Statistical Insights and Fraud Techniques for Telecommunications Sector in Egypt

Ahmed A. Mawgoud
Department of Technical Affairs
National Telecommunications Regulatory Authority
Cairo, Egypt
aabdelmawgoud@tra.gov.eg

Ibrahim Ali
Department of Technical Affairs
National Telecommunications Regulatory Authority
Cairo, Egypt
iramadan@tra.gov.eg

***Abstract*— National Telecommunications Regulatory Authority (NTRA) has investigated the telecommunication performance in the service providers in Egypt between the periods of February 2018 till February 2019. Fraud is a multi-billions pounds' problem around the world. The problem is the huge financial loss of revenue that can affect the trustworthiness and performance of the telecommunication corporate. Egypt is one of the developing countries that are witnessing a rapid-growth development in its telecommunications infrastructure. As a result of the increment rate of corporate and internet users, fraudsters are exploiting the vulnerabilities to gain illegal revenue through the subscribers. The telecommunications sector in Egypt has suffered in the last two decades from different types of telecom fraud cases which have damaged the financial sector in both telecommunication side and governmental side. In this paper, we present:**

a) Statistical insights on users, mobile operators and Internet companies for the telecommunications sector in Egypt in 2018/2019.

b) An illustration for the common fraudulent methodologies that are used against both users and telecom operators in Egypt.

c) A discussion on the consequences of fraud cases with a suggested framework as a proactive methodology to prevent the escalated threat of telecom fraud.

Keywords*— *Statistical insights, Fraud Prevention, Fraud Detection, Telecommunication, Egypt

I. INTRODUCTION

The rapid growth rate of technology and internet in telecommunication industry led to the appearance of new fraud techniques that cause serious damage for both mobile operators and subscribers worldwide. Fraud cases have always been a huge concern in the telecommunications sector. In Egypt, due to the growth of internet infrastructure and mobile industry in the last decade, the subscribers start having more control and access to the network and the applications. As a result, the rate of fraud against subscribers and mobile operators has increased rapidly because of the new methods and vulnerabilities appeared by the passing time [1]. Telecom frauds impact the telecommunication industry negatively on both the quality of service part and the financial one. Some of the fraud negative consequences can be avoided. On the contrary, there are certain type of fraud in which they occurred they cause a severe impact on the infrastructure for both internet service provider and mobile operators [2]. As an example, fraudsters seize intentionally the high trust level that the subscribe have in Calling Line Identification (CLI) to commit fraud during calls by spoofing legal numbers; in order to extract personal information, bank account (debit cards - credit cards). Regularly, those cases occurred in an automated environment and mostly in developing countries with weak authorities; as fraudsters knows that it will be difficult for any party to detect their actions or prevent their damages [3]. International Revenue Share Fraud (IRSF), it is a type of telecom fraud that is considered as one of the top ranked type fraud technique in which the fraudster generates calls to specific ranges of national numbers in various countries [4].

The Communications Fraud Control Association (CFCA) released a report in 2017, it estimates the overall loss from the International Revenue Share Fraud to be US$6.1 billion that is considered more than 40% of the second ranked type (Interconnect Bypass). CFCA report also ranked the top five countries worldwide that originate fraudulent calls which are (United States, Spain, UK, Russia and Palestine). It also shows a decrement in global telecom fraud by 24% in 2017 report compared to 2015 survey (from over $39 billion to $30.1 billion) [5]. However, the rate of complaints from the mobile operators to the national regulatory increase each year, as a result the problem of the telecom fraud should be addressed as a priority to prevent the resultant loss of those illegal operations.

Each year, the financial field suffers from escalated risks of different fraud schemes that are committed by fraudsters against both mobile operators and information technology sectors. Thus, this should be faced with proactive procedures to detect and prevent the damages of each committed fraud technique [6]. This paper introduces yearly users' statistics in telecommunication sector in Egypt; as an initial study for a future solution for the telecom fraud techniques that represent challenges in the Egyptian telecommunications sector in specific and the MENA region in general.

This paper is organized as following. Section 3 represents statistical insights for Egyptian telecommunications sector:

1. Mobile devices.
2. Internet Users.
3. Established IT Companies.
4. Internet Subscribers Geographical Distribution.

Section 4 presents four different types of telecom fraud types with an illustration of the technique for each one's. Section 5 is a discussion on the suggested solutions to detect and trace the fraudsters in the telecommunications sector along with the proactive methodologies to face the escalated challenges for possible new types of fraud [7].

Table 1 shows the acronyms list that are used in the paper.

978-1-7281-4801-4/20/$31.00 ©2020 IEEE

TABLE I. LIST OF ACRONYMS

Acronym	Meaning
SIP	Session Initiation Protocol
CDR	Call Detail Record
NTRA	National Telecoms Regulatory Authority
ISP	Internet Service Provider
PRS	Premium Rate Service
CFCA	Communications Fraud Control Association
PBX	Private Branch Exchange
USB	Universal Serial Bus

II. LITERATURE REVIEW

Telecommunication fraud is an international active international concern, several studies use both artificial intelligence and data mining to prevent various types of telecom fraud. Mainly, there are three main categories of telecom fraud:

1- *Telecom service provider fraud system:* it is the most complicated scheme as it has the ability it exploits the telecom service provider using traffic redirecting, SIP and regulatory loopholes [8].
2- *Subscribers' fraud:* it is a category where the fraudsters gain control over the subscribers' account to make free phone calls [9].
3- *Conducted over the Telephone:* this category covers all general types of known fraud schemes [10].

In [11], the result shows the deep impact of using data mining techniques for high accuracy detection level of cloning telecom fraud, this is achieved by using rule generation techniques. Researchers in [12] introduced a voting scheme from three classifiers to detect fraud on the subscribers' account, they concluded that the voting scheme has an accuracy level higher than individual classifiers, which is considered to be suitable for business cases where the cost of misclassification high rate on the subscribers and thus affect the process of decision-making; as the voting scheme provides high accuracy in prediction process in order to take the required decision. In [13], the researchers have presented many combined techniques of data mining techniques, which was considered as a strong approach for detecting and preventing subscription fraud in mobile telecommunication. The authors in [14] used a Naïve Bayesian network method to develop a subscription fraud detection system that was based on probability and statistics, their results have approved the efficiency of Naïve Bayes algorithm as it showed smartness in dealing with various types of data and providing a high accurate classification. The researchers in [15] have worked on a real-time approach to analyze subscribers' call behaviors and detect suspicious behavior based on previously imported CDR Dataset. This dataset is continuously updated which is followed by a change of the new data coming from the call stream constantly. In [16], researchers in their experiment used a rule-based approach to build a fraud telecommunication detection system, this approach needs fine-tuning of distinct levels to avoid false alarms.

III. STATISTICAL INSIGHTS FOR EGYPTIAN TELECOMMUNICATIONS SECTOR

In Egypt, the telecom regulatory authority gathers a fixed set of data from the mobile operators monthly to ensure the applied policies and analyze the given data for suspicious illegal behavior. In a study that was made by NTRA between February 2018 and February 2019, studying the relation between the mobile subscribers and mobile devices is important to come out with analysis of the subscription growth rate and the escalated threats behind this growth. As shown in figure 1, the rate of mobile devices is higher than the subscribers in both 2018 and 2019 with about 2%. The yearly growth rate of subscribers' in Egypt is 7% yearly, while the mobile devices' growth rate is 9.58%.

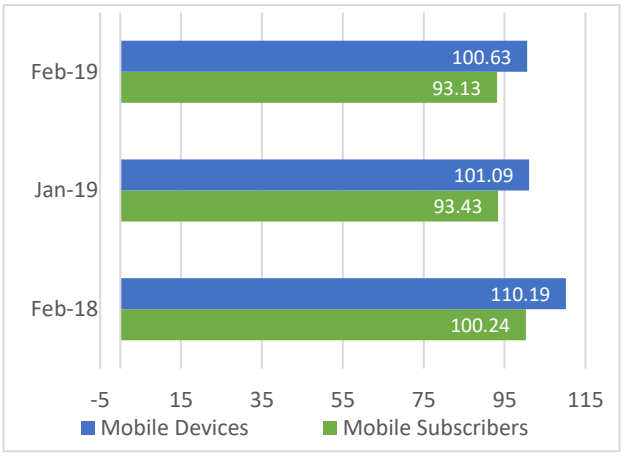

Fig. 1. Mobile Subscribers Vs Mobile devices statistics in Egypt 2018 vs 2019

Figure 2 below, show the number of internet subscribers –by millions- from the internet service providers ISP in Egypt whether from using mobile phones or USB modems.

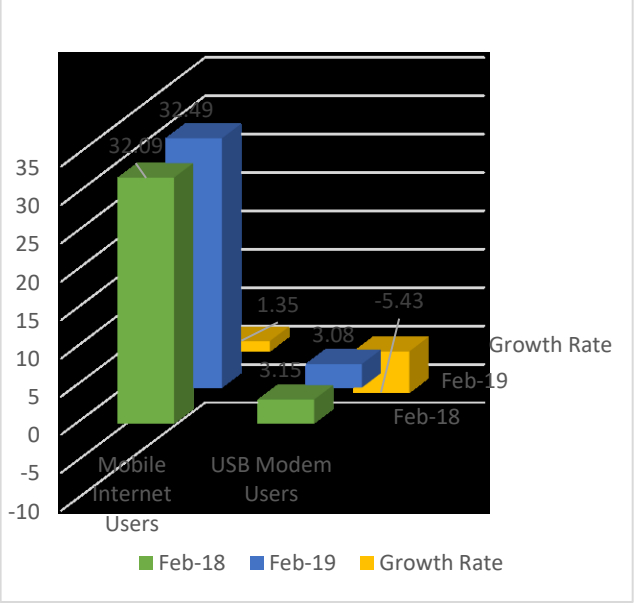

Fig. 2. Internet users in Egyptian mobile operators 2018 / 2019

Egypt is considered as one of the highest countries in MENA region that is threatened with cyber-attacks due to

its high population and developing telecom infrastructures. As shown from above that the increment rate of subscribers with mobile devices has increased with 1.35% yearly. On the contrary, there was a decrement of the users with USB modem by -5.43%, which makes the mobile devices at high risk to fraud process [17]. The increasing of internet users in Egypt are because of two reasons, the first one is the high rate of population growth in the last forty years, while the second one is the development of telecom infrastructure and network technology. In figure 3, a representation of internet subscribers' geographical distribution in Egypt, as it shows that Cairo the capital is the highest rank with 39% while Sinai is the lowest one with only 6%.

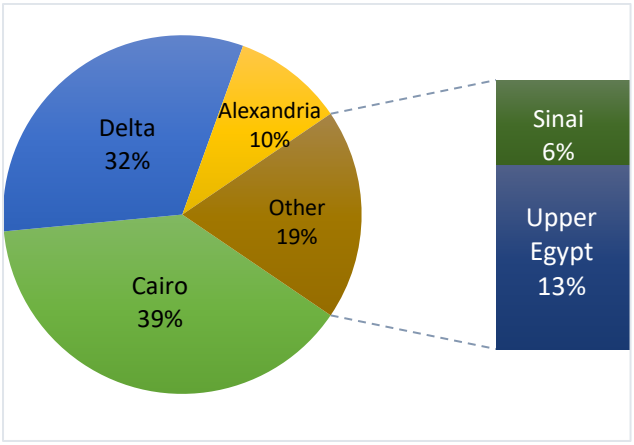

Fig. 3. Geographical distribution of Internet subscribers in Egypt 2019

Although, landline phones are not as vulnerable as the mobile phone, but it still threatens with scams and illegal phone calls known with PRS. Figure 4 represents the relation between central capacities and landline users in Egypt. Additionally, figure 5 shows that the highest percentage of landline subscribers are from home users 86% while government spends around 3% from the overall subscribers.

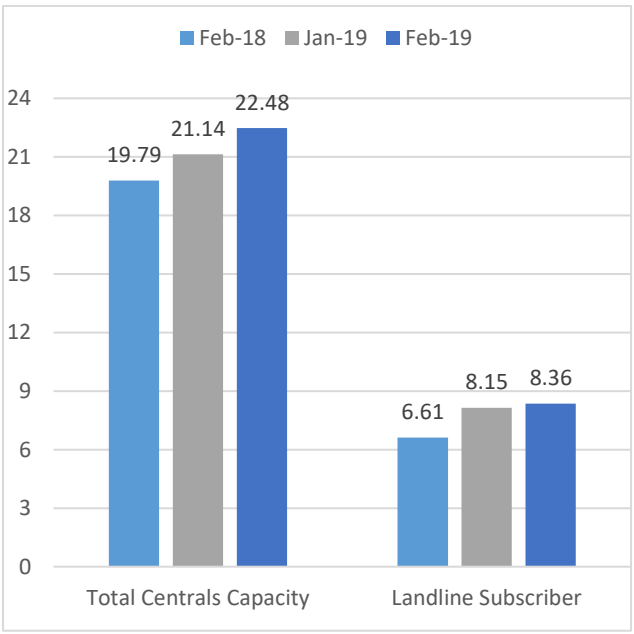

Fig. 4. Landlines & Centrals Statistics in Egypt 2018/2019

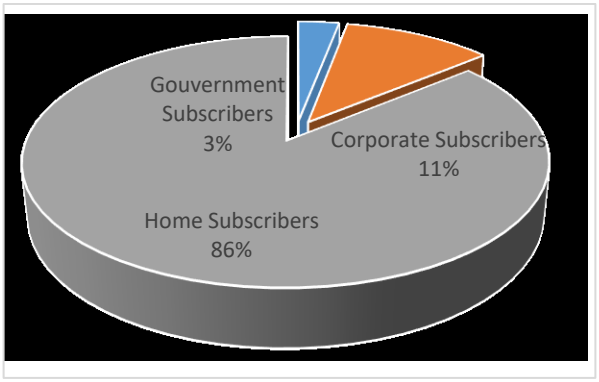

Fig. 5. Landlines Subscribers Types

The overall yearly investment in telecommunication sector worldwide can be described as a toxic rate growth. However, as shown in figure 6, illustrates the newly investments last year in Egypt in telecom industry with millions, the majority of share capital went to the information technology infrastructure with a growth rate 78% than the year before, while it is obvious that information system sector is suffering from decrement rate with 33%.

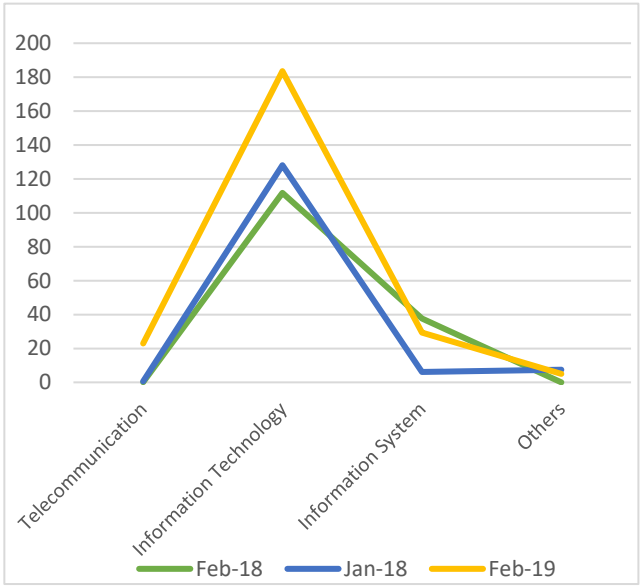

Fig. 6. Share capitals for newly established telecom companies in Egypt 2018/2019

Surprisingly, the newly invested companies in telecom industry was not established in the capital Cairo, but the majority went to Upper Egypt as shown in figure 7 below, Giza and Menoufia had the highest investment between Feb-18 to Feb-19 with newly constructed 9 companies, Upper Egypt cities combined had witnessed the launch of new twenty-five companies.

However, this is not enough to supporting the Telecom sector rates in the Egyptian stock exchange in 2018/2019 as it was affected with a negative rate -83%.

Figure 8 illustrates this drop in the Egyptian stock with points.

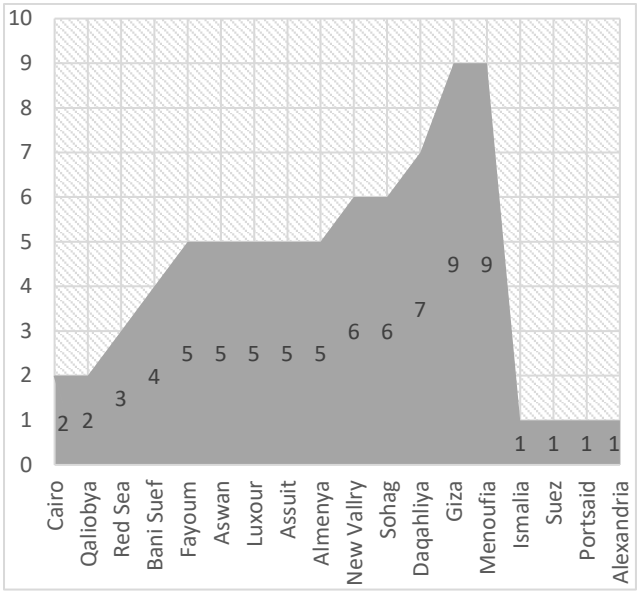

Fig. 7. Geographical distribution of new constructed companies in telecom sector Feb 2018 – Feb 2019

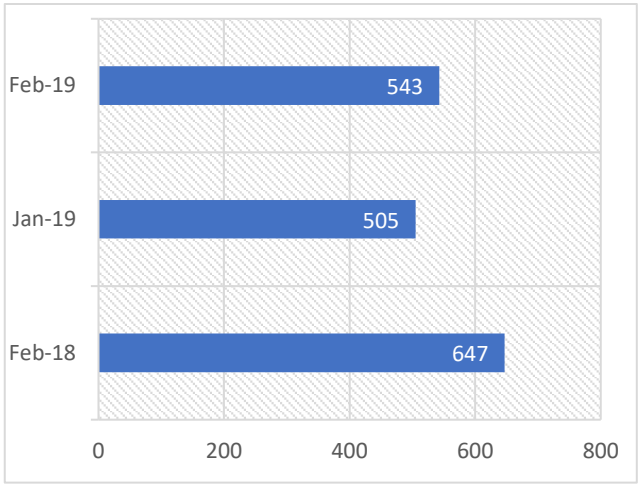

Fig. 8. Telecom sector rates in the Egyptian stock exchange

IV. Telecom Fraud and Miuses Techniques

Telecommunication fraud is the use of subscribers, mobile operators or government's products or services with the intention of gaining illegal money. Telecommunications service providers are mostly defenseless against telecom fraud. Fraudsters are able to manipulate telecom regulations to their benefits and against the telecom service provider, with complex techniques that are difficult to identify, trace or even judge. In Egypt, most of the mobile operators took proactive steps to detect and prevent the damages -of various fraud techniques alongside with the regulatory authority- to reduce both reputation and financial damages [18]. Some of the fraud incidents information are usually kept confidential due to the national security and the actual loss are never announced.

According to CFCA survey in 2011, a private sector was initiated to minimize the risk of frauds against the carriers [19]. Table 1 shows the resultant financial loss caused by the top five common fraud types in telecommunication industry worldwide in billions.

TABLE II. Top Fraud Cases Reported to CFCA in 2011

#	Fraud Technique	Financial Loss
1	International Revenue Share Fraud	$3.73 Billion
2	Credit Card Fraud	$2.30 Billion
3	Compromised PBX/Voicemail	$4.85 Billion
4	By-pass Fraud	$2.72 Billion
5	Subscription/Identity Theft	$4.21 Billion

Telecommunications industry turns into more of a commercial services and value added services such as mobile money transfers and payment, the cross-industry experience turns out to be more valuable. In the beginning of telecommunications industry, fraud management in telecommunications was fresh and undeveloped. Yet we witness that immaturity today in developing countries where they have little gratitude for credit checks and whether a subscriber is likely to provide revenue for telecom operators. There are multiple convincing reasons for the co-operations between both banking and telecommunication sector and share intelligence. In some cases, in the market it's quite challenging to bring the clients of both sectors together, as both sides are suspicious that the other will steal its subscribers.

Many countries –specially the developing ones- suffer from high rate of telecom fraud. Different types of fraud cases were mainly developed to steal both data money and money from the subscribers, which h leads to lower the trust of the telecom service provider. With the rise of financial inclusion and mobile wallets, the fraud cases have increased in the last decade, this led to the need to come out with pro-active methods to face such threats. Figure 9 below provides the rate of formal financial usage in world countries by population number.

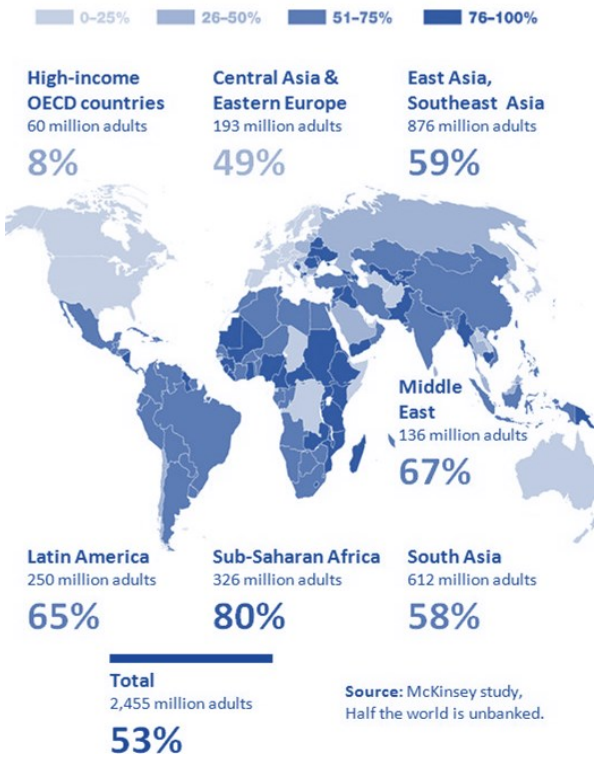

Fig. 9. Percentage of adult population worldwide that do not use formal banking financial services

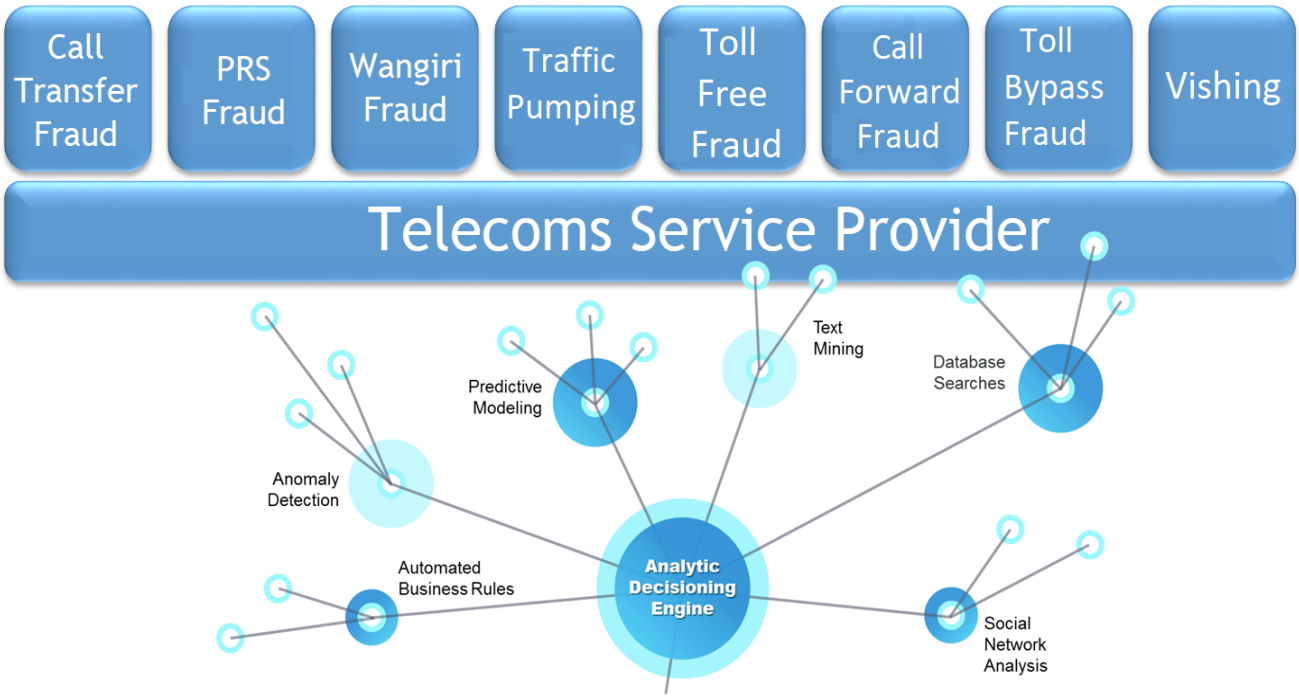

Fig. 10. Fraud methods in telecoms sectors with analytic decision techniques (TM Forum 2015)

Figure 10 above illustrates various common fraud incidents occurs in telecoms service provider and the followed analytic engines used in worldwide telecom operator (i.e. Text Mining, Anomaly Detection, Social Network Analysis, Automated Business Rules and Database Services).

A. Call Transfer

It is a common type of telecom fraud that represents a huge concern for soft switch consumers. In this type, the fraudster attacks the PBX to use its services for making free international calls. This can be done through initiating the compromised PBX to transfer the call to the fraudster's own phone service, then the fraudster uses the phone service of ordinary subscriber –who is considered as a victim- to make calls to international locations using the hacked soft switch. As a result, the operator cannot bill the subscriber as the fraudsters should be detected and prevented by the force of the law [20]. Figure 11 below illustrates in a work flow how the hacker can use the PBX to bypass international calls illegally through the soft switch.

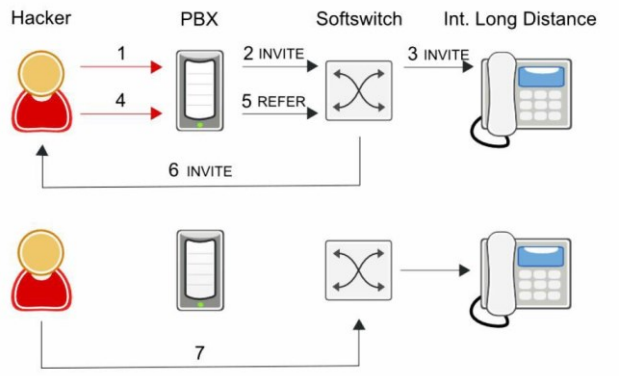

Fig. 11. Call transfer use case scenario

Call Transfer Technique:

The fraudster's phone service exploits unsuspicious PBX to make an international call, then the PBX sends SIP request to the soft switch. Subsequently, the soft switch routs the call request to the international carrier. Fraudster reconfigure the PBX to blind transfer call to fraudster phone service, then the PBX sends SIP permission to the soft switch to blind transfer the call to the fraudster phone service and the soft switch opens a session to send an SIP REFER transfer call to the fraudster phone service. Fraudster's subscriber makes the call to long distance location through soft switch. Once the call is transferred out of the network range, it is nearly impossible to be tracked by most of soft switches. As a result, the fraudsters are only having limited amount of both revenue and traffic before the mobile operators detect any suspicious event in their network.

B. False Answer Supervision

Fraudsters use false answer supervision to gain revenue through billing the subscribers with false answer supervision; as there is no existence for a connection between the caller and the called party. This technique is preferable by fraudsters to direct the call into a completed call in order to bill the caller and share a rate from the revenue. This type of technique damages the service provider or the operator with both reputation part and financial part [21].

Figure 12, it illustrates the method in which the fraudster can manipulate the call routing destination from the normal route to a pre-configured destination; this is mainly done to gain illegal revenue through forcing the subscriber to pay a higher rate than the normal one and transfer the rate differences to the fraudster account.

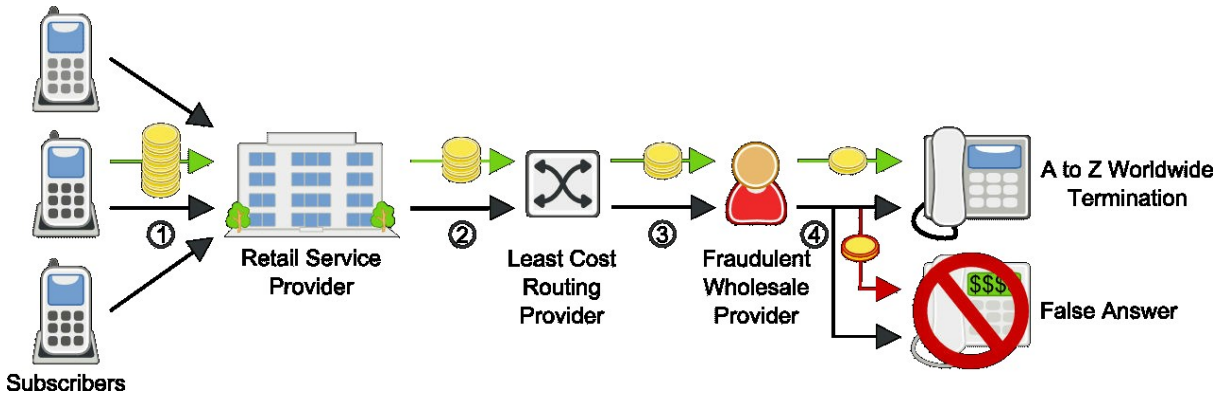

Fig. 12. False answer supervision use case scenario

False Answer Supervision Technique:

Subscribers start making a normal call, then the service provider starts routing the call to the lowest cost provider (third party), after that the third party routes the call to another provides that shows good rates according to the general cost of the destination place and completes the call. However, in the false answer supervision the call is being routed to a high cost destination with a false answer. Then the subscriber will be automatically charged for a complete call –even if the call did not complete-.

C. Premium Rate Service (PRS)

Premium rate service has existed for a long time in telecommunication industry worldwide as part of the business. The charge rate of this number is higher than the normal rate; as the revenue of the PRS calls is shared between the fraudster and the service provider in countries that do not have legal rule to regulate such services. However, PRS is easy to exploit in fraud cases; as the paid money represents a tough incentive to push traffic to a phone number. Furthermore, traffic pumping is a technique that the fraudsters use illegally to push high traffic to their premium rate number [22].

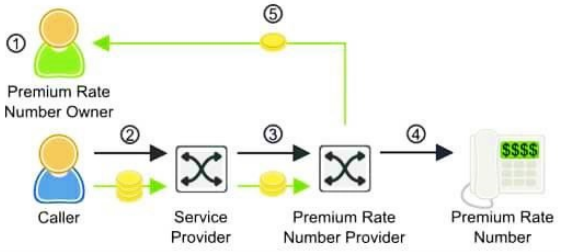

Fig. 13. Premium rate service (PRS) use case scenario

PRS Fraud Technique:

The owner of the premium rate number starts marketing illegally for the presented services to the telecom subscribers through (SMS, mail, notification…etc.), then the subscriber assigns the call to a premium rate number. Finally, the call is terminated by the Premium Rate Number provider to an IVR system.

1- The subscriber is charged with a premium rate (Extra fees than usual).
2- The operator pays the Premium Rate Number provider from the subscriber.
3- The provider of the Premium Rate Number pays a rate of the revenue to the number owner.

D. Wangiri Fraud

Wangiri is a Japanese definition that means (one and cut), which means one ring and cut off the call. This scheme of telecom fraud depends on a single ring method as a quick approach for making money. Fraudsters usually setup an application to the computer and randomly call a wide range of numbers with just one ring; to make the subscriber re-call that number again [23].

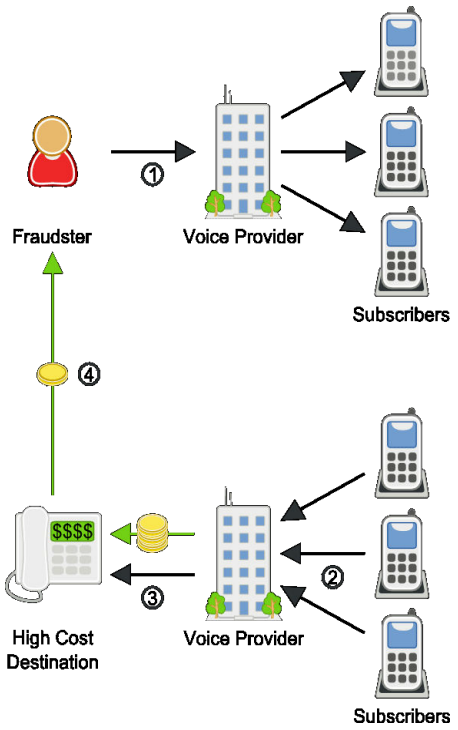

Fig. 14. Wangiri use case scenario

Wangiri Fraud Technique:

The fraudster set up call for a wide range of random numbers then hangs up after one ring. It is a method for illegally charge the subscriber with high cost destinations when he/she calls back. However, when the subscriber sees the missed call from the strange number on the phone, then the subscriber call back without knowing the actual cost of the destination. The fraudster gains his/her illegal money

through sharing the revenue from the subscribers' calls with the telecom operator.

Wangiri fraud is a Japanese word that means 'one ring and drop'. Calls regularly cut off just as the phone rings, leaving a missed call message from a global or unknown number.

V. Discussion

The properties of the telecommunication industry in Egypt was presented through statistics alongside with the common fraud techniques. In the last five years the financial damages occurred -to both governmental sector and mobile operators- are estimated by hundreds of million in the last decade [24]. Illegal bypass is the most important challenge. It is a fraud act to bypass licensed carriers through terminating international calls to the networks using unlicensed operators. The technique is to send calls through the internet to SIM boxes that redirects the illegal VoIP traffic. However, the systems usually take time to become effective in classifying the illegal calls and blacklisting them. As a result, there is need for using effective methodologies as a proactive method to prevent fraudsters operations against telecommunication sectors.

Data Mining Techniques are having wide usage in network systems, especially when it comes to huge amount of data in many fields (i.e. banking, healthcare, and telecommunications). Data mining can be very useful to trace the subscribers' call logs from the sender to the destination is a need to detect illegal network traffic to prevent suspicious behaviors against subscribers.

Figure 15 shows review a work flow to prevent telecommunications' different types of fraud through data mining methods with the following steps (classification – clustering - outlier detection - prediction and visualization) that allows the detection and prevention of frauds.

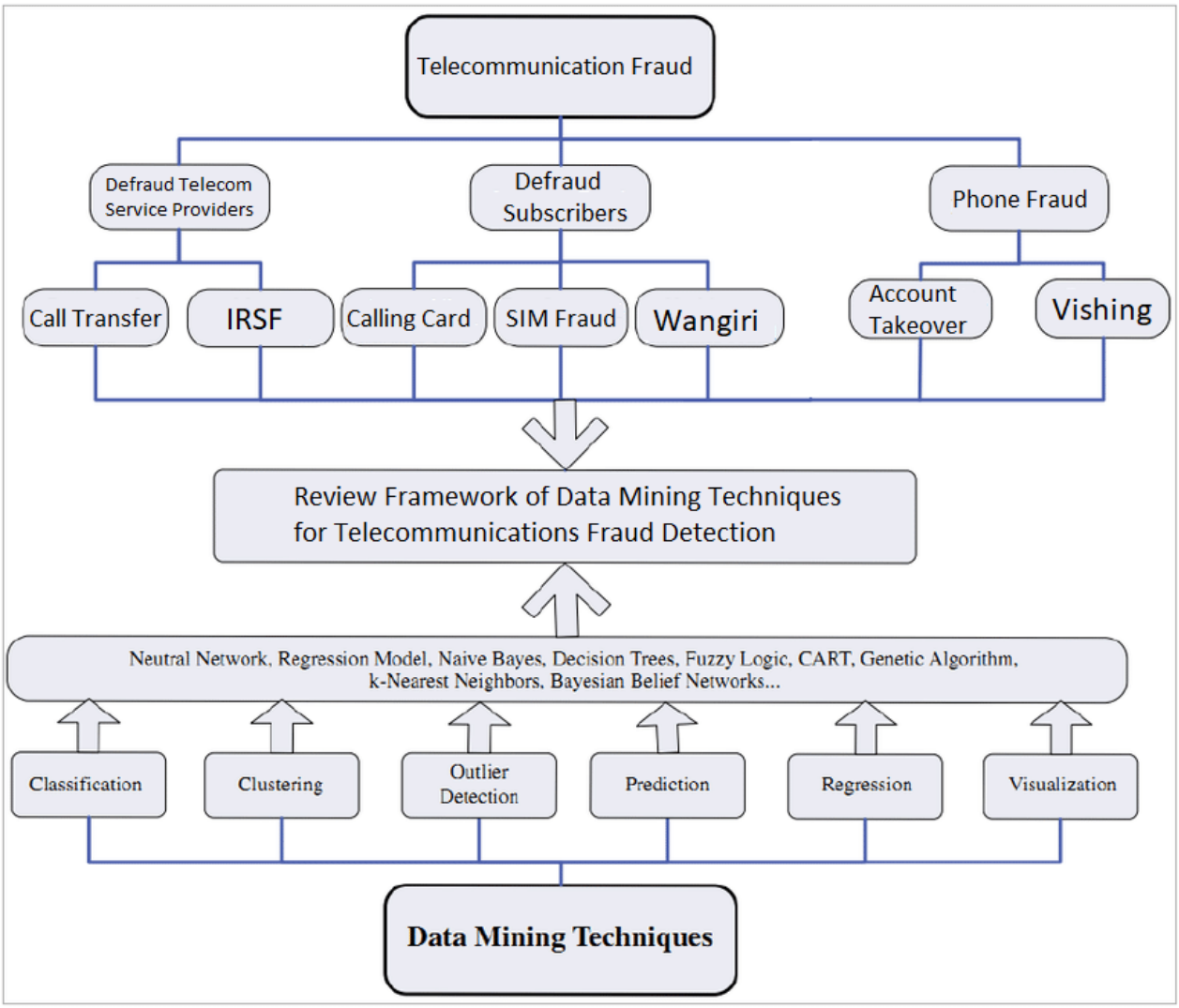

Fig. 15. Review framework of data mining methods for telecommunications fraud detection

From the figure above, an unbalanced data set is categorized by an uneven class distribution where the total of fraudulent cases (positive) is significantly lesser than the total normal cases (negative). This will affect the classifier that is most likely to categorize data has fitting to the normal case then to the fraud case. At first, a general examination is created based on the data features and the Naive Bayes model, which is the classifier chose to do the irregularity detection on those tests. After the features are presented, a character engineering phase is done with the determination to expand the data contained in the data generating a deeper relation with the data itself and model features. Previously proposed techniques that consist of sampling the most copious class (normal) before testing it. Finally, the future

work depends on studying the effects of altering the essential class distribution constraint in the Naive Bayes model and estimate its performance. The second suggested model is to estimate margin values the in case it is applied to the model output, assist to carry more positive samples from earlier negative classification. Most of the suggested data mining methodologies in telecommunications fraud are mainly validated over a monte-carlo test, using the dataset with and without the engineered features.

VI. Conclusion

In conclusion, telecommunications regulatory systems are developing their policies to face the escalating threats of fraud techniques against telecom sector, those techniques are hard to detect, trace and prevent. However, most of the telecom fraud cases occur in a time when the monitoring from the operators at its lowest level.

In this paper, we have provided statistics about the telecoms sector in Egypt in 2018/2019; to give a full image about the possible threats from the fraudsters in telecom industry. Then the most common fraud cases in Egypt were discussed with their techniques (Call Transfer - False Answer Supervision - Premium Rate Service - Wangiri Fraud). Data mining techniques are considered as operative solutions that proved its efficiency in other fraud sectors like financial sector.

References

[1] D. Olszewski, "Employing Kullback-Leibler divergence and Latent Dirichlet Allocation for fraud detection in telecommunications", Intelligent Data Analysis, vol. 16, no. 3, pp. 467-485, 2012. Available: 10.3233/ida-2012-0534.

[2] B. Cuttler, Media and telecommunication issues. New York: Nova Science Publishers, 2011.

[3] G. Stevenson, "Computer Fraud: Detection and Prevention", Computer Fraud & Security, vol. 2000, no. 11, pp. 13-15, 2000. Available: 10.1016/s1361-3723(00)11018-8.

[4] A. Rozenas, "Detecting Election Fraud from Irregularities in Vote-Share Distributions", SSRN Electronic Journal, 2017. Available: 10.2139/ssrn.2934485.

[5] Vanillaplus.com, 2011. [Online]. Available: https://www.vanillaplus.com/wp-content/uploads/2015/03/global-fraud_loss_survey2013.pdf. [Accessed: 09- Aug- 2019].

[6] D. Forte, "Electronic voting: practicality vs. fraud", Computer Fraud & Security, vol. 2009, no. 7, pp. 7-9, 2009. Available: 10.1016/s1361-3723(09)70085-5.

[7] "Fraud management solution that detects analyses and prevents fraud", Panamax Inc, 2019. [Online]. Available: https://www.panamaxil.com/fraud-management. [Accessed: 08- Mar- 2019].

[8] www2.deloitte.com, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-advisory-data-synthesis-In-fraud-detection-for-tsp.pdf. [Accessed: 16- Jun- 2019].

[9] F. Goncalves and B. Iancu, Building Telephony Systems with OpenSIPS - Second Edition. Birmingham: Packt Publishing, Limited, 2016.

[10] C. Pollard, "Telecom fraud: the cost of doing nothing just went up", Network Security, vol. 2005, no. 2, pp. 17-19, 2005. Available: 10.1016/s1353-4858(05)00202-3.

[11] K. Kurien and D. Chikkamannur, "A Survey of Methodaology of Fraud Detection Using Data Mining", International Journal of Trend in Scientific Research and Development, vol. -1, no. -6, pp. 38-42, 2017. Available: 10.31142/ijtsrd2482.

[12] D. Forte, "Electronic voting: practicality vs. fraud", Computer Fraud & Security, vol. 2009, no. 7, pp. 7-9, 2009. Available: 10.1016/s1361-3723(09)70085-5.

[13] R. Bhowmik, "Data Mining Techniques in Fraud Detection", Journal of Digital Forensics, Security and Law, 2008. Available: 10.15394/jdfsl.2008.1040.

[14] M. Flores, J. Gámez and A. Martínez, "Domains of competence of the semi-naive Bayesian network classifiers", Information Sciences, vol. 260, pp. 120-148, 2014. Available: 10.1016/j.ins.2013.10.007.

[15] F. Yousaf, M. Liebsch, A. Maeder and S. Schmid, "Mobile CDN enhancements for QoE-improved content delivery in mobile operator networks", IEEE Network, vol. 27, no. 2, pp. 14-21, 2013. Available: 10.1109/mnet.2013.6485091.

[16] V. Jain, "Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining", International Journal of Information Technology, vol. 9, no. 3, pp. 303-310, 2017. Available: 10.1007/s41870-017-0036-5.

[17] A. A. Mawgoud, M. Hamed N. Taha, N. El Deen M. Khalifa and M. Loey, "Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures", in *International Conference on Advanced Intelligent Systems and Informatics*, Cairo, Egypt, 2019, pp. 912-921.

[18] Trustonic. (2019). Revenue Protection for MNOs & MVNOs, Mobile Fraud & Theft Prevention. [online] Available at: http://www.trustonic.com/solutions/asset-lifecycle-protection-service-for-mobile-operators/ [Accessed 6 Jul. 2019].

[19] PrivSec Report. (2019). Telecommunications: the battle against fraud - PrivSec Report. [online] Available at: https://gdpr.report/news/2017/05/29/telecommunications-battle-fraud/ [Accessed 6 May 2019].

[20] Technical Assistance Center. (2019). PBX Fraud: Stay Informed Against Fraudulent Calls. [online] Available at: https://assist.voxox.com/hc/en-us/articles/200635875-PBX-Fraud-Stay-Informed-Against-Fraudulent-Calls [Accessed 5 Feb. 2019].

[21] Wiki.voip.ms. (2019). False Answer Supervision FAS - VoIP.ms Wiki. [online] Available at: https://wiki.voip.ms/article/False_Answer_Supervision_FAS [Accessed 7 Apr. 2019].

[22] Ofcom. (2019). Premium rate services (PRS). [online] Available at: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/premium-rate-services [Accessed 12 Aug. 2019].

[23] Harley, D. and Harley, D. (2019). Wangiri Telephone Fraud – One Ring to Scam Them All | WeLiveSecurity. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2014/02/10/wangiri-telephone-fraud-one-ring-to-scam-them-all/ [Accessed 1 Oct. 2019].

[24] V. Jain, "Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining", International Journal of Information Technology, vol. 9, no. 3, pp. 303-310, 2017. Available: 10.1007/s41870-017-0036-5.