National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

Mobile Cloning

Dipanshu Dinesh Nadkarni[1], Prof. Shreya Bhamare[2]

[1]Department of MCA, University of Mumbai,
Email:dipanshunadkarni@gmail.com

[2]Department of MCA, University of Mumbai,
Email: 17.shreya@gmail.com

Abstract— *The studies demonstrates how cell telephones are evolved with new changes via the development within the technologies. Mobile phone cloning is the copy of identification of 1 cellular telephone to every other cellular smartphone. The payments for the calls go to the original users/subscriber. Cloning is the method of taking all the secured information that is stored in an unique user's mobile phone and illegally programmed the identical facts into some other mobile phone discussed on this paper. The result is that the "cloned" mobile cellphone is capable of make and receive calls and all of the bill costs for the ones fraud calls are dispatched to the original user's/subscriber. The provider issuer community does not be capable of make distinction among the original cell smartphone or the "cloned smartphone". Nowadays tens of millions of mobile phones user's, makes use of global system for mobile communication (GSM) or Code division multiple access (CDMA) which have dangers of being mobile phones cloned. If personal identification number (PIN) and Electronic Serial number (ESN) are recognized, then the mobile smartphone can be cloned in seconds. Here we've got mentioned some professionals and cons about this generation. This generation is basically used by hackers to clone the mobile cellular phones of the consumer's to retrieve their records/credentials and they may be not aware of this reality. As a result, person's must face lot's of difficulties.*

Keywords— Cloning, Code Division Multiple Access (CDMA), Electronic Serial Number (ESN), Global System for Mobile Communication (GSM), Personal Identification Number (PIN).

I. INTRODUCTION

Mobile phones are very vital in our existence. Cell smartphone works on 3 e's of communication consisting of ease of use, financial and efficient. It's also very plenty worried in making fraud calls. The cell telephone as a hardware is difficult to make comfortable as a distinct manufacture are worried of their production [1]. The form of devices holds the special level of security amongst themselves. The safety methods in CDMA (Code Division Multiple Access) and GSM (Global System for Mobile Communication) cellular phones are different and equal because the loop hole in security of those mobiles. One of the essential security is cloning of cellular phones. It isn't handiest the big danger in India however different countries additionally. This paper will talk the outcome of cloning and additionally different methods to prevent cloning. Cloning is an unlawful practice of taking the records from a cellphone and makes use of this information for crook purposes[2]. The information is criminally programmed in any other cell phone. The second phone is referred to as "cloned" mobile. The cloned cellular is build and get calls and the prices for those calls are billed to valid/authentic users.

FIGURE 1: Selection of mobile phones that can be cloned

National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

II. HISTORY OF MOBILE CLONING

Cellphone cloning [1] started out in 1990 on Motorola bag telephones. It was on it's peak for the duration of mid of 90's and captured Motorola brick telephones which includes a classic, the extremely traditional and model 8000. Mobile phone cloning is carried out in excessive utilization vicinity a couple of service imparting and fraudulent environments. The loop hole on mobile cellphone permits the smooth cloning of mobile phones. ESN/MIN pair isn't always encrypted while using phone to the MISC cell switching middle for further authentication. Therefore, just by scanning ESN/MIN pair, the smartphone can be cloned. If both ESN or MIN is modified, the service company will take delivery of the call and invoice it to the valid person or provide the services blind to the reality that it isn't always a disconnected receiver.

In step with media reviews [3], these days the Delhi (India) police arrested someone with 20 mobile-phones, a laptop, a SIM scanner, and a writer. The accused turned into jogging an alternate illegally in which he cloned CDMA primarily based cell telephones. He used software program named Patagonia for the cloning and furnished cheap global calls to Indian immigrants in West Asia.

III. HOW IS MOBILE CLONING DONE

Cloning involves editing or replacing the EPROM (Erasable Programmable read-only memory) inside the telephone with a new chip which could allow you to configure an ESN (digital serial wide variety) thru a software. You would also must change the MIN (Mobile Identification Number). whilst you had correctly modified the ESN/MIN [1] pair, your cellphone changed into an powerful clone of the alternative smartphone. Cloning required access to ESN and MIN pairs.

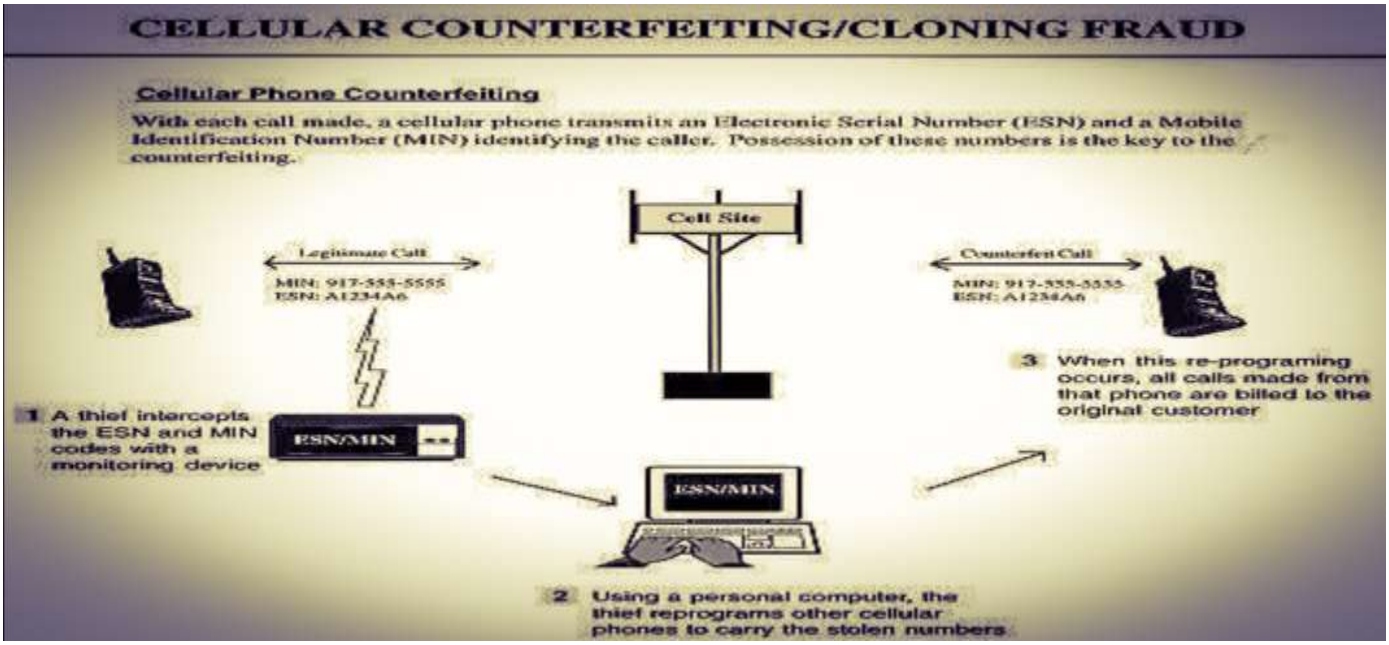

FIGURE 2: Mobile phone cloning process

Cloning has been effectively established underneath GSM, however the manner is not clean. With technically state-of-the-art thieves, customers are fantastically helpless against mobile phone fraud. Normally they turn out to be aware of the fraud best as soon as receiving their phone payments. Carrier vendors have adopted sure measures to save you cell frauds.

3.1 Cloning GSM Mobile Phones

GSM handsets, on the opposite, are safer, consistent with specialists. Every GSM smartphone has a 15 digit digital serial variety (referred to as the IMEI) [4]. It isn't always a mainly secret little bit of information and also you don't need to take any care to maintain it personal. The important data is the IMSI, which is saved at the detachable SIM card that contains all of your

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

subscriber statistics, roaming database and so forth. GSM employs a reasonably state-of-the-art asymmetric-key cryptosystem for over-the-air transmission of subscriber records. Cloning a SIM the usage of information captured over-the-air is hard, though now not impossible. As long as you don't lose your SIM card, you're secure with GSM. GSM includes use the COMP128 authentication algorithm for the SIM, authentication middle and network which make GSM a much comfy technology. GSM networks also can be hacked. The procedure is straight forward : a SIM card is inserted right into a reader. After connecting it to the pc using statistics cables, the cardboard info are transferred into the pc. Then, the usage of freely to be had encryption software at the internet, the card information may be encrypted on to a blank clever card. The end result : A cloned cellular smartphone is ready to misuse.

FIGURE 3: GSM cloning

3.2 Cloning CDMA Mobile Phones

Cellular telephone thieves monitor the radio frequency spectrum and steal the cellular cellphone pair as it's far being anonymously registered with a cellular website. The technology makes use of spread-spectrum techniques to percent bands with more than one conversations. man or woman's information is likewise encrypted and transmitted digitally. CDMA handsets are especially susceptible to cloning. First era cellular mobile networks allowed fraudsters to tug subscription statistics (consisting of ESN and MIN) from analog air interface and use this records to clone phones. A tool known as as DDI (virtual facts Interface) can be used to get pairs through absolutely making the device cellular and sitting in a hectic traffic vicinity and acquire all of the information you want. The stolen ESN an MIN statistics had been the programmed into a present day CDMA handset, whose present application was erased with the assist of downloaded software program. The customer then programs them into new telephones in an effort to have the identical range as that of the original subscriber.[4]

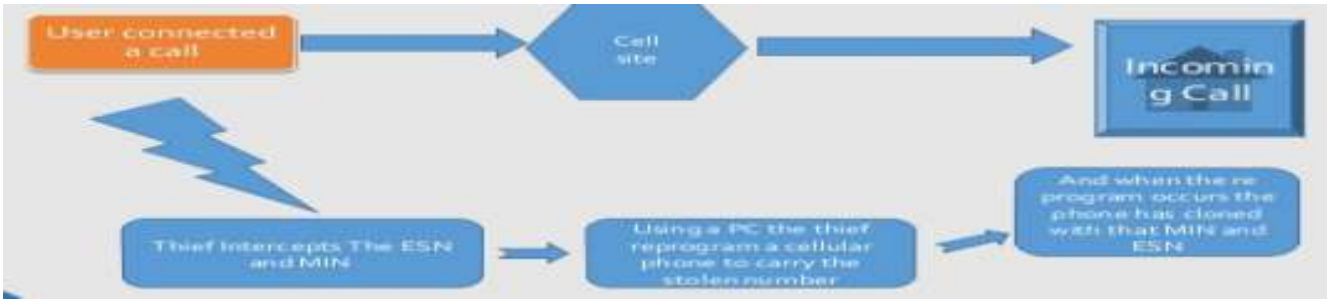

FIGURE 4: CDMA cloning

However looking on the latest case, it is quite viable to clone both GSM and CDMA sets. The accused in Delhi case used software program called **Patagonia** to clone handiest CDMA phones (Reliance and Tata Indicom). However there are software packages that can be used to clone even GSM phones (e.g. Airtel, BSNL, idea). in order to clone a GSM phone, know-how of the worldwide mobile gadget identity (IMEI) or instrument number is sufficient.

3.3 What is Patagonia ?

Patagonia is a software program to be had in the marketplace that is used to clone CDMA cell telephones. Using this software program a cloner can take over the manipulate of CDMA cellphone i.e. cloning of smartphone. There are different software program's to be had in the marketplace to clone GSM cellular cellphone. This software program's are without difficulty

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

available inside the market. A SIM can be cloned time and again and they can be used at extraordinary places. Messages and calls despatched through cloned telephones can be tracked. However, if the accuses manages to clone the IMEI number of the phones, for which software program's are to be had, there's no way he may be traced.[4]

IV. METHOD OF DETECTING CLONED MOBILE PHONES

Here are diverse methods to hit upon cloned telephones at the networks :[1]

4.1 Duplicate Detection

The network sees the same telephone in several places on the same time. Reactions include shutting all of them off in order that the real client will contact the operator due to the fact he misplaced the offerings he is deciding to buy, or tearing down connections in order that the clone customers will switch to any other clone however the real user will contact the operator.

4.2 Velocity Trap

The cell phone appears to be moving at impossible, or maximum unlikely speeds. For example, if a name is first made in Helsinki (capital of Finland), and 5 minutes later, some other name is made however this time in Tampere (another town in Finland), there ought to be two telephones with the identical identification of the community.

4.3 RF (Radio Frequency)

Fingerprinting is at the start a army technology. Even nominally identical radio system has a distinguishing "fingerprint", so the community software stores and compares fingerprints for all of the telephones that it sees. This way, it's going to spot the clones with the identical identification but one of a kind fingerprints

4.4 Usage Profiling

Profiles of customers' phone utilization are stored, and whilst differences are noticed, the patron is contacted. credit Card organizations use the identical method. as an example, if a consumer generally makes simplest neighborhood community calls however is putting calls to overseas countries for hours of airtime, it indicates a probable clone..

4.5 Call Counting

Both the phone and the community preserve song of calls made with the telephone, and ought to range greater than the normally allowed as soon as call, service is denied.

4.6 Pin Codes

Prior to placing a name, the caller unlocks the smartphone through entering a PIN code and then calls as usual. After the call has been completed, the consumer locks the telephone by getting into the PIN code again. Operators may additionally proportion PIN statistics to allow more secure roaming.

FIGURE 6: Operators sharing PIN information

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

V. HOW CLONING CAN BE DETECTED ?

5.1. Following are the ways to check whether the mobile phone is cloned or not. [2]

Consumer's can generally find out whether someone has made a identical to your cell telephone by using paying close attention to the conduct in their cellular cellphone itself. If consumer receives frequent incorrect quantity call on their telephone or their cellular phone hangs up regularly and user is going through problem in placing outgoing calls then they need to understand that their mobile telephone is being cloned.
The following maximum crucial signal is your cell cellphone bill. If you be aware uncommon calls or texts seems on the cellphone bills of person and those calls had been now not made by means of users, or an usual growth in interest, you need to extract your provider issuer without delay.

5.2. Following are the different ways that help the service provider to detect whether the phone is cloned or not. [2]

Patron's can typically discover whether or not a person has made a equal to your cell smartphone by the use of paying near attention to the behavior in their cellular cellular telephone itself. If consumer gets common incorrect quantity call on their smartphone or their mobile telephone hangs up frequently and person goes thru problem in placing outgoing calls then they need to remember the fact that their cell cellphone is being cloned.

The subsequent maximum crucial signal is your cell cellular telephone bill. in case you be conscious unusual calls or texts seems at the cellular telephone bills of individual and those calls had been no longer made by means of customers, or an typical increase in interest, you want to extract your company provider at once. A cloned mobile phone may have same numeric identity but a exceptional radio fingerprint. The radio finger printing is commonly utilized by cellular phone operator to prevent mobile smartphone cloning. If the service issuer spots the equal fingerprint of one existing unit, it quickly suspends the provider. The pattern of customers is studied and if any difference is discovered the patron is contacted for this kind of motive.

Every cell cellphone data the logs of applied services. The service company also maintains the tune of same logs. If the telephone is cloned then there is difference among the log record of organization and subscriber.

VI. HOW TO PREVENT CLONING ?

Carrier providers have adopted positive measures to prevent cell fraud. Those include **encryption, blocking off, blacklisting, person verification and site visitors evaluation**. [6]
Blacklisting of stolen telephones is some other mechanism to save you unauthorized use. A system identity sign in (EIR) permits community operators to disable stolen mobile phones on networks round the sector.
User verification the usage of non-public identity quantity (PIN) codes is one approach for purchaser safety towards mobile cellphone fraud. Assessments carried out have proved that United States of America determined that having a PIN code decreased fraud by using greater than 80%.
Visitors evaluation detects mobile fraud by using using synthetic intelligence software program to come across suspicious calling styles, which includes a sudden increase within the duration of calls or a sudden increase within the quantity of global calls.
The software program also determines whether or not it's miles bodily feasible for the consumer to be creating a call from a current area, primarily based on the place and time of the preceding name. currently, South Africa's two provider companies, MTN and Vodacom, use site visitors evaluation with the international Mobile system identity (IMEI) – a 15 digit range which acts as a unique identifier and is commonly imprinted on the returned of the cellphone beneath the battery – to hint stolen mobile phones.

VII. ADVANTAGES AND DISADVANTAGES

7.1 Advantages [5]

7.1.1 If your phone has been misplaced, you may use your cloned cellular smartphone.
7.1.2 In case your smartphone got broken or if you forgot your cellphone at home or some other place, Cloned cellphone can be very useful.

7.2 Disadvantages [5]

7.2.1 It could be used by the terrorists for crook activities.
7.2.2 It can be utilized by the cloner for fraud calls and for illegal money transfer.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

VIII. CONCLUSION

In nowadays's technology where cell phone is one of the critical additives of our existence, the threats and threat associated with its safety are growing at a higher tempo. The cellular smartphone as a tool is itself now not secure because the replica of cellular telephones can be without problems generated [12]. In United Kingdom and US the mobile phone cloning changed into entered in 1998 but in India, its miles still growing and entered in 2005. The future elements to shield the mobile telephones are very high as now crimes related to cellular phones are regarded. It can also assist to remedy criminal cases.

To conclude, mobile phone communication is one of the most reliable, green and significant. The usage of the gadget can be changed in both positive and negative approaches. Lamentably due to the security requirements it's far very smooth to break and additionally takes very less amount of time. [14] Furthermore, cloning can be effortlessly increased and also can be applied without difficulty. Consequently, it have to be considered that the security which is currently used isn't pleasant to secure the gadget in future. So it is very essential to confirm the working of safety machine time-to-time and also should exchange or update it over each month or year as soon as. Preventing steps ought to be taken by means of the community provider and the government to prosecute crime associated with cellular telephones isn't always regarded.

REFERENCES

[1] IEEE journel for mobile communication
[2] Security in the GSM network by Marcin Olawski
[3] Sankaranarayanan, "Mobile phone cloning", Wireless and Optical Communications Newtworks(WOCN), 2010 Seventh International Conference in Sept,2010
[4] Mislen, R,. Casey, E., & Kessler, G (2010). The growing need for an on-scene triage of mobile devices. Journal of Digital Investigation.
[5] http://www.slideshare.net.
[6] Introduction to Telecom Communication converging Technologies 1st Edition Kimberly Massey.
[7] 3G Networks 1st Edition --- Clint Smith, Saniel Collins.
[8] Wireless and Cellular Communication 3rd Edition --- William C.Y.Lee.
[9] Fundamentals of Mobile and Persuasive Computing --- Frank Adelstein, Sandeep Gupta.
[10] Mobile Communication Government of India Reports.
[11] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks, John Wiley and Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, England, 2005.
[12] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks", IEEE Computer, August 2004.
[13] K. Martinez, J. K. Hart and R. Ong, "Environmental sensor networks", IEEE Computer Journal, Vol. 37 (8), 50-56, August 2004.
[14] Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring", Proceedings of the 1st ACM International workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 88-97,2002.
[15] "Underwater acoustic sensor networks: research challenges", Ad Hoc Networks, Vol. 3(3), 257-279, May 2005.
[16] Cellular Telephone Cloning Final Report.2000, Economic Crimes Policy Team United States Sentencing Commission, January 25, 2000.