Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

Research Paper

Analysing Central Equipment Identity Register (CEIR) Model for Mobile Handset Tracking in India

Management

KEYWORDS : IMEI, Mobile tracking, Central Equipment Identity Register (CEIR), EIR, Telecom central database, Mobile theft.

Prof.Yatin Jog	Asst. Prof at Symbiosis Institute of Telecom Management, Symbiosis International University, India
Pushpendra Thenuan	Student at Symbiosis Institute of Telecom Management, , Symbiosis International University, India
Dhruv Khanna	Student at Symbiosis Institute of Telecom Management, , Symbiosis International University, India
Ashlesha Chavan	Student at Symbiosis Institute of Telecom Management, , Symbiosis International University, India

ABSTRACT

There are 980 Million wireless subscriber with 12 Telecom Service provider (TSPs) in India as on Sept 2015. Each TSP has their own Equipment Identity Register (EIR) to register International Mobile Equipment Identity (IMEI) number of mobile handset which is used for tracking of devices. In traditional telecom infrastructure this EIR is separate for each TSP and updated regularly. If the subscriber loses his or her mobile handset, the telecom service provider blocks the IMEI of that handset in its own network to make the handset useless and cannot be misused by the thief. But if the thief changes the SIM card, the mobile handset is latched to other network in which the IMEI of that handset is not blocked, thereby giving the thief an authorized access to the network. These issues were continuously happening in the past and TRAI observed these limitations with the existing model and came up with a new model that includes a central equipment identity register (CEIR) database in the system.

Our paper review traditional EIR model, limitation of EIR and proposed CEIR model based on qualitative analysis of TSPs responses and quantitative analysis of public responses. After enabling CEIR model TSPs can track any mobile device throughout the network.

Introduction

There were 980 million wireless connections in the country as on Mar 2015[1]. With the sprouting importance and needs of mobile phones and variety of new and latest applications and operating systems, the handset has become an important item particularly in terms of the amount of peculiar data/information stored in it. In today's scenario, mobile phone thefts are a major problem in countries all over the world. This has a very high security dimension. It is a key driver behind city crimes and robbery and also a threat to national security. It can also cause a loss of personal data which could be fatal for the mobile owner and this data can be misused. In such case mobile IMEI number will be tracked which is registered in Service provider's EIR at MSC.

The earlier method which was used was that in case of a theft, a complaint was lodged with the service provider and on the basis of the complaint the service provider blocked the SIM card. The complaint was lodged with the call centre of the service provider. The call centre of the operator authenticates the identity of the customer who has registered the complaint for the lost handset and then blocks the SIM in their networks. A new duplicate SIM is issued to the customer according to rules and regulations.**As per this procedure the service provider just ensures that its network is not misused,** however no action is taken for blocking of the lost handset or for tracking the lost mobile or its usage by any other person or organization. A person can only file a complaint to the operator or the police for the lost mobile handset but the recovery rate of such handsets becomes almost zero as it is easy to hide them due to their size.

In the calendar year 2008, it was found that a large number of handsets were either working without any IMEI / ESN number or having all zeros in their IMEI/ESN numbers. Such mobile handsets were athreat as companies/agencies were not able to trace them. Further, it was observedthat at that point of time many operators had not implemented EIR register for the tracking of IMEI number in their networks. Therefore, for security purpose, all TSP's were directed by DoT on 6th October 2008 to make provision for EIR in their systems so that calls can be rejected from those handsets which have all zeroes in their IMEI number or are without any IMEI number. After this direction from DoT all the operators implemented EIR register in their networks. This direction given by DoT also has a loophole. The operators have their own EIR and they do not share their EIR with other operators. In such a scenario a person can use the same handset using a different SIM card of another operator and the phone cannot be traced as the IMEI number stored in the EIR of one operator is not shared with the other operator and cannot be mapped. This has led to the rise of another problem, which needs to be rectified as early as possible[2].

As per the current call flow system for GSM, the IMEI number of a device is usually shared when the exchange properties in the MSC/VLR define whether the IMEI check is performed or not. If it is performed, the MSC/VLR requests the mobile station to send its IMEI number. The downlink message Identity Request contains information about what the mobile should send back. In case of an IMEI check, the mobile receives a request to send back its IMEI number. The same Identity Request message can be used in other situations to order the mobile to send back its IMSI number. The IMEI sent by the mobile is checked against the information in the network's Equipment Identity Register (EIR). If the EIR returns the answer "white listed" the mobile is allowed to use the network. If the response is "black listed" it will be rejected. The EIR can also return the answer "grey listed" or "unknown". In these cases the operator can decide whether the mobile is permitted access to the network[3].

To solve the issue in the current system a Central IMEI Database register can be formed which can be implemented in two ways: either through building of a centralized database system which will contain the information of all EIR's of all the networks and the second method is by jointly maintaining the Central IMEI Database register either with the help of operators or with the help of a third party[2].

By the implementation of the above method the loopholes of the current system can be dissolved and the devices could not be used further and upon the recovery of the lost device it can

Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

be given a facility of unlocking the IMEI number after the verification of the owner of the device is done and to prohibit reprogramming of IMEI number, a legislation should be formed which should address the issue of reprogramming of IMEI numbers through the OS of the mobile device.

Existing System:
Equipment Identity Register (EIR): Equipment identity register (EIR) is a database that contains all the IMEI/ESN numbers of the handsets of all the subscribers latched to a particular cellular network. IMEI is a unique identity code which is given to all the GSM handsets. When the handset is connected to a particular network, MSC request for IMEI of that handset and then it is sent to EIR for further authorization process.

Need of EIR:

As the mobile penetration increase all over the world, there were many issues and complaints of mobile thefts and loss of handsets. When the handset is lost, the person informs the service provider about the stolen handset issue by calling the call centre of the service provider. The subscriber's identity is checked and authenticated and then the SIM belonging to the particular network is blocked by the service provider, thus ensuring that the mobile connection of that particular subscriber is not misused. The service provider also offers a duplicate SIM card on demand by the subscriber. But there was no provision made to track the handset and retain it back. The recovery of the stolen mobile handset was almost impossible.

An initiative was taken by TRAI to resolve this issue by using EIR database with the help of EIR, the cellular operators can keep a track of all the handsets latched to their network. In case the handset is stolen or any unauthorized access happens from that handset which is lost, it can be marked as unauthorized and can be forbidden from accessing the network. The handset can be traced through EIR database. But there were many technical and administrative problems in blocking the IMEI /ESN numbers. The cellular service providers were not capable to integrate EIR into their system and block the IMEIs. In the year 2008, there were many mobile phones who came into the market without having IMEI numbers or IMEI with all zeros and thereby causing difficulty in tracing those handsets. Therefore, for security purpose, all TSP's were directed by DoT on 6th October 2008 to make provision for EIR in their systems, so that the call gets rejected from the handsets which have all zeroes in their IMEI number or are without any IMEI number. Subsequently all service providers have presently made provision of EIR in their network.

The EIR contains three lists of IMEIs in its database:

White list which includes IMEIs of all the authorized handsets allowed to access the network

Grey list which includes IMEIs of all the handsets to be kept under observation for tracking.

Black list which includes IMEIs of all the unauthorized handsets to be barred from network.

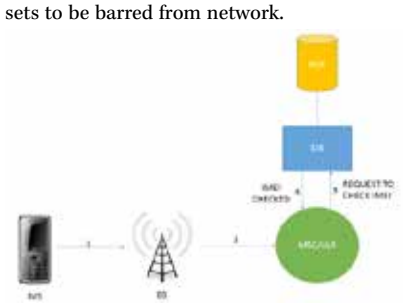

Figure 1. Call Flow-IMEI updating in EIR

Steps for EIR Call Flow:
STEP 1) When a handset is roaming it gets connected to a new MSC/VLR of that area. It first attempts to perform a registration procedure with the VLR. In the absence of EIR in a network, VLR sends a location update message to the HLR and updates the HLR about the current location of the mobile station or handset.

STEP 2) When the EIR function is implemented and deployed in a network, validation of IMEI of the MS/handset attempting to register is carried out before completing the whole registration procedure and updating the HLR.

STEP 3) In the network having EIR, the new MSC/VLR sends a request to EIR before updating the HLR about the new location. This message contains the IMEI of the MS which is attempting to register. Sometimes this message also contains the IMSI of the subscriber's SIM cardcurrently being used.

STEP 4) After receiving the request from MSC/VLR, EIR searches the IMEI of MS in its White, Grey, and Black lists to find the match of the IMEI. Then the EIR gives response to MSC depending upon the result of the search. The response may contain the equipment status of the MS (whether the searched IMEI for the MS/ Handset is allowed or not, depending on its status of the IMEI in the White, Grey or Black lists) or a User Error stating the IMEI is invalid. Based on the status provided in the response by EIR, MSC either continues the registration procedure or rejects it. If the IMEI is allowed then MSC allows the MS to continue with the authentication procedure or if the IMEI is blacklisted or invalid, MSC rejects the MS and stops the further authentication procedure. If the IMSI is also provided in the message, then EIR before sending the response to MSC, checks the IMSI to one which is provisioned with the IMEI of the MS. If the match on IMSI is found by EIR then it overrides any black list condition found on the IMEI and allows the MS to connect to the network.

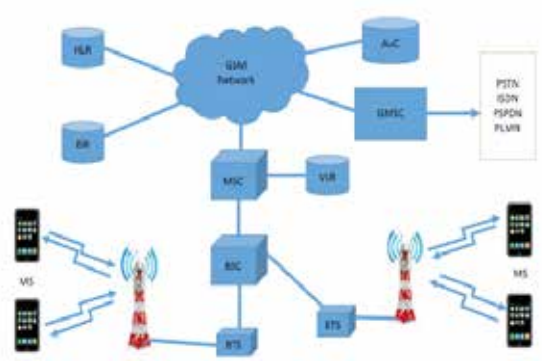

Figure 3. GSM Call Flow

Limitations of Existing model:
The existing model only deals with the IMEI numbers in the EIR database of a particular network to which the subscribers' handsets are connected. According to the existing model, if the subscriber loses his or her handset, the service provider blocks the IMEI of that handset in its own network to make the handset useless and cannot be misused by the thief. But if the thief changes the SIM card, the mobile handset is latched to other network in which the IMEI of that handset is not blocked, thereby giving the thief an authorized access to the network[4]. These issues were continuously happening in the past and TRAI observed these limitations with the existing model and came up with a new model that includes a central equipment identity register i.e. CEIR database in the system.

TRAI Recommended Model:

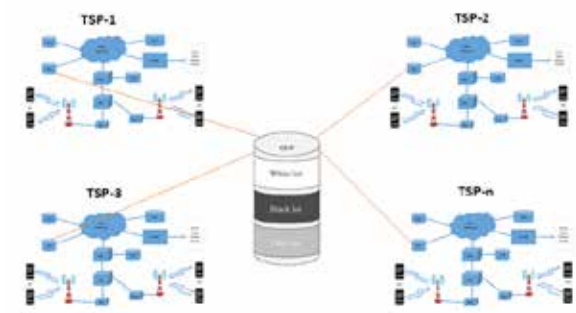

Figure 3.Central Equipment Identity Register (CEIR) Model

CEIR is a central EIR database which integrates IMEI numbers of EIR of all the networks. As the information is stored in the CEIR, it will be periodically updated in the EIR of all the networks. This helps in blacklisting the IMEI of a stolen handset in all the networks and blocking their use in all the VLRs of all the networks. However, to establish and maintain CEIR it involves cost both in terms of OPEX and CAPEX. Also there is a possibility of network delays which will take place on call by call basis[5]. The following conditions are considered to establish a CEIR:

CEIR can be jointly maintained through the associations of service providers.

CEIR can be maintained by a third party.

Issues relating to the implementation of CEIR:
CEIR is the central database and a repository of all the blocked IMEI numbers of the mobile handsets. The question arises that CEIR should be maintained nationally or zonally. In case the CEIR is maintained nationally then the database will contain all the blocked IMEIs of all the circles all over nation and the size of the database will be large. In case of zonal CEIR, there will be issue of interconnecting all the zonal CEIR so as to make the data of the IMEIs available to all the service providers[6].

The second issue is about the recovery of the cost of implementing and maintaining the CEIR. The operator either absorb the cost incurred to build the CEIR or recover the cost from the customers by providing the facility of blocking the IMEI of the stolen handset[7].

The next issue deals with the reprogramming of IMEI of the stolen handset. Since most of the mobile handsets are software based, they are easily reprogrammable. The IMEI number of a handset can be easily changed after being stolen and making the recovery of the handset impossible[8]. So this is the major issue in blocking the IMEI of a stolen handset. There has to be legislations and stringent acts to curb reprogramming of IMEI numbers of the mobile devices.

Analysis of Survey Responses:
We had conducted a survey at various technological and management institution where people have great knowledge on Telecom and Information technology. Sample size of public survey is 52 out of which 75% belonged to age group of 22 to 26 years,13.5% belonged to age group of18 to 22 years and 11.5% belonged to age group of above 26 years who are Post Graduate students and Industry experts having wide area of experience in Telecom and ICT industry. They have given their neutral responses and thus we havedone analysis on the responses to the questions that were published in the consultation paper of TRAI.

Secondly, in case of TSPs, we have conducted the qualitative survey on the 14 operators and analyzes their responses given on those similar questions.

Thirdly, we have shortlisted the top 5 companies on the basis of their market share , customer data base , customer satisfaction and retention level and have also analyze their responses. And at last we do the comparative analysis of each question based on the public and TSPs responses pie chart.

Effectiveness of Blocking of IMEI:
Survey:

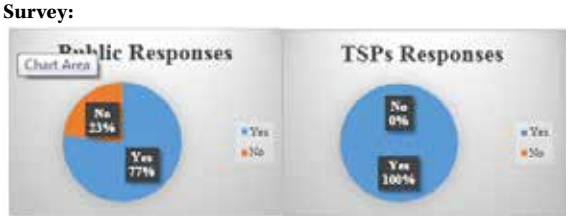

Figure 4. In order to reduce/discourage mobile theft do you think the blocking of IMEI is an effective solution?

Table 1.Responses of TSPs

S. no	Operator	Responses
1	Bharti Airtel	Blocking IMEI is an effective and important solution for preventing the usage of stolen handset which is resold in the market and the mobile industry is adding up to 18-19 million subscribers on a monthly basis.
2	BSNL	The blocking of IMEI number of lost/ stolen mobile handsets is an effective solution provided action is taken to address the issue of illegal reprogramming to end it.
3	COAI	As per COAI, Blocking of IMEI is necessary but first there should be a legislation to stop/curb the reprogramming of mobile phones by software programming and there are various technical methods that are being used to reprogram the IMEI number.
4	Idea Cellular	The blocking of IMEI is an effective solution to curb the stealing or misuse of mobile handsets but there are various ways by which IMEI can be reprogrammed and sold in other countries.
5	Reliance Com	The blocking of IMEI number can be an effective solution to curb GSM handset theft. However, there are millions of handsets available in the market with duplicate IMEI numbers out of which 10% may have been reprogrammed.

Analysis:
Table 2.Responses of TSPs

S. no	Organization:	Statistics
1	Bharti Airtel[2]	18-19 million of mobile phone users are added every month in India.
2	TRAI[1]	980 million users in India.
3	Airwide Solutions[9]	Around 250000 devices were blocked after implementation of IMEI number in Australia and a reduction of around of 25 % since implementation[10]

Based on the responses and the survey conducted we believe that blocking of IMEI is very important. There are around 980 million mobile phone users in India. The tracking and blocking of IMEI number is essential and a very effective solution for preventing the theft of mobile phones. The telecom industry is adding up to 18-19 million subscribers on a monthly basis[2] and based on the data available, around 10% of current phones in use, have their IMEI's reprogrammed[11]. It is the only solution available to us with the use of current technology[12]. As

Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

per the statistics available, with the implementation of blocking of IMEI number, in other countries like Australia, the Australian Mobile Telecommunications Association(AMTS), was able to block around 2,50,000 devices in Australia[9]. Thus we analyse that blocking of IMEI number is a very important step that can help in reducing the theft of mobile phones in India.As per the survey, the 77% public says that blocking of IMEI should be implemented while 23% says that it should not be implemented. But according to TSP's blocking of IMEI should be implemented.

Increase in load on the network in case blocking of IMEI is implemented:

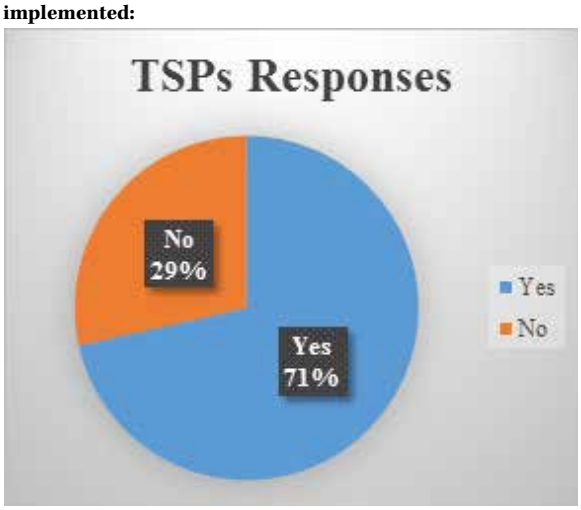

Figure 5.In case blocking of IMEI is implemented, to what extent load on the network will increase?

Table 3.Responses of TSPs

S. no	Company Name	Operator Responses
1	Bharti Airtel	There will be an additional load on the network if blocking of IMEI is implemented because operator has already installed EIR in their network which is continuously increasing the capacity as and when the requirements are coming.
2	BSNL	There would be only marginal incremental load on the network as EIR is already installed and is operational.
3	COAI	According to COAI the load will be there on the network and hold time will be more and hence delay will also be more leading to increase in cost.
4	Idea Cellular	Once IMEI blocking is implemented, there may be a need for "Triple Dipping" within the network i.e. three different databases pertaining to MNP, DNDC and IMEI may be need to be dipped into prior to call completion thereby resulting in higher hold times for the customers.
5	Reliance Com	The load on the network will eventually increase as the list of the blocking of IMEIs will keep on increasing with the time. Therefore, there should be a specific retention period given by the authority for blocking of IMEI number.

Analysis:

As per the responses of the companies, there will be an increase on load of the network. Currently, all operators have implemented EIR register as per the guidelines of DoT. Due to this, there will be an additional load on the operator's EIR and the EIR to CEIR network for processing and exchange of IMEI list data[13]. As per a company, with typical EIR implementation, 0.3 BH IMEI Check/subscriber is normal recommended value. From CANDI, it comes ~ 1% (even less) drop in capacity[12]. Some companies also suggest that there will be no extra load initially, but as time passes on the database increases and there will be an increase on the load of the network[14].According to the responses of TSP's 71% believe that load will increase while 29% believe that load will not increase.

Maintaining CEIR at national level or zonal level:

Survey:



Figure 6. Should CEIR be maintained at national level or zonal level?

Table 4.Responses of TSPs

S. no	Company Name	Responses:
1	Bharti Airtel	CEIR should be maintained at national level with disaster recovery site. The estimated size of the database would be approx. 3-4 million customers and should ideally be maintained by the government or by third party organization.
2	BSNL	CEIR should be maintained at national level only as maintaining at zonal level will not serve the purpose, because stolen mobiles of one zone can be easily transferred to the other zone for re-use.
3	COAI	COAI believe that it should be maintained at National Level with disaster recovery site.
4	Idea Cellular	Not mentioned anything regarding who should maintain CEIR.
5	Reliance Com	According to Reliance CEIR should be implemented at National level and not at Zonal level, but also the national CEIR can be ineffective as these phones can find their way out of national border, therefore according to them the national CEIR should be integrated with Global CEIR.

Analysis:

Assuming the mobile subscriber base in the country to be around 980 million at present, initiallya theft rate of around 1% should be considered. However, there should be a system to ensure enough capacity for the increasing subscriber base and their requirements[15].

The data size for India IMEI blacklist records can be estimated as follows: Assumption: 980M subscribers, 10% individual IMEI blacklist records, Each record would be up to 0.5KB, depending on the data fields used.

This will give a database size up to 98M x 0.5KB = 49GB database. The database size can be expected to grow at least at the rate of growth of subscribers, say 25% per year [13]. As per the responses of the survey and the operators and various other associations, the CEIR should be maintained at national level with a disaster recovery site in place. This would help in national security and the cost can also be shared between the government and the operators and the national CEIR should be integrated with global CEIR[16]. But according to an organization no CEIR is required in India as EIR is capable of doing it[14]. According to the survey 69% people believe that it should be implemented at national level, while 31% believe that it should be implemented at zonal level. But according to TSP's responses it should be implemented at national level.

Funding aspects of Centralized EIR:
Survey:

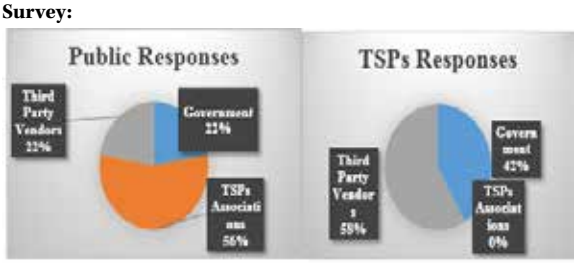

Figure 7. Please comment on cost and funding aspects of Centralized EIR?

Table 5.Responses of TSPs

S. no	Company Name	Responses
1	Bharti Airtel	The total implementation cost of CEIR would be decided by Government or the third party appointed by the authority. The cost of deploying the CEIR is estimated around US$ 4 million.
2	BSNL	The cost of CEIR can be estimated once the dimensioning of the equipment is known. However, the funding of CEIR can be done through the funds available with TRAI/DOT and cost can be recovered from the customers.
3	COAI	According to COAI the cost should be borne by the government and the additional cost by service providers should be reimbursed by the government.
4	Idea Cellular	IMEI blocking would involve considerable changes in the current customer facing processes, inter-operator escalation issues, handling of subscriber queries on IMEI blocking, etc. This would involve both capital expenditure as well as operating expenditure on an ongoing basis and operators are not in a position to invest further after implementation of MNP.
5	Reliance Com	Firstly, CAPEX is required to set up the CEIR in the network. To keep the EIR updated, it has to be connected to MSC on real time basis. Hence for constant updating and maintenance of EIR database, OPEX is required. The task of implementing this project can be given to DIT/NIC. The funding for CEIR can be raised from the government on the lines NDN registry is setup and maintained or the funding can be done from TRAI consumer education fund.

Analysis:
As per the responses of the operators and the survey, we believe that there are multiple factors that are involved in the cost and funding aspect of Centralized EIR. The factors would involve servers, various kinds of hardware and software, processing and storage capacity, cost of connectivity, administrative costs of data centre and hosting, regular maintenance, upgrades and security etc.[17]and also the fact once the dimension of the equipment is known. Operators also present a view that the cost of establishing the CEIR should be either shared by the government with the operators or the government should reimburse the cost of setting up of CEIR to the operators[18]. According to the survey 22% of people believe that CEIR should be funded by third party vendors, 22% believe it should be maintained by government, while 56% believe that it should be maintained by TSPs Associations. But according to TSPs responses 58% believe that it should be maintained by third party vendors, and 42% believe it should be maintained by government[3].

Legislation to prevent re-programming of mobile devices:
Survey:



Figure 8. Should there be Legislation to prevent reprogramming of IMEI of mobile devices in India?

Table 3.Responses of TSPs

S. no	Company Name	Responses:
1	Bharti Airtel	Bharti Airtel agrees with TRAI that by just blocking the IMEI number we cannot curb the increasing theft rates and there should be a legislation to ensure that reprogramming of IMEI does not take place.
2	BSNL	There should be a legislation to prevent re-programming of mobile devices. Apart from monetary penalties, criminal charges should be pressed against the people indulging in such illegal activities.
3	COAI	According to COAI, Legislation making reprogramming of a handset an offence is absolutely necessary. This would also prevent cloning of IMEIs of handsets of genuine customers.
4	Idea Cellular	Many software are freely available on internet so there is a strong possibility of the IMEI number of the stolen handset getting changed before being resold or reused. Therefore there should be a legislation with stringent penalties enabling the law enforcement agencies to take action against the people indulging in such illegal activities.
5	Reliance Com	In case the handset is reprogrammed and a duplicate IMEI number is embedded in the stolen or lost mobile handset, then it becomes difficult to track the original IMEI number. The purpose of blocking IMEI number fails in this case. Hence, there should be a legislation to prohibit reprogramming of IMEI number.

Analysis:
As per the outcome of the survey and the operators' responses along with various other associations, we believe that there should be a legislation in place which should curb the reprogramming of IMEI number. In case the IMEI number is blocked and someone reprograms the IMEI number then the whole process of setting up of CEIR database and its implementation takes a beating and the whole purpose behind it fails. Thus we need a very serious law to stop such processes which will help and aid the process[11]. According to the survey, 84% people believe that there should be a legislation to curb reprogramming of IMEI number while 16% say that it may be implemented. But according to TSP's all operators believe that there should be a legislation to curb the reprogramming of IMEI number.

Conclusion:
IMEI tracking is very essential in today's scenario since mobile theft cases are increasing day by day. It is also necessary for national security. Telecom Service Provider (TSPs) already have the provision of blocking the IMEI numbers using EIR which is separate for each operator. But the issues of mobile theft are still prevailing because the SIM card can be changed to a different network and it is not possible to track the subscriber's mobile handset. This lead TRAI to come up with the idea of implementation of CEIR database which will include all the IMEI numbers of the subscribers belonging to any operator's network in the country. Hence, even if the thief insert a new SIM of a different network, he will not be able to connect to that network. To implement CEIR, there will be hardware changes, whose cost for the setup and implementation of CEIR database system will be

Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

around US $4millions.The estimation of the amount of data that the database will store is considered to be around 49GB. If this CEIR model is implemented then there may be a chance that there will be an increase in delay for the setup of the call and its establishment. To decrease this delay, we need to use very high end latest technology equipment's, whose cost may be more than the expected price. There should be a legislation in India which will be getting passed very soon for the curbing of the re-programming of IMEI number and the database system should be funded and maintained either by a third party organization or the government and should be maintained at National level.

References:

[1] TRAI, "TELECOM REGULATORY AUTHORITY OF INDIA -Highlights of Telecom Subscriptionm Data as on 31st January, 2015," Telecom Regulatory Authority of India, DATA 18 / 2015, 2015.

[2] Airtel Bharti, "Airtel Bharti response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Airtel, 2010.

[3] COAI, "COAI response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," COAI, 2010.

[4] G S Gundu Rao, "Consumer care socity response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Consumer care socity, 2010.

[5] TRAI, "TRAI Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Telecom Regulatory Authority of India, Colsultation paper 14/2010, Aug. 2010.

[6] Videocom Telecom, "Videocom response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Videocom, 2010.

[7] Idea, "Idea response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Idea, 2010.

[8] TTSL, "TTSL response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," TATA Teleservices Ltd, 2010.

[9] Airwide, "Airwide response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," 2010.

[10] AMTA, "Australian Mobile Telecommunications Association IMEI blocking Graph." 2011.

[11] Reliance, "Reliance response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Reliance, 2010.

[12] Ericsson, "Ericsson response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," EIL/B-10:0219, 2010.

[13] Telecordia, "Telecordia response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," 2010.

[14] WiExp UK, "WiExp response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," 2010.

[15] AUSPI, "AUSPI response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," Assosciation of unified telecom service providers of india, AUSPI/12/20, 2010.

[16] MSAI, "MSAI response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," mobile standard alliance of india, 2010.

[17] Vodafone, "Vodafone response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," vodafone, 2010.

[18] BSNL, "BSNL response on Consultation Paper on issues relating to blocking of IMEI for lost/stolen mobile handsets," BSNL, 2010.