR) data were collected, relevant attributes were selected and pre-processing such as data cleaning, integrating and aggregating tasks were performed. The experimental results depict that RF classifier using cross-validation on SW aggregation mode achieves a better classification accuracy (96.2%). ANN is placed on second with its overall performance accuracy and its detection delay, SVM algorithm using cross-validation exceeds the desired detection delay (49,965 second) with poor performance accuracy. RF classifier algorithm using SW aggregation mode overcomes the trade-off detection accuracy and detection delay.

In the same year, Veloso, Gama et al, (2020), in a paper titled “A case study on using heavy-hitters in interconnect bypass fraud “the authors explore the application of three deterministic algorithms and one probabilistic, that combined can help to identify possible abnormal behaviors. Interconnect Bypass Fraud (IBF) is on the top three (worldwide), most common frauds in the telecommunication domain. Typically, the Telecom Companies can detect IBF by the occurrence of bursts of calls, repetitions, and mirror behaviors from specific numbers. The goal of their work is to discover as soon as possible numbers with abnormal behaviors and based on this assumption we developed: (*i*) the lossy count algorithm with fast forgetting technique; and (*ii*) the single-pass hierarchical heavy hitter algorithm that also contains a forgetting technique; as well as the application of the HyperLogLog sketches, and the application of sticky sampling algorithm. They further applied the four algorithms in two real datasets and did a parameter sensitivity analysis. The results show that their two proposals (Lossy Counting with fast forgetting and the Hierarchical Heavy Hitters) can capture the most recent abnormal behaviours, faster than the baseline algorithms. Nonetheless, these four algorithms combined can make the fraud task more difficult and can complement the techniques used by the Telecom Company.

In 2021, the first state of the art literature review about SIM box fraud detection was published by (Kouam, Viana and Tchana, 2021) entitled “SIMbox bypass fraud in Cellular networks: Strategies, evolution and detection Survey”. The paper surveys both the existing literature and the major SIMBox manufacturers to provide comprehensive and analytics knowledge, on SIMBox fraud, fraud strategies, fraud evolution, and fraud detection methods. In the paper, the author provided the necessary background on the telephony ecosystem while extensively exploring the SIMBox architecture required to understand fraud strategies. The goal of these co-authors was to provide a complete introductory guide for research on SIMBOX fraud detection, which remain little investigated. At the concluding part of their paper, the author presented an insight into tomorrow’s SIMbox fraud detection challenges.

In line to this, several security firms have offers their services on SIMbox fraud prevention and detection (Telekom Austria, n.d; Xintec, n.d) but details of their detection techniques are not disclosed for confidential

reason. Despite the known advantages of these new methods, some operators have been slow to adopt some of the techniques for integration on their network. With SIM box fraud reaching a new height, we have now reached a point where operators must begin treating these methods as essential to their business, and all operators across the Middle East and Africa must begin fully integrating them as a core component of their strategy. Only through this strengthened effort will we be able to begin to turn the tide in battling this fraud.

GENERAL THEORETICAL CONCEPTS ON SIM BOX FRAUD: HOW DOES IT HAPPEN?

Imagine you get an incoming call from unknown local number (MSISDN) when you picked up the phone call; it is discovered to have originate from a friend or relative (i.e. family member) living abroad (Airn, 2018; Okumbor and Ateli, 2019). This perhaps put you in a dismay (i.e. disbelief) state of thought as to how it is possible for someone in foreign country to route phone call of such an international magnitude and delivers to you for which the displayed number on your phone screen is a local one (MSISDN). You ponder as to whether such person (i.e. caller) in question (friend, relative) is back in the country and/or switch mobile SIM card for the call initiation or disguised to fool around and toys on your intelligence about the arrival without your prior notice. However, if after the conversation it actually turns out the person isn't playing prank as extemporize by him/her and firmly verified by you that the caller is still residence abroad. This means the person (i.e. Caller) has perpetrates and abating a derogatory form of telecom fraud known as Simboxing or bypass fraud arbitrarily referred as call masking/ call refilling and otherwise termed call line identity (CLI) spoofing (Nwanchukwu, 2020).

What is SIM-Box Fraud and Over the Bypass Fraud (OTT)?

SIM-Box fraud

This is otherwise known as bypass fraud or voice traffic termination fraud or interconnected bypass fraud, call reselling, Grey call fraud and others. This fraud is rated among the top five fraud types globally in the Telecommunication industry (Okumbor and Ateli, 2019; Kouam et al., 2021). Most common implementation of interconnect bypass fraud is known as SIMBoxing. Bypass fraud route utilizes a VoIP gateway and an attached GSM Gateway (SIM-box) in the destination country (Marah, et al., 2015; lavastorm.com). SIM-Box devices are telecommunication devices that can install large numbers of SIM cards. SIM-box uses VoIP technologies to enable international mobile calls to be routed through VoIP directly into a relevant GSM network (Marah et al., 2015). This circumstance requires that the fraudsters have access to advanced technology. The technologies (Algahwi, 2019) in a thesis work referred to as a PC-based software platform providing the ability to create, modify, manage and deploy and simulated-based contents: Aircraft, Cars, Ships, Weapons, E-learning materials and more across a multitude of domains such as training, research and development, operations analysis, and entertainment. Bypass fraud uses several of least cost call termination techniques like SIMboxes to bypass the legal call interconnection and diverting international incoming calls to "on" or "off" network (GSM /CDMA) calls with VoIP or satellite gateway, which is making international calls appear to be local calls. Thus avoid paying charges for international calls termination which operators and government regulators are entitled to (SubexInc, n.d; Marah et al., 2015). However, SIM-box fraud is affecting not only Nigerian telecommunication sector but also telecom operators in other African countries like Ghana (Laary, 2015), Kenya, Ethiopia (Amanfu, 2018), and Asian continent (Sallehuddin et al., 2015) and likewise the entire globe. In the work of (Airn, 2018) SIM-Box is descriptively categorized into international SIM-Box and roaming SIM-Box fraud.

OTT bypass fraud

This is one of the most prevalent and sub-types of SIM box frauds. Here, a normal phone call is diverted over IP (Internet Protocol) to voice chat application on Smartphone, instead of being terminated over the normal telecom infrastructure (Sahin, 2017). OTT by pass fraud is divided into two parts (On-net and Off-net bypass) in the work of (Alghawi, 2019).

On-net bypass

In on-net Bypass fraud calls are routed through same operators SIMs which are placed in SIM box, it this scenario MT (Mobile Terminator) operator gets the maximum loss as all calls are local on-net calls so MT Operators gets the opportunity loss of earning international termination charges (Alghawi, 2019; Airn, 2018).

Off-net bypass

off-net bypass call is routed and terminated from the different operator so MT operator gets local termination charges instead of international termination charges. In that fraud, MT operator gets the marginal opportunity loss of international carriers but in comparison of international termination and local termination charges have a massive difference so that is also high impact on revenue at the retail level for operators for Off-net Bypass (Airn, 2018).

Categories of SIMBOX fraud

International SIM-Box fraud

According to Airn, (2018), Cataleya, (2016) in a paper,

international SIM box, traffic aggregator carriers sit outside the destination country where the interconnect rate is comparatively high, such as Pakistan, India, Bangladesh, Indonesia, and many others and route the international traffic to pirate carrier (illegal Carrier) and feed traffic to SIM-Box and then call is terminated to MT (Destination address). In some cases, these traffic aggregators are getting traffic directly from operators too, and their interest is simply to make a profit by terminating traffic at a much lower rate. And they do that by handling over traffic to illegal terminators in the target country. The idea behind international SIM box bypass; the international traffic over internet cloud, bypass the international gateway exchange. The fraudster usually takes advantage of cheap local tariffs, bundle offers, which earns lower per minute revenue to operators than interconnect rate that can earn from international carriers. For example, In Pakistan's case, for example, the operators are losing about half a cent compared to one cent per minute on the interconnect rate. The loss to licensed international carriers is about 5 cents and the government about 2 cents per minute. The winners are the fraudsters, who need a very small investment to steal big money (Figures 7, 8 9, 10, and 11) for clarification. As shown in (Figure 11), if international traffic is routed through a legitimate path which is shown in blue dotted line then total 8.0 ¢/minute will flow from transit operator and destination operator for termination of the call. If call is routed through illegal carrier (Pirate carrier means carrier which is used to bypass the international call to SIM-Box for getting marginal benefits where the termination cost is high comparatively) the fraudster have to pay 5.0 ¢/minute to intermediate carrier and rest 4.5 ¢/minute (Pirate Carrier provide 5 ¢/minute to sim box so that sim box have to pay only 0.5 ¢/minute for landing local traffic so total profit earned by SIM-Box is 5 ¢/minute – 0.5 ¢/minute = 4.5 ¢/minute (Airn, 2018).

Roaming SIM-Box fraud

In Roaming SIM-Box fraud, the SIM which is inserted in SIM-Box device belongs to those countries where either roaming charges or IUC charges are less or may be both. Let us consider an example if the call is received at MT level and Tanzania CLI reflects at receiver level but calling party is calling from Uganda so that is a case of roaming fraud. Basically in roaming fraud is hard to detect as the customer is Uganda customer is roaming in Tanzania so there will be a delay in CDR or TAPIN data processing from roaming or latching operator so the fraudster will enjoy the benefits from SIM boxing and Roam Fraud in that scenario in that case. Roaming fraud comes is picture basically in African Countries where the international IUC charges are less (Airn, 2018).

SIM-Box device

SIMbox device is also called SIM-bank; it is one of the hardware modules of GSM termination equipment. The main function of this element is to store an array of SIM-cards, which can take part in voice termination process. A SIM card is a small memory module that contains, among other pieces of information, a unique serial number (ICCID) identifying that SIM card and an international mobile subscriber identity (ISMI) identifying a subscriber.

While SIMbox is a hardware which is used to bypass the legitimate or normal route for incoming international call (Figures 12 and 13). SIM-Box device have SIM slots, antennas and Ethernet ports that can be used to get the SIMbox equipment connected to the internet. SIMboxes are used as part of voice over IP gateway installation and the function of SIMbox is used to make and terminate international incoming call as local call. A fraudster can forward (initiate) international calls through local phone numbers in the respective country to make it appear as a local call. In this process SIMboxing connects the VOIP calls to a local cellular voice network through a collection of SIM cards and cellular radios. In a normal course the calls will be received by the network service provider and call tariffs will be charged. In SIMboxing, calls will bypass the normal path of connection, appearing to originate from customer phone, to a network provider. The calls are then delivered at a subsidized domestic rate instead or international rate. Such an activity has its negative impact on availability, reliability and quality of service for legitimate consumers. Besides, it also creates network hotspots by injecting huge volume of tunneled calls, thereby causing revenue loss to network operators. Kala (2019) elucidated more on common implementation of interconnect bypass fraud otherwise known as SIMboxing. The cost of SIMbox equipment has goes up to about 200,000 USD in (Kala, 2019) and is easy to order for it purchase publicly at an online global telecom market.

Figures 13 and 14 illustrates a typical international call which is routed through a regulated licensed interconnection.

Alghawi, (2019) buttress that SIM box make use of Technology; that is a PC-based software platform providing the ability to create, modify, manage and deploy any simulation-based content – aircraft, cars, ships, weapons, e-Learning material, and more – across a multitude of domains, such as training, research and development, operations analysis, and entertainment. And contains a wide range of software modules empowering users with infinite possibilities in creating new products and environments.

Three Forms of SIM box Environment

These includes:

(i) SIM BOX Toolkits; a development environment
(ii) SIM BOX Server; a central management environment
(iii) SIM BOX Runtime; a delivery environment

Several configurations of SIM box are generally

Figure 7: Architecture of Bypass frauds (Marah et al., 2015).

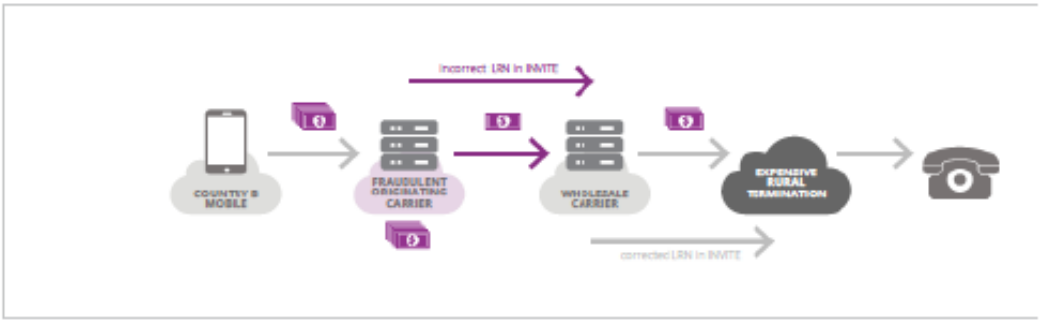

Figure 8: Architecture of Bypass frauds (Cataleya, 2016).

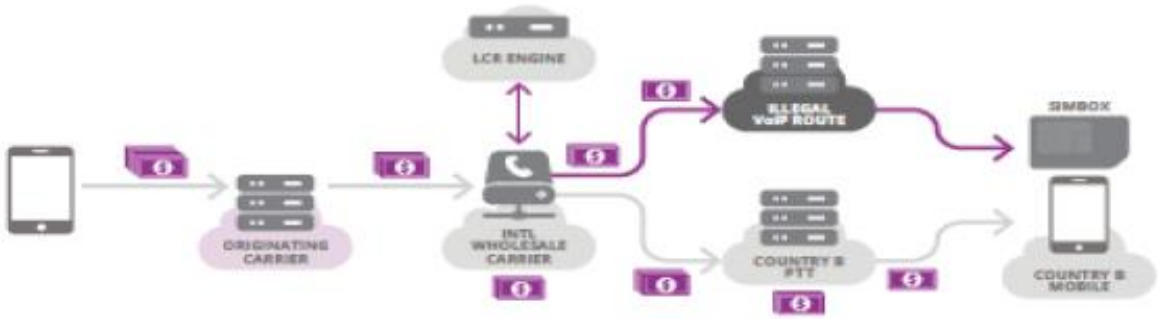

Figure 9: International SIM-BOX fraud

available, the most widely used ones are for 60 SIMS and another one is for 120 SIMS. One system can include as many SIM boxes as one wish, which gives ability to use any amount of in the termination system. Module-based structure of the merchandise hardware parades a good variety of potentialities to its users, such as:

(i) SIM cards could be placed separately from GSM modules (this option will require high-quality Internet connection between GSM gateway and SIM Box).
(ii) SIM cards which take part in termination of voice traffic and SMS termination to different destinations/countries could be placed in the same spot, making it easy to control their activity. It is vital to own many GSM gateways settled in several countries or in several regions of an equivalent country. All SIM cards that square measure concerned in termination are also settled in one or a lot of SIM Boxes placed within the same spot (Alghawi, 2019; Ayamga, 2018).

How is SIM-Box fraud carried out?

Let us assume client A is located in China and client B is located in Nigeria. In a typical call, when client A is calling client B, the call is routed through the telephone network in India (labelled as "Foreign PSTN core") to

Figure 10: SIM-BOX STOLEN SIM

Figure 11: International SIM-Box frauds (Airn, 2018, Cataleya, 2016).

Figure 12: Two models of SIM-Box devices (New module of 32 SIM card GSM SIM-Box and 128 SIM cards call center SIM-Box devices) source: (Kala, 2019; Mola, 2017).

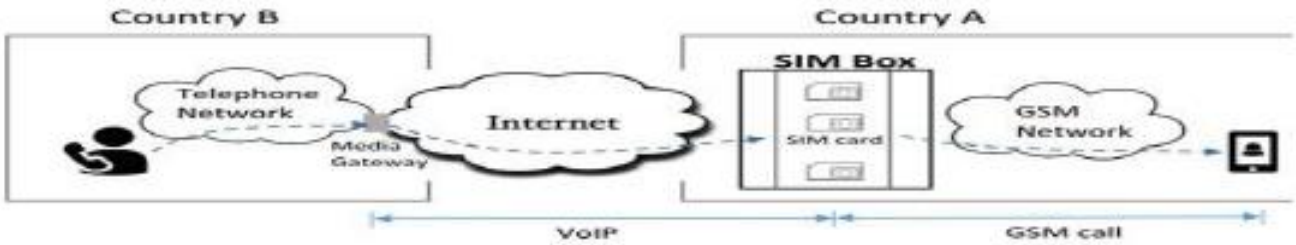

Figure 13: SIM-BOX Processes

Figure 14: Basic Bypass Call Flow Architecture (Alghawi, 2019).

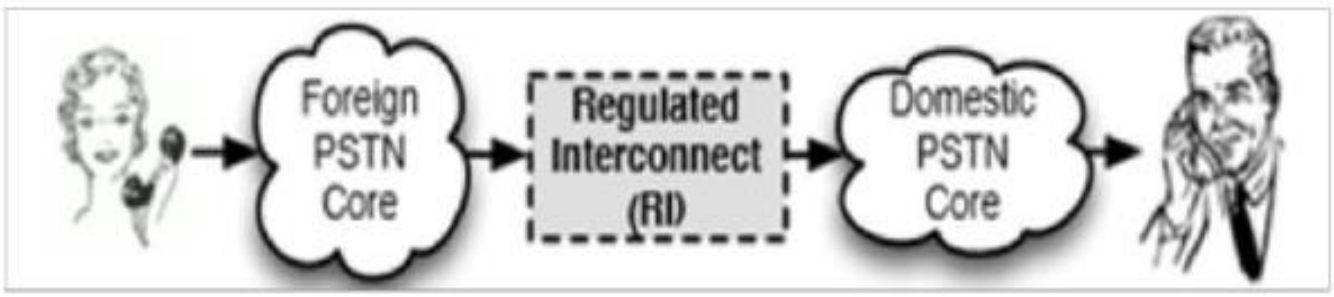

Figure 15: usual International call routed through regulated licensed interconnect.

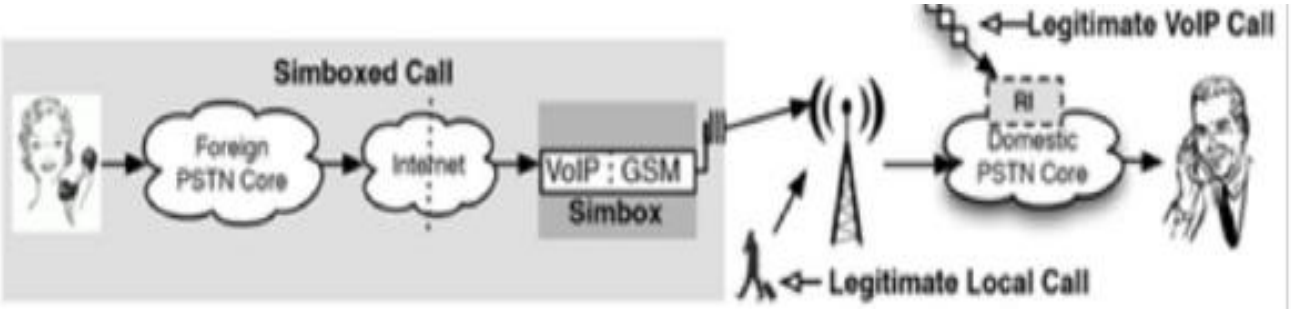

Figure 16: A SIMbox International Call

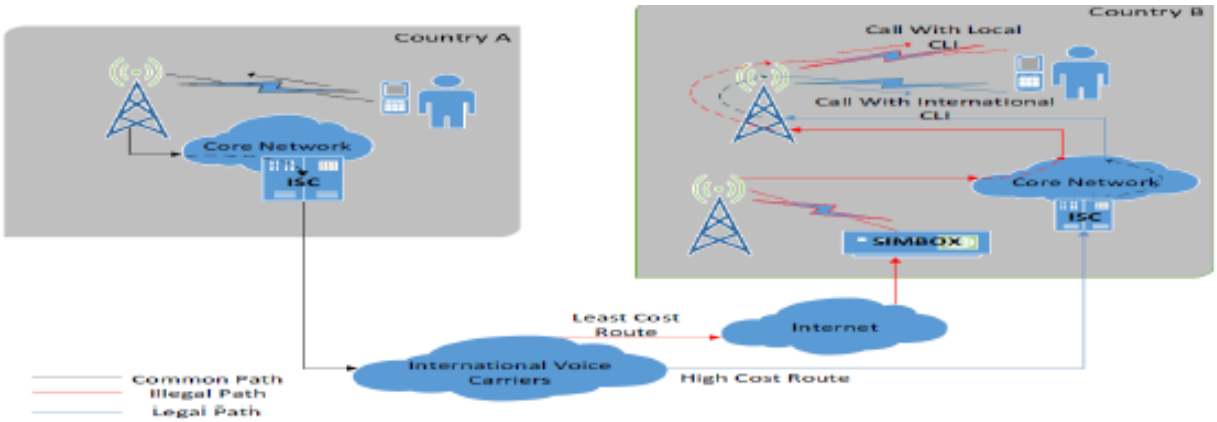

Figure 17: On-Net Bypass fraud

an interconnect between client A and client B network in UK. This passes through client B's domestic network (labelled as "Domestic PSTN Core") and communication establishes between client A and client B. If client A and client B are not in neighboring countries, there can be many interconnects and intermediary networks. This is very critical the connections are heavily monitored for billing purpose and quality. It can be seen that VoIP calls initiated from services such as Skype that terminates on a mobile phone also passes through regulated interconnect. A SIM-Box call is represented in (Figures 15, 16, 17 and 18). A SIM-Boxed international call avoids regulated interconnect by routing the call to a SIM-Box which completes the call using the local cellular network. In a SIM-Box case, client A call is routed through domestic network, but instead of passing through the regulated interconnect, the call is routed over internet protocol (VoIP) to SIM-Box in the destination country. In so doing, the SIM-Box places a separate call on the cellular network in the destination country, then routes the audio from IP call into the cellular call, which is routed to client B through the domestic network. The same is illustrated in (Figures 17 and 18). The main disadvantage here is neither of end users is aware that the call is being routed through a SIM-Box. This causes a contractual breach of trust between two Internet Service Providers (ISPs) who have agreed to route traffic between their networks. The intermediaries own profit from reduced prices.

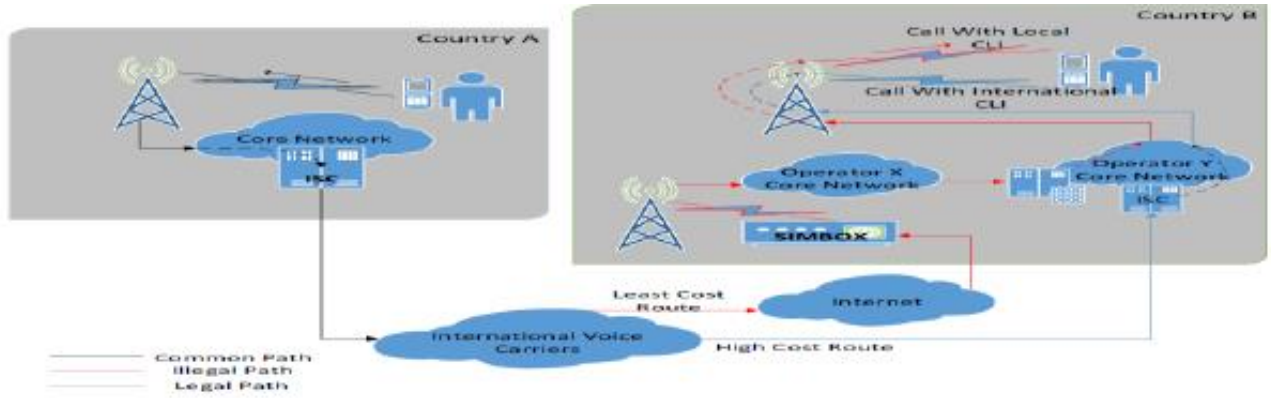

Figure 18: Off-Net Bypass (Source: Kehelwala, 2017).

Figure 19: Test call Generator solution by vendor (Mouton, 2015).

Two types of attack can take place. Firstly, hijacking of international call; secondly, hijacking and re-injecting of an international call. First type has been diagrammatizing in (Figure 15).

In the second type, SIM-Boxes re-inject telecom voice traffic into the mobile network masked as mobile customers and operator has to pay for the re-injected calls as illustrated in (Figure 16).

For more simplicity and clarifications about the SIM box fraud modalities; (Alghawi, 2019) in a thesis work extemporizes the concept as follows: In order to understand as to how SIM box affects the telecom operators, we would need to understand the basics of a GSM network and the billing process first.

Scenario 1: On-net Call

Let assign reference variables to the operator and the subscribers.
Telecom Operator = T
First Subscriber of Operator T = S1
Second Subscriber of the Same Operator = S2

If a customer S1 of company T calls a friend S2 who has a subscription at the same company, the call flow will be as below:

Cellphone of subscriber S1 transmits to the nearest antenna or BTS (Base Transmitter Station) of company T. The BTS passes the call through the central computer or switch of company T, where the receiving party is recognized as being a customer of company T as well, and then the switch sends the call to the BTS where subscriber S2 has made contact fixed lines or be it glass fiber or such. Subscriber S1 will get billed for the call. Since all the traffic is on the network of company T, they do not have to pay anyone. This is called an on-net call, where the calls are generated between customers of the same network.

Scenario 2: Off-Net Call

Fist Telecom Operator = T1
Second Telecom Operator = T2
First Subscriber of Operator T1 = S1
Second Subscriber of operator T2 = S2
Call flow for Subscriber S1 of operator T1 calling a

friend S2 who has a subscription at the operator T2:

Cellphone of S1 transmits the network data to the nearest BTS of operator T1. The BTS passes the call through the switch of operator T1, where the receiving party is recognized as being a customer of operator T2. Switch T1 connects the call to the Switch of operator T2, that forward the call to the BTS of T2 where subscriber S2 made contact and then radio signals the call to the handset of S2. Customer S1 still gets billed for the call. As it is evident, now half of the call (the start) is on the network of T1 and the other half (the termination) of the call makes use of company T2's network. So operator T2 sends operator T1 a bill for making use of their network, which they have to maintain. This bill is called termination fee, which every telecommunications operator has to bear for off-net calls (Ayamga, 2018).

Scenario 3: International Call

Telecom Operator in First Country = TC1
Telecom Operator in Second Country = TC2
Telecom Operator in Third Country = TC3
Telecom Operator in Fourth Country = TC4
First Subscriber of Operator TC1 = S1
Second Subscriber of operator TC4 = S2

Call flow for subscriber S1 of operator TC1 calling a friend S2 who has a subscription at the operator TC4. Cellphone of S1 transmits the network data to the nearest BTS of operator TC1. The BTS passes the call through the switch of operator TC1, where the receiving party is recognized as being a customer of operator TC4. Since the operator TC1 recognizes that this is an International call, it would need to transmit the call beyond the geographical limits of its own country. It is commercially and even technically not feasible for an operator to set up network all over the world. Hence, the operators will try to pass the call to its most feasible and nearest operator (TC2 in this case) who will in-turn pass the call to TC3 from another country. TC3 is expected to terminate the call in TC4's network. In technical terms, Switch TC1 connects the call to the Switch of operator TC2, which forwards the call to TC3. TC3 then connects to the switch of TC4 who passes on the call to the BTS of TC4 where subscriber S2 made contact and then radio signals the call to the handset of S2. Customer S1 still gets billed for the call. As it is evident, now quarter of the call (the start) is on the network of T1 and the other half (the passing) of the call is through the network of TC2 and TC3. And finally the last quarter (the termination) is through company TC4's network. So operator TC4 sends operator TC3 a bill for making use of their network, TC3 sends a bill to TC2, and TC2 to TC1 which they have to maintain. Termination charges for international calls are comparatively very high as compared to local rates. This charge is called international termination fee, which every operator has to pay for international calls. Naturally, since TC1 has to indirectly bear all of the margins/costs. TC1 will pass on all the charges and their required profits to the subscriber S1. Hence, international calls are very costly (Ayamga, 2018).

To bypass that international termination fee, one fraudster can have a SIMbox to terminate international traffic on the radio network of an operator. The fraudster (generally an international inter connect operator) will try to terminate the call in TC4's region via SIP/VoIP. With a SIM box you can convert VoIP calls to GSM calls, using that box and activated SIM cards. The trick is that, since the call enters through VoIP, and then it is converted to GSM through SIM box using local SIMs, it will reflect in TC4's network as local call. Hence, the interconnect operator would not need to pay the hefty international termination charges. So the fraudsters get some SIM cards with a tariff of 5 fils per on-net call each for network TC4. He places it in the SIM box and then begins to advertise. Normally when another international operator wants to terminate a call to a customer of company TC4 they have to pay let's say AED: 2.00 per minute to company TC4. (Not the actual price, but for making it easy to understand) But they only have to pay that when traffic is connected through the switches. The fraudster then can approach company TC1 and tells them that he is able to terminate all their traffic towards customers of company TC4, but for only AED: 1.00 per minute. Company B agrees because that tariff is AED: 1.00 per minute less than if they handover the traffic via the interconnect operators. They now send their traffic to the SIM box of the fraudster that converts the traffic to mobile calls, just as if it was a giant handset with multiple SIM cards in it. Since the fraudster only has to pay the subscription fee and a tariff of 5 fils per minute while receiving AED: 1.00 per minute he is making a profit of 95 fils per minute, per SIM. He off course pays his bill right away because he wants his SIM cards open. Since the traffic is huge 5 fils per minute per SIM means, he earns a minimum of AED: 1,368.00 each day per SIM. So, if he has 10 SIMs, he is earning AED: 13,680.00 a day just by having that SIM box active. Company TC4 then has a customer that has a monthly bill of let's say AED: 2,304.00; at first they are happy with such customer that pays his bills every month. But even though they are gaining AED: 2,304.00, they lose more than AED: 40,000.00 each month, because, if all that traffic was presented at their international switch they would have billed company TC3 AED: 43,200.00 for those calls So the fraudsters get some SIM cards with a tariff of 5 fils per on-net call each for network TC4. He places it in the SIM box and then begins to advertise. Normally when another international operator wants to terminate a call to a customer of company TC4 they have to pay let's say AED: 2.00 per minute to company TC4. (Not the actual price, but for making it easy to understand) But they only have to pay that when traffic is connected through the switches. The fraudster then can approach company TC1 and tells them that he is able to terminate all their traffic towards customers of company TC4, but for only AED: 1.00 per minute. Company B agrees because that tariff is AED: 1.00 per minute less than if they handover the traffic via the interconnect operators. They now send their traffic

to the SIM box of the fraudster that converts the traffic to mobile calls, just as if it was a giant handset with multiple SIM cards in it. Since the fraudster only has to pay the subscription fee and a tariff of 5 fils per minute while receiving AED: 1.00 per minute he is making a profit of 95 fils per minute, per SIM. He off course pays his bill right away because he wants his SIM cards open. Since the traffic is huge 5 fils per minute per SIM means, he earns a minimum of AED: 1,368.00 each day per SIM. So, if he has 10 SIMs, he is earning AED: 13,680.00 a day just by having that SIM box active. Company TC4 then has a customer that has a monthly bill of let's say AED: 2,304.00; at first they are happy with such customer that pays his bills every month. But even though they are gaining AED: 2,304.00, they lose more than AED: 40,000.00 each month, because, if all that traffic was presented at their international switch they would have billed company TC3 AED: 43,200.00 for those calls. This loss is just through one SIM. It grows exponentially if there are multiple SIMs involved.

Types of SIM-Boxes routes in communication network

In general, there are three types of routes that are used in communication networks. These include:

i. White Route: both source (MO) and destination (MT) have legal termination.
ii. Black Route: both source and destination have illegal termination.
iii. Grey Route: the termination is legal for one entity or country, but illegal for the other end.

Characteristics of SIM-Box fraud

Mouton (2015), extenuate the characteristics of SIM box fraud by declaring that:
1. SIM box fraud creates a lot of quality issues.
2. People experience more delay, echoes, and noise on the line.
3. And these quality issues, in turn, cause people to make shorter duration calls.
4. More dropped calls are experienced, too, because the prepaid balance often runs out on the SIM card.
5. And because the telephone number is not visible (i.e. masked) on the phone, you are not sure who is sending you a call.

SIMbox fraud scheme and architecture

More about this concept where exclusively described in the work of (Kouam et al., 2021).

METHODS USED TO COMBAT FRAUD IN TELECOMMUNICATION INDUSTRY

This section however presents all existing solutions for detecting and preventing SIMBox fraud in the literature; concerning their operational mode, and these solutions are prearranged into two categories: active and passive solutions (Kouam et al., 2021). Prior the categorization, different methods have already been devised by researchers and software vendors. From the literature survey done. The approaches are primarily divided into two categories: an absolute analysis and differential approaches; in which (Marah, Elrajubi and Abouda, 2015) suggested another focuses approaches for detection and prevention of fraudulent scenario that uses both cases, where analysis is mostly achieved by means of either statistical and probabilistic analysis techniques such as (data pre-processing, calculation of various statistical parameters, clustering and classification and computing user profile) and Artificial intelligence such as (machine learning techniques like decision trees, neural networks, support vector machines, pattern recognition) applied on the customer information databases like call history, demographic information and others to detect pattern of suspicious behavior. Airn, (2018) presented and elucidated on

A statistical method for fraud detection

This comprises of the:

B Party Diversity: By checking the B Party Diversity (Calling Number diversity) we can trace the SIM box. In Ideal case scenarios, B Party diversity is between 95-98%. By checking B party diversity can estimate the SIM box but in that method marketing, sales and corporate calling are excluded.

Around the Clock calling: If the customer is making call 24 X 7 that means it is suspicious usage pattern because it resembles machine calling pattern or Algorithm based calling pattern.

Geographical Location: - Geographical location should be less than 03. For Ideal, SIM box Scenarios Geographical location is 01 so by taking the traces of geographical location we can detect the SIM box pattern like why the customer is making calls from one location or without movement so it is also an important parameter to detect SIM box.

Outgoing V/s Incoming calls: Incoming calls should be less than outgoing calls. Basically, in SIM box Scenarios ratio outgoing calls are 90% or more as compared to incoming calls.

International Calls V/s Local Calls: International calls should be less than Local calls. Basically, in SIM box Scenarios ratio, Local calls are 90% or more as compared to international calls. In SIM box, international traffic is fed so that it converts international traffic to local calls so mostly calls will be local calls in SIM box scenario. If SIM box traffic is programmed like it is reflecting international calls so all calls will be derived from random series or **'+'** so that we can

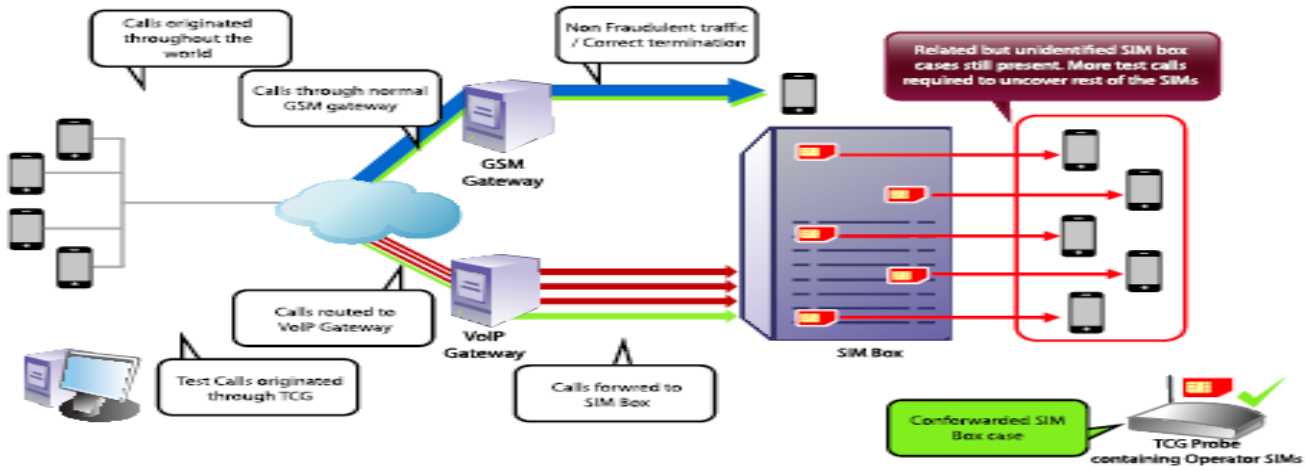

Figure 20: Test call generation platform.

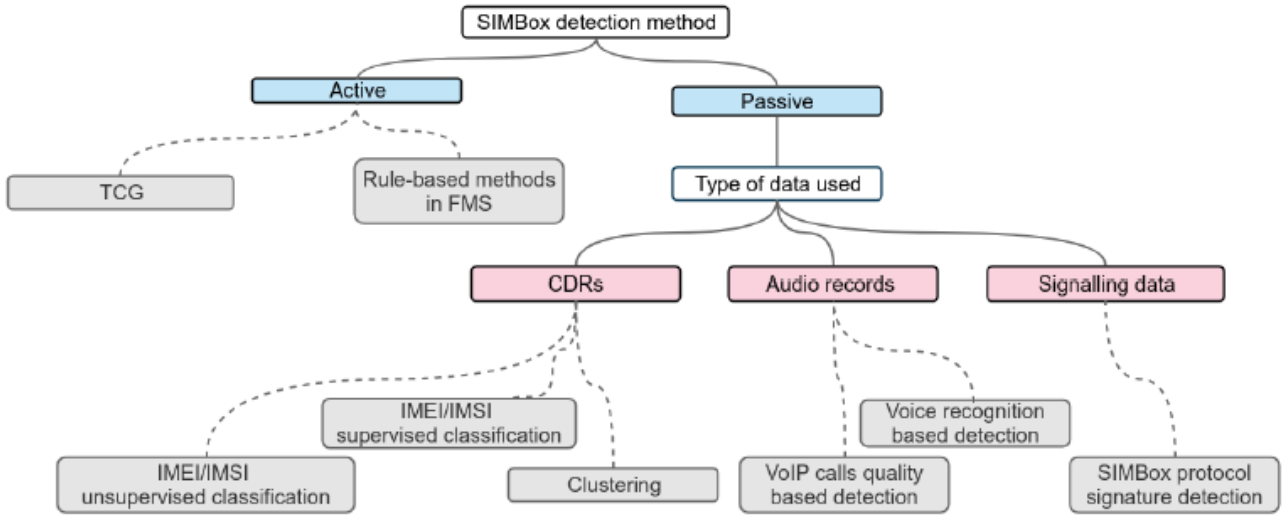

Figure 21: Categorization of existing SIM box fraud detection Method (Source: Kouam et al., 2021)

analyse one parameter of SIM box.

Less or No GPRS Usage: For ideal SIM box scenarios no GPRS usage found or very less GPRS usage found in SIM Box Cases**.**

Less or No SMS Usage: For ideal SIM box scenarios no SMS usage found or very less SMS usage found in SIM Box Cases.

At Receiver Level: For SIM box Scenarios at receiver end's Local CLI, reflects of that country code will reflect so if we come across that scenario while taking the international call so same will be immediately reported to the operator for blocking those SIM box series.

Call quality Analysis: It might be a factor of SIM box while in case of SIM box scenarios the call quality drops so at operator level if the customer is the same location is making a complaint about call quality so that can be a case of SIM box. Lately numbers of dissimilar techniques and apparatus have also been devised by software vendor to battle SIM fraud and its contemporaries some of whom (Mouton, 2015; Mouton, 2017; Latvia RIGA, 2015; Cataleya; 2016; Vodafone, 2012 and others) presented. As traditional approaches for fraud detection have showed limited effectiveness (Wise-Anthena, 2017).

In a Ph.D. thesis (Sahin, 2017) enumerates seven different fraud detection and prevention techniques that include: Test call generation platforms, Rule-base approaches, whom (Kouam et al., 2021) categories as an Active method.

Figure 22: Effect of SIMBox fraud (Source: Sowe, 2018).

While, Audio Based Approaches Graph Analysis, profiling user behaviour, Machine learning based techniques are some of their categorized Passive methods due to imbibing usage of CDR for delving fraud. As cognizance was not on Honeypots. Ighneiwa and Mohamed (2017) suggest FMS (Fraud Management System and SDC (SIM Card Distribution Control) as another solution of SIMbox fraud detection. Marah et al. (2015) devise Monitoring call pattern and user profiling using Fuzzy logic; and (Choueikh et al., 2018) included deep Convolution neural networks. In recent time, case-based reasoning, Generics Algorithm, Constraint programming and many others were seen as the latest inclusion. Kouam et al. (2021) gave a pictorial representation of their categorization of SIM box fraud solution of detection in (Figures 20, 21 and 23).

Test Call Generation

Test Call Generation or Detection is one of the effective methods to detect SIMs used in SIM box traffic which is routed through local path for termination. The incoming call here appear from Local CLI while receiving an international call; that means that international calling path is routed by illegally SIM box technology so same data or number (Airn, 2018).

Test call generation in another vein, is an active method used to detect bypass fraud, where telecom operators test different international routes to their network in order to ensure whether calls go via legitimate routes or SIM-Box routes (Kouam et al., 2021). This method is employ in detection of fraud with no false positive (i.e. when a normal subscriber unspecified to be a SIM-Box). However, this method is probabilistic in nature and costly in terms of the need to test huge number of international routes. Also fraudster use tricks to avoid test call detection, most especially in the case of the anti-spam method; this is discussed further in section 6.

According to Sahin (2017), the Test Call Generation (TCG) platforms provide call origination points worldwide (from various networks in various countries) to enable the operators to generate traffic from remote points to their own networks. Virtual SIM cards, calling cards or VoIP technology can be used to generate calls from different networks.

The commercial TCG platforms often provide automated periodic testing and web interfaces to schedule and manage the test calls. They are often used by the operators for testing the accuracy of billing systems and QoS, as well as for fraud detection. For instance, monitoring the call start time, end time and duration can help to detect FAS fraud. Moreover, monitoring the received caller ID of a call, and comparing it with the actual caller ID may allow to detect SIM box and PBX based interconnect bypass fraud, as these fraud schemes are likely to alter the caller ID. Certainly one of the biggest advantages of test calls is their speed (Moulton, 2015). AlBougha (2016) describe the advantages and disadvantages of using TCG for SIM box detection.

Fraud Management System (FMS)/ Blacklisted IMEI

A fraud management system seeks measures to detect the anomalous usage of SIM cards. FMS analyses Call Details Records (CDR) data to make usage profiling that distinguishes normal users from SIMboxers (fraudster). The CDR analysis in Fraud Management Systems (FMS) is great for detecting IRSF and other frauds, because it's relatively weak at false answer supervision fraud and advanced SIM Box bypass. Why? The fraudsters have gotten better at flying below the statistical bell curves. This is precisely why active probing and testing of very specific interconnection routes, such as those with a bad history — has proven to be such an invaluable aid in locating and blocking SIM boxes that an FMS may take hours to detect. Mouton, (2015) therefore, propose to combine the virtues of FMS-CDR Analysis and test call generators to create a single integrated tool with a hope for improvement and better performance.

Blacklisted IMEI

Airn, (2018) described Blacklisted IMEI by using Blacklisted IMEI in FMS (Fraud Management system) we can maintain that list which is already blacklisted in any fraud and again some traffic is generated on those numbers so we get alert for the same so we can trace the SIM boxing and others fraud in minimal span of fraud run time.

SIM Card Distribution Control (SDC)/ Duping Methods

SIM cards are fundamental in the bypass cycle and fraudsters must maintain an ample supply of SIM cards can to remain in business. However, SIM card distribution control makes this process difficult. Requiring government IDs and limiting the number of SIM cards per ID will prevent fraudster from obtaining a large number of SIM cards to install in their SIMBoxes. This was part of the policy effort make by Dr Isa Pantami, the Nigerian Minister of Communication and Digital Economy to get the telecom subscribers SIM cards integrated with their National Identification Number (NIM) and for profile updating, failure to comply the SIM card shall be disconnected from the network. However, some of the policies made as regards these have been circumscribed due to its non-favourability to telecom investors.

Duping methods

Airn, (2018) in his work said duping method could be carried out by inspecting single MSISDN. This could allow the trace of all the MSISDN that is used or activated by Single IMEI and after that; it can do further traffic analysis and can trace all the series of SIM box numbers. In addition to these, it can trace all the IMEI in those SIM places after; it can figure out all the SIM that are activated or used by IMEI that data can be extensively analyzed for getting SIM Box MSISDN's.

Rule based approaches

In the case of rule based approach fraud detection method usually requires, a fraud analyst to prepare a set of rules to either identifies anomalies in the data, or detect fraudulent pattern or behaviours based on previous observation (Subscription record history) (Sahin, 2017). In this simple-based approach, certain data (e.g. CDR) features (such as call duration or the number of call within a stipulated period) are monitored and an alert is trigger, if the fixed threshold is violated (Sahin, 2017). An example a rule-based approach to detect anomalous telephone calls. The method described used subscriber usage CDR (call detail record) data sampled over two observation periods: study period and test period. The study period contains call records of customers' non-anomalous behaviour. Customers are first grouped according to their similar usage behaviour (like, average number of local calls per week, etc.). Gopal and Meher (2007) developed a probabilistic model to describe their usage for customers in each group. Next, maximum likelihood estimation (MLE) was used to estimate the parameters of the calling behaviour. Then the thresholds were determined by calculating acceptable change within a group. MLE was used on the data in the test period to estimate the parameters of the calling behaviour (Fayemi and Olasoji, 2014). Despite having allocated significant resources to prevention, conventional rule-based SIM box fraud prevention has consistently led to incorrect outcomes (Wise-Anthena, 2017). AlBougha (2016) makes a comparison between TCG and rule base approach on SIM box fraud detection.

User profiling behaviours

User profiling aims to leverage the past behaviour of a subscriber to build a model of his typical, expected behaviour. Usage characteristics (such as the average call duration, number of daily international calls) and other customer-related information (credit score, tariff plan) can be used to create a behaviour profile, which will be monitored for deviations and abnormal behaviour (Sahin, 2017; Rosset, Murad, Neumann, Idan, and Pinkas, 1999; Hilas and Sahalos, 2005). This approach can be used to detect fraudulent behaviour of retail customers (e.g., subscription and superimposed fraud). Compared to the rule based approaches, user profiling has the advantage of treating each user individually, instead of imposing the same set of fraud rules to all users. Hilas et al., (2008) evaluates the efficiency of different user profiling methods to detect faudulent user behaviour on 2500 days of CDR data collected from a PBX with 6000 users. Each user's call data is first modelled based on five different user profiling methods. As the authors have pre-labelled data on fraudulent accounts, they compared the accuracy of user profiling techniques, by employing both supervised and unsupervised learning methods. They find that profiling based on the accumulated weekly behaviour gives the best results.

User behaviour can be leveraged to detect voice spam as well. Studies propose various behaviour features for the caller (such as the ratio of inbound/outbound calls, diversity of the call destinations, rejected call count) that can be used for spam detection. More information can be found in (Tu, Doupé, Zhao and Ahn, 2016).

In addition, SIMBoxes also show specific behaviour patterns (e.g., they do not move, always make outbound calls, never send or receive SMS), which can be used by operators for SIM-Box detection. To avoid such detection mechanisms, fraudsters often use virtual SIM cards, and advanced SIMBoxes that can simulate human behaviour.

Graph analysis

In this approach CDR data were represented as a voice call graph is to visualize the connections between callers and callees, and detect fraudulent patterns.

Source and destination numbers are deployed to represent the set of nodes, and the calls become the directed edges. The weight of an edge can be the number of calls, or the total call duration between the nodes (Henecka and Roughan, 2015).

Jiang et al. (2012) use two year CDR data from a Tier-1 cellular network operator in the US. The CDRs include calls from domestic numbers to international numbers. First, a voice call graph is constructed and the very large connected components are decomposed to identify community structures, where a set of source numbers make calls to a set of destination numbers. Such structures are then analyzed for fraudulent action. Authors classify the detected fraud activities as types of voice spam and international revenue share fraud, by correlating the data with online user complaints. Balasubramaniyan et al., (2007) use the notion of social networks to represent the call history as the previously formed links (previous communications) between the caller and callee. This information is combined with data on call durations to identify the spammers and prevent them from calling legitimate users.

Data Mining/Analytics and Artificial Intelligence approach (M.L and D.L)

In 2013, Sharma et al., said fraud detection methods in the telecom industry can be related to data mining techniques or machine learning algorithms. Data mining is defined as an extraction of interesting (non-trivial, implicit, previously unknown and potentially useful) information or patterns from data in large databases. These techniques involve the training of datasets using various M.L approaches. Data mining and machine learning techniques have been frequently used for fraud detection in different domains, including telecommunications. In fact, telecommunications were one of the first industries that adopted machine learning technologies due to the huge amount of high-quality data they store (Weiss, 2005).

In general, machine learning approaches use certain behavior patterns as features of the machine learning algorithm. Most of the academic work in this field focus on applying machine learning on CDRs to detect subscription and superimposed fraud as well as SIMboxes.

Elmi et al. (2013) uses supervised learning algorithm based on Artificial Neural Networks (ANN) to detect SIM box fraud. The dataset is gathered from a mobile operator and it includes CDR data from both legitimate subscribers and subscribers belonging to a fraudulent SIM box. All the CDRs come from one cell of the network and 234K CDRs gathered in 2 months are analyzed. The features used in the classifier include the subscriber ID, total incoming and outgoing calls per day, total duration of calls per day and similar statistics about the calls during night. The classifier has 98.7% accuracy in identifying the SIM cards that are used in the SIM box device.

A similar study is conducted by Murynets et al. (2014), with a much larger dataset and different set of features used for classification. In this work, CDRs gathered from 500 fraudulent SIM box devices and 93000 legitimate accounts in one and a half years' period were analyzed. The aim of the study is to differentiate legitimate and fraudulent devices (IMEIs) using a classification algorithm. The average duration and total number of incoming and outgoing calls per IMEI (with corresponding origination and destinations), account age, the number of SIM cards (IMSIs) per IMEI and the number of base stations that an IMEI connected to within one week are some of the features used. The analysis shows that SIMboxes are usually static, they connect to a few base stations, they are associated with many IMSIs and they initiate a significant number of calls. Due to the huge amount of data, authors perform some pre-processing steps to eliminate obviously legitimate accounts. The proposed classification methodology gives 99.9% accuracy.

Generic algorithm

This was introduced in the field of computational biology. These algorithms belong to a larger class of evolutionary Algorithm (EA). It generates solution to optimization problem using techniques inspired by natural evolution, such as inheritance, selection, mutation and cross over. Since, the algorithms have been applied in various with promising results (Sahin 2017). Patidar and Sharma (2011) detected a fraudulent transaction through the neural network along with the genetic algorithm. Genetic algorithm was used for making the decision about the network topology, number of hidden layers, and number of nodes that were used in the design of neural network for the problem of credit card fraud detection.

For intrusion detection, the Generic Algorithm (GA) is applied to derive a set of classification rules from the network audit data. The support confidence framework is utilized as fitness function to judge the quality of each rule. The significant features of the GA are its robustness against noise and self-learning capabilities. Also, it techniques reported in case of anomaly detection are high, its attack detection rate and lower false positive rate were awesome.

However, despite having allocated significant resources to the detection and prevention, conventional approaches to fight SIM-Box fraud mannerism have consistently led to incorrect outcomes. The telecom industry now needs different solution. To safeguarded against the: (i) Traditional detection methods in order to identify leakages in revenue, but make it hard to accurately pinpoint the source.

(ii) False positives which can lead to the operator taking action on legitimate users.

(iii) Fraudsters break even at twenty-three minutes of fraudulent calls. They understand traditional detection methods and change their patterns accordingly.

In our subsequent research big data analytics/mining and deep learning techniques of Auto Encoder+ K-

means methods and M.L algorithm (Dense model, Random Forest, Adaboost, and XGB) is proposed to bring a solution to SIM Box fraud problem affecting Nigeria telecom sector to cluster the numbers of fraudulent subscriber against legitimate from the record (CDR). Among which comparative analysis with be perform to ascertain the best modl. Our approaches are essential to identify anomalies and brings celerity and accuracy to fraud detection.

Audio Based Approach

According to Sahin, (2017) Audio Based Approach; comprises of call audio features that can be used to detect packet losses (that often occur in VoIP networks) and identify the audio codecs applied to a call, which can be used to detect the types of networks a call is initiated from and has traversed over (Vijay et.al., 2010). This information helps to detect VoIP based phishing attacks and other suspicious calls. A recent study of (Reaves et al., 2015) aims to detect SIMboxes by analyzing the audio signals for each individual call at a cell tower serving to a SIM box. The idea is to detect the audio degradation caused by a VoIP-to-GSM gateway, by observing the frame losses in the GSM-encoded audio. The proposed method achieves 87% accuracy in detecting the calls bypassed over a real SIM box. A disadvantage of audio based fraud detection approaches is the difficulty of accessing the call audio streams, and real-time processing of this huge volume of data. Call audio can also be used as a channel to transfer data between the caller and the callee. For instance, the AuthLoop protocol (Reaves et.al, 2015) uses the audio channel to provide a TLS-like authentication method to verify the caller ID information. The advantage of this approach is that it works independently of the underlying call technology.

Honeypots Analyzing via VoIP Attack

Several honeypot architectures are proposed (Ighneiwa and Mohamed, 2007; Nassar et.al. 2007; Rodrigo et al., 2011) to collect and analyze the attacks targeting IP-PBX (IP based Private Branch Exchange, e.g., Asterisk2) servers, SIP proxies and soft phones. These honeypots can be used to detect malicious call signalling messages, DoS attacks, SPIT (Spam over Internet Telephony) calls and voice phishing attempts targeting enterprise phone systems. Gruber et al. (Markus, Christian, Florian et al., 2013) deploys an IP-PBX server with vulnerable user accounts (e.g., accounts with weak passwords) and an uplink to PSTN, which enables outgoing calls. Authors capture several ‘toll fraud’ attacks (which refers to PBX dial-through) and find that all the calls initiated by the fraudsters target international destinations or premium rate numbers.

Telephony honeypots

Telephony honeypots is aim to collect data on the incoming phone calls received by a set of phone numbers (Sahin, 2017). The phone numbers are usually directed to an IP-PBX that uses a set of phone lines to receive calls and allows to process them (e.g., answer, record, forward). The phone numbers that will be assigned to a telephony honeypot can be chosen in different ways, depending on the purpose of the honeypot. For instance, a honeypot that aims to collect data on voice spam will better use a set of numbers that have been returned by users who receive too much spam (‘dirty’ numbers), instead of using ‘new’ numbers (previously not assigned to anyone). It is also possible to ‘seed’ (i.e., advertise) the phone numbers in various platforms (e.g., online social networks, questionable websites Payas et. al. 2015) to attract more calls from fraudsters. A telephony honeypot can be interactive (responding to the call and interacting with the caller) or low interaction (not responding to the calls, or passive response). In the previous work (Payas et al., 2015; Reaves et al., 2015), researchers propose the following types of interactions for telephony honeypots:

(i) No interaction (CDR only): The calls are either immediately terminated e.g., with a busy tone or “not in service” message. The honeypot records the call metadata.
(ii) Low interaction: The calls are allowed to ring for some time before the hang-up, or they are answered with silence or some background noise.
(iii) High interaction: The calls are answered and the honeypot interacts with the caller via a voicemail message, an automated voice response mechanism (such as playing pre-recorded or text-to-speech messages), or a live agent talking to the caller.

For the low and high interaction honeypots, call audio can also be recorded in addition to the metadata, depending on the legal restrictions on call recording. Note that deploying high interaction honeypots are much more challenging, as they require to engage in a meaningful interaction with the caller. Detail about the study of high interaction honeypots is contained in (Sahin, 2017) Ph.D. thesis.

Fraud detection evasion by fraudsters (how fraudster evade detection)

Fraud activity is a major problem in telecom industry and to mobile operators. Marah et al. (2015) describe fraud detection as an approach deploy in trying to detect illegal usage of a communication network. Fraud evasion is the defences approach deployed by fraudster to escape from being scooped. Fraudster and anti-fraud circumstance are endless scenarios, every-time detection technology advances; fraudsters are developing their approaches to evade detection and to maximize profit (Marah et al., 2015). Wu, Li and Zhou (2018) use the province to discuss the fraud detection method that is basically divided into two kinds of misuse detection and anomaly detection.

The misuse detection method is mainly to model the known fraud characteristics, and then the user uses these established models to detect the user's communication behaviors. If a matching model is found, this user will be judged to be fraudulent. The main advantage of this detection mode is that it is simple and convenient, but its disadvantage is that the false alarm rate is high. The anomaly detection method is based on the user's daily behaviors as a standard and associates fraudulent behavior with daily behavior. When the user's consumption is unconventional, this will be recorded as a record. When this behavior occurs many times, the user is tracked and sent out. Warning, the main advantage of anomaly detection is that it can detect fraud patterns that have not previously appeared (Feizhang, yiwenliang and hongbindong, 2006). Telecommunications users are the object of telecommunication fraud detection. The characteristics of different users' communication behaviors are also different (Wu et al., 2018). The normal communication consumption behavior of users is easy to obtain. Given the diversity of fraud. This section describes two (2) different methods of anti-spam and HBS employed by hi-tech thieves to avert SIM blocking and detection.

Anti-Spam (Test Call Detection)

Anti- spam is an effective approach deploys to detect SIM card inserted into an illegal SIMboxes via generating test call (TCG) by savoring different routes to a known local network numbers. The inbound calls will appear weather it is coming from a local number or from an international number, if it was coming from a local number then it must be associated with some SIM card used in SIM-Box and easily processed by the fraud department. However, the fraudster analyzes the voice call traffic coming towards their SIMboxes and based on usage and other pattern they could determine whether the calls were real subscriber calls or they were originated from a TCG system. They could then either block the test calls or prevent them from reaching the SIM-Box, to begin with or re-route the calls to a legitimate route so as to avoid detection.

Human Behaviour Simulation (HBS)

Murynets et al. (2014) work revealed some features that could be used to identify SIM-Box fraud; if it is iscovered that:

- The SIM-Box is not moving
- Most calls are out bounding (outgoing) calls
- No usage of network service like SMS, MMS, GPRS, and others.

However, smart SIMboxes are designed to simulate or mimic the behavior of normal subscriber (customer) by using Human Behavior Simulation (HBS). A technique which makes detection of fraudster's very difficult, if no advanced detection algorithm were employed.

HBS encompasses the following: SIM Migration, SIM Rotation, and Usage of other Network services, family list and call forwarding (Kouam et al., 2021).

SIM Migration (Movability)

Hi-tech thieves are deploying many gateways in different locations, for example, one in the city Centre and another in shopping mall or some other crowded place and once in a while they swap the SIM cards between the gateways, so it would look like that the user is moving. The swapping operation could be done either manually or automatically using software. According to (Alghawi, 2019), In SIM card Migration, the system is capable of registering the SIM cards on different GSM –module with a specified frequency. If the user has numerous GSM gateway positioned in different part of the city, system will make SIM card conduct calls from every gateway in turn, creating an illusion of subscriber's movement. This will help the users to protect their card from being blocked by the mobile operator (Alghawi, 2019; Ayamga, 2018).

SIM rotation

SIMboxes can be detected easily if fraudsters operate their SIMs around the hour excessively, so they limit their usage by rotation of the SIMs as workers shifts. This will make SIMs operates in limited hour in a day, which simulates the behaviour of ordinary customers. Alghawi, (2019) stated that one of the optimization algorithm of the fraudster system is SIM Rotation. SIM cards among every SIM Box is divided into teams, each of these groups can be attached to a separate GSM module of a VoIP gateway. Over times, the system is ready to create changes among every cluster, changing SIM cards which is responsible for making voice calls from one location to another. This is not solely permits the user (you) to optimize resources consumption of each single "SIM", however, additionally provides a clear stage to cut back their employment and consequently the suspicious of the mobile operator (Alghawi, 2019; Richard et al., 2018).

Usage of other network services

Most of the SIMboxes are using just voice calls service and that makes them vulnerable to detection. In order to mitigate this issue smart SIMboxes are making calls and sending SMS to each other. Also, sometimes they use some internet services provided by the network operator.

Family list

Traditional SIMboxes just re-routes the call from VoIP to the GSM network, so they make calls to large number of different network subscribers. A smart way to avoid this is by using family list, where each SIM is

assigned to re-route calls to a specific list of numbers. This leads to the escaping the trap of large different numbers detection.

Call forwarding

The call forwarding feature allows a call intended for a SIM card used in the SIMBox to be forwarded to a specific number, so that a human agent can answer the call (Kouam et al., 2021). It can be edited according to the three following conditions:

- Unconditional: it allows to forward all incoming calls unconditionally;
- Busy: it allows to forward incoming calls only when the called number is busy;
- Not reachable: it allows to forward incoming calls when the called number is not reachable or cannot register to the mobile operator network;
- No reply: it allows to forward incoming calls when there is no reply from the called number.

Summarily, HBS (Human Behaviour Simulation) makes dealing with bypass fraud difficult and time consuming.

Impact of sim-box fraud on stakeholders, nation and telecommunication industry

SIM-Box frauds have dissimilar implication on telecom operators, regulators, Government and subscribers (Consumers). Mola (2017) in his work elucidates on few effects of SIM-Box fraud that include:

- Revenue loss due to call termination
- Revenue loss due to service inaccessibility and missing call back.
- Damage to an organization's image (i.e. reputation) and operations.

(Bad quality of services) and Additional investment.

While Murynet et al., (2014), Wise-Anthena, (2017) in another work described this effect and features of same fraudulent SIM-Boxes that trending to constitute:

- Economic loss
- Degrades the local services where they operate
- Worsened brand image and creates customer dissatisfaction.

Okumbor and Ateli (2019) discussed the challenges faced by stakeholders as a results of SIMboxes

- Revenue loss and Availability of Simboxes in the Open Markets
- Avoidance of SIM blocking

Marah et al., (2015) contribution creates awareness on it vulnerability threat to national security architecture of a nation in par with the aforementioned effects mentioned by previous authors. Sowe, (2018) presented pictorial categories of the SIMBox fraud effect.

Impact of SIM-box fraud on economic

The effect of SIM box fraud on economy is premeditated to siphons revenue from the side of both government tax collectors and telecom operators as well from service subscribers. This is possible due to the level of ignorant, illiteracy and ineptitude among consumers of telecom services. Most importantly the technical and operational loopholes humanely divulge by telecom experts that are gainfully delve by cyber fraudsters to dupe of treasures.

National Communication Commission and Nigerian Telecom Sector Regulatory Challenges on SIM boxes

Regulatory challenges

i. Government's intervention in setting the call termination rate:
ii. Incumbent operator managing the international gateway:
iii. Lack of tools to measure, track and monitor international incoming calls:
iv. Laws which criminalizes SIM-Box fraud: No law on this effect except for the general cybercrime activities, which is postulated in the (Cybercrime Act, 2015).
v. Lack or in circulation of National ID cards
vi. Lack of tools to verify IDs during SIM registration process
vii. Procure National and International measurement and monitoring system
viii. Task force for the effective and efficient detection of SIM-Box operation
ix. Advisory note for the policy makers to draft laws which criminalizes SIM-Box fraud
x. Influx of foreigner migrations into Nigeria without proper proliferation of document due to porous border, lack of security architecture and inefficient of immigration and border patrol personnel checking entries and exit from the country
xi. Lack of access-ability, obtainability and availability of dataset (i.e. CDRs) provisions by telecom companies and communication commission (NCC) and related agencies for research: This seems to be a problem in the country as most bodies fails in relinquishing dataset for research due to privacy and confidentiality attached; in order to safeguarded against revilements of organization secrecy which may dent its reputation. This would have help in research to delve insights on organizational dealing and customer behavioral trait in which data science expert would advise over.

Stages involves in the process of sim box fraud occurrences

The stages in process where SIMboxes is occurring is elucidated in a blog (commsrisks.com); therein, this

were highlighted:

False pre-registered SIMs: This act is perpetrated through the negligence of SIM card registrar. It occurs when false information is supplied during the pre-process of SIM registration and ill capturing method of user identity. As a results of aid and abetting fraud encourage with bribe to get thing done quickly, without minding the implication factors.

Bulk supply of SIMs: This occur from the side of SIM vendors as they failed to take cognizance records of SIM detail (Serial number, IMSI, IMEI and other) purchased by retailer from them due to their procrastination and SIM Bulkiness inventory record.

Carriers teams buying discounted bypass termination: Buying a discounted bypass termination could necessitate the fraudulent activities of bypass fraud.

Carrier's staff running their own bypass termination: This is abounding due to selfishness.

Fraud prevention staff on the Simboxer payrolls: This is committed from the side of telecom staff. It happens in form of social engineering and phishing. Due to greed and insatiability of contract agreement with their immediate employee.

Way Forwards / Solution and Recommendation to the Challenges of SIMbox Fraud

The difference in approaches adopted by different countries to deal with the fraud makes it difficult for operators to develop a unified strategy to fight SIMbox frauds. In Nigeria, most service provider's uses TCG and CDR analysis for fraud detection. While Ethio telecom is government owned and the sole telecom operator in Ethiopia uses rule based approaches for its fraud detection, so are many others countries. In few countries, IP interconnection services are treated as legal whereas they are banned in other countries due to the regulatory issues associated with such activities. For example, the Ghanaian and Nigerian government has declared SIM boxes illegal and made several arrests in this regard. The recent developments around Sim-box fraud has further aggravated the challenges faced by telecos. With no scope for regulatory remediation, the only way forward for them is to prevent these attacks using advanced technologies. Traditional approaches like Call Detail Record (CDR) analysis and TCG are becoming ineffective in dealing with modern SIM box strategies due to the latency and false positives associated with those methods. These had given rise to the application of Artificial intelligence method. As the market evolves, we suggest that operators should look towards a unified approach that can help them address the crisis in a much proactive manner (Okumbor and Ateli, 2019). The developments around machine learning and test call group (TCG) analysis have favored the growth of an integrated solution to combat the fraud in a cost-effective manner. The approach builds the capabilities of the traditional models but integrates the advancements in artificial intelligence and self-learning rules.

Okumbor and Ateli (2019) in their work provided a recommendable solution which this research supports its notions for lasting solution to the problem of SIM Box fraud in Nigerian Telecom industry. In order to have a lasting solution to the SIM Box fraud, we recommend the following measures:

We recommend that regulators must task service provider and implementers to provide location-aware system and enhanced bypassed traffic detection. Such system has the capability of providing the global position system GPS coordinates for the exact location of the SIM Box and also to identify fraudulent VoIP calls in real-time. Such proposed intelligent solution could be software or hardware device programmed to intelligently detect cases in real-time and then enforce immediate blocking of the SIMs detected.

National Commissions responsible for regulation should put measures in place to reduce the sale of pre-paid SIM cards by mobile telecommunication companies.

Regulators must speed of the implementation processes of SIM registration and sanction must be taken against any network operator whose SIM is used for perpetrating crime without proper profiling.

More research work should be done in development of intelligent system that can detect, locate and report the fraud for onwards investigations.

To avoid financial losses, real-time information of any suspicious or potentially fraudulent activity can be instantly identified and brought under control with fraud management system. Such that automation of fraud detection process, implementation of organizational standards, customized policies, rules, and thresholds are built around the regulator specific needs and operational requirement.

Government must put in place legal framework to ensure that the law enforcement agencies, regulators, Network service providers and operators collaborate to bring the perpetrators of this fraud to justice.

On the issue of National ID card circulation; we suggest for an integration of nationale profiles in the databases of FRSC, NIMS, INEC, Immigration agency (Passport offices) to checkmate the culprit of the heinous act without record duplicity compromise.

CONCLUSION

In this paper, we presented an elusive literary survey on SIMBox fraud concepts and the detection techniques while establishing a fact-finding with the

plethoric historical unrestraint of SIMbox fraud and reason for it premeditation by hi-tech thieves. The effort makes so far by researcher and anti- fraud vendor in the field as been extemporized as well as the implacable impact of the nefarious fraudulent activities. While a lasting solution and recommendation is professed. In our forthcoming work, we seek to present a hybrid enhanced model for SIM-Box fraud detection, which shall be a first in the research sojourn of SIMBOX fraud detection with an implementation.

Acknowledgements

The authors acknowledge NCC for the useful information provided in the course of this research work. Also, we acknowledge the tremendous cooperation of Nigerian mobile telecommunication company and fraud department of MTN.

Conflict of interest

We hereby declare that there is no conflict of interests.

REFERENCES

Abuhamoud, N., Alsadi, I and Ali, S. (2021). Detecting SIMBox Fraud Using CDR Files and Neo4j Technology. 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 25-27 May 2021, Tripoli-Libya, Pp 1-5.

Adeoye, A. A. and Adelowo, O. T. (2015). Internet Access, use and Monitoring Policies in Selected Organization in Ibadan, Nigeria. Global Journal of Management and Business Research: A Administration and Management, 15(11): 14-26. Online ISSN: 2249-4588 & Print ISSN: 0975-5853

Adepetun, A. (2019, March 27). Government Charged as SIM Boxing Menace rips Africa. The Guardian Online Magazine. https://guardian.ng/technology/government-charged-as-sim-boxing-menace-rips-africa/

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, 13 (4): 19-29. Retrieve from http://www.cscanada.net/index.php/css/article/view/9394 DOI: http://dx.doi.org/10.3968/9394

Adjaoute, A. (2006). Systems and Methods for Dynamic Detection and Prevention of Electronic Fraud. United States Patent US007089592B2Patent No.

Africa, D. B. (2015). Cameroun: 22, 2 milliards fcfa de pertes en 2015 sur les appels t´el´ephoniques frauduleux parsimbox."

Africa, V., (2018). Well Known Sakawa Boy Finally Repents and Confesses- YouTube. [online] YouTube. Retrieve from https://www.youtube.com/watch?v=lwjMJf7FLhs [Accessed13 April 2019].

Africanews (2021). Technology Companies join Forces in the Fight against Cyber fraud. Retrieved from https://www.africanews.com/2021/04/12/technology-companies-join-forces-in-the-fight-against-cyber-fraud//

Afrinvest (2020). The Nigerian Telecommunications Industry Report: A transformative Past, Resilient Future, Initiation of Courage. www.afrinvest.com .

Airn, V. (2018). Analysis and detection of SIM box, International Journal of Advance Research, Ideas and Innovations in Technology, 4(3): 330-334, ISSN: 2454-132X. Retrieved from: www.ijariit.com.

Ajanaku, L. (2020). Call Masking, SIM boxing blue. The Nation Online Magazine.

Alghawi, N. (2019). A Study on SIM Box or Interconnect Bypass fraud, Dissertation Submitted in fulfillment of the requirement for the degree of M.Sc Informatics, The British University, Dubai, U.A.E.

Al-Atassi, N. (2016). SIM Boxes and Internet of Things Pose Rising Fraud Threats in Middle East and Africa. Retrieved from https://www.SIM-Boxes-and-Internet-of-Things-Pose-Rising-Fraud-Threats-in-Middle-East-and-Africa-The-Syniverse-Blog.htm/

Al-Atassi, N. (2016). SIM Boxes and Internet of Things Pose Rising Fraud Threats in Middle East and Africa. Retrieved from https://www.SIM-Boxes-and-Internet-of-Things-Pose-Rising-Fraud-Threats-in-Middle-East-and-Africa-The-Syniverse-Blog.htm/

Aliogo, U. (2021). 'Nigeria Lost N5.5tn to Cybercrimes in 10 Years'. https://www.thisdaylive.com/index.php/2021/04/26/nigeria-lost-n5-5tn-to-cybercrimes-in-10-years/

Allafrica.com (2018, June 13). Nigeria: Rising Waves of e-frauds Put Economy at Risk Retrieved from https://allafrica.com 13-June 2018 [Accessed Date APRIL 17, 2019]

Allafrica.com (2018). Nigeria: Rising Waves of e-frauds Put Economy at Risk Retrieved from https://allafrica.com 13-June 2018 [Accessed Date APRIL 17, 2019]

Alraouji, Y, and Bramantoro, A. (2014). International Call Fraud Detection System and Techniques, Buraidah AlQassim, Saudi Arabia. Retrieved from http://dx.doi.org/10.1145/2668260.2668272

Alsadi, S. and Abuhamoud, N. (2020). Study to use NEO4J to analysis and detection SIM-BOX fraud. *JOPAS, 17(4):* 1-6. Retrieved from: https://www.researchgate.net/publication/339149562

Aranuwa, F. O (2013). Hybridized intelligent data analysis model for fraud detection in mobile communication network. AcadEMIC Journal of Science Res. 1(5), 082-089.

Ayamga, D. (2018). Telecommunication Fraud Prevention Policies and Implementation Challenges. MSC Degree Project. Luleå University of Technology Department of Computer Science, Electrical and Space Engineering.

Barson, P., Field S., Davey N., Mcaskie G. and Frank R. (1996). The Detection of Fraud in Mobile Phone Networks. Neural Network World. 6(4): 477–484.

Becker, R. A., Volinsky, C., and Wilks, A. R. (2010). Fraud Detection in Telecommunications: History and Lesson Learned.Technometrics, 52(1), 20-33. doi: 10.1198/TECH.2009.08136. http://dx.doi.org/10.1198/TECH.2009.08136

Blatt and Kaufman (2017). Big Data Analytics for Telecom Fraud Detection. United State Patents. Patent No.: US 9.699.660B1, Date of Patent: July 4, 2017.

Bolton, R. J. and Hand, D. T. (2002). Statistical Fraud Detection: A Review. *Statistical Science*. 17: 235–249.

Cataleya (2016). Fighting Voice fraud with Big Data Analytics Building identification and Mitigation into Global Networks. Retrieved from: https://www.cataleya_fraud_prevention_white_paper.pdf_adobe_reader

CFCA (2015). Global Fraud loss survey Communication Fraud Control Association. Retrieved from: http://www.cfca.org/fraudlosssurvey Communication Fraud Control Association, 2015 Global Fraud Loss Survey [Internet]. 2015.

Chouiekh, A. and El Hassane Ibn El Haij (2018). ConvNets for Fraud Detection Analysis. The First International Conference on Intelligence Computing in Data Sciences. Procefia Computer Science 127 (2018), 133-138. Retrieve from www.sciencedirect.com

Communication Fraud Control Association (CFCA) (2015). Global Fraud loss Survey [Internet]. 2015[Cited 2016 Dec 3]. Retrieved from https://goo.gl/HT9IER

Communication Fraud Control Association, "2017 Global Fraud Loss Survey", www.cfca.org/fraudlosssurvey/.

Communication Week (2017, February 17). NCC to Tighten Noose on Call Relling, Masking andSimbox Fraud. Retrieve from http:// www.nigeriacommunicationweek.com.ng [Accessed Date April 7, 2019].

David-admin, (2017). SIM Box fraud and OTT bypass biggest threats to mobile operator revenues. Revector. Retrieved from: Error! Hyperlink reference not valid.

Editorial Board (2017). Nigeria and Internet fraud. Retrieve from https://www.Nigeria and internet fraud—Opinion— The Guardian Nigeria Newspaper – Nigeria and World News.htm.

Elmi, A. H., Subariah, I. and Roselina S. (2013). Detecting SIMBOX Fraud Using Neural Network. IT Convergence and Security 2012. Springer Netherlands, 2013, 575-582.

Emmanuel, A. B., (2019, January 30). NCC Said Nigeria has lost billions to Telecom-related fraud. Retrieved from: https://www.nairametrics.com [Accessed Date April 17, 2019].

Emsaieb Geepalla, Nasser Abuhamoud, Abdulla Abouda (2018). Analysis of Call Detail Records for understanding User Behaviors and Anomaly Detection Using Neo4J. 5th International Symposium on Data Mining Applications pp 74-83. https:// link.springer.com/chapter/10.1007/978-3-319-78753-4-7

Fayemiwo, M. A. and Olasoji, B.O. (2014). Fraud detection in mobile telecommunication. International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), 3(4), 11612-11620. www.ijirset.com

Fayza, B. (2019, December 9). SIM Box Fraud – A Growing Concern https://www.insidetelecom.com/sim-box-fraud-a-growing-concern/

Frank, I and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution.*(IJCRSEE) International Journal of Cognitive Research in Science, Engineering and Education, 1(1), retrieved from*: www.ijcrsee.com.

Gent, A. (2017). Fighting fraud on mobile networks. *Computer Fraud and Security*, 2017(2), pp.10-13. https://www.sciencedirect.com/science/article/abs/pii/S1361372317300143

Goantifraud (n.d). Articles, Retrieved from https://goantifraud.com/en/blog/categories/article.

Henecka, W. and Roughan, M. (2015). Privacy-Preserving Fraud Detection Across Multiple Phone Record Databases. Published in: IEEE Transactions on Dependable and Secure Computing (Volume: 12, Issue: 6, Nov.-Dec. 1 2015).

Hollmton, .J. (2000). User profiling and classification for fraud detection in mobile communications networks, Helsinki University of Technology.

Ighneiwa. and Mohamed, H. (2017). Bypass fraud detection artificial intelligence approach.arXiv preprint arXiv:*1711.04627*, pp. 3–6, 2017.

Kaakinen, M., Keipi, T., Rsnen, P. and Oksanen, A. (2017). Cybercrime victimization and subjective wellbeing: An examination of the buffering effect hypothesis among adolescents and young adults," Cyberpsychology, Behavior, and Social Networking, vol. 21, 10.

Kala, N (2019). A study on Internet bypass fraud: national security threat. Forensic Research & Criminology Journal. 7(1): 31. 35.

Kalau, N (2021, July 22). What are the 10 economic problems that Nigeria is facing? Legit.ng. Retrieved from: https://www.legit.ng/1116681-what-10-economic-problems-facing-nigeria.html.

Kehelwala, K. G. (2017). Real-Time Fraud Detection in Telecommunication Network using Call Pattern Analysis . Sri Lanka : University of Moratuwa Sri Lanka.

Kouam, A., Aline C. V., Alain T. (2021). SIMBox bypass frauds in cellular networks: a survey. [Research Report] INRIA. HAL Id: hal-03105845. https://hal.inria.fr/hal-03105845v3.

Kun Niu, H. Jiao, N. Deng, and Z. Gao, (2016). A real-time fraud detection algorithm based on intelligent scoring for the telecom industry. Proceedings –*2016*International Conference on Networking and Network Applications, NaNA *2016*,vol. 1, Pp. 303–306.

Leadeship.ng (2018, July 19). Call Masking –NCC to deploy high technology for tracking fraudster. Retrieve from https:// www.google.com/am/s/leadership.ng/2018/07/19/call-masking-ncc-to-deploy-high-technology-for-tracking-fraudsters/

Leardership.ng (2019). Nigeria Loses Over N197bn to Digital Fraud Annually – Osinbajo. Retrieve from https://www.google.com/am/s/leadership.ng/2019/01/30/Nigeria-loses-over-N197bn-to-digital-fraud-annually-osinbajo/

McAfee Inc. (2014). Net losses: Estimating the global cost of cybercrime. Retrieved from https://www.mcafee.com/ca/resources/reports/rp-economic-impact cybercrime2. Pdf

Modi, K. and Dayma, R. (2017). Review on fraud detection methods in credit card transactions in 2017. International Conference on Intelligent Computing and Control (I2C2), pp. 1–5.

Mouton, K. (2015). Integrated Test Call and CDR Analysis: Tool in the Fight Against SIM Box and OTT Bypass Fraud. *Black Swan Telecom Journal, May 2015.* Retrieve from http://bswan.org/test_call_sim.asp[01.09.2015 13:54:08].

Mouton, K. (2017). Stealth Test Calls: A powerful new weapon in the Fight to Block Simbox Bypass. *Black Swan Telecom Journal, June 2017.* Retrieve from Www.bswan.org.

Murynets, I., Zabarankin, M., Jover, R. P., and Panagia, A. (2014). Analysis and detection of SIMbox fraud in mobility networks. Proc. - IEEE INFOCOM, Pp. 1519–1526.

NCC, C. (2015). Policy and E. A. Department, An assessment of international voice traffic termination rates.

Nexis,L. (2013). True cost of fraud 2013 study: Manage retail fraud. Retrieved from http://www.lexisnexis.com/risk/ insights/2013-true-cost-fraud.aspx.

Nwafor (2018). How 'rogue networks' use SIMbox to steal from govt, tecos. Retrieve from https://www.-vanguardngr-com.cdn.amp

Nwanchukwu, J. O. (2020). NCC unveils strategy for curbing call masking, refilling under Danbatta. Retrieve from: https://dailypost.ng/2020/01/16/ncc-unveils-strategy-for-curbing-call-masking-refiling-under-danbatta/

Nwogbo, K. (2018). Nigeria: call masking-NCC makes U-turn, blames SIMbox operator. https:// allafrica.com [Accessed Date April 7th 2019].

Nyarko-Tirenkyi, A. (2020). Ghana Loses U.S. $9.8 Million to Cybercrime, Other Criminal Activities in 2019. https://allafrica.com/stories/202003030563.html

OECD Policy Responses to Coronavirus (COVID-19), (2020, Sept 30). The impact of coronavirus (COVID-19) and the global oil price shock on the fiscal position of oil-exporting developing countries. https://www.oecd.org/coronavirus/policy-responses/the-impact-of-coronavirus-covid-19-and-the-global-oil-price-shock-on-the-fiscal-position-of-oil-exporting-developing-countries-8bafbd95/

Ogwueleka, F. N. (2009). Fraud Detection in Mobile Communications Networks Using User Profiling and Classification Techniques. Journal of Science and Technology, 29 (3), 31-42.

Ogunfuwa, I. (2020, Febuary 4). Nigeria telecom industry may lose N141.1bn to fraud –Report. Retrieved from: https://punchng.com/nigeria-telecom-industry-may-lose-n141-1bn-to-fraud-report/.

Okumbor, N. A., and Ateli, A. J. (2019). Grappling with the Challenges of Interconnect Bypass Fraud, IOSR Journal of Mobile Computing and Application (IOSR-JMCA), 6 (1):, 35-41 e- ISSN: 2394-0050, P-ISSN: 2394-0042. www.iosrjournals.org

Osuagwu and Umeh, J., (2018). Nigeria: Rising Waves of e-frauds Put Economy at Risk. Retrieve from https://allafrica.com.

Proshare Technology (2017). The Nigerian Telecommunication Sector-Challenges and Cautious Optimism. Retrieve from www.proshareng,com [Accessed Date April 15, 2019].

Papernaia, N. (2021). Stop SIMbox fraud in your network with AIS Handshake/Commsrisk. Retrieved from www.commsrisk.com.

Purnamasari, P. and Amaliah, I. (2015). Fraud Prevention: Relevance to Religiosity and Spirituality in the work place. 2nd Global Conference on Business and Social Science-2015, GCBSS-2017, 17-18 September, Bali, Indonesia. Procedia-Social and Behavioral Science 211 (2015) 827-835.

Reaves, B., Shernan, E., Bates, A., Carter, H., (2015). Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. Proceedings of the 24th USENIX Security Symposium August 12–14, 2015, Pg.833-848, Washington, D.C. ISBN 978-1-931971-232.

Reaves, B.G. (2017). Authentication Techniques for Heterogeneous Telephone Networks. A dissertation presented to the graduate school of the University of Florida in Partial fulfillment of the requirements for the Degree of Doctor of Philosophy University of Florida. research: combining rigour, relevance and pragmatism. *Information Systems Journal*, 8(4), Retrieve from: http://www.s3.eurecom.fr/docs/eurosp17_sahin.pdf [Accessed Date April 13 2019].

Revector, (n.d). Simbox fraud and ott bypass biggest threats to mobile operator revenues."

Sahin, M. and Antipolis, S. (2017). SoK: Fraud in Telephony" [online] S3.eurecom.fr.

Sahin, M., (2017). Understanding Telephony Fraud as an Essential Step to better fight it. *Ph. D. Theses. Ecole Doctorale Informatique, Telecommunication et Electronic*. Paris. ED 130 September 21st, 2017.

Sallehuddin, R., Ibrahim, S., Azlan, M. Z., and Elmi, A.H. (2015). Detecting SIMBox Fraud by using Support Vector Machine and Artificial Neural Network security. (New York, NY, USA, 2010), CCS 10, ACM, p. 109-120. DOI:10.11113/jt.v74.2649

Serianu, USIU-Africa and Demadiur (2016). Nigeria Cyber Security

Report. Retrieve from https://www.paladion.net.
Sowe, A. (2018). The Effects Of Sim Box Fraud on QoS.PURA. Retrieved from Armadou_sowe.pdf-adobe Reader.
Serianu, USIU-Africa, ISACA, Bostwana, Liquid Telecom, Kabolik and Demadiur (2017). African Cyber Security Report. Theme: Demystifying Africa's Cyber Security Poverty Line. Retrieve from http://www.serianu.com
Subexinc (n.d). White paper Bypass fraud-Are you getting it right? Retrieved from: http://www.subex.com
Tawashi, H. A (2010). Detecting Fraud in Cellular Telephone Networks "JAWWAL" Case Study.A Thesis Presented in Partial Fulfillment of the Requirement for the Degree in "MBA", Islamic University of Gaza, Deanery of Graduate Studies, and Faculty of Commerce Department of Business Administration.
Telekom Austria, (n.d).SIM Box Detection Service. Telekom Austria, http://goo.gl/Ac12d.
The Nation (2020). Call masking, SIM boxing blues Retrieved from: https://thenationonlineng.net/call-masking-sim-boxing-blues/
TransNexus, Inc. Introduction to VoIP Fraud White Paper. (2012). Available at: http://www.transnexus.com.
Ugoeze, N. O. (2016). N89.55 Billion lost yearly to cybercrime in Nigeria. *The Guardian Nigerian Newspaper-Nigeria and world news.htm*. [Accessed Date April 8, 2019].
Umeh, J., (2018). Nigeria's Telecom industry loses $3bn to call masking — NCC. Retrieve from https://www.vanguardngr.com/2018/09/nigerias-telecom-industry-loses-3bn-to-call-masking-ncc/. Accessed Date 20/10/ 2018
Umoru, H., (2017). $450 lost to Cybercrime in Nigeria-Senate. Retrieve from http:// www.vanguardnews,htm. [Accessed Date: Nov 6, 2018] uploads/2017/03/Telephony-Fraud-White-Paper.pdf [Accessed April 2, 2019].
Veloso, B. Gama, J, Martins, C, Espanha, R., Azevedo, R., (2020). A Case Study on using Heavy-hitters in Interconnect bypass fraud. ACM SIGAPPP Applied Computing Review, 20(3): pp 47-57. https://doi.org/10.1145/3429204.3429208.
Yeshinegus, G. (2013). Predictive Modeling for Fraud Detection in Telecommunications: The Case of Ethio Telecom. Addis Ababa University School of Graduate Studies School of Information science. Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science.pg. 1-140
Xintec, (n.d). SIMbox detector. Xintec, http://goo.gl/AUZbe.
Yelland, M. (2013). Fraud in mobile networks. Computer. Fraud Security. vol. 2013, no. 3, pp. 5–9.