POLICY FRAMEWORK TO STREAMLINE ILLEGAL INTERNATIONAL VOICE CALL TERMINATION

W.H. Madusanka Sampath Weerasinghe

(169232N)

Degree of Master of Science

Department of Electronic and Telecommunication Engineering

University of Moratuwa

Sri Lanka

October 2021

POLICY FRAMEWORK TO STREAMLINE ILLEGAL INTERNATIONAL VOICE CALL TERMINATION

W.H. Madusanka Sampath Weerasinghe

(169232N)

Thesis submitted in partial fulfillment of the requirements for the degree Master of Science in Telecommunications

Department of Electronic and Telecommunication Engineering

University of Moratuwa

Sri Lanka

October 2021

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant permission to University of Moratuwa, the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: Date:

The above candidate has carried out research for the Masters Dissertation under my supervision.

Name of the supervisor: Eng. A.T.L.K. Samarasinghe

Signature of the supervisor: Date:

ABSTRACT

Telecommunication service providers around the world lose billions of dollars annually due to various fraudulent activities. Illegal call termination, which is also know and SIMBox fraud and extreme IDD usage related to International Revenue Share Fraud (ISRF) are identified as two of most challenging telecommunication frauds prevalent in the world, which causes a considerable percentage of revenue loss. These fraudulent activities not only deteriorate the operator revenue but also it degrades the customer experience. This is considered as a national issue, due to which the country loses revenue as tax revenue loss and faces security concerns as these calls bypass lawful intercept systems. Having no common platform to address this issue is a problem prevailing in many countries. Therefore, as a solution for this, a common framework is proposed, where all the operators in a country can inter-work, with the proper intervention of regulatory body of the country.

The relevant work was reviewed with a literature survey and the gaps were identified. The drawbacks in the current process were identified via a census carried out among the mobile operators in the country and with a focus group discussion with the regulatory body. The different aspects for the framework were outlined by analyzing the data gathered and a centralized system for IDD fraudulent number tracking was designed where a proper coordination within the operators and the regulatory body can be achieved. ISRF related suspected number sharing mechanism was introduced using the common platform.

A common framework was established as the output, where identified issues can be minimized. The common framework consists of three major aspects. Establishing a centralized system for IFDD fraudulent number tracking, adding reforms to the existing regulations, and increasing user awareness are the three aspects covered with the proposed common framework. With the proposed centralized system and it is possible to achieve higher revenue and lower fraudulent activities within a country with an increased IDD call quality.

Keywords: IDD Bypass Fraud detection, Common framework, Telecommunication Regulatory Body

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the department of Electronics and Telecommunication, university of Moratuwa for providing me this opportunity to carry out this research. My immense gratitude goes to Eng. A. T. L. K. Samarasinghe, Senior Lecturer, Department of Electronic and Telecommunication Engineering for providing me the guidance and insights throughout the research.

Further I would like to thank the members from Telecommunication Regulatory Commission of Sri Lanka for the assistance in providing required information about the current regulations and issues. I am also extremely thankful to all the mobile operators in Sri Lanka for providing information about the fraud detection.

Finally, I would like to thank all the lecturers of department of university of Moratuwa, my wife and my family and my friends for the support extended throughout.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
ANN	Artificial Neuron Network
BTS	Base Transceiver Station
CDR	Call Detail Record
CEP	Complex Event Processing
CFCA	Communication Fraud Control Association
CLI	Caller Line Identification
CEIR	Central Equipment Identity Register
FMS	Fraud Management System
IDD	International Direct Dialing
GDP	Gross Domestic Product
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISRF	International Revenue Share Fraud
ITU	International Telecommunication Union
MLP	Multi-Layer Perception
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Director Number
MT	Mobile Terminated
PSTN	Public Switched Telephone Network
QOS	Quality of Service
RMSE	Root Mean Square Error
SBC	Session Border Controller
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TCG	Test Call Generation
TRCSL	Telecommunication Regulatory Commission of Sri Lanka
VoIP	Voice over IP protocol

1 INTRODUCTION

1.1 Background

Telecommunication industry plays a major role in distance communication and driving the nations towards technological advancement at large all over the world. While telecommunication industry has become one of the major income sources of a country, currently over 5.2 billion unique mobile subscribers are being served [1]. Mobile industry contributes 4.7% of the overall Gross Domestic Product(GDP) and it is in the increasing trend with the evolution of new technologies. However, operators around the world lose billions of dollars annually due to the fraudulent activities. According to Cyber-Telecom Crime Report 2019 by Trend Micro Research, Europol's European Cybercrime Centre, an estimated amount of 12 billion USD is lost to the operators around the world due to various frauds [2]. The percentage of revenue loss due to frauds is considerable to the operators, which minimizes the profits.

Illegal termination of International Direct Dialing (IDD) calls, which is also called as 'grey calls' is one of the major frauds prevailing in most of the countries, which causes degradation of service to the end user while reducing the profits to the operator. Abnormal usage scenario related to International Revenue Share Fraud (ISRF),[3] is another phenomenon, where customer generates abnormal call patterns due to fraudulent activities. Fraud detection algorithms are developed to minimize the effect of above two fraudulent activities and focused on the accuracy of the detection and duration. One of the major challenges of overcoming lower detection rates is lack of the information availability across other networks. Therefore, geopolitically, most of the telecom operators have to combat this battle alone by disbursing their own funds without a cross reference from other networks or regulatory intervention. Therefore, it is essential to integrate a common body to the process of fraud detection, by enabling it to have holistic view and information across different network operators within a single country. Since the revenue loss is directly related with the detection time of a fraudulent number, it is vital to identify a fraudulent number within a minimum possible time and the relevant actions have to be taken not only within a single

operator's network but also all the network operators within the same destination country.

1.2 Overview of Illegal IDD Call Termination

Illegal call termination is one of the most complicated frauds prevailing around the world, which has evolved with the advancement of the technology. This is also known as 'grey call' or 'bypass call'. This scenario happens when fraudsters route and incoming international call via internet using Voice over IP protocol (VoIP) and avoid legal routing path. Then the Mobile Terminated (MT) Call is terminated to the receiving party by using a local SIM (Subscriber Identity Module) card of the local operator of the destination country as a local call.

Generally, a regulatory body, or a group of companies around the world impose and agreed tax on call termination for national calls and international termination calls. Grey calling usually happens when their international termination rate is higher than that of national calls. 70% of the international calls are routed via illegal routes in Nigeria as at 2019 [4]. A significant amount of revenue is lost to both operator and to the destination country/regulatory body, as these calls are charged as local calls with a lower rate. Figure 1.1 depicts the price difference of legal IDD termination call and the revenue steal by the fraudsters.

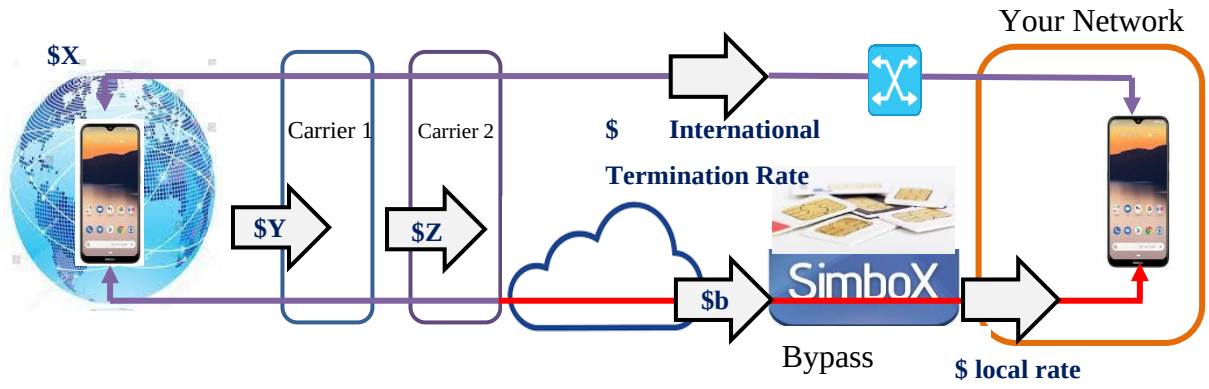

Figure 1-1: Illustration of price difference between legal and illegal IDD call termination paths

Generally, the international termination rates are higher than local termination rate. Fraudsters exploit this price difference to grab the revenue via bypass calls.

The number of International Termination minutes are in a declining trend globally as well as in Sri Lanka [5]. Figure 1.2 depicts the declining trend of International Voice Minutes in consecutive year. One of the major reasons for the decrease of the international voice minutes is the grey calls. When an originally IDD termination call is routed as a grey call, it is calculated as a local call in the statistics.

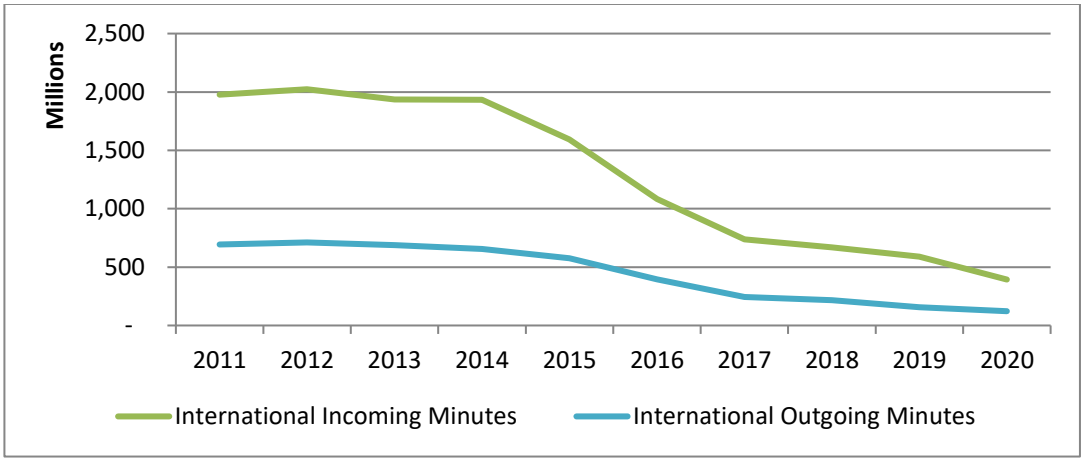

Figure 1-2: Yearly International Termination and Outgoing Minutes in Sri Lanka

Source: Statistics- Telecommunication Regulatory Commission of Sri Lanka", Trc.gov.lk, 2020 [5]

The bypassed calls are first routed via internet using VoIP and then handled by the devices called SIMBoxes, which contains hundreds of local SIM cards of the destination country. SIMBoxes have the capability of handling both VoIP protocol and GSM protocols. SIMBoxes convert VoIP calls to GSM network generic calls and a locally terminating call [6]. With the advancement of the technology, fraudsters have developed these SIMBoxes to have the capability of containing hundreds of sims and location update capability of different locations within the country. Some SIMBoxes have the capability of imitating human behavior, causing detection more complex. International Mobile Equipment Identity (IMEI) is the unique identification number programmed into each communication handset. However, sophisticated SIMBoxes are now deploying the capability of swapping IMEI for a single Mobile Station International Subscriber Director Number (MSIDN).

IDD bypass fraud can be divided in to two major categories.

1.2.1 On-net bypass

Call routing schemes involves different stakeholders in the routing path and vary vastly depending on if the call is domestic, which means within the country, or international. The calls within country are again divided to two methods as On-network calls and Off-network calls. A call generated within the country is said to be On-network, which is also called as On-net, when both caller and the called party parties are from the same telecom operator. Off-network calls also known as Off-net calls are identified as calls generated among calling and called parties are from different telecom operators.

Generally, fraudsters possess SIM cards from all the networks of the destination country. When the bypassed MT call is traversed through the same network of the destination number, it is identified as an On-net Bypass call. If the On-net charging rates are considerably cheaper considered to Off-net rates, fraudsters use On-net bypass largely. Figure 1.3 depicts On-net bypass call route. Detection algorithms exploits the fact that availability of complete information of fraudulent number, to optimize the detection accuracy.

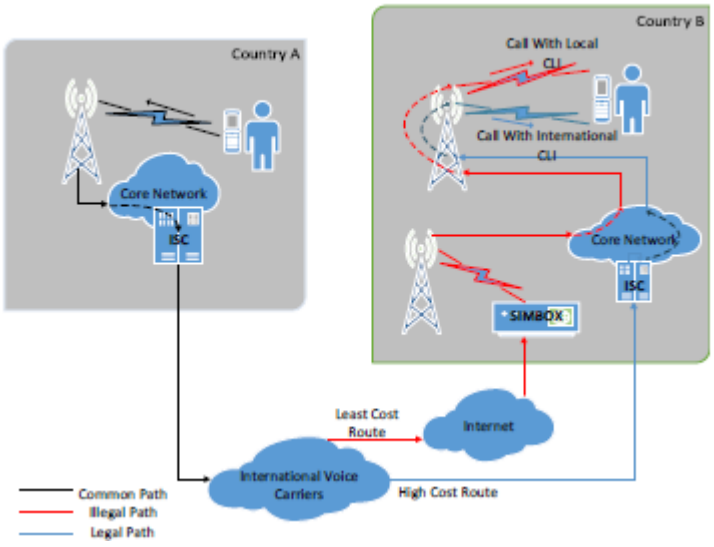

Figure 1-3: Illustration of On-net bypass scenario []

Source: [13]

1.2.2 Off-net Bypass

Off-net SIM card is used to terminate the call to receiving party in Off-net bypass scenario. If the local interconnection charge is much lower compared to international termination rates, this scenario can be observed. It is challenging to identify the Off-net bypass numbers, due to the limited information availability with the destination network. Since there is no clear visibility about location information, owner information, history information, duration information of the Off-net numbers, the detection accuracy is compromised.

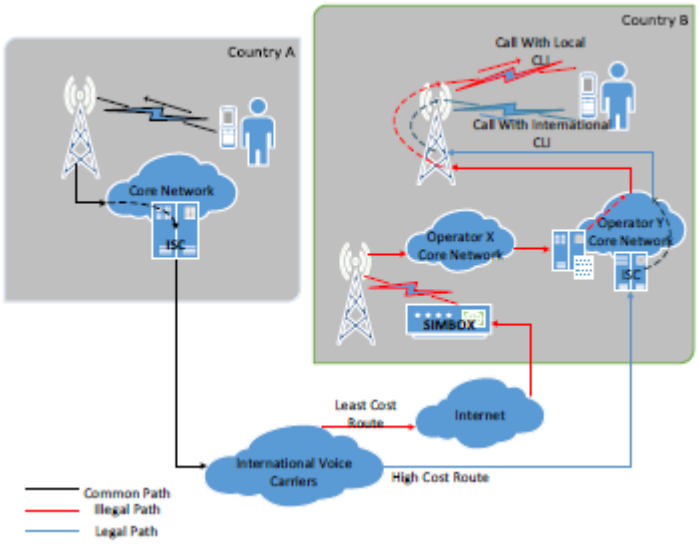

Figure 1-4: Illustration of Off-net bypass scenario

Source: [13]

1.3 Abnormal IDD call behavior related to International Revenue Share Fraud

An abnormal number of calls are generated to IDD destinations with premium rates, due to the activities of scammers. The IDD rate for the premium countries are much higher, whereas it can be 4,5 times the normal IDD rate. One of the major methods victims falls into this is the missed call reception from the premium IDD destination. The Incoming call from the Premium network only lasts for 1,2 seconds which causes the receiving party to call back and check. Then the victimized network has to pay a large amount for the call termination. This is also called as ‘One Ring Scam’.

There are 2 major fraud detection categories, which are described in next section.

1.4 Major Fraud Detection Categories

Grey call detection mechanisms can be categorized in to 2 categories whereas each of those categories has pros and cons related.

1.4.1 Passive Detection

Passive detection is the analysis of the logs in the system to identify the fraudsters. When an outgoing or incoming call is originates in a network, logs are generated in several routing nodes, such as Mobile Switching Center (MSC), Online Charging System , SBC (Session Border Controller). Call Detail Record (CDR), is one of the most valuable information sources of a telecom operator which captures the information of a single calling event such as calling party, called party, location information, duration etc.

CDR are generated in MSC mainly and in other network nodes. CDRs are used to analyze calling patterns of the fraudsters to formulate detection algorithm. The rich information available in CDR can be utilized to identify the behavioral pattern of the past fraudulent numbers [7], which can then be used to detect the current fraudulent numbers. Since CDRs are created in the nodes in near-real time, the passive detection can also be carried out in near real time.

CDRs are loaded into databases and queries are used to identify the grey call numbers. For On-net bypass detection operator has the luxury of using the end-to-end information available about both originating and terminating party. Data mining techniques are pattern matching techniques are exploited to identify the fraudulent numbers. In order to achieve higher accuracy, the false positive rate has to be as less as possible. If a genuine subscriber is identified as a fraudulent user and being blocked, it can lead to customer churn from the network. On the other hand, if a fraudulent number is identified as a genuine number, it can incur a large revenue loss to the company and to the country.

Detection time is another key parameter of the detection process. Since acquiring a SIM card costs a small amount in most of the country, fraudsters tend to use more and more new SIM cards, if one SIM is blocked. If the detection and blocking is delayed,

the fraudster can recover the cost of the SIM. It is more challenging for off net scenario. This arouses the requirement of near real time detection and communication process with the involvement of a common regulatory body.

1.4.2 Active Detection

Active detection is identifying the fraudulent numbers using test traffic originated from the different Originating countries to a particular destination country. Various parameters are used to verify that the call is routed via a grey route, such as Calling Line Identifier (CLI), Originating time of the call, Release time of the call, Call duration etc. When an IDD call is terminated via an illegal route, the receiving CLI is displayed as a national number of the destination country whereas it is compared with the original calling party from the test tool. Another way of analyzing the grey calls is to analyze signaling traffic of the destination country. This involves in introducing signaling probes to the network, which is a costly approach.

1.5 Motivation

Mobile operators are losing revenue of billions of dollars annually, due to illegal call termination and abnormal usage pattern issue. Since there is a tax component imposed by the regulatory body of a country for international call termination, the county also loses billions of dollars due to this fraud. Therefore, regulatory body of a country can involve in detection process to enhance the detection accuracy.

Even though various detection algorithms are developed to identify the fraudulent users, there is a significant barrier faced by each researcher or mobile operator when the dataset available is only confined to the own network itself. In order to optimize the pattern matching various data fields are used included in the CDR. However, since location and history details of the fraudulent numbers of other networks are not available for a network of interest, the detection algorithms cannot be optimized to achieve more accurate results for off-net scenario.

Detection can be identified as two major categories: passive detection and active detection. It is essential to outline framework for the regulatory body that has the access to rich information of all the operators within a country whereas individual

operator cannot analyze. With a proper framework regulatory body can contribute to t both active and passive detections of the fraudsters. This facilitates all the operators in a country to combat this battle in more efficient and legitimate methodology. This will conserve the billions of dollars lost annually to both operators and to the country.

1.6 Research Objectives

- Identify existing detection techniques of grey calls, negative impacts of Illegal Call Termination and Abnormal Call Scenario related to ISRF and identify the existing solutions
- Identifying the drawbacks and limitations in current IDD fraudulent number communication process in the country.
- Formulating a common policy framework and provide recommendations covering different aspects identified via data analysis

1.7 Organization of the thesis

The thesis is comprised of 6 chapters. Chapter1 provides the introduction of the research area with a detailed description about the illegal call termination. Chapter2 consists of the findings from the literature survey. Negative impacts of Illegal Call Termination and Abnormal Call Scenario to the operators and to the regulatory body of a country are presented. Further, the fraud detection techniques are evaluated to identify the requirement of a common framework. Problem formulation is included in chapter 3. Proposed framework and the recommendations are presented in the Chapter4. Finally, the future works are limitation of this research are included in the Chapter6.

Annex-A contains the operator questionnaire used to evaluate the limitations of the fraud detection process and to identify the requirement for a common framework, for operators in Sri Lanka.

2 LITERATURE SURVEY

This chapter discusses the different fraud detection techniques used for identifying illegal IDD call termination under passive detection and active detection. Further, the techniques used for identification of Abnormal IDD call behavior related to International Revenue Share Fraud is presented. Works related to describe negative impact experienced by the Mobile operators, End users and Regulatory body of a country is included in the next sub section. Further, the current solutions available to avert this situation in included.

2.1 Detection techniques

Grey call detection mechanisms can be categorized in to 2 categories as 'Passive detection' and 'Active Detection'

2.1.1 Passive detection

With the passive detection methods, the logs are analyzed after the call event takes place, usually without a manual human intervention. Passive detections can also be identified as different categories based on the data type analyzes. In the literature, CDR based, Audio records based and signaling data based passive detections can be identified.

2.1.1.1 Grey Call Detection Techniques using CDR

CDR based detection focuses on content of the CDRs and the occurrence of the CDR. Majority of the passive detection techniques are based on Machine Learning or Complex Event Processing (CEP). When machine learning is used it is approached as a classification problem, where either SIM card (Identified using IMSI) or IMEI is the entity to be classified. Most of the CDR based fraud detection techniques are approached with major three steps: data preparation, model building and evaluation.

a) Data Preparation

In data preparation, data understanding, feature identification and pre-processing is carried out. In the literature, several feature types are used.

Feature type1: Call behavior

Since the call behavior pattern of a SIMBox MSISDN is different compared to normal human behavior. Having outgoing calls usually for a set of distinct receiving numbers, a smaller number of incoming calls, large number of outgoing calls within a short period of time are identified as call behavior patterns of SIMBox numbers. [8], [9] are based on the features of above category. Authors in [10] considers the total count of outgoing call made during a small-time window W and tries to detect the fraudulent numbers based on the repetitive nature of outgoing calls within small time period.

Feature type2: Mobility

Generally, fraudulent SIM cards are stationary while originating calls, which results in movement between the Cell IDs is minimal. The most served Cell Ids are identified as hot cells. Murynets et al. use total number of different Cells used within a given period, number of calls made, number of calls made within the same location, cumulative distance traversed by an individual for the detection data preparation.

Feature type3: Mobile service usage

Since the SIMBox users' usage other services (other than voice service), are minimal, authors in [10] have exploited this to identify the fraudulent users

Feature type4: Entity properties

Fraudsters use hundreds of SIM cards within a single SIMBox. Number of MSISDNs per IMEI is used by authors in [11] in addition to the customer age, customer segment. Since the fraudulent SIM cards are detected and blocked, the average customer age is less than compared to a normal subscriber and the outgoing call volumes are high within the customer age.

b) Data modeling and evaluation

ANN method: Several classification models found in literature are described in this section. Artificial Neural Network (ANN) consists of input layer, few hidden layers and output layers, where optimal weights for the interconnections are calculated during the training process. According to the Elmi et al. [8], they have used Artificial Neural Network (ANN) to detect this type of frauds. Due to the certain characteristics of ANN, such as capability to generalize, ability to learn complex pattern & trends even with noise interruptions & better performance, this method was used and Multi-Layer Perception (MLP) has used as the classifier. Nine features were derived from CDRs values of each features were calculated for each calling number.

In MLP the Artificial Neural Network consists of neurons which are the computational units and can categorize as input, output and hidden. Connection between neurons are called edges and they are connected to subsequent layers but not to same layer. Weighted sum of inputs was fed in Sigmoid function, a nonlinear activation function, to calculate single output. This output will be the input to the next layer. To minimize training errors, Back Propagation algorithm is used, and weights of the edges were adjusted continuously.

Total dataset was divided into ten subsets and nine were used for the training of the model. Another subset was used as the test dataset. Therefore, this is called 10-fold cross validation. To find highest accuracy with optimum ANN, authors has altered four parameters and they are number of hidden layers, number of neurons per hidden layer, learning rate and momentum. The speed at which the ANN reach to the minimum value for Sum Square Error is represented by Learning rate parameter. Momentum means the rate in which the ANN reaches neighborhood of optimality at the beginning level of algorithm. The values of momentum and learning rate are lies in between zero and one. Authors have unmasked the optimum ANN by experimenting 240 neural networks and has compared prediction accuracy, generalization error, model building time, precision and recall. They found that higher values of learning rate and momentum is decreasing the accuracy level. They could obtain the highest accuracy of 98.7% with the momentum of 0.3 (lower) and learning rate of 0.6 (moderately high) together with two hidden layers. Learning and classification has taken 17 seconds with detection of lower values for false positive and false negative.

Authors in [12] has proposed a similar Neural Network detection approach they have used Sign function as the activation function. Kashir et al. [12] tested 5 NN variants for a dataset with 8695 general subscribers and 50 SIMBox subscriber numbers and varied the optimizing algorithm. The accuracy obtained was 99.87% with the Bayesian algorithm and an RMSE of 0.01654.

Complex Event Processing (CEP): In order to exploit real time feature identification, CEP is used as event stream processing technique. CEP uses appropriate toosl to query a data stream prior to the storage in database. CEP matches incoming events continuously against predefined patterns. This allows the identification of fraudulent numbers proactively.

Complex event in in CDRs are used by authors in [13] to identify fraudulent numbers, using CEP, which is depicted in figure 2.1. At time equal $\boldsymbol{t}$, a call attempt is generated from the national outgoing number A1, to subscriber B1 of another operator (Off-net). A1 is previously detected as a fraudulent number and blocked. At time $\boldsymbol{t + \Delta t}$, same B1 subscriber receives a call attempt from A2 of same operator (On-net) and it is successful. At time $\boldsymbol{t - \Delta t}$, B1 has initiated a call to $\boldsymbol{I1}$, an international number. In such situation, there is a high probability of A2 to be a fraudulent number [13]. The authors have used such seven patterns to recognize a fraudulent phone number based on On-net ot Off-net scenario. They have used 26 features from the real time CEP queries, using free-licensed WSOA CEP tool [25]. they achieved F1-scores of 0.786 and 0.789 for On-net and Off-net numbers detection, respectively with features obtained from one day CDR. 25 On-net and 15 Off-net fraudulent subscriber count is used out of 1,573,680 customers.

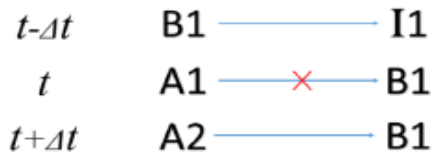

Figure 2-1: Complex events in a CDR created by SIMBox [13]

Veloso at. El. in [14] also exploits CEP queries to detected fraudulent numbers who generate high volume calls within a small time window. The authors have used Lossy Counting algorithm, which computes frequency counts exceeding a defined threshold over data streams. This was improved with Fast Forgetting Algorithm designed to capture the repetitiveness.

Even though, the CDR based detection techniques are used to optimize the accuracy of the detection algorithm, due to unavailability of information about the other operators' fraudulent numbers, the overall efficiency of the fraud detection process of a country is affected.

2.1.1.2 Abnormal IDD calling behavior detection using CDR

Telecommunication operators encounter different abnormal usage scenarios for all the services such as voice, SMS, GPRS, MMS etc. due to socio-economic changes in the country or due to fraudulent activities. 'One Ring Scam' is a situation where customer receives a call with a small duration as 1,2 seconds from premium numbers. When customer cannot answer the call, he tends to call back to the premium number, which costs comparably an exorbitant amount [15] but rejects to pay the operator. This is also known as 'Dial and disconnect scam' and as 'Wangiri',. 'Wangri' has come from Japan where the scam originated years ago and means one-ring-and-cut. (One ring and done.)

Operators around the world have taken a lot of measures to avert this by educating their customer bases about this scam. AT&T has launched a blog on Cyber Awareness where they have informed the customers about possible practical scenarios and how to identify whether it is an IDD call or a normal call [16]. They have created the awareness among customer base how not to hang on such fraudulent calls, which can charge more.

2.1.2 Active detection

Active detection of illegal detection is commonly considered as classical methods, because it can be identified as the first response of the telecommunication companies to the SIMBox fraud. This requires a significant involvement from the operator and additional resources and tool to deploy. Active detection methods can be broadly identified as Test Call Generation (TCG) and there are some Rule-based methods also.

a) Test Call Generation (TCG)

TCG is carried out by setting up a destination network in the country of the interest to receive multiple call from different test numbers from different countries. Since the calls have to be initiated from different countries within a short period of time, specific test tools are used to generate IDD calls from specified networks. The test calls are generated through many different interconnect voice routes around the globe. Once the call is received, the CLI is compared with the original calling number and acted upon

detecting a mismatch. Since the fraudsters are using CLI hiding methods, special SIMs with CLI Restriction Override (CLIRO) are used for the active detection testing [17].

There are no false positive decisions made with TCG methods, as the fraudulent number can be exactly identified. Therefore, TCG method is widely used for fraud detection by both operators and regulators around the world. TCG works with probability of terminating a test call from the grey route with respect to an original route. More the number of test calls, more likely it is to be detected a grey route, but this requires extensive amount of money and intervention. In [18], TCGs are generated in intelligent way to tackle fraudsters. Even though, TCG method accuracy is very high, fraudsters have developed means and method to avoid test calls by several identification methods. Therefore, this method is used as a conjunction with passive detection methods around the telecommunication operators around the world.

2.2 Negative Impacts experienced due to Illegal Call Termination

The impact of the illegal call termination fraud has impact to the Mobile operator of the country, end customer and Regulatory body/government of the country. The following section describes the impact to each segment separately.

2.2.1 For Telecom Operators of the Country

According to Fraud Loss Survey conducted by Communication Fraud Control Association (CFCA) [3], the revenue lost annually due to interconnect bypass fraud, 2.71 Billion USD is lost. Generally, the international call terminate charge is higher than local call termination charges. Therefore, per minute revenue loss that has to be absorbed by the Mobile Operator is considerably high compared to the investment carried out to deploy the IDD termination service.

The regulatory body or a standardizing body of a company imposes tax on international termination and the Mobile operator's profit margin is decided based on that. Due to illegal IDD call termination, a Sri Lankan telecom operator loses 0.06USD per minute.

According to Professor Leonard Waverman in [19], it is mentioned that "*international telecommunication pricing structures have important implications for national telecommunication sectors given that revenues from international calls is seen as means of cross-subsidizing domestic calls"*. This implicates the importance of securing revenue from international voice call termination.

Other consequence of this scenario is the inaccuracy of the statistics of IDD call termination. Since the call is routed via internet using VoIP protocol and then injected back to the local network, the CDR contains the Originating Party as a local number. Hence, the actual IDD call termination statics cannot be obtained. This issue is worse in countries which have International Gateway monopolies, where illegal bypass is said to be 30%-60% of the total traffic [20].

SIMBoxes can serve hundreds of SIM cards at a given point of time. Since all the SIM cards are latched to the nearby BTS (Basestation Tower System), it can cause congestion to the actual customers of the local network in the destination country. This can lead to customer issues of call busy and disconnection scenarios.

Brand Image can be tarnished due to above reason and it can result in customer churning. Another impact is that inbound roamers are not reachable when illegal call termination occurs. If the destination number is an in roamer, then fraudster trying to terminate the route the call through SIMBox will not be successful due to routing failure when a call is routed via a SIMBox. This can cause issues with the roaming partnerships with other networks over the world. Another concern is the legal interception issues, where Originating party is recorded as a local number, whereas it should have been an international number.

2.2.2 For Regulatory Body/Government of the Country

Taxes are imposed on various telecom operating services all around the world, where it contributes with a 4.1 trillion USD worth of economic value to the world GDP. Taxation revenue is one of the major income sources of a country. If the international termination rates are liberalized and streamlined properly, government get the benefit of receiving much required foreign currency to the country. Higher tax revenue

contributes to the increased GDP of the country resulting upliftment of the living standards of the citizens of the country.

The government in Sri Lanka loses 0.06 USD per minute for each illegally terminated call. In Sri Lanka, Voice minutes 393 Million International Voice Minutes are terminated.

Table 2-1 : Yearly terminated voice minutes in Sri Lanka (Local and international)

	Incoming Calls	
Year	**Local**	**International**
2011	37,683,542,412	1,977,309,199
2012	41,578,695,297	2,023,274,456
2013	41,633,469,455	1,935,790,037
2014	43,435,808,621	1,933,590,274
2015	44,756,667,740	1,592,185,803
2016	44,692,460,946	1,083,162,252
2017	44,696,707,013	736,184,103
2018	46,151,666,021	668,694,184
2019	55,963,712,985	589,061,117
2020	61,464,764,054	393,330,936

Source: Statistics- Telecommunication Regulatory Commission of Sri Lanka", Trc.gov.lk, 2020 [5]

It is estimated that millions of USD is lost for Sri Lankan government and to the operators annually. Since half of the deferred revenue is tax portion, the government loses half of the portion from IDD MT revenue annually, if calls are traversed through illegal path. However, there is no recent literature to be found considering the illegal terminations as a country in whole for Sri Lanka.

Another concern of illegal call termination is the legal interception issues that had to be faced by the regulatory body of a country. Since the recorded information are false, it raises consequences in verifying call records. Since call records are used for crime investigation, these false records can lead to legal misinterpretations [21]. In addition to that, it is evident that the fraudsters cannot import the sophisticated SIMBoxes with a government legal clearance. There are rules and regulation imposed for importing telecommunication equipment to a certain country, where only authorized parties are allowed to. However, these fraudsters smuggle this telecommunication equipment to

the country resulting security threats to the country. Higher grey call frauds can be identified as an indication of higher rate of rules violation in equipment import. According to [21], India have clearly stated that illegal call termination is a security threat as it hides the original CLI of the calling party. As per the industry estimates, 20% of international calls are via grey routes as at 2018 [21].

Another aspect is the inaccuracy of the statistics available about international termination market, which are used for various purposes around the world.

2.2.3 Impact to the End Customer

The receiving party of the destination country is the other culprit of this fraud. The main issue is the absence of CLI for the receiving call. Receiving party cannot see the actual IDD calling number where the call is actually being initiated. Therefore, customer is misled as a local call instead of an IDD call. Another consequence is that if the customer could not answer the call, there is no way he can call back to the original IDD number. As the customer pays to receive a premium service, customer could be disappointed with this service and eventually it can lead to customer dissatisfaction and increased number of customer complaints.

Another major concern of the illegal call termination is the low Quality of Service (QoS) experienced by the customer. Various researches have analyzed the voice activity detection in both frequency and time domain [22]. In case of bidirectional VoIP flow, the voice quality is dependent on the jitter. The VoIP packet arrival rate is distributed in Gaussian around the mean value of jitter. Transmission delay and buffer space are major causes for the jitter. Since above factors cannot be guaranteed during the illegal routing, severe QoS issues can be experienced by the end user.

In addition to that, customer cannot obtain billing proof for the call records or cannot rely as an evident for the IDD call reception when required. Voicemail is being used for certain customer segment, but with the illegal call termination, voicemail cannot be retrieved. In terms of call originating party in the other country the call setup time is higher than the legal PSTN call setup time.

2.3 Existing regulations in Sri Lanka to restrict illegal call termination

According to TRCSL (Telecommunication Regulatory Commission of Sri Lanka), as the regulatory body of Sri Lanka, bypassed international call is considered as an illegal action according. '*VOIP is not allowed in Sri Lanka for the purpose of to by-pass international telecommunications services'* under the Telecommunications Act No 25 of 1991 and its amendment Act No 27 of 1996. The regulatory body of a country is generally very vigilant is providing provision for VoIP protocol related services in order to streamline illegal call termination. The regulatory body of Sri Lanka has the guidelines in unblocking VoIP ports, protocols and applications in order to prevent illegal international call terminations [29].

Under the gazette notification, the VoIP connections are restricted based technical parameters included in table 2-2. Hence, this provides a clear guideline which can be used to terminate any illegal VoIP connectivity, if investigated.

Table 2-2: Technical Parameters to block the VOIP application

No	Technical Parameters/Conditions	Description
01	Type of connection	Symmetric broadband, leased line, international Private leases circuit except asymmetric broadband Connections using technologies like ADSL,GPRS,3G,HSPA,Wimax etc
02	Bandwidth	≥ 1Mbps
03	Protocol/Application	VOIP related application, protocol, ports etc. Suspected to be used for illegal bypass such as SIP H.323,IAZ.RTP,MGCP.H.248,Megaco,SCCP,and it's associated ports like H323 (TCP1720),SIP (TCP/UDP 5060-5061)

Source: [29]

By identifying the legitimate requirement of implementing VoIP connections, the guidelines have been introduced under the gazette declaring the categories of users / customers/clients to claim unblocking of VOIP application.

Categories of users/customers/clients eligible to claim unblocking or exemption from the blocking of VOIP application according to the gazette are as follows[29].

- Licensed PSTN Operators
- An EGO operator who has obtained an interconnection from the PSTN operators and the interconnection is in operation subject to verification from the TRCSL
- Licensed ISPs subject to verification from the TRCSL
- Authorized call centers or BPOs approved by the TRCSL
- Any customer who communicates with his own officers within the country.
- Any customer who is handling international logistics, international banking and IT/Software development and support service etc.
- Any customer who uses above listed protocols/ports for any other application which is not used to establish and terminate illegal voice bypass subject to verification from TRCSL

The regulatory body of the country only allows the VoIP connectivity if sufficient reasons supporting the request to unblock the VOIP are provided. Once the VoIP facility is allowed, that customer list monitored by the regulatory body of the country, and it is used for verification activities related to illegal voice call bypass.

The existing practice of communicating the detected fraudulent numbers is via a daily email method. If an offnet number is detected as a suspected fraudulent number, it is shared with the relevant mobile operator via an email. Currently there is no SLA defined across all the operators for verifying the offnet fraudulent numbers.

2.4 Available solutions

Research have been conducted to detect the fraudulent calls using various pattern matching techniques as discussed in section 2.1. However, the accuracy of the detection techniques has been limited due to the unavailability of the sufficient information of the Off-net operators. Generally illegal call termination issue is faced by most of the operators in a particular country or all of the operators in the country. Hence, a common approach is required to address this concern. In this section the

works related to common approach is presented. The international termination rates (ITR) refer to the charges defined by mobile traffic carriers in case of carrier-to-carrier charges. Accounting and charging in international telecommunications services are carried out based on the recommendations by the International Telegraph and Telephone Consultative Committee (CCITT). There are many components engaged in setting up cost of termination and completing an IDD call by telecommunications service providers. Firstly, the cost related to customer mobile device to international gateway of the originating country. Second cost component is related to the transmission through the international hubs. Third component is the cost related for accessing the network of the terminating country.

It is evident that when the termination charges are much higher than the local terminated call, more fraudulent incidents are reported. One of the approaches to deviate illegal call termination is price liberalization [20]. With the price liberalization the revenue that fraudsters are deteriorated and illegal call termination decreases. Therefore, price liberalization is one of the methods to avert this. Figure 2.2 depicts the MTR price for international calls trend from 2010 to 2019.

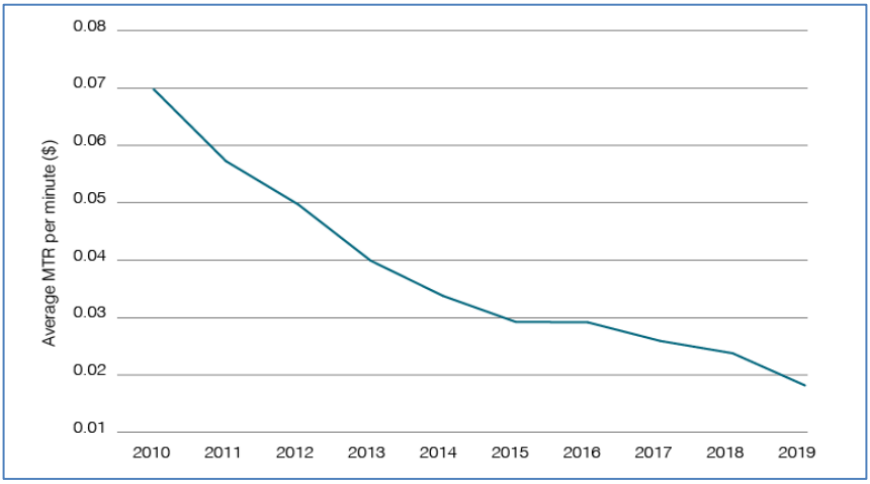

Figure 2-2: Average MTR Worldwide, 2010-2019

Source: Termination Rates Continue Downward Trend, By Pete BellOct 10, 2019

According to [21], India has considered the price liberalization to combat international bypass fraud. They have expected that if the arbitrage opportunity is plugged or kept to a minimum, the attractiveness of the grey route for carrying international incoming voice traffic would be lost, and thereby, the carrier route for international

incoming traffic would witness a legitimate growth. Therefore, regulatory body has lowered the price of the incoming calls to match to local termination rates via a price revision.

However, in contrast to liberalization, Pakistan and Bangladesh and some African countries have introduced price monopolies starting from 2008. Surcharge taxes have been introduced causing reduction in legal international minutes which in turn reduce profits for the mobile operators and corporate tax receipts for the government. This has led to increase of the illegal call termination via illegal SIMBoxes, where fraudsters acquiring higher revenue due to surcharge taxes [23].

Another solution that has been carried out in Bangladesh was a revision of the network topology to avert illegal call termination issue. VoIP based illegal call termination has raised up to 80% of the international call by 2007 in Bangladesh [26]. The government and regulatory body of the country decided to restructure the network topology according to International Long-Distance Telecommunication Service (ILDTS) Policy in 2007.

However, this is a lengthy and time-consuming process and may not be feasible for some of the other countries around the world as the topology of the incumbent operators in a country has to go through a hectic change process.

Creating incentive for network providers of the country to monitor bypass fraud is another framework model that has been suggested in [26]. This is also relevant and applicable to that particular country only as it requires a specific network topology to be functioning.

Another model that has been suggested in work [26] is feedback system implementation with the use of customers of the destination country. Since the customer experience the fraudulent incident, customer can identify even though the call is an IDD termination, the CLI is to be a local MSISDN. Hence, an incentive scheme is suggested to be implemented for the subscribers who report calls that are suspected to be illegally re-routed via a VoIP path. In order to reward the customer for their effort, incentive scheme is introduced. In this scenario, there could be a customer

hype created to suspect the integrity of premium voice service created by a network operator compared to other OTT (Over the Top) services. Since all the communication is encrypted at each level of the call route, PSTN calls are considered to be the safest communication method that customer can rely on. With this scheme, customers can lose their trust about the operator about the information confidentiality and integrity.

According to the literature survey carried out, it is evident that there is a gap available in the detection techniques where the information accessibility is limited. The impact of the illegal call termination identified as in the literature survey is quantitative and qualitatively considerably high. The work done on defining a framework to avert this situation has their own pros and cons. Therefore, there is a research gap as to where to find a suitable and effective common framework to a country to follow.

3 PROBLEM FORMULATION

As per the literature survey carried out, the illegal call termination and abnormal call scenario related to (ISRF) are major frauds identified in the current telecommunication industry and the related consequences are faced by end user, mobile operator and the destination country's government/regulatory body. It is evident that there is a requirement of integrating all the networks of a particular country with a common body such as the regulatory body of a country, in order to resolve this issue. This common body can be identified as either as the regulatory body of the country or a consortium consisted of the members from all the operators within a given country. It is essential to detect the fraudulent users within minimum possible time in order to minimize the revenue impact. Therefore, the problem the research is focused on can be identified as **"How to outline a common framework to different network operators in a particular country in order to improve the accuracy of illegal IDD termination detection within minimum time span?".**

Since this issue is prevalent in most of the countries where the MTR is high, Sri Lanka, a developing country in the Asia Pacific region, can be identified as a candidate to analyze this issue. Even though the information gathered in this thesis is related to Sri Lanka, the findings and framework suggested in Chapter 5 can be applicable to anywhere in the world with minimal modifications as per each regulatory background of the country.

3.1 Low visibility of the fraudulent users outside the own network

Since the illegal bypass is carried out using own network and Off-net SIM cards by fraudsters, it is essential to identify the key parameters of Off-net numbers in order to optimize the detection methods. The location details, IMEI details, history call records, are not available for the Off-net CDRs available in a gateway MSC in the interest. Hence, it is a problem which can be addressed by having a common party with a bird's eye view of the fraudulent number base.

3.2 Unavailability of tracing capability based on unique parameters across different networks within a single country.

Generally, IMEI is the unique parameter of a device. IMEI uniquely identifies an individual user equipment, thereby provides a means for controlling access to GSM networks based on ME models or individual units. IMEI consists of 15 decimal digits, which includes details of origin, model, and serial number of the device. However, with the evolvement of the technology, fraudsters swap IMEI of a single SIM card using software-based method, making the detection is not solely possible based on IMEI number.

However, when a customer purchases a SIM card from a local operator, there are a set of information required to be given. In Sri Lanka, the NIC (National Identity Card) details is a mandatory requirement in buying a SIM card. Another common parameter common across different networks is the location details. Currently tracing is not possible over these parameters across different networks within a single country. This has to be addressed via a common protocol.

The gap of communication of the fraudulent MSISDN among the different networks within a single country is another factor contributed to the efficiency of fraud detection and the time taken to block a SIM card after been identified as a fraudulent number. It is feasible to handle the tasks and obstacles related internal communication within a single operator company, but in order to establish a common communication channel it is required to have a common framework and a common party.

Another aspect that has to be considered is physical raiding of the fraudulent users once a fraudster is identified. Generally, the operator's support is required to fulfill this yet am operator cannot perform this activity without a regulatory authority's intervention. Hence, this is another aspect considered in formulating common framework.

3.3 One Ring Scam

One ring scam is prevalent in a lot of countries and mobile operators take counter measurements to avoid this. However, most of the time, the operators have to rely on

their own call patterns or external logs to identify such scenarios. Currently there is no communication between the operators within the country for this. Combatting against One Ring Scam is another aspect to be considered for the common framework.

3.4 Defining constructs and indicators for Census data collection

To identify the current scope of intervention and support from the regulatory body of the country, below constructs were identified for descriptive analysis and indicator for each construct is listed.

Table 3-1: Indicators and used for measure in questionnaire

Measure	Indicator	Question	Reference
The support received from the regulatory body of the country, for fraud detection in terms of detection is satisfactory	provision of parameters and inputs by the regulatory body	Regulatory body provides parameters and inputs required for bypass detection	Author
	provision of other operators' bypass numbers	Regulatory body provides bypass numbers of other all other operators seamlessly	Author
	availability of a common platform	Common platform has been setup by regulatory body with an overall visibility	Author

4 DATA COLLECTION AND DATA ANALYSIS

4.1 Census conducted for mobile operators in Sri Lanka

As discussed, and reviewed in literature survey, the main 3 parties affected from illegal call termination are mobile operators, end customer and the government/regulatory body of the destination country. Generally, mobile operators in the destination country are mainly engaged in fraud detection activities. This chapter contains the data collection and analysis. Questionnaire with mobile operators, focus group discussions and one-to-one interviews were carried out as data gathering techniques.

The questionnaire was designed based on the key findings identified from the literature survey to identify the current establishment and requirements for a common framework. The questionnaire consists of 3 sections. First section of the questionnaire aimed at collecting data about the existing setup of the fraud detection system of each company. Second section consisted of 5-point Likert scale (1-Strongly Disagree, 2 – Disagree, 3- Neutral, 4- Agreed, 5- Strongly agreed), where respondents were asked to rate the levels of support and intervention of the regulatory body of the country. Final section of the questionnaire consists of the questions to collect details about the One-Ring Scam and to collect the suggestions of the respondents.

Sri Lanka has a highly competitive market in mobile industry, with a total population of 21.919 million people and with a total mobile subscription count of 29.243 million, resulting 131.1 mobile subscriptions per 100 inhabitants [5]. Currently there are 4 licensed mobile operators operating in the country, after the merge of 2 operators in 2018[6]. Therefore, the census was conducted on the population itself as there is no requirement of sampling the population. Census was conducted with the engagement of teams who handles the interconnections and fraud detection in each company.

Mainly descriptive statistics were used to identify the current establishment of the fraud detection systems of mobile operators in the country. Descriptive statistics helps to identify the features of the data. One sample t-test was used to assess whether the mean value is statistically significant from the neutral value 3.

4.1.1 Mobile operator census results

This section summarizes the descriptive statistics analyzed to understand about the current fraud detection systems used by the mobile operators in the country.

Table 4-1: Descriptive statistics of the census

Variables related to current fraud detection system setup	**Categories**	**N**	**%**
Methods of detections used in the FMS by the operator	Active detection only	0	0%
	Passive Detection only	0	0%
	Both active detection and passive detection	4	100%
Scenarios detected by the FMS	Onnet bypass only	0	0%
	Offnet bypass only	0	0%
	Both onnet and offnet bypass	4	100%
company detect Abnormal IDD call scenario	Yes	0	0%
	No	4	100%

As shown above all the 4 operators use both active and passive detection as a methodology and they detect both onnet and offnet bypass numbers. In addition to that 100% of the operators detect abnormal IDD call scenarios also. It is vital to identify this result, as this reveals that the scope of forming a framework can be outlined based in terms of providing a common platform or common visibility rather than to form detection methodologies itself. Mean ranking[28] and one sample t-test

In order to identify the current support and intervention from the regulatory body regarding the international fraud detection, 2 issues were analyzed using the indicators. The mean value was calculated based on the Likert scale used in the questionnaire (1- Strongly Disagree, 2 – Disagree, 3- Neutral, 4- Agreed, 5- Strongly agreed).

Table 4-2: Mean ranking

Issue Number	Statement derived from the indicators	N	Mean	STD
1	The support received from the regulatory body of the country, for fraud	4	1.4175*	0.500558

	detection	in	terms	of	detection	is			
	satisfactory								

Based on the one sample t-test performed, the significance of the difference between the test value of 3 and the mean values are also indicated, where *p<.05.

The mean value for issue #1 is 1.4175, which indicates that the level of support from the regulatory body for fraud detection is an area which needs to be improved. The respondents believe that there has to be a common information dissemination platform.

Hence, the one sample t-test result provides a key insight in designing the common framework for streamlining illegal international voice call termination.

4.2 Focus group discussion with regulatory body in Sri Lanka

TRCSL being the regulatory body act as the regulatory agency for telecommunications in Sri Lanka, which was established under the Sri Lanka Telecommunication (Amendment) Act No. 27 of 1996. Focus group discussion was conducted in order to identify the current situation of the country in terms of illegal call termination.

During the information gathering from focus group, it was identified that currently there is a setup established to combat illegal call termination. According to annual reports of TRCSL in subsequent years, TRCSL's surveillance unit has done numerous investigations to racket these fraudsters.

1. Current communication of fraudulent numbers to each operator in the country

It is commendable to identify the actions taken by TRCSL to combat illegal call termination issue which have been carried out by the surveillance unit during the last years. According to the current establishment, once a fraudulent number is detected, some operators communicate the same to relevant operator via email with TRCSL team in copied. Since this is not formed with a common framework, the tendency and integrity in communicating the fraudulent numbers cannot be guaranteed. Since there is no reverse verification of the fraudulent numbers from a common body, some of the communicated numbers are left without taking any action for blocking.

Another aspect that can be developed is increasing the efficiency of fraudulent number communication within the operators in the country. Since the fraudsters gain the maximum benefit within the time period, before a number being blocked, it is essential to reduce the time taken to detect a number and to time taken to act on that number. In On-net scenario, the respective mobile operator can take the action to block the number from their own network. In contrast, for On-net scenario, it is required to get the fraudulent number verified from the relevant other mobile operator, in order to take a permanent action.

2. Complete visibility of the fraudulent numbers and information synchronization

With the current establishment, the regulatory body and the operators have a limited visibility of the fraudulent numbers. Since the fraudsters use hundreds of SIM cards from multiple mobile operators, they possess the capability of swapping mobile networks even for same receiving party. Hence, as the operators, they cannot gain the overall visibility of these fraudulent numbers. Since regulatory authority has the control over the rules and regulations related to telecommunications, it is the most preferrable entity to gain the holistic view of the fraudulent number base.

With the current establishment, the regulatory body cannot gain the holistic view and information about the fraudulent numbers, as there is no centralized system to cater this requirement. Once a fraudulent number is detected as an On-net number, generally that On-net number is not communicated to all other network operators in the country. Since the fraudsters use the same SIMBox for different mobile operators, behavioral patterns can be further optimized, if an operator has complete view of the fraudulent numbers.

Hence, it can be identified that, the existing establishment for fraudulent user identification and communication has its drawbacks in terms of efficiency, time consumption and lack of overall visibility. This can be minimized by formulating a common framework, which involves regulatory body and operators in the country, in order to work as an eco-system to work for averting illegal call termination, as a country. In order to increase user awareness and common visibility over ‘One Ring Scam’ identification, same can be included to the common framework.

5 POLICY FRAMEWORK AND RECOMMENDATIONS

As per the problem formulation carried out in chapter 3, the data collection, analysis, and interpretation were carried out and the related information is presented in chapeter4. According to the data analysis, a viable framework should be identified to address the issues. According to the census carried out with the mobile operators, several aspects were identified in terms of operator impact, customer impact and regulator/government impact.

As per the operator questionnaire data analysis, it was clearly identified that there is no common platform to gain the parameters related to identify fraudulent numbers from other networks which affects the accuracy, and time taken for fraud detection. In addition to that with the focus group discussion with regulatory body, it was evident that currently a real time update and visibility across all the networks in the country is not available. Even though existing regulatory policies imposed to avert this issue is in action, still it is not sufficient to combat these fraudsters, which arises the requirement of reform of the regulatory policies of a country. In the case of 'one ring scam' issue, currently there is no inter communication between the telecom operators in the country and the existing user awareness activities can be improved.

Based on above, the aspects considered in forming the framework and the framework components are included in table 5.1.

Table 5-1: Policy framework components and related aspects

#	Aspect identified during the data gathering and analysis	Policy Framework component that should be included
1	TRC - Currently overall visibility of the fraudulent IDD termination numbers across all the networks within a single country is not available for the regulatory body of the country	A central system should be implemented to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country

2	Operator - The accuracy and effectiveness of the bypass detection method is decreased due to the absence of the behavioral patterns and information of Off-net numbers. Currently, there is no common communication for 'One Ring Scam' issue among the operators	A central system should be implemented to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country. The scope of information shared with each operator, has to be controlled by the regulatory body.
3	The overall time taken to block a fraudulent number is increased due to the delays in post detection steps: communication to the other operator, verification from the other operator. This leads to more revenue leakage, with the increment of the delay in blocking fraudulent number	A central system should be implemented to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country
4	Fraudsters tracing via common parameter identification across different network information is not available. This leads to repetitive work and inefficiencies in overall detection and blocking process	A central system should be implemented to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country
5	Currently a documented process of fraudulent number blocking is not available. SLA (Service Level Agreement) needs to be maintained to avoid delays in verification of fraudulent numbers from other networks, when a fraudulent number is reported by the network of interest	Adding reforms to the existing regulations
6	End user is one of the affected parties and the user awareness about the illegal	A mechanism to increase user awareness and get the support of

	call termination and 'One Ring Scam' is not sufficient	the public to identify the fraudulent numbers.

5.1 Comparison of methods for the framework components

5.1.1 Establishing a centralized system for IDD fraudulent number tracking

Implementing a central system is a key component of the frameworks, which addresses several identified concerns as discussed in table 5.1. It is vital to identify the involved parties and the communication structure to achieve desired goals. According to the data gathering and interpretation, the designed central system should cater below requirements.

- Near-real time update of the fraudulent numbers
- Interconnection with different operators in the country
- Backup service of the system in case of a failure recovery
- 24x7 service
- Confidentiality and security of the data
- Dashboard system and event generation

According to the census, all the operators have already deployed fraud detections systems, which are called FMSs. Hence, it is possible to expedite that fact to develop the centralized system from there onwards, which does not require extensive fraud detection processing in the centralized system itself. Hence, it is possible to integrate or extend the data identified via mobile operator’s FMS to centralized system.

The high-level architecture is outlined in figure 5.1, where there are 3 main layers of the system. Data collection layer is responsible for gathering data from the mobile operators.

Data analysis and processing layer is responsible for storing and analysis of the information received from the data collection layer. According to [6], the number of mobile users in Sri Lanka exceeds 29 million and it is in a growing trend. Therefore, the storage and processing system must be scalable to cater growing requirement.

The Interpretation and presentation layer presents the processed information in dashboards and carry out communication, notification and event generation based on the severity.

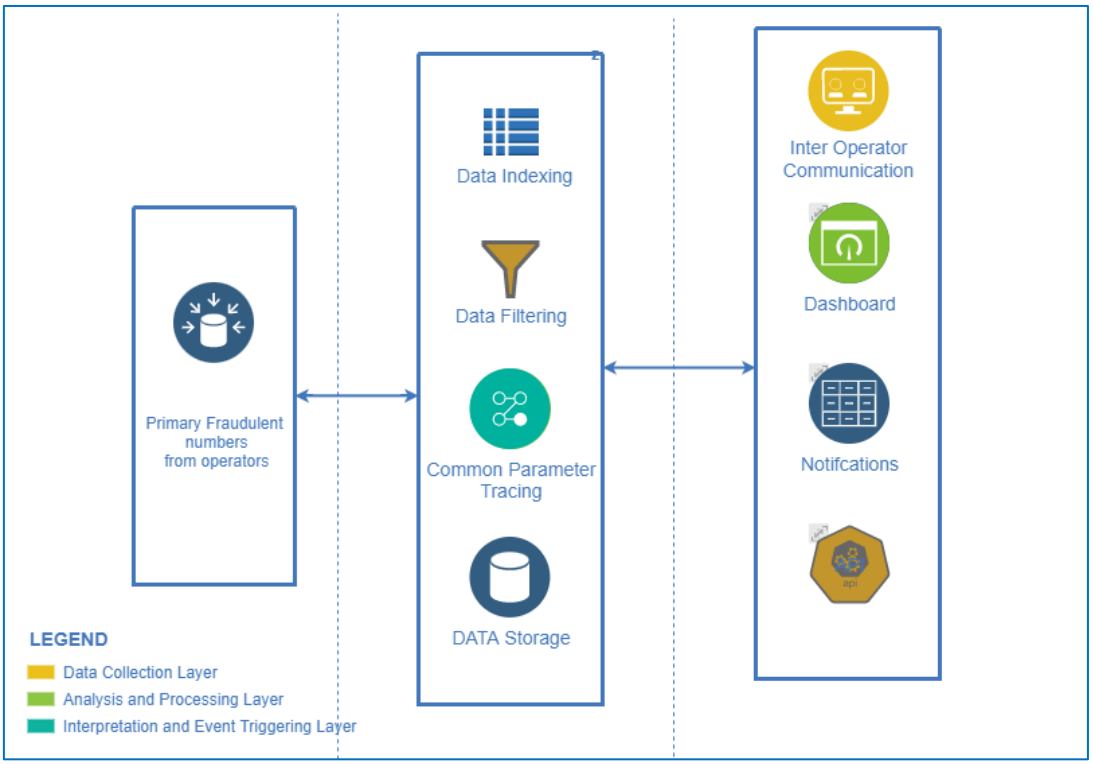

Figure 5-1: Main layers of the centralized system

1. Implementing a near-real time updating centralized system with onsite hardware at regulatory body premises

Figure 5.2 depicts the implementation architecture of near-real time updating centralized system with onsite hardware that should be deployed at regulatory body premises of a country. It is possible to avoid deployment of complex integrations and processing of whole CDR events in a single platform, by exploiting the already detected fraudulent number information. This is achieved by integrating near real time update of the database, which does not require storing any CDR in the centralized system.

The databases will work on active-standby mode to achieve higher redundancy. the carrier-grade hardware should be used for this. As this is beneficial to all the mobile operators in a country, the regulatory body should discuss with the telco vendors with

the support of telecom operators in the country. The bandwidth between the mobile operator and regulatory body of the country will not be critical as the amount of data communicated in an update, can be managed with a leased line. Firewall is maintained at the data entry point of the centralized system to improve the security and to avoid security breaches. Only the pre-communicated connections are allowed via the firewall from telecom operator to central system.

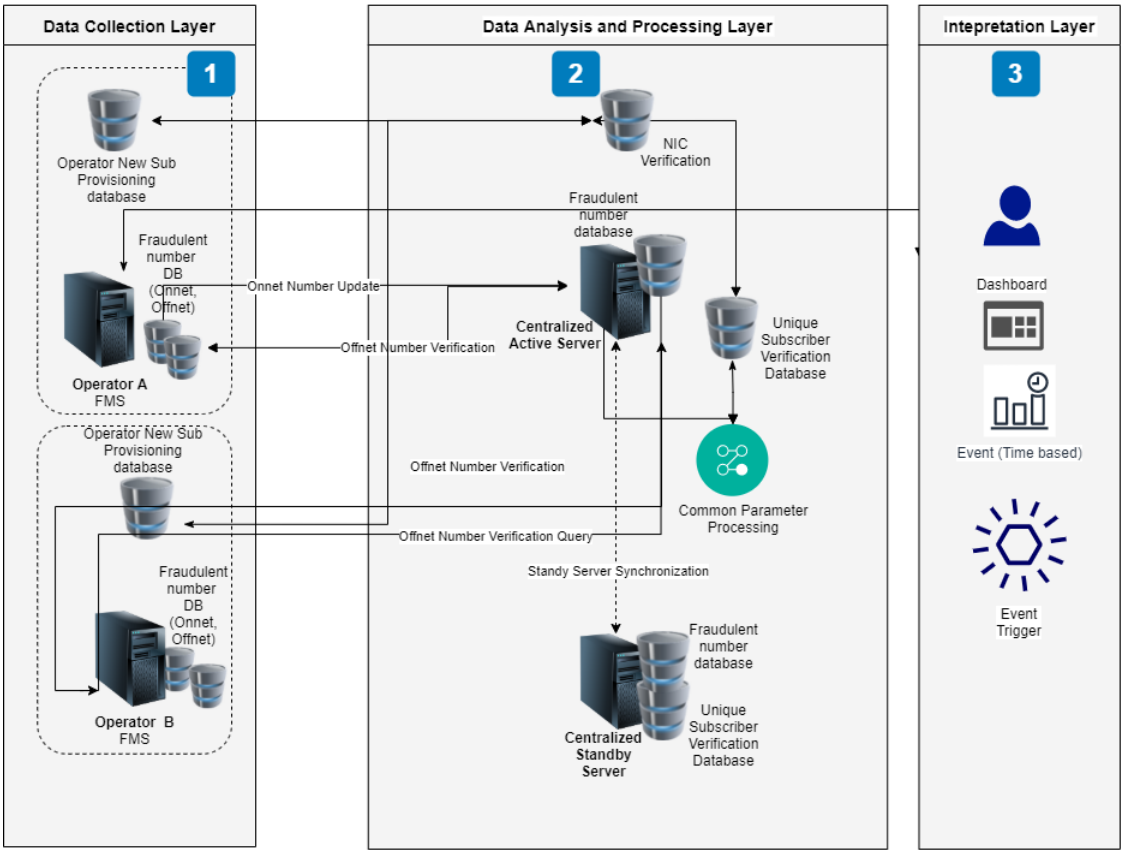

Figure 5-2: Architecture of centralized system deployed as regulator premises

2. Implementing a near-real time updating centralized system with remote hardware in third-party cloud

The centralized system can be deployed in an enterprise cloud, which is maintained by regulatory body of the country. The advantages of this deployment is less hardware deployment time and less human resource requirement for deployment and maintenance. Since the servers are maintained at third party remote site, the maintenance become less complex. Since the third-party partner typically manages the

setup and maintenance, the regulatory body can directly focus on data processing and communication activities. The scalability is comparably high in this approach.

One of the key advantages of this deployment is the saving in cost. If on-site hardware is maintained, separate support and maintenance team must be deployed for the operations, whereas a server room requirement also needed to be maintained. Mobile operators in the country should connect to the centralized system deployed in the remote server through a firewall.

However, it will be challenging to maintain the security requirements when the system is maintained in a third-party cloud due to possible data breaches. Since with the centralized system, the sensitive information data of all the mobile subscribers are maintained, the integrity and security of the information plays a prime role. Therefore, possible data breach is a challenge in this deployment. Malware injection, insecure APIs are some other security risks related to this remote server deployment.

3. Implementing a near-real time updating centralized system integrated with a centralized Central Equipment Identity Register (CEIR)

IMEI is a unique identifier allocated to a handset attached to a network. When an end customer uses a mobile service, this unique identifier is reported to the network. As described in section 3.2, the fraudsters use IMEI swapping method to avoid illegal bypass detection systems. Therefore, it has been challenging for the mobile operators to identify fraudulent numbers, as they behave as genuine customers. However, generally mobile operators use EIR systems to log the user equipment details of their subscribers. Therefore, we can expedite this fact to trace the fraudulent numbers. Currently, if a new device is registered in a network, it has to be registered under the regulatory body's database also. Therefore, it is possible to track the IMEI behavior with the use of CEIR[27]. It is possible to verify the IMEI of the reported equipment with respect to the fraudulent call generating numbers. Currently there is no visibility over the Off-net numbers, even if IMEI can be verified over the same network. The number of different IMEIs changed within 24 hours, 7 days should be used to track the fraudulent numbers across other networks.

It is challenging to stabilize the Central Equipment Identity Register (CEIR) database across all the networks and across all the devices, as the old devices are not registered with this system. However, the legitimate customers should be identified with the use of IMEI identification over the past years.

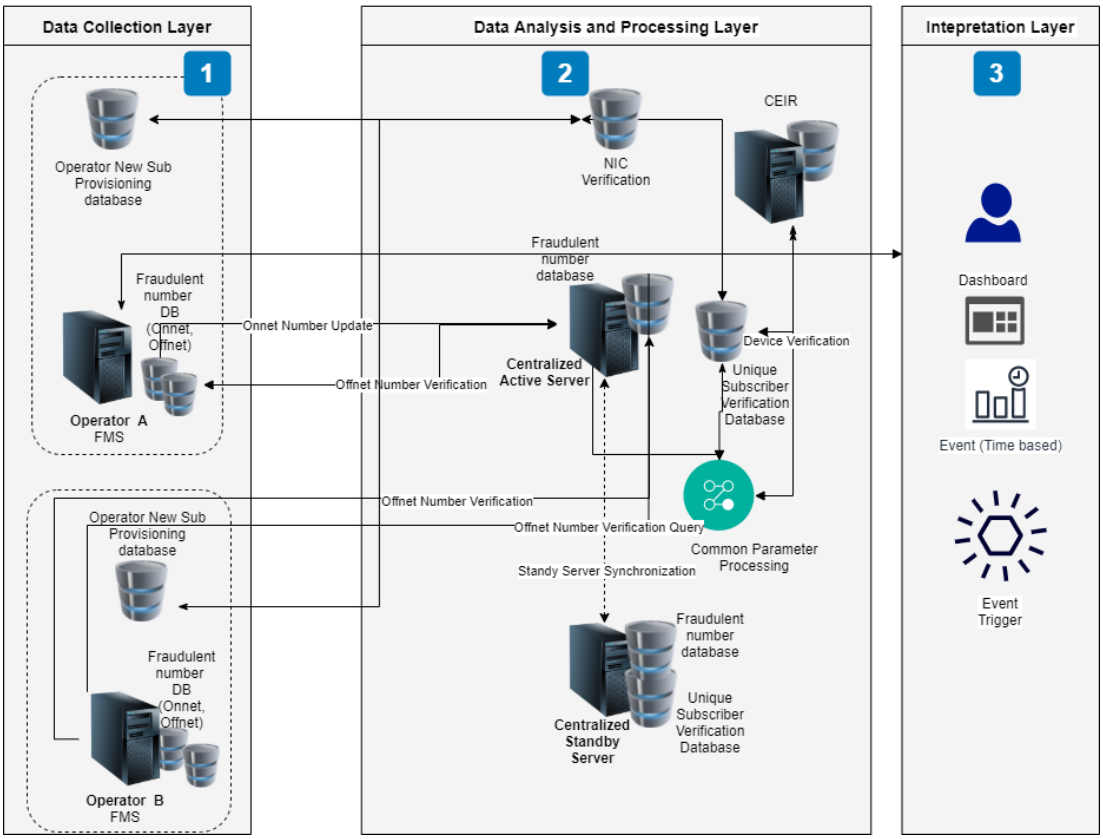

Figure 5-3: Architecture of Centralized system with CEIR Integration

Once a new device is used within a mobile operator, the respective IMEI is detected and reported to CEIR. The whitelist and blacklisted IMEIs are maintained in the CEIR once the IMEI is checked across GSMA database and regulatory body records. Since the fraudsters can use invalid IMEIs which are matched as blacklisted IMEI, then those can be blacklisted and updated in the database. Since all the operators have the visibility of the backlisted IMEIs, they can act accordingly. Even though fraudsters swap the IMEI numbers, still the same IMEI can be randomly used in 2 networks. Currently if one network detects such MSISDN and IMEI, it is not visible to other operators. Therefore, the second operator loses revenue until that fraudulent MSISDN in blocked. With this deployment, it will help to track the fraudulent MSISDN using

the IMEI. Operators do not solely depend on the IMEI details to identify a fraudulent number. Therefore, the detection effectiveness and accuracy increase with this deployment.

Figure 5.3 depicts the architecture for implementing a near-real time updating centralized system integrated with a centralized CEIR.

This implementation requires complex integration with CEIR or individual EIR systems of each operator in the country. It is required to synch the IMEI database of an operator to central EIR. The fraudulent number tracking can be done, with the use of IMEIS of identified fraudulent numbers.

5.1.2 Addition of reforms to existing regulations

Currently the regulatory body of Sri Lanka has taken regulatory actions and procedures to avert this telecom fraud prevalent in the country. In this section, the reforms that can be added to the existing regulations are mentioned.

1. Identify fraudulent numbers via customer complaint portal and provide incentives to encourage the customers

As identified in the literature survey and information gathering, the end customers face a lot of issues due to illegal call terminations. Customers cannot dial back after such call and they experience low call quality issues. Active detection resembles with the fraudulent number identification by the customers. If an end customer provides a fraudulent number, it can be categorized as 100% accurate. The fraudulent numbers provided by the end customers must be verified with the call records details and internal logs. When a fraudulent number is received from an end customer, it has to be notified to the respective mobile operator. Then the given timestamp and call records are matched with MSC CDRs and the complained call should be verified. The identified number should be further analyzed according to detection techniques and verified.

Incentives should be given to the end customers to encourage more case reporting. This can be achieved with the coordination of the respective mobile operator.

2. Introduce SLA and performance monitoring rules for FMS performance of mobile operators.

It is ironical to understand the divide and conquer behavior used by fraudsters to gain maximum profits from a country, whereas the same mobile operators have failed to share intelligence and insights to battle against the fraudsters. Generally, there are multiple mobile operators exist in a single country and fraudsters use the same to terminate the international calls. If at least one operator in the country does not work vigilantly to detect and block fraudulent numbers, the country loses the battle against the fraudsters. Therefore, it is the responsibility of the regulatory body to monitor and drive bypass detections with a proper set of rules and regulations.

Since the regulatory body of a country can act as a common body, it can impose rules and guidelines for fraudulent number communications. According to the census information, all the operators in the country has their own FMSs but the amount of information shared among the operators or the percentage of Off-net or On-net number communication cannot be guaranteed. From the detection to blocking a number across all the networks, the time duration taken is a key parameter which defines the loss to the company and to the country. Hence, regulatory body should introduce new rules for the SLA to be followed by the operators to communicate fraudulent numbers and FMS performance. Regulatory body should audit the performance of FMSs outcome in this way.

3. Deploying physical raids with the assistance of mobile operator Pico BTS

As reviewed in the literature survey and information gathered from the data collections, it is evident that, fraudsters have evolved from time to time, to avoid being detected as fraudulent bypass numbers. Hence, it is vital to detect the fraudulent numbers and take necessary actions to terminate those fraudulent activities. Even if the fraudulent numbers are blocked from a certain mobile network/network within a country, if the source is not traced, then the problem persist. Therefore, it is important to physically raid these locations, such that the individuals controlling this fraud can be identified and penalized.

As described in section 2.1 several location related parameters are used to identify the fraudulent numbers. Hence, it is possible to exploit that fact to geographically locate the fraudsters. After the pattern analysis, one or few cells can be identified as the hot cells where fraudsters can operate in. Once a hot spot is identified, it is challenging to pinpoint the fraudster exact location, as there could be multiple service cell sites and multiple possible geo locations.

In this situation, regulatory authority can work in collaborate with the mobile operators to pinpoint these locations. Specially designed fraudulent detection equipment has been already developed by the commercial vendors, where the geo location can be identified. Another alternative solution is to use the picoBTS to track the location by monitoring the latched MSISDNs with a real time monitoring platform. In this way, the search radius can be reduced and then the busting can be carried out with the support of local police department of the country.

5.1.3 Increasing user awareness

As per the focus group discussions and data gathering information, currently mobile operators have established various user awareness campaigns using SMS notification pushing to the customers about ISRF frauds. However, currently, the illegally bypassed calls are not considered to be central of attraction of the customer awareness campaigns due to the low call volumes. Therefore, in order to cover end user awareness gap, via the common framework, end customer education has to be carried out.

5.2 Proposed framework and recommendations

The major objects of the research interest are illegal call bypass issue and ‘One ring Scam’, which was reviewed in literature survey in section 2. Data gathering and analysis is carried out based on the problem formulation, which assists the construction of a common framework to avert above issues. Six aspects were identified based on the data analysis where the concerned areas lie on. three major components were identified to include in the common framework. Section 5.1 highlights the available methodologies for common framework. In this section, the proposed framework and suggestions are discussed.

The major three components of the common framework identified based on the analysis, are as below.

1. A central system should be implemented to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country. The scope of information shared with each operator, has to be controlled by the regulatory body.
2. Adding reforms to the existing regulations
3. A mechanism to increase user awareness and get the support of the public to identify the fraudulent numbers.

Operators detect and block large volumes of fraudulent numbers, yet the overall problem does not go away. Fraudsters succeed despite the anti-fraud efforts of the operators, if at least one of the operators in a particular country acts lose on the bypass detection. If one operator does an excellent work of detecting illegal bypass in its network, then the fraudsters will simply step up their attacks on the other operators in the country. Therefore, in national level, the problem goes deeper. Therefore, the national regulator can step up and coordinate the SIM Box bypass problem directly using this framework.

5.2.1 Establishing a centralized system for IDD fraudulent number tracking

As the major aspect of the framework, a centralized system should be developed to track fraudulent numbers, so that regulators can gain macro level understanding of the SIM Box fraud occurring across the country. Once the fraudulent activities are understood, the regulator can then develop a strategy to prioritize the defensive measures based on each mobile network.

The most suitable approach that should be implemented with a shortest time is identified as ‘Implementing a near-real time updating centralized system with onsite hardware at regulatory body premises’. This method has higher data security over the other 2 methods, due to enhanced security due to server maintenance in the regulatory premises itself. The integration with CEIR can be considered as a future work once this method is deployed. Centralized system serves major 2 activities. First one is the

processing of bypass detection. Other activity is maintaining common platform to identify ‘One Ring Scam’ issue. First major activity is discussed in the following.

The main layers of the centralized system are data collection layer, data analysis and processing layer and interpretation and presentation layer as depicted in figure 5.1. The main data feedback is the fraudulent numbers identified by the mobile operator, using active and passive detection methods. They should update central database when a fraudulent number is detected. In passive detection, the behavioral patterns are analyzed to detect the fraudulent numbers with low false positive rate. Since one of the main objectives of maintaining a central database is to keep the holistic view and to optimize passive detection of Off-net numbers, data fields in table 5.2 needs to be communicated along with the fraudulent number. Customer NIC, most served location details, most served IMEI, number of IMEIs used within last 30 days, connected date parameters are fed to process tracing across different networks based on a common parameter. In addition to the fraudulent number update, it is required to update common database when a new SIM card is provisioned in a network. This is to identify the authenticity of the end customer and to be used for common tracing activities.

Table 5-2: Data fields updated from operator FMS

Field Name	**Field Type**	**Description**
calling_party_id	String	Subscriber identity number of the user who originates the call
called_party_id	String	Subscriber identity number the user who is intended to receive call– last identified bypass call
release_dir	String	Indicate which party disconnected the call initially – last identified bypass call
time	Integer	Date and time when call attempt reached to the system- – last identified bypass call
duration	Double	The duration between answer time and disconnect time- – last identified bypass call
call_dir	String	Indicates whether mentioned transaction is for incoming call to local network or outgoing call from local network- – last identified bypass call
nic_of_customer	String	NIC number of the customer
first_connected_ date	Date	First connected date of the customer

most_served_cellID	String	Most served CellID
number_of_imei_7_days	Integer	Number of IMEIs used within last 7 days by the same a number

In addition to above parameters, served location and last call details are communicated to the central database, which are only accessible by the regulatory body.

The fraudulent numbers are mainly categorized as On-net and Off-net. According to the user census and focus group discussions, it was identified that currently, detected On-net numbers are not communicated to all the other operators in the country. Mostly the fraudsters use SIM cards from all the operators within a country to terminate an illegally routed call and they tend to swap SIM cards randomly for call termination. If one operator (Operator A) detects a certain fraudulent number or a set of fraudulent numbers which should be identified as from a single source, all the other operators (Operator B, Operator C etc.) are not aware of that fraudulent numbers. Sometimes operator B or C would not be able to detect the fraudulent numbers from above fraudster source until few days. However, if the On-net fraudulent numbers are communicated to other operators, then other operators can expedite this rich information and detect fraudulent numbers on their own networks faster.

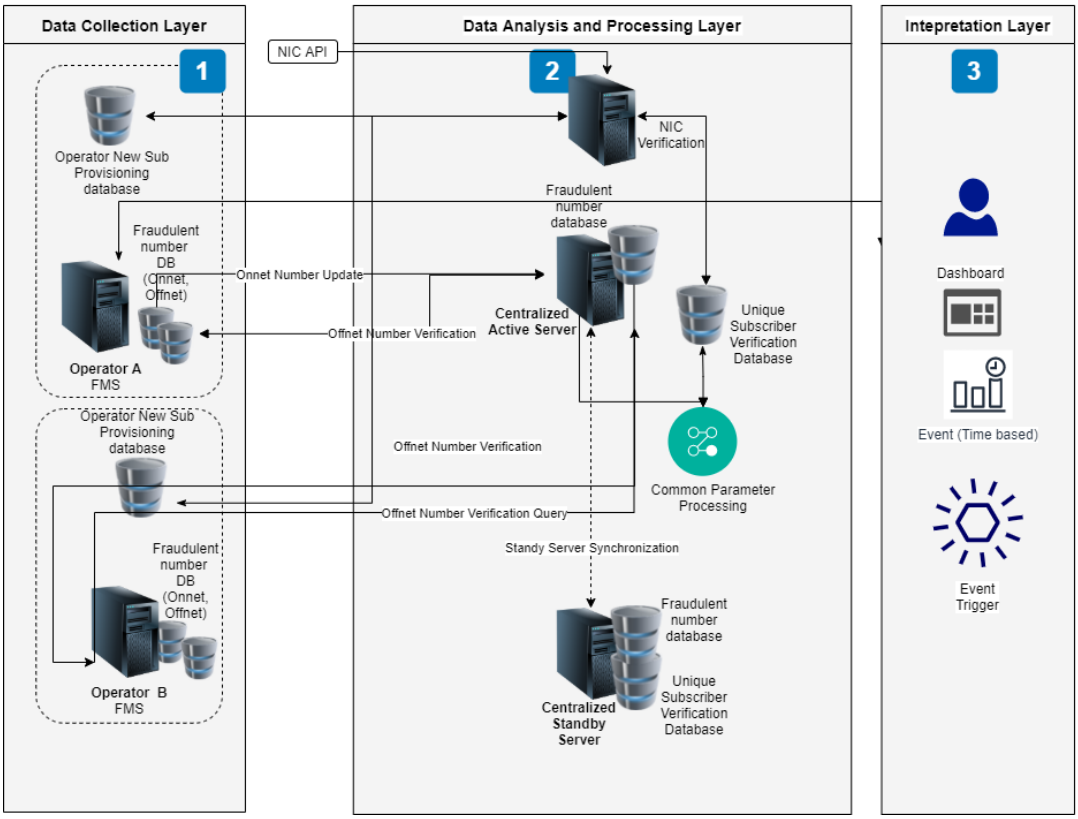

Figure 5-4: Architecture of Proposed Centralized System

Other type of data feed is the MSISDN verification related details. When a new MSISDN is registered in a particular network, the user information details should be updated in central database. Currently, 5 SIM cards are issued under a single NIC. Fraudsters tend to use fake NICs for the new SIM cards purchased. However, in some cases, it was identified there are fraudulent numbers registered under same NIC, while having 1 or 2 legitimate SIM cards. Currently, since there are no records over the Off-net numbers, the NIC tracing is cannot be fully covered. After deploying the centralized platform, it is possible to track all MSISDNs attached to a single NIC across various mobile networks. Since there are 4 mobile operators in the country, a single NIC can obtain 20 SIM cards. A valid NIC should be validated based on NIC validation database of the country. Since the complete NIC database maintaining is challenging, the NIC query happens via an external API provided by an external party. In Sri Lankan context the NIC query API is provided by the department for registration of persons. The NIC query API is only provided to an authenticated party with a proper justification for the usage of the NIC query API.

Figure 5.4 depicts the proposed architecture for the centralized system. In the Sri Lankan context, currently 4 mobile operators are in presence, where the FMSs of these operators are connected to centralized system. The overall mechanism of the centralized system is as follows. When a fraudulent number is detected by a mobile operator, it is updated in their FMS databases and sent the same update to fraudulent number repository at central database at regulatory body. Since these numbers are categorized as On-net and Off-net numbers, an On-net number is considered to be a valid fraudulent number when received. The status of an Off-net number is maintained in the status as 'to be verified'. If 'operator A' reports an Off-net fraudulent number from 'operator B', then first it is updated in centralized database and it is sent only to the relevant 'operator B' for verification. SLAs is defined as 24 hours to verify weather the number is a genuine number or a fraudulent number. If operator B fails to update the verification within 24 hours, then SLA breach time will be calculated, and reminders will be sent every 24 hours. Once the verification is finished and response obtained from 'operator B', that Off-net fraudulent number status will be updated as 'verified' and updated for all other operators' access.

Once a verified fraudulent number is updated in the centralized system, all the operators get the number and the parameters related to behavioral patterns. Hence, each operator should feed these parameters to their internal FMSs to optimize the detection algorithms. Complex events are used for bypass detection in [13], whereas it can be further optimized with the events identified with common visibility over Off-net fraudulent number usage patterns. As with the above example, 'operator C' or 'operator D' should check whether there are call records from that fraudulent number, which was identified by 'operator A' as an Off-net number of 'Operator B'. If the MT records are available, then Operator C and D can optimize why it has not been captured from their internal FMSs and optimize the detection algorithms. Another aspect is that detected On-net numbers are currently not communicated to all the other operators. With the centralized system, all the operators including regulatory body gains the visibility over these numbers. All the operators and regulatory body can gain visibility from the dashboard of the system, how many numbers have been detected in each hour, day, monthly level and other important graphs.

Since it is not feasible to dump all the call records to the centralized system, it works with the inputs obtained from individual operators. With the centralized system, it can process these common parameters and behaviors, to trace the possible fraudulent numbers or fraudster locations. Since the customer unique data such as NIC, IMEI, location details are available within the system, centralized system can process these details to identify the hotspots of the fraudster activities. Even though fraudsters use fake NICs, still there is a probability of detecting a fraudulent number in another network, using the same NIC. If a fraudulent number 1 of Operator A uses a NIC1, currently it is not traceable over the other networks. With the centralized system, all the IMEI, and NIC details are updated which enables all the operators trace over this common parameter and provide update to the centralized system. Another major parameter obtained in the serving CellID or CellID range of a fraudster. If operator A verifies 100% that a fraudster is working withing a certain CellID range, currently that valuable information is not visible to the other operators. With the centralized system, it can trace over these details to identify their own networks' fraudulent numbers. Since the sharing models are used in access network level, the location or CellIDs of different networks can overlap.

Other major activity of the centralized system is to maintain a common platform for identifying 'One Ring Scam' issue. According to the user census, apart from the internal CDR records, currently they use, carrier, remote operator and roaming partner notification and proactive online monitoring systems to detect these IDD numbers. Those IDD numbers are generally from the countries with high premium rate. Hence, it is vital to reduce time duration taken to identify these numbers, to minimize the possible revenue loss. Once such suspected number is detected by an operator, it is updated in the centralized system and then broadcasted to all other operators connected to the centralized system. In this way it is possible to approach this issue with a divide and conquer method, where a single identification will benefit all the operators in the country. It is possible to deploy these attacks to different networks in different time stamps with delays. With this centralized system, those numbers can be pre-identified, so that it is possible not to wait until the network generates a lot of calls to these suspected numbers and verify.

In forming a common framework for a particular country, it is vital to focus on the financial aspect, engaged with several areas. The major cost component of this framework is the deployment of the centralized system in the regulatory premises. As explained in 5.1.1, the system consists of 3 layers: data collection, data processing and interpretation layers. Fraudulent number detection process involves a rigorous data gathering and data processing activities and it is carried out by the individual operators, which is already a prevalent established process. The centralized system receives the fraudulent numbers identified by the operators and the centralized system is involved in correlating these numbers with identification unique parameter (such as NIC), and event triggering based on the identification. Hence, the computer processing requirement is less compared to the FMS system processing.

The processing power can be decided based on mobile subscriber base in the country2. The processing and storage requirement can be calculated with a parametric values based on below parameters.

- Usage pattern of the subscribers in the country
- Number of operators in the country
- Subscriber base of each operator in the country
- Number of illegal call volume, call count detected within last 5 years

Since this framework has been introduced as a common solution, the exact hardware requirement can be varied as described above.

When the cost components are identified, it is essential to outline the possible monetary sources for the deployment of the system. Below are 3 major funding mythologies possible

1 The total cost for the implementation of the centralized system is born by the regulatory body of the country
2 The total cost for the implementation of the centralized system is born by a common fund established by the regulatory body, where operators in the country contribute with annual payments

3 The total cost for the implementation of the centralized system is devided between regulatory body and a common fund(controlled by the regulatory body of the country)

Since both the regulatory body of the country and the operators benefit from the centralized system equally, the third funding method is proposed with the common framework. In Sri Lankan context, (common fund) has been established by the regulatory body and all the licensed operators are liable with an annual payment to the fund. Hence, with third funding method, the centralized system can be deployed.

With the introduction of a centralized system goals in table 5.3 are achieved via the common framework.

Table 5-3 : Goals to be achieved via a centralized system

Goal to be achieved via centralized system	**Methodology**
Gain national visibility over bypass fraud	this is achieved via the near real time update of the centralized database
Improve accuracy and effectiveness of fraudulent number detection	This is achieved via sharing the fraudulent numbers across the networks, such that each operator can use these parameters and optimize detection algorithm
Reduction of overall time duration from detection, verification to blocking steps	This is achieved via maintaining SLA for each detection and counting SLA breached durations.
Fraudster tracing via common parameter	This is achieved by the number processing in the centralized system, with the availability of customer unique information and location information
Parameter sharing for ‘One Ring Scam’	This is achieved by broadcasting the identified suspected numbers to other operators via a centralized system

5.2.2 Addition of reforms to existing regulations

Another aspect of the framework is to drive the telecom operators in a country towards alleviating this common issue, via a common guideline. It is vital to have adherence of all the mobile operators towards this national goals. Adding reforms to existing regulations can achieve this.

Among to reforms three discussed reforms, two are identified as the feasible implementation within a minimum time duration. Those two reforms to be included in the common framework are as below.

5.2.2.1 Identify fraudulent numbers via customer complaint portal and provide incentives to encourage the customers

End customer intervention to avert illegal bypass is a successful method practice in some countries [26]. A user-friendly online GUI should be developed for the customers to report fraudulent IDD MT calls. Since these incidents are 100% accurate, if the end customer provides an actual scenario, it is possible to exploit this to identify fraudsters. End customers receiving MSISDN, MO calling party CLI, Date, Time should be obtained via the mandatory parameters. Once such record is updated, those details should be verified using the CDRs and logs in the respective operator. It is possible to provide incentives to these end customers in terms of free IDD minutes, from the respective operator as a reward for the complaint logging. The amount of free incentive should be decided collaboratively. Compared to the possible revenue loss that can be occurred, providing an incentive is beneficial to the operators. This encourages customers to report such incidents.

In addition to online GUI, a SMS short code or USSD short code should be introduced to report such incidents for the customer who does not have online access. Same incentive should be those customers too.

5.2.2.2 Introduce SLA and performance monitoring rules for FMS performance of mobile operators.

In order to make the detection and communication process efficient, it is required to monitor the overall process by the regulatory body. Therefore, it is important to

monitor the performance of the FMSs to make sure that all the network operators play a genuine role in detecting fraudulent numbers. With the implementation of the centralized system, it facilitates to generate statistics of the number of detected fraudulent numbers and the frequency. According to the operator census information, and information analysis, there is no guarantee over the reporting of the fraudulent numbers to other networks. By imposing performance monitoring this can be achieved.

The major performance can be identified as the number of fraudulent calls detected in an operator network as a percentage of the subscriber base. If one operator fails to detect the fraudulent numbers, it can also be derived from the shared information within the centralized system. If 'operator A' fails to detect a set of their On-net numbers, but same number set has been detected by another network as Off-net numbers, then the reverse calculation can be carried out to check how many illegally terminated minutes has occurred within 'operator A' network based on the past CDR. In this way, regulatory body should verify the credibility of the data provided by the operators. SLA should be introduced to avoid delays in the fraudulent number reporting and communication.

Another verification method to validate how well the operators in their market are applying control systems is to run own TCG by the regulatory body. Since these are random and independent numbers, regulators can analyze the respective CDRs after requesting from the mobile operators to gain more deep knowledge about the fraudulent numbers. This can be carried out with proper privacy and trade secret handling with the collaboration with the operators. An API can be called to check the CDRs only for the identified numbers via TCG by the regulator.

Since bust operations using the picoBTS of each mobile operator is not ready to go, it is considered as a future activity under the reforms. Once the hot spots are identified, the regulatory body can "drive-by" antenna location in specific neighborhoods to identify the correct location, and then can make arrets with the support of police officers.

5.2.2.3 Implementing restrictions based on already identified fraudulent NIC numbers

Avoid issuing numbers under the NIC numbers that were identified as fraudulent numbers. In this way the fraudulent users can be tracked and further issuance of SIM cards under the same NIC can be restricted. The requirement of this is to make sure that same NIC is not used for further fraudulent activities.

Currently 5 SIM cards can be obtained for a single NIC in Sri Lanka. Hence the fraudsters use this to gain more sim cards from the market. By restricting SIM card issuance from one operator, then it is possible to avoid penetrating across the other networks. At the time of provisioning a new SIM card by an operator, the NIC is verified from the centralized database. Once an attempt to purchase a new SIM card under fraudulent NIC is detected, each operator can trace back to the customer can take necessary actions with the involvement of the regulatory body. Currently, there is no method to detect those fraudulent numbers at the time of sim issuance. Even if a fraudulent number is identified afterwards, there is no method to trace to the physical person who has purchased this SIM card. Since the centralized database consisted of all the numbers provisioned under 1 NIC, then if one operator does not operate correctly to restrict the issuance of the SIM cards under fraudulent NICs, it can also be identified. The regulatory body can impose a penalty on that.

5.2.2.4 Introducing a consortium for implementing the proposed policy framework

Implementing the policy framework can be carried out based on the existing regulatory architecture within a given country. One of the major challenges in implementing the policy framework is the restrictions faced by regulatory body in terms of accessing customer sensitive data that has to be fed into the centralized system. Hence, the proposed policy framework can be put into action via a common consortium which is formed by all the operators in a particular country.

Since the advantages of implementing the policy framework is born by all the operators in a country, operators can agree with a common consortium forming, so that the new framework is driven under this common consortium.

The advantages of implementing the reforms and policy framework via a consortium can be identified as follows. By establishing new rules for accessing customer sensitive data for centralized system, current limitations can be overcome. Another advantage is the transparency that can be achieved by each operator. Since the consortium is comprised of all the operators, the activities can be directly monitored by the members of the consortium themselves. Since the consortium has the members from the operators, the implementation of the system can be optimized with the direct involvement from the operators.

Some of the disadvantages of forming a consortium can be identified as follows. Establishing a new consortium will be more time consuming compared to the centralized system implementation by the regulatory body of the country. Another challenge is forming common agreement with the involvement of all the operators in the country, whereas a regulatory body can use its powers to extent some demands to all the operators within a country.

Goals mentioned in table 5.4 are achieved by adding reforms to the existing regulations.

Table 5-4 : Goal to be achieved via adding reforms to existing regulations

Goal to be achieved via adding reforms to existing regulations	**Methodology**
Avoid delays in reporting and guarantee of fraudulent number reporting	This is achieved via introducing performance monitoring guidelines and SLA for fraudulent number communication

5.2.3 Increasing user awareness

As the third fragment of the common framework, user awareness campaigns should be carried out to educate the end users about these frauds. Even though customer portal for issue reporting is introduced, customer education should be carried out to get the responses and to inform about the rewards for the customer, if a scenario is reported.

Since money loss due to ‘One Ring Scam’ issue is experienced by the end customer, it is required to educate the customer not to call back for the suspected numbers.

With the introduction of online GUI, already identified suspected numbers are shown in the GUI together with the recent timeline. With this, customer can access the website to check the available number base, if he receives a suspected missed call or SMS campaign to call those numbers.

TV advertisement, leaflet distribution, newspaper advertisement, social media campaigns are some of the available methods for increasing customer awareness. Comparing the reachability of those methods, TV advertisement can be identified as the most suitable method for user awareness. If the TV awareness campaign is carried out by a single operator, the audience may receive the wrong message that only that particular network is having that issue. Hence, regulatory body should roll out the TV awareness campaign with the mention of all the operators within the country.

With the user awareness campaign, the goal in table 5.5 is achieved.

Table 5-5: Goal to be achieved via increasing user awareness

Goal to be achieved via increasing user awareness	**Methodology**
Avoid customers from calling back to ‘One Ring Scam’ numbers and educate about bypass calls	This is achieved via carrying out TV advertisement and online website information

5.3 Comparison of existing regulations and proposed policy framework

In Sri Lankan context, the current regulations had been declared under the Telecommunications Act No 25 of 1991 and its amendment Act No 27 of 1996[30]. Since the Act has been amended about 26 years prior to this work, the proposed policy framework can be amended as an improvement to battle against the illegal bypass

fraud. Since, the bypass fraudsters find ways and means of counter-attacking all the preventive measures taken by the operators and the regulatory body, strengthening the regulations will enhance the capability to make the fraud detection and avoidance process more effective.

One of the major differences between the existing regulations and proposed framework, is that different aspects have been covered in each. The existing regulations cover the restriction of providing new VoIP paths, and to restict telecommunication apparatus without regulatory consent. It has restricted trade, manufacture, import, sell, offer for sale, deal in transfer, hire, lease, demonstrate, maintain or repair, any telecommunication apparatus, except under the authority of a license issued by the commission in such form as may be determined by the commission, under section 21[30]. With the proposed policy framework, new policy regulations are introduced for the actions to be taken after fraudulent number detection, whereas similar process is not included in the existing regulations. New policy framework consists of

- SLA for the fraudulent number communication to the common platform
- SLA for offnet fraudulent number verification (whether the suspected fraudulent number is a genuine number or an actual fraudulent number) for the operator.
- Penalty for each operator in breaching the agreed SLAs
- NIC verification for new number provisioning – restriction of issuing new SIM cards under the same NICs, that has already been identified as a fraudulent subscriber

The proposed policy framework consists of the minimizing the propagation of fraudulent numbers further, based on information extracted through already detected fraudulent numbers.

Another difference is the method of fraudulent number communication. As per the current practice, once a fraudulent number is detected, it is updated via a daily email to the other operator. With the proposed system, the communication will be near real time and operators are bound to respond for the identified fraudulent numbers.

Currently the On-Net fraudulent numbers are not communicated to the other operators in the country, with the proposed centralized system, the On-Net fraudulent numbers are updated in the centralized system. Every operator can exploit this and optimize the detection algorithms developed in each FMSs.

5.4 Policy framework implementation plan

Policy framework implementation can be carried out as an direct deployment via the regulatory body or via a consortium consisted of all the mobile operators in the country. For both the deployment methods, below overall steps can be followed.

1. All the mobile operators in the country should provide the consent to regulatory body for the disclosing identified fraudulent numbers
2. All the mobile operators in the country should connect with centralized system deployed at regulatory body's premises or a core-room established by the consortium, to communicate the information in near real time
3. All the mobile network operators should update the relevant details of the new SIM connections together with SIM provisioning the network
4. Once an Off-net fraudulent number related to own network is received, operator should respond within the agreed SLA time
5. All the operators should update the FMSs performance reports to be reviewed by the regulatory body
6. Once common parameter tracing is implemented, operators should assist the process by providing the required event information
7. End customer should be allowed to report the incidents via customer portal
    - Customers are allowed to report incidents via website
    - Customer are allowed to report via SMS and USSD methods
    - Operators should provide incentive in terms of IDD call time or monetary value once the incident is verified, within an agreed time period after the reporting

6 CONCLUSION AND FUTURE WORK

This chapter concludes dissertation with the summary and possible future enhancements.

Common framework consisting of three core components are designed to address the problem identified in 5.1. Below three aspects were covered through the proposed common policy framework.

1. A central system is designed to update the On-net and Off-net fraudulent numbers across all the telecom networks within the country. The scope of information shared with each operator, can be controlled by the regulatory body as per the proposed architecture of the implementation
2. Adding reforms to the existing regulations were achieved with the introduction of customer complaint portal and by introducing SLA and performance monitoring rules for FMS performance of mobile operators.
3. User awareness increase methodology is identified as communication through television channels.

This common policy framework can be adopted to different countries or regions by performing minor changes to suit to the operator FMS setup of the relevant country. Since the regulatory body of a country has the basic control and connectivity among the different operators, this can be achieved with an agreement from all the operators to adhere to this common framework.

The objectives outlined in section 1.6 are achieved as described below.

- Identify existing detection techniques of grey calls, negative impacts of Illegal Call Termination and Abnormal Call Scenario related to ISRF and identify the existing solutions– literature survey was conducted, and the respective areas were covered.
- Identifying the drawbacks and limitations in current IDD fraudulent number communication process – this was achieved through the mobile operator census survey and focus group discussion with the regulatory body of the country.

- Formulating a common policy framework and provide recommendations covering different aspects identified via data analysis – A common policy framework is introduced covering the three aspects explained in section 5.2

6.1 Research limitations

The major challenge faced during the research was the limited access to the sensible data of the mobile operators. Since the fraudulent detection is currently carried out solely as an operator dependent activity, none of the mobile operators are ready to share the actual stats related to the fraudulent detection performance. Hence, it is hard to act or introduce such framework without the intervention of a common regulatory body from the very scratch level. In order to conduct a regression analysis to identify the relationships between the accuracy levels and contributing factors is not feasible with this study as the exact accuracy level data is not accessible from the operators in the country. Hence, multiple regression was not used. Further, based on the data gathered, it is possible to expect a concentrated distributed data set(compared to a homo-cardinality), as almost all the detections strategies within the operators are identical.

6.2 Future work

In this research, the common framework has been outlined based on the most feasible and less time-consuming components, so that it can be started without much delay. It is identified that integration of CEIR can be carried out as an activity develop this common framework. With the integration of CEIR, it will facilitate further blocking of illegal IMEI numbers, which in turn reduce the SIMbox fraud. Common parameter tracing can be optimized with the use of CEIR.

Another aspect to be looked at, as a future work is to use test call generation tool integration to the proposed centralized system. It is evident that regulator has to have a proper methodology for verification of the effectiveness of the individual bypass detection systems and their performance. TCG can be used as an independent approach where the regulator can randomly carry out testing by using different SIMs of all the operators within a country. Commercial testing functionality serving tools are available for that purpose, which has the scheduling capability. Since the test numbers

are picked by the regulator and owned by the regulator, it is possible to request the CDRs of the test numbers, without intervening the privacy of live customers' data.

Rewarding and penalizing operators to ensure policy compliance is another reform activity that can be carried out as a future activity. In order to carry out this activity, the centralized system has to be evolved to become a stable system to generate the correct reports. The mobile operators also need time to adopt to this framework, to check the compliance in this higher level.

When the enforcement is weak towards the fraudsters, they invest more money in deploying more SIMBoxes to capture more revenue. Raids and arrests can reduce this tendency. The regulatory body should coordinate with operators to identify the hot spots of the fraudsters and then use the special Radio frequency measurement units to pinpoint the fraudster location. Portable PicoBTSs can be used to track the cell locations by changing the radio signaling parameters. Then the police can quickly intervene to confiscate SIMBoxes and make arrests.

7 REFERENCES

[1] GSMA, "The Mobile Economy 2020", Gsma.com, 2020. [Online]. Available: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf. [Accessed: 22- May- 2021].

[2] Trend Micro Research, "Cyber-Telecom Crime Report 2019", 2019.

[3] "Fraud Loss Survey 2019", Cfca.org, 2019. [Online]. Available: https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf. [Accessed: 22- May- 2021].

[4] "International Call Termination in Nigeria [NTAnews24 Video Transcript] - en.ANTRAX", en.ANTRAX, 2021. [Online]. Available: https://en.antrax.mobi/nigeria-international-call-termination/. [Accessed: 22- May- 2021].

[5] "Statistics- Telecommunication Regulatory Commission of Sri Lanka", Trc.gov.lk, 2020. [Online]. Available: https://trc.gov.lk/images/pdf/SOV_Q42020.pdf. [Accessed: 22- Mar- 2021].

[6] "SIM box - Wikipedia", En.wikipedia.org, 2020. [Online]. Available: https://en.wikipedia.org/wiki/SIM_box. [Accessed: 22- Aug- 2021].

[7] I. Murynets, M. Zabarankin, R. P. Jover and A. Panagia, "Analysis and detection of SIMbox fraud in mobility networks," IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 2014, pp. 1519-1526, doi: 10.1109/INFOCOM.2014.6848087.

[8] R. Sallehuddin, S. Ibrahim, A. Zain, and A. Elmi, “Detecting sim box fraud using neural network,” in IT Convergence and Security 2012, K. J. Kim and K.-Y. Chung, Eds. Dordrecht:Springer Netherlands, 2013, pp. 575–582.

[9] ——, “Detecting sim box fraud by using support vector machine and artificial neural network,” in Jurnal Teknologi, vol. 74, Apr. 2015, pp. 137–149.

[10] B. Veloso, S. Tabassum, C. Martins, R. Espanha, R. Azevedo, and J. Gama, “Interconnect bypass fraud detection: a case study,” Annals of Telecommunications, vol. 75, pp. 583–596, Oct. 2020.

[11] I. Murynets, M. Zabarankin, R. P. Jover, and A. Panagia, “Analysis and detection of simbox fraud in mobility networks,” in IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, Apr. 2014, pp. 1519–1526.

[12] M. Kashir and S. Bashir, “Machine learning techniques for sim box fraud detection,” in 2019 International Conference on Communication Technologies (ComTech), Apr. 2019, pp. 4–8.

[13] K. Kehelwala, H. Bandara, R. Yasaratne, P. De Almeida, I. Ilesinghe, and P. Wickramasinghe, “Real-time grey call detection system using complex event

processing," IET, Sri Lanka, Tech. Rep., 2015. [Online]. Available: http://theiet.lk/wp-content/uploads/2017/10/22-p7.pdf

[14] B. Veloso, S. Tabassum, C. Martins, R. Espanha, R. Azevedo, and J. Gama, "Interconnect bypass fraud detection: a case study," Annals of Telecommunications, vol. 75, pp. 583–596, Oct. 2020.

[15] Federal Communications Commission, "'One Ring' Phone Scam", 2019. [Online]. Available: https://www.fcc.gov/consumers/guides/one-ring-phone-scam. [Accessed: 20- Apr- 2021].

[16] "Protecting Consumers From One-Ring Scams", Federal Register, 2021. [Online]. Available: https://www.federalregister.gov/documents/2021/01/13/2020-27652/protecting-consumers-from-one-ring-scams. [Accessed: 01- May- 2021].

[17] Black Swan Telecom Journal, "Araxxe on the art of deception and analysis in sim box fraud warfare," Article, Feb. 2019. [Online]. Available: http://bswan.org/araxxe art of deception.asp. [Accessed: 22- May- 2021].

[18] "CSG Assure Illegal Bypass Detection, SIM Box Detection - CSG", CSG. [Online]. Available: https://www.csgi.com/portfolio/digital-wholesale/assure/assure-sim-box-detection/. [Accessed: 23- Mar- 2021].

[19] "AN ASSESSMENT OF INTERNATIONAL VOICE TRAFFIC TERMINATION RATES", Ncc.gov.ng, 2015. [Online]. Available: https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/681-the-principles-of-international-termination-rate/file. [Accessed: 23- May- 2021].

[20] "Gateway Liberalization", Gsma.com, 2016. [Online]. Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/09/GSMA-Gateway-Liberalisation.pdf. [Accessed: 23- Aug- 2021].

[21] "THE TELECOMMUNICATION INTERCONNECTION USAGE CHARGES (FOURTEENTH AMENDMENT) REGULATIONS, 2018", Trai.gov.in, 2021. [Online]. Available: https://www.trai.gov.in/sites/default/files/Regulation_IUC_Eng_12012018.pdf. [Accessed: 20- Mar- 2021].

[22] M. Rasheed, A. Khaliq, A. Sajid and S. Ajmal2, "Identification of Hidden VoIP (Grey Traffic)", Journal of Computer Networks, vol. 1, no. 2, pp. 15-27, 2013. Available: 10.12691/jcn-1-2-1.

[23] "ITU Regional Economic and Financial Forum of Telecomunications/ICTS for Arab Region", Itu.int, 2015. [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2015/EFF/Pres/Bahrein%20Session%202%20-%20ALTERNATIVE%20CALLING%20PROCEDURES%20%20v4%20PS.pdf. [Accessed: 23- May- 2021].

[24] "Mobile taxation: Surtaxes on international incoming traffic", Gsma.com, 2011. [Online]. Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2011/09/Mobile-taxation-Surtaxes-on-international-incoming-traffic-Executive-Summary-English.pdf. [Accessed: 23- Mar- 2021].

[25] S. Traut and P. Purich, Getting Started Guide for Oracle Complex Event Processing, Oracle, Aug. 2012, version 11.1.1.6.3. [Online]. Available: https://docs.oracle.com/cd/E23943 01/doc.1111/e14476/overview.htm#CEPGS106

[26] R. Samarajiva, "Carrots and sticks: Principles of effective regulation to curb illegal bypass in international voice traffic", *Academia.edu*, 2012. [Online]. Available: https://www.academia.edu/2887389/Carrots_and_sticks_Principles_of_effective_regulation_to_curb_illegal_bypass_in_international_voice_traffic. [Accessed: 23- May- 2021].

[27] A. Saputhanthri and K. Samarasinghe, "Policy Framework and Recommendations to Minimize the Usage of Stolen and Counterfeit or Substandard Mobile Communication Devices", Ieeexplore.ieee.org, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/8818788. [Accessed: 17- May- 2022].

[28] Weerasinghe, W & Ajward, Roshan. (2019). ISSUES OF CORPORATE GOVERNANCE PRACTICES IN SRI LANKA: PERCEPTIONS OF PROFESSIONALS. Vol. 2. 1-19.

[29]"VOIP Unblocking - Telecommunications Regulatory Commission of Sri Lanka", *Trc.gov.lk*, 2014. [Online]. Available: https://www.trc.gov.lk/voip-unblocking.html. [Accessed: 23- May- 2021].

[30]"Sri lanka Telecommunications (Amendment)", *LawNet*, 2016. [Online]. Available: https://www.lawnet.gov.lk/sri-lanka-telecommunications-3/ [Accessed: 08- Jun- 2022].

8 ANNEX A – SURVEY WITH MOBILE OPERATOR

Illegal Call Termination(Bypass Fraud) avoidance with a common framework

This survey is conducted as a data gathering for MSC research project in University of Moratuwa. The purpose is to identify the current obstacles faced by Mobile operators in Sri Lanka in combating bypass fraud and to identify requirements to outline a common framework to avert this.

Thank you very much for your time and cooperation!

* Required

1. Do you think that higher international call termination rates is the main reason for higher illegal call termination minutes in Sri Lanka? *

   Mark only one oval.

   - ◯ Yes. I think so.
   - ◯ No

2. If your answer is 'No' for the above question, is it due to 'Lower intervention from regulatory body' Or any other reason?

3. Does your company have a Fraud Management System (FMS) to detect bypass international termination calls? *

   Mark only one oval.

   - ◯ Yes
   - ◯ No

4. Does your company use Passive detection methods (CDR, logs based), active detection methods(Test Call Generation) or both of them? *

   Mark only one oval.

   - ◯ Active Detection only
   - ◯ Passive Detectin only
   - ◯ Both Active Detection and Passive Detection used

5. If you use Passive detection what is/are the major challenge/challenges of Passive detection? *

Section 2 : On-net and Off-net Bypass Scenarios

6. Does your company perform onnet bypass detection and offnet bypass detection? *

   Mark only one oval.

   - ◯ Onnet Bypass
   - ◯ Offnet Bypass
   - ◯ Both Onnet and Offnet Bypass

7. Which one is higher : is it Onnet bypass minutes or Offnet Bypass minutes? ** No sensitive information needed. It is sufficient to indicate which one is higher.

8. Which scenario has lower accuracy level in fraud detection? *

Mark only one oval.

- ◯ Onnet Bypass Detection
- ◯ Offnet Bypass Detection

9. What are the major challenges faced in off-net bypass detection? *

10. If you already detect an offnet bypass number, is it communicated to the relevant offnet operator? *

Check all that apply.

- ☐ Yes
- ☐ No

11. If yes, for the above question what is the communication method?

Mark only one oval.

- ◯ via Email
- ◯ Call and inform
- ◯ Other: _____

12. Assume there are 4 telecommunication operators in the country as A, B, C, D. If your company is A, do you have the complete visibility of bypass number base of all the B, C, D operators? *

Mark only one oval.

- ◯ Yes
- ◯ No

13. What are the current intervention and support received from regulatory body in Sri Lanka for bypass call detection and prevention? *

Check all that apply.

	Strongly Disagreed	Disagreed	Neither Agree Nor Disagreed	Agreed	Strongly Agreed
Regulatory body provides parameters and inputs required for bypass detection	☐	☐	☐	☐	☐
Regulatory body provides bypass numbers of other all other operators seamlessly	☐	☐	☐	☐	☐
Rules and regulations for telecommunication equipment import is sufficient to control SIMBox smuggling	☐	☐	☐	☐	☐
Common platform has been setup by regulatory body with an overall visibility	☐	☐	☐	☐	☐
Legal actions taken to identified fraudsters is satisfactory	☐	☐	☐	☐	☐

14. What are the drawbacks do you identify in bypass detection process as a whole in Sri Lankan context(considering operators, regulatory body and end customers)?

15. What do you expect from the regulatory body of Sri Lanka for fraud detection and legal action procedure via a common framework? *

Abnormal IDD call scenario (One Ring Scam)	Customers call back to premium IDD numbers based on fraudulent missed calls.

16. Does your company detect Abnormal IDD call scenario (One Ring Scam)? *

Mark only one oval.

- ◯ Yes
- ◯ No

17. Is the detection purely based on the logs(such as CDR, logs) available in company's network nodes itself or do you receive any aid from regulatory body also? *

Mark only one oval.

- ◯ Internal logs only
- ◯ Internal logs & inputs from regulatory body
- ◯ Other: _____

18. What do you expect from regulatory body to avert this 'One Ring Scam' issue?

_____

_____