e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:03/Issue:11/November-2021 Impact Factor- 6.752 www.irjmets.com

# ANALYSIS OF SECURITY RISKS ASSOCIATED WITH IMEIS AND UNWIPED DATA OF DISPOSED MOBILE HANDSETS

**Raja Sharma**[*1]

[*1]Department Of ECE, Bhagwan Parshuram Institute Of Technology, GGSIPU, New Delhi, India.

## ABSTRACT

With the latest advancement's in the mobile technology and continuous drop in the cost of mobile hardware, mobile handsets had reached to the hand of around 80 percent of people of the world. As per Telecom Regulatory Authority of India (TRAI), there were 1168 million wireless connections in India as on 28 February, 2021. Also with the growing importance of mobile phones and variety of new applications, consumers are using them for storing a number of personal details like phone contacts, bank account details, PIN etc. The handset has become a valuable item particularly in terms of the personal data and sensitive information stored in it. Once discarded, anyone can power up the device and hack in to look through its contents, including personal and confidential information. To prevent such serious attacks some methods are presented in this paper. This paper presents brief about the IMEI number and security risks associated with IMEI's and unwiped data of discarded/stolen mobile handsets. This paper also list out the guidelines for IMEI security in India which are currently being followed throughout the country. At the last some recommendations are proposed which if implemented will greatly help the government and law enforcement agencies to ensure the security of both IMEI as well as sensitive unwiped data present in discarded/stolen mobile handsets.

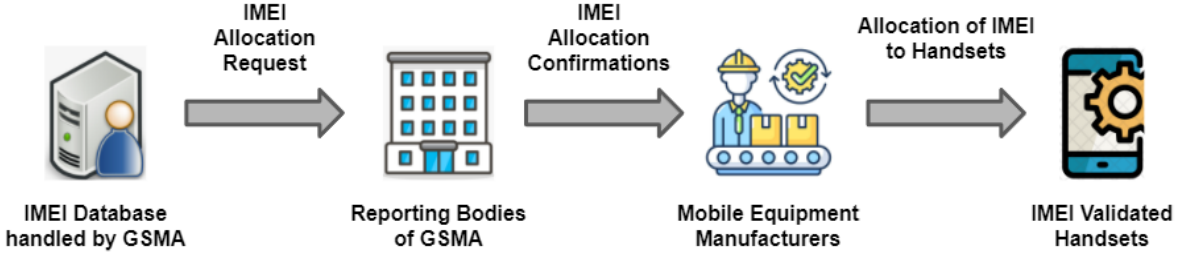
**Keywords:** IMEI, IMSI, Confidential Data, Security Risks, Mobile Handset.

## I. INTRODUCTION

The International Mobile Equipment Identity (IMEI) is a unique identification code for each mobile device used in Global System for Mobile (GSM) network. The IMEI is a 15 digit number that is used to identify the device. The format of IMEI consist of 8 digits Type Allocation Code (TAC), 6 digits Serial Number (SNR) and last digit for check. All digits have the range of 0 to 9 coded in the form of binary coded decimal. Values outside this range i.e. 0 to 9 are not permitted. The IMEI also reveals the manufacturer, make & model, type approval details, frequency bands supported by device and country of production. A typical IMEI depicts as below:

| TAC (8 Digit) | Serial No (6 Digit) | Check Digit (1 Digit) |
|---|---|---|
| NNXXXX YY | ZZZZZZ | A |
| TAC | Type Allocation Code, formerly known as Type Approval Code | |
| NN | Reporting Body Identifier | |
| XXXXYY | Mobile Equipment (ME) Type Identifier defined by the Reporting Body | |
| ZZZZZZ | Allocated by the Reporting Body but assigned per ME by the manufacturer | |
| A | Check digit, defined as a function of all other IMEI digits | |

## II. IMEI ALLOCATION PROCESS




The IMEI numbers are allocated to the Mobile Equipment manufacturers or Brand owners (Type allocation Holder) by GSMA, which is an international body representing the interests of worldwide telecom operators. It performs its role through its authorized representatives (Reporting Bodies) and keeps records of the IMEIs that

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:03/Issue:11/November-2021 Impact Factor- 6.752 www.irjmets.com

are allocated to mobile device manufactures/Brand owners including information on some of the technical capabilities (e.g. Frequency bands supported by device, device power level class etc.) of the mobile device associated with the allocated IMEI in the IMEI Data Base. Presently the reporting bodies authorized by the GSMA are as following.

| Reporting Body Identifier | Reported Body Agency |
|---|---|
| 01 | IMEI allocated by Cellular Telecommunications Industry Association (CTIA), USA |
| 35 | British Approvals Board for Telecommunications (BABT), UK |
| 86 | Telecommunications Terminal Testing & Approval Forum (TAF), China |
| 91 | Mobile Standard Alliance of India (MSAI), India |
| 99 | Global Hexadecimal Administrator (GHA), USA |

## III. IMPORTANCE OF IMEI NUMBER

The main purpose of an IMEI number is the identification of mobile handset. Telecom Service providers and manufacturers share IMEI numbers to enable tracking of mobile devices that may be stolen or illegally compromised. Equipment Identity Registry keeps the record of IMEI of mobile number active in network. IMEI is also used to verify whether a call has been made from a specific handset or not. But IMEI of the mobile handset can be changed to impersonate others quite easily. For instance, if a person with ill intentions has retrieved the IMEI number of discarded mobile handset and uses it on another mobile handset then it will be difficult to trace the real owner of the mobile handset. Moreover, such retrieved IMEI numbers can be used to circumvent the blacklist of IMEI of stolen mobile handsets. Additionally, if the IMEI number is compromised then someone could potentially gain easy access to the apps which use IMEI as an identifier.

## IV. GUIDELINES FOR IMEI SECURITY IN INDIA

In year 2009, it was observed that a large number of low cost mobile handsets without having a unique identifier called International Mobile Equipment Identity (IMEI) number prescribed by Global System for Mobile Association (GSMA) were getting imported. Besides the taxation issues, such handsets also pose potential security threats and serious health hazards. Taking cognizance of the situation, the Directorate General of Foreign Trade (DGFT) issued the Notification No. 14/ 2009-2014 dated 14th October, 2009 prohibiting import of Mobile Handsets' (classified under ITC (HS) Code '8517') without International Mobile Equipment Identity (IMEI) Numbers or with all Zeroes in IMEI and Import of CDMA mobile phones' (classified under ITC (HS) Code '8517') without Electronic Serial Number (ESN)/Mobile Equipment Identifier (MEID) or with all Zeroes in ESN/MEID.

Recently, it has come to notice that the importance & associated cost of mobile handsets has also resulted into import of duplicate, compromised and non-genuine Mobile handsets. Also M/s Micromax Informatics limited filed a Writ Petition in the Hon'ble High Court of Delhi in which they requested Hon'ble High Court to direct the Respondents to prohibit the entry/ import of mobile phone with duplicate or fake IMEI Numbers by modifying the notification no. 112 dated 16/06/2009 and Notification no. 14 dated 14/10/2009 and to further direct destroying such counterfeit mobile phones. Hon'ble High court of Delhi directed for necessary decision and notifications on fake/Duplicate IMEI. After due consultations with Ministry of Home Affairs, DGFT, Department of Customs and Industry, the amended Notification has been issued vide Notification No. 107/(RE-2013)/2009 2014 dated 16th Jan, 2015.

The Department of Telecom (DoT) had also issued a standard operating procedure in May 2015 to prohibit the import of mobile phones with duplicate, fake and non-genuine international mobile equipment identity. Earlier, the allocation of IMEI was being managed by Mobile Standard Alliance of India (MSAI), an erstwhile reporting body of GSMA in India. But now a new system called as Indian Counterfeited Device Restriction (ICDR) system has replaced the MSAI operated system. ICDR has been developed by the Centre for Development of Telematics - R&D unit of Department of Telecommunications for implementing the SOP.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:03/Issue:11/November-2021 Impact Factor- 6.752 www.irjmets.com

ICDR is an innovative and sophisticated solution customized to meet and control the importing of cloned, unauthorized and illegally compromised mobile devices into the country. ICDR manages the allocation of IMEI numbers. DoT had communicated this to industry bodies and concerned government departments in a letter dated January 28, 2020. The new system has been operationalized on a pilot basis on the web portal of Central Equipment Identity Register (CEIR). The CEIR is being used to block all services on stolen or lost mobile phones on any network even if the SIM card is removed or the IMEI number of the handset is altered to a new number.

## V. LAW CONCERNING IMEI SECURITY IN OTHER COUNTRIES

For accurately tracing the mobile handset in the network by Law Enforcement Agencies, mobile handsets without the unique IMEI and modification of IMEI number have been prohibited by law in many countries. In the United Kingdom, under the Mobile Telephones (Re-programming) Act, changing the IMEI of a phone, or possessing equipment that can change it, is considered an offense under some circumstances. In Britain, IMEIs have been allocated by BABT (or one of several other regional administrators acting on behalf of the GSM Association) to legitimate GSM terminal manufacturers without the need to provide evidence of approval. In the United States, it is not yet illegal to change the IMEI of a phone.

## VI. SECURITY OF UNWIPED DATA OF DISPOSED MOBILE HANDSETS

Presently the Mobile Handset User Device in Telecom Network is being used for Voice & data communications. As per TRAI, there were 1168 million wireless connections in the country as on 28 February, 2021. With the growing importance of mobile phones and variety of new applications, consumers are using them for storing a number of personal details like phone contacts, bank account details, PIN etc. The handset has become a valuable item particularly in terms of the personal data and sensitive information stored in it. Once discarded, anyone can power up the device and hack in to look through its contents, including personal and confidential information. Therefore, it is suggested that users should wipe out all of its data before disposing it off.

Any device with storage capabilities or having memory cards inserted should be securely wiped of data before disposal as they contain sensitive information, contact lists, photos and other files collected over time. It is important to note that mobile handsets have to be functional for wiping their contents.

The United States Computer Emergency Readiness Team (US-CERT) advises the following when destroying mobile phones and tablets:

1. Remove the memory card from your device, if inserted.
2. Remove the SIM card.
3. Select Master Reset, Wipe Memory, Erase All Content and Settings.
4. Physically destroy the memory card and SIM card both. Memory cards are typically reusable and SIM cards reusable in a phone that has the same carrier.
5. Ensure the full termination of your old account and/or switch to your new device.

## VII. CONCLUSION

During the study it is found that the more than 91 percent of mobile users in India are unaware of the IMEI retrieval mechanism i.e. Indian Counterfeited Device Restriction (ICDR) system launched by the Centre for Development of Telematics - R&D unit of Dept. of Telecommunications. Therefore in order to implement such advanced mechanism at ground level, Government should collaborate with local NGOs and educational institutes to start digital security skills training campaigns or knowledge sessions for those people who are unaware of such innovative and sophisticated solution. Training should focus on explaining - What is IMEI, Importance of IMEI number embedded in their handset, how to block the IMEI before disposing off or after losing the handset, and benefits of using such IMEI retrieval mechanism. Participants should also be demonstrated real time blocking and unblocking of IMEI of a handset on the web portal of Central Equipment Identity Register (CEIR).

Implementation of below given essential recommendations will greatly help the government and law enforcement agencies to ensure the security of both IMEI as well as sensitive unwiped data present in discarded/stolen mobile handsets. Recommendations of this research paper are as follows: -

1. Government/Concerned Authority of the country should implement strategies to counter the issues related to data security and privacy of the content in the discarded/stolen mobile handsets. They should advise and encourage users to use some standard application to wipe the contents before disposing their handsets.
2. Comprehensive guidelines specific to disposal of the Mobile handset clearly defining responsibilities of the manufacturer, seller, consumer, telecom service provider, and disposer agency may be issued.
3. IMEI retrieval mechanism such as ICDR should be advertised via all modes of communications to make all IMEIs from the discarded mobile devices accountable to avoid their misuse and ensure the security of discarded/stolen handset.
4. There is need to conduct advance research and upgrade the present security mechanism of IMEIs, so that after modification devices will be able to provide more protection and better security mechanism against mobile theft.

## VIII. REFERENCES

[1] K. Kumar and P. Kaur, "Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number", Int. J. Comput. Sci. Mob. Comput., vol. 4, no. 5, pp. 527-533, 2015.

[2] Dept. of Telecommunications (Security Wing) SOP (Version 1.0) for Implementation of Central Government notification prohibiting import of mobile phones with duplicate, fake and non-genuine International Mobile Equipment Identity, May 2015.

[3] S. J. Alsunaidi and A. M. Almuhaideb, "The Security Risks Associated With IMEIs And Security Solutions," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-5, doi: 10.1109/CAIS.2019.8769521.

[4] Linda Pesante, Christopher King, and George Silowash. "Disposing of Devices Safely", US -CERT, Oct 2018.

[5] https://www.ryerson.ca/ryerson-works/articles/how-to/2019/your-device-may-be-dead-but-your-data-isnt/

[6] https://drfone.wondershare.com/erase-android/android-data-erase-app.html