IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 7, Issue 5 (Sep - Oct 2020), PP 21-27
www.iosrjournals.org

Grappling with the Challenges of Interconnect Bypass Fraud

Okumbor N. Anthony[1], Ateli A. Joy[2]
[1](Dept. of Computer Science, Delta State Polytechnic, Otefe-Oghara, Nigeria)
[2](Dept. of Computer Science, Delta State Polytechnic, Ogwashi-uku, Nigeria)
Corresponding Author: Okumbor N. Anthony

Abstract: *With the development of the telecommunication technologies and the big market size of telecom products has given rise to interconnect bypass fraud. Interconnect fraud is a bypass fraud that occurs when international traffic that should be routed through a legitimate international gateway is routed to bypass those gateways using voice over internet protocol VOIP through the Internet and terminated via Simboxes as local calls. In this paper, we examined the framework and issues associated with this type of fraud and identified that the Simbox bypass fraud has become a challenging threat to telecom companies in some parts of Africa and Asia. In grappling with the challenges associated with this fraud, the synergies of traditional approaches like Call Detail Record (CDR) analysis are becoming ineffective in dealing with modern Simbox strategies due to the latency and false positives associated with those methods hence we proposed the approach that builds the capabilities of the traditional models but integrates the advancements in artificial intelligence and self-learning rules to eliminate the fraud*

Keywords: *SIM (Subscriber Identity Module), Simbox, Bypass Fraud, VOIP (Voice over Internet Protocol), IP (Internet Protocol).*

I. Introduction

The global system for mobile communication (GSM) is the world's most popular standard for cellular radio and personal communication equipment through the globe. Its success has exceeded beyond the expectation of virtually everyone but today is faced with issues and challenges. Obviously, the importance of the movement of coded data and information from one point of the globe to another by means of electrical or electromagnetic devices cannot be over emphasized. However, in Nigeria today and other sub-Sahara regions, the poor quality of service and international call masking is largely attributed to interconnect fraud. Imagine a situation you receive a phone call from a relation abroad with local number will definitely look strange, this is basically the bypass fraud. Interconnect 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/Fixed calls through the use of VoIP or satellite gateway, thus avoiding revenue for international calls termination which operators and government regulators are entitled

It is one of the top five fraud types facing the global mobile telecommunications industry. Simbox was identified in the Communications Fraud Control Association's CFCA Global Fraud Loss Survey Report, 2013. Simboxing compromises cellular network infrastructure by overloading local base stations and causes customer dissatisfaction thus call quality can be degraded and subscribers who receive Simbox calls are unable to identify the caller prior to answering the call. It is a setup in which fraudsters install SIM boxes with multiple low-cost prepaid SIM cards. The fraudster can terminate international calls through local phone numbers in the respective country to make it appear as if the call is a local call. SIM box or GSM gateway fraud takes place when individuals or organizations usually unlicensed, purchase hundreds of SIM cards offering free or low cost calls to mobile numbers. These are then used to channel calls away from mobile network operators and present them as local calls on their networks losing mobile operators significant call revenues. International calls are sent by carriers via the internet to SIM-boxes which redirect this illegal VoIP traffic to mobile networks. This enables them to bypass the international gateway exchange. In this paper, we examined the concept of the bypass fraud (simbox), the framework how the fraud thrives and identified the issues and challenges associated with this telecommunication fraud thus proffer solutions to surmount the problems.

II. Background

Over the past few years, telecommunication companies in Africa have been hit by several telecom frauds. SIM box fraud, also known as the interconnect bypass fraud, is one of the major frauds affecting the dynamic telecom market in Africa. Before now several telecoms operators play fast game on each other by way of masking incoming calls to a Nigeria subscriber from abroad and deliver the calls to the subscriber with a local number as if it were a call from within the country only for the receiver to observe on connection that he or she is talking to someone abroad. A masked call happens when an international calling number (Caller Line

Identity) is masked as local number traffic. It is a deliberate attempt by the fraudster to avoid paying the correct International Termination Rate (ITR) for international calls, but to benefit by paying Local Termination Rate (LTR). According to a survey by the Communication Fraud Control Association CFCA [1] reported that the mobile telecom industry lost more than 29.2 billion US dollars in 2015 alone due to telecom fraud. Besides those big losses, telecom fraud causes other indirect losses to mobile operators, like: network congestion, deny of service and decrease in quality of service. However, the growth of mobile subscribers in Africa is driven by low call prices and availability of cheaper handset. The competition arising from over-the-top (OTT) providers has put an additional pricing pressure on telecommunication companies, forcing them to design new bundled offerings encompassing data, voice and SMS. Such bundles bring much lower per-minute revenue for the operators as compared to traditional services [1]. Fraudsters operating the SIM boxes are taking advantage of this scenario to bypass the formal call termination systems that fetch higher tariffs to telecoms companies. The calls routed through the internet protocol IP networks are terminated using local SIM gateways, thus compromising the formal interconnection networks and bringing heavy losses to the telecoms who have invested in building the networks. Traditionally, Africa countries are known to have higher interconnection tariffs compared to other regions, which further explains why such frauds are prevailing in Africa. According to CFCA report, the most prevalent fraud occurring at the network level is as shown in Figure 1.

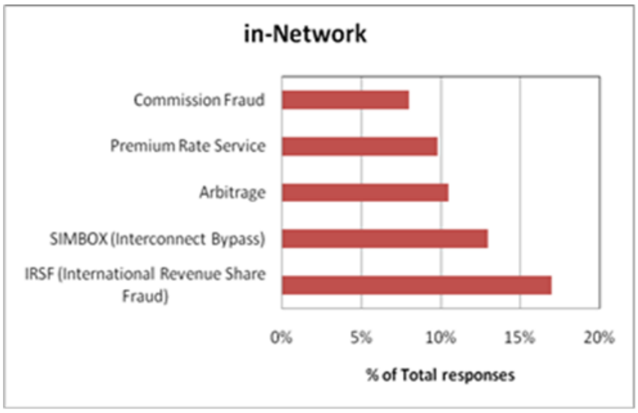

Fig 1. CFCA Report Fraud Reponses

The Fig. 1, depicts that International revenue share fraud (IRSF) and bypass (Simbox) fraud are the largest contributor to the overall fraud losses according to CFCA. As Africa seems to be the hub for mobile network fraud, more than eighty percent mobile operators have experienced Simbox fraud.

III. Literature Review

The mechanism of electromagnetic wave propagation is diverse, poor quality of services such as frequent call drop, echo during radio conversion, cross talk, poor inter and intra connectivity, network congestion, fraudulent activities and many other network problems, may be attributed to poor quality of services deliver to the end user of the GSM Mobile Unit (MU). In consideration of this, [2] reported that GSM network in Nigeria is currently faced with the challenge of customers' dissatisfaction in the quality of service offered by the existing network operators. Today cellular phones have become an indispensable part of our everyday life and these cellular networks are responsible for generating and distributing of radio signals that are used by cellular phones over wide geographic areas [3]. In general security is required for every telecom device, and as cities provide Internet connectivity to ample variety of devices, security becomes a very critical challenge. In the telecom industries, existing research work is mainly focusing on subscription and superimposed types of fraud. However, another type of fraud called SIM box bypass fraud has become a challenging threat to telecom companies in some parts of Africa and Asia. The success of this fraud depends on obtaining SIM cards. Therefore, the effects of SIM box bypass fraud vary across countries. In countries where unregistered SIM cards are not allowed and the government laws recognize the SIM box devices as illegal equipment, the effect is less compared to countries where obtaining of SIM cards by customers is very cheap or even free and government laws do not prohibit unregistered subscribers. The fact that this type of fraud is not a problem for all telecom companies worldwide might justify the reason why the publicly available research on this type of fraud is very limited [4].

Though telecommunication industry suffers major losses due to fraud there is little comprehensive published research on this area mainly due to lack of publicly available data to perform experiments on. One limitation faced by researchers is getting secondary data from cellular operators for experiments. The data to be used for the experiments contains confidential information of customers and in most cases law and enforcement authorities prohibit exposing the confidential information of customers [5]. On the other hand, any broad research published publicly about fraud detection methods will be utilized by fraudsters to evade from detection [6, 7]. Most research investigated Call Detail Record (CDR) analysis combined with machine learning algorithms to detect fraudulent Simboxes [8, 9, 10] and few others used Audio analysis [11].

IV. Framework of Simboxing

SIM boxes are programmed to mimic the activities of a normal call user. The equipment can have SIM cards of different operators installed, so a single SIM box can operate with several GSM gateways located in different parts of the world. The availability of SIM cards at cheaper prices and the lack of law enforcement over the sale of prepaid SIM cards have also favored the growth of SIM box fraud. Figure 2 shows Simbox and its components.

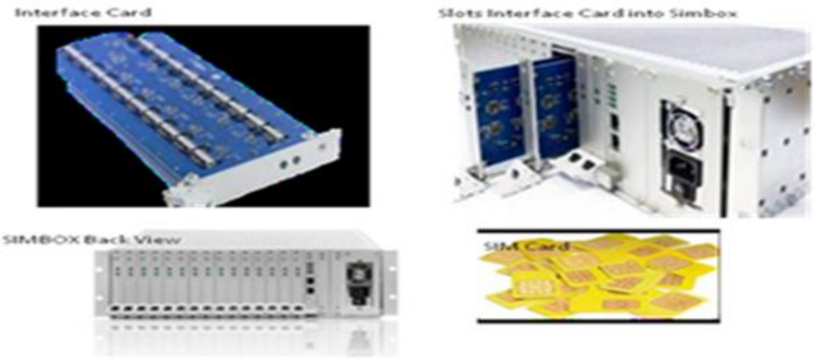

Fig. 2, Simbox and its components

The way Simboxing works is that International voice traffic termination fraud, which is Simbox fraud occurs when international traffic that should be routed through a legitimate international gateway is routed to bypass those gateways and is terminated via Simboxes as local calls. This scenario requires that the fraudsters have access to advanced technology, which is capable of making international calls appear to be cheaper. Figure 3 below demonstrates bypass fraud using least cost call termination techniques like SIM Boxes, to bypass the legal call interconnection and diverting international incoming calls GSM through the use of VoIP or Satellite gateway, thus avoiding revenue for international calls termination which operators and government regulators are entitled.

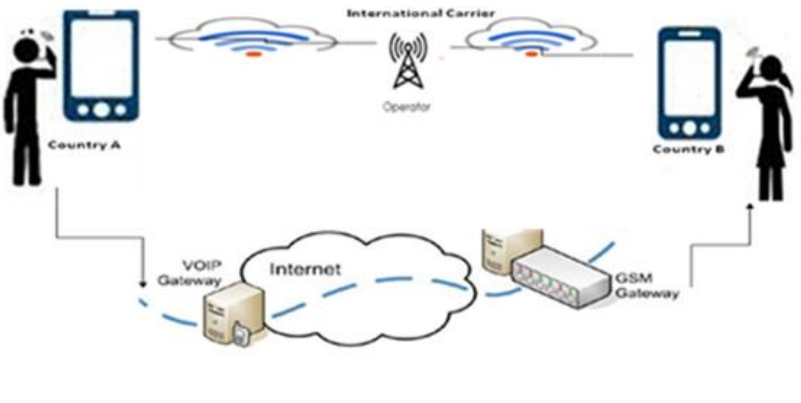

Fig 3. A unified Model of Bypass Structure

To further understand the framework of how bypass fraud is committed, firstly we describe the legitimate way for international calls. Assuming that mobile operator MO (Caller A) and MT (Caller B) live in different countries. Caller A makes a call to caller B over the mobile operator. The mobile operator of country A takes the call and sends it through his international gateways to carriers (Transit operators). The transit operator then routes the call through legitimate paths and pay a toll to transit operator for landing call to the destination address. When a call is routed through the legitimate path then transit operators and MT operator earns international charges for termination of the call. Basically in bypass fraud scenario fraudster abuse the international traffic and reroute the traffic illegally by using VOIP (Voice over internet protocol) through sim box.

V. Issues Associated with Interconnect Fraud

The major issue why Simbox fraud is hard to overcome is the fact that the use of prepaid SIM cards whose true owners (even when registered) and physical addresses are hard to trace compared to post-paid SIM cards that are only given to known customers after a thorough credit vetting exercise that often involves physical visits to customer premises/offices.

The second issue is the huge difference between the incoming international interconnect rates and the local tariffs that make the fraud very profitable. Telecom companies have aggressive packages and promotions in form of bundles and unlimited accesses to calls for a given period, mostly on the same network aimed at lowering the churn rates to attract new customers. These are the same packages that are exploited by fraudsters. Even conmen thrive partly because of these offers that give them unlimited access to on-net calls. The fraudsters are smart, technology aware and mask themselves to look like genuine customers.

However, global fraud experts agreed that the cause of simboxing is the differentials between international call rates and local rates which create opportunity for the fraudsters. International bypass fraud is a prolific and costly fraud in today's mobile industry [12]. Fraudsters take advantage of the rate differentials between international and local calls to profit from calls that should be billed by the local mobile operator at higher international rates but instead get billed at local "on-net" rates. Similarly, the global telecom company AT&T, agreed that, Simbox voice fraud occurs when the cost of terminating domestic or international calls exceeds the cost of a local mobile-to-mobile call in a particular region or country.

The impact is huge in terms of the loss in revenues to telecommunication companies and taxes to the government. It is estimated that Africa loses up to 150 million US dollars every year to interconnection frauds. Reports suggest that two years back Simbox fraud had brought in losses of 12 to 15 million minutes' worth of revenue to Kenyan government and operators, and about US$5.8 million to Ghana government [13].

The effects therefore are that telecommunication companies pay tax to the government based on the revenue they earn. For example, in Uganda, telecom companies pay 2% of all their gross revenue to the Uganda Communications commission. This means once their revenue is low, the amount paid to the regulator dwindles.

Another striking issue is the quality of calls that is very poor due to congestion of SIM cards on the same mast; calls fail to go through when the SIM cards are blocked by operators or when the SIM cards run out of airtime or packages. In addition, there are dropped calls when the SIM cards run out of airtime/benefits from the operators and customers are unable to call back in case of missed calls since the genuine caller's international number is not displayed.

A. Challenges Faced By Stakeholders

- *Revenue loss to Simboxing:* As mentioned earlier the issue of revenue loss to simboxing is a major challenge faced by cellular operators. Countries with little to no differential between international termination costs and local call rates, simboxing is non-existent, but in countries like Ghana, Rwanda and Tanzania where there is significant differential between the two rates, Simbox fraud exists as shown in Table 1.

Table 1: Effect of Arbitrage on Simboxing

Country	Intn'l Term Cost	Local Call Rate	Arbitrage	SIMBOX Fraud
Nigeria	$0.03	$0.07	-$0.04	No
South Africa	$0.04	$0.04	$0.00	No
Ghana	$0.19	$0.03	$0.16	Yes
Tanzania	$0.22	$0.03	$0.19	Yes
Rwanda	$0.22	$0.09	$0.13	Yes
Uganda	$0.26	$0.10	$0.16	Yes
Benin	$0.18	$0.12	$0.06	Yes

Source: [14].

If Ghana were to adopt an approach similar to countries like South Africa, probably the rise in international incoming traffic resulting from the cheaper rates would make up the loss from reduced rates. As Table 1 above demonstrates how removing the price differential removes the Simboxing opportunity.

- *Availability of Simboxes in open market*: Sim boxes are now available in several open markets including popular e-commerce platforms for less than $1000 per unit. To worsen this situation, Over-the-top (OTT) providers like Vibers are now explicitly selling their call termination capabilities to lure roaming customers to such bypass activities. In addition, the challenge now faced by OTT development is the recent Skype offering of free calls to mobiles and landlines in some advanced countries like the United States and Canada from India. These evolving trends convey the scale at which the SIM fraud is growing, calling for immediate action from telecommunication companies to safeguard their revenue streams. To surmount this challenge, employing measures such as active detection by making test calls that help the service provider detect SIMboxes and use of external vendor like LATRO Systems to locate and disable SIMBOX operations.

➢ *Avoidance of Sim blocking:* One serious challenge is the avoidance of Sim blocking. Every attempt to improve detection technology, fraudsters develops their method to avoid detection and increase profit. Some of the methods used by fraudsters to avoid SIM blocking includes but not limited to [15].

a) Human Behavior Simulation (HBS): According to literature, some features can be used to identify SIMbox fraud, for example: The SIMbox is static; most calls are outgoing calls; no usage of network services like SMS, GPRS; and others. However, smart SIMboxes are designed to mimic the behavior of normal customers by using Human Behavior Simulation (HBS). This technique makes detection of fraudsters very difficult if no advanced detection algorithms were used. HBS encompasses the following:

i) *Migration of SIM:* Fraudsters are deploying many gateways in different locations, for instance, some in crowded places, shopping malls or one in the city center and once in a while they swap the SIM cards between the gateways, so it would look like the user is on move. The swapping operation could be done manually or automatically using software. The strategy of implementing geo-location solution will expose the location of the equipment and their operators for confiscation and prosecution

ii) *Lists of Family:* Conventional SIMboxes reroute the call from voice-over-internet protocol (VoIP) to the global system for mobile communication (GSM) network, so they make calls to large numbers of different network customers. The use of family lists is a smart way to avoid this, where each SIM is assigned to reroute calls to a specific list of numbers, the detection of large different numbers could be avoided.

iii) *Other Network Services Usage:* The use of SIMboxes using voice services 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.

iv) *Rotation of SIM:* The detection of SIMboxes can be easy if fraudsters operate their SIMs excessively around the time of work, so they limit their usage by rotation of the SIMs as workers shifts. This will make SIMs operate in limited hours a day, which simulates the behavior of ordinary customers. To mitigate this passive detection is employed using an analytical system such as FraudBuster. This analytical system has intelligent algorithms that are able to identify if the call behavior is from a SIMBOX or not.

b) *Anti-Spam:* Test Call generation (TCG) is one of the effective ways to detect SIMs used in SIMboxes, by using different routes to known local network numbers. The incoming call will appear weather it is from an international number or from a local number; if it was from a local number then it must be associated with some SIM card used in a SIMbox and easily processed by the fraud department. Moreover, the fraudsters analyze the voice call traffic coming toward their SIMboxes and based on usage and other patterns they could determine whether the calls were real subscriber calls or were originated from a TCG system. They could then either block the test calls and prevent them from reaching the SIM box, or reroute the calls to a legitimate route so as to avoid detection.

From the forgoing, the challenges are quiet enormous, as advanced measures must be taken to tackle this problem. In this work, we proffer a unified solution to surmount these challenges.

B. The Way Forward And Solution

Globally, 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 these frauds. IP interconnection services are treated as legal in a few countries whereas they are banned in other countries due to the regulatory issues associated with such activities. For example, the Ghanaian government has declared SIM boxes illegal and made several arrests in this regard.

The recent developments around Sim-box fraud have 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 are becoming ineffective in dealing with modern SIM box strategies due to the latency and false positives associated with those methods.

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. 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.

VI. Recommendation

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.

VII. Conclusion

This paper presented that with the development of telecommunication and technology, and the big size of telecom market that found very attractive to fraudsters, traditional types of fraud has been replaced with more complex ways of frauds known as bypass fraud. This research focused on Simbox fraud that occurs when international traffic that should be routed through a legitimate international gateway is routed by VOIP (Voice over internet protocol) technique to bypass those gateways and is terminated via SIMboxes as local calls, in which the scenario requires that the fraudsters have access to advanced technology, capable of making international calls appear to be cheaper. Simboxing framework, how it works and issues associated with the fraud were discussed. We identified that SIM box bypass fraud has become a challenging threat to telecom companies in some parts of Africa and Asia. In concluding, we noted that the recent developments around Sim-box fraud have further aggravated the challenges faced by telecoms. With no scope for regulatory remediation, the way forward for them is to prevent these attacks using advanced technologies. The approach should build the capabilities of the traditional models that integrate the advancements in artificial intelligence.

Acknowledgements

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

References

[1]. http://www.cfca.org/fraudlosssurvey Communication Fraud Control Association, Global Fraud Loss Survey [Internet]. 2015 [cited 2016 Dec 3] (Telecom Industry Report, 2015).

[2]. J. C. Ogbulezie, M. U Onu., J. O. Ushie and B. E Usibe, "Propagation models for GSM 900 and 1800 MHZ for Enugu, Nigeria" Network and communication technologies, Vol.2, No.2

[3]. C. Emeruwa, "Comparative Analysis of Signal Strenght of Some Cellular Networks in Umauahia Eastern Nigeria". Journal of Electronics and communication Engineering Research. Volume 2.

[4]. H. E. Abdikarim, S.Ibrahim and R. Sallehuddin, "Detecting SIM Box Fraud Using Neural Network", Springer Science+Business Media Dordrecht 2013

[5]. C. Hilas and P. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection", Knowl Based Syst 21(7):721–726

[6]. M. Taniguchi, M. Haft, J. Hollmen and V. Tresp, "Fraud detection in communications networks using neural and probabilistic methods". In: Proceedings of the 1998 IEEE international conference on acoustics speech and signal processing, vol 2. IEEE, Los Alamitos, pp 1241–1244

[7]. N. L Azgomi, "A taxonomy of frauds and fraud detection techniques". In: Proceedings of *CISTM 2009*, Ghaziabad, India, pp 256–267.

[8]. R. S. A Elmi and H. S. Ibrahim, "Detecting SIM Box Fraud Using Neural Network", IT Converg. Security. vol. 215, pp. 575–582, 2013.

[9]. R., S. Sallehuddin, A. Ibrahim, M. Zain, and A. H. Elmi, "Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network", Int. J. Innov. Comput., vol. 4, no. 2, pp. 19–27, 2014.

[10]. I, M. Murynets, R. P. Zabarankin, and A. Panagia (2014), "Analysis and detection of SIMbox fraud in mobility networks," Proc. - *IEEE INFOCOM*, pp. 1519–1526, 2014.

[11]. B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor, "Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge", USENIX Secur. Symp. 2015, pp. 833–848, 2015.

[12]. Latro Enterprise Report, 2018

[13]. U. Neeraj, Digital Marketing for Sabex. Product marketing magazine for revenue Assurance and Fraud. 2018.
[14]. MTN, Global Fraud Loss Survey Report, 2017.
[15]. I. Ibrahim and S.H, Mohamed, Bypass Fraud Detection: AI Approach, Journal of Uni. of Benghazi, 2015.