A
Dissertation On

Mobile Security, Phone Tracking and IMEI Cloning Detection

Submitted in Partial Fulfilment of the Requirement
For the Award of Degree of

Master of Technology

In

Software Technology

By

Saurabh Kumar
University Roll No. 2K15/SWT/516

Under the Esteemed Guidance of

MANOJ KUMAR
Associate Professor, Computer Science & Engineering, DTU

COMPUTER SCIENCE & ENGINEERING DEPARTMENT
DELHI TECHNOLOGICAL UNIVERSITY
DELHI – 110042, INDIA

STUDENT UNDERTAKING

Delhi Technological University
(Government of Delhi NCR)
Bawana Road, New Delhi-42

This is to certify that the thesis entitled **“Mobile Security, Phone Tracking and IMEI Cloning Detection”** done by me for the Major project for the award of degree of **Master of Technology** Degree in **Software Engineering** in the **Department of Computer Science & Engineering**, Delhi Technological University, New Delhi is an authentic work carried out by me under the guidance of Manoj Kumar.

Signature:
Student Name
Saurabh Kumar
2K15/SWT/516

Above Statement given by Student is Correct.

Project Guide:
Manoj Kumar, Associate Professor
Department of Computer Science & Engineering
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude and respect towards my guide **Manoj Kumar, Associate Professor, Department of Computer Science & Engineering.**

I am very much indebted to him for his generosity, expertise and guidance I have received from his while working on this project. Without his support and timely guidance, the completion of the project would have seemed a far-fetched dream. In this respect I find myself lucky to have my guide. He has guided not only with the subject matter, but also taught the proper style and techniques of documentation and presentation.

Besides my guide, I would like to thank entire teaching and non-teaching staff in the Department of Computer Engineering, DTU for all their help during my tenure at DTU. Kudos to all my friends at DTU for thought provoking discussion and making stay very pleasant.

Saurabh Kumar
Master of Technology, Software Engineering
2K15/SWT/516

ABSTRACT

Today are so many clone mobile phone available in Open market like Find my iPhone by IPhone, Find Device by Xiaomi, Protect Your Phone by Motorola etc. but still lost phone recovery is very poor and it's very difficult to track your lost phone and huge market of stolen phone. There are so many clone phone available in market which does not meet safety standard due to which customer has to suffer its side effect like more radiation poor quality and OEM name is getting misused and customer may loose the trust.

The purpose of this project to discourage the duplicate and stolen mobile phone market and discourage phones theft, we want to secure mobile phone user interest and ease law enforcement authorities for lawful interception, our agenda to implement software help to track the lost and stolen phones, Detect IMEI Cloning and provide mobile data Security.

Currently All Available Android phone software fails if thief perform some below steps Like User Data is wiped using factory reset or master reset or thief bring stolen phone in Download state and flash new binary or with some hack thief edit the current IMEI with Some other mobile available IMEI or some Fake IMEI. In current situation is almost impossible to track after these state.

The implementation of new solution this would resolve mentioned problem and also discourage the stolen mobile phones also allow blocking of lost/theft mobiles across mobile networks and aware consumers by making them aware of the information related to fake and cloned mobile equipment's also provide Mechanism to report loss/theft of mobile equipment.

TABLE OF CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOL, ABBREVIATIONS

Long Term Evaluation (LTE)

Home Location Register (HLR)

General Packet Radio Service (GPRS)

Universal Mobile Telecommunication System (UMTS)

Radio Interface Layer (RIL)

Short Message Service (SMS)

International Mobile Subscriber Identity (IMSI)

International Mobile Equipment Identity (IMEI)

Mobile Country Code (MCC)

Mobile Network Code (MNC)

Advanced Encryption Standard (AES)

Subscriber Identity Module (SIM)

Virtual Mobile Number (VMN)

First in First out (FIFO)

Embedded Multi Media Card (eMMC)

Card Identification number register (CID)

Original equipment manufacturer(OEM)

CHAPTER 1

INTRODUCTION

1.1 General Concepts

CONCEPT OF IMEI: Mobile security with IMEI

Nowadays, mobile phone is popular target of snatcher and thieves so protecting them some practical approach required to keep their mobile phone safe. International Mobile Equipment Identity (IMEI) used widely for unique identify of mobile phone. IMEI is a unique 15 - digit code which is used to uniquely identify a unique GSM mobile phone. User can check it by dialing *#06#. The IMEI number is also mentioned on the compliance plate under the battery. The code having four groups that look like this:

aaaaaa--aa-aaaaaaa-a.

The first 6-digit code is the Type Approval Code (TAC) which having information OEM and its model information. Its first two digits represent the country code. The other code is final assembly code. Second group of code having information manufacturer. The third set is information of serial number of phone and the last single digit code is an additional number (usually 0). Its revered code that can be used in future, its means EIR having all valid mobile phone database. When a mobile register in particular network then its IMEI number get registered.

When a phone is on, then IMEI code is checked against a database of blacklisted or grey-listed phones in the network's Equipment ID Register. This Equipment ID Register decide whether the mobile registration to network to do and receive Message and call.

Grey-listing - In Grey-listing user can allow to use mobile phone but it getting monitored in background and current SIM information and location will be used for tracking.

Blacklisting - In Blacklisting not allow user to get it register to the network.

1.2 Motivation

Today every day thousands of mobiles phones lost and stolen and its effective cost are in millions. To avoid misuse of lost phones we use International Mobile Equipment Identifier (IMEI) tracking and blocking technique. But current exiting technique in android mobile having many limitation and now days' thief and hacker are smart enough to break exiting security. There are various tracking mobile phone software available but still tracking and recovery of lost mobile phone result is not good. In this thesis we will go through why tracking and recovery is difficult in current scenario, how this can be improved and how solution will overcome with it.

Also it has been noticed duplicate mobile phone with having similar hardware configuration like (ROM, RAM, and Front/Rear Camera, Display, etc.) are available in market and use to sale customer with branded OEM name, in many cases they use same IMEI number which has allocated to other OEM manufacturer. Currently there is no mechanism so that user can verify authenticity of his mobile phone, our aim to discourage grey market and duplicate mobile phone to providing mechanism so that user can verify its authenticity.

1.3 Related Work

Existing Approach

There are some software's provided by OEM like Find my iPhone by IPhone, Find Device by Xiaomi, Protect Your Phone by Motorola etc. but still lost phone recovery is very poor and it's very difficult to track your lost phone and their huge market of stolen phone also there is no mechanism to identify the cloned mobile phones.

Why Tracking Becomes Tough

User Data wiped out is not difficult in android phone various guides on the subject talk about the factory reset wiping out "all user data". Even mobile phone is locked state still factory reset is possible. Once user data is wiped out various installed tracking software is not able to work. Nowadays thief are smart they are aware about existing loopholes in existing tracking and mobile security software. So they use to flash new Binary all tracking installed tracking software data will be lost and tracking software will not work. In some cases hacker is able to edit IMEI number in android phones after changing correct IMEI to some fake IMEI or cloned IMEI no tracking mechanism to track it. Even blacking and Grey-listing marked on EIR network is not able to detect it.

CHAPTER 2

LITERATURE REVIEW

2.1 What is GPS, How its work

Global Positioning System (GPS) is a satellite-based navigation system that uses a network of 24 satellites and help to maintain 3-D locating data to GPS receivers. Initially this was launched by United States Department of Defense for military purpose. Today, Global Positioning System is open for everyone to benefit and works in conditions, currently there is no charges to use GPS.

Today almost smart phones come with having GPS embedded in it. GPS enabled devices means GPS receiver present in mobile phone and GPS receiver's takes help of calculation of difference in time of transmission and receipt of sent signal from satellite and this use to calculate the separation of phone from satellite.

2.2 Existing Approach

Today we have many software available to track the lost phone, various OEM provide tracking software. IPhone is costly smart phone is market and due its high cost its first target of thief.

Phone provide tracking mechanism to track his smart phone. For Tracking I phone you must need Apple ID and tracking option must be enable in device. For tracking we need to use "Find My iPhone" app on another iPhone phone then you need to enter Apple id and password of lost phone, this it will used for authentication of valid owner of phone, after passing the authentication he can select his lost phone and press view to locate the current location of phone if phone is turned off then it will last known location. Same to the Apple phone, Android mobile phones having a power to track the lost phone using GPS technology. For Android phone google account will used for authentication and the tracking will be done via Android Device Manager.

For tracking of a Windows OS Phone same to other type mobile phone providers, a Windows OS phone needs Microsoft Account for authentication via Web using Windows Phone website. Samsung also provide “Find my Mobile”(FMM) for tracking of lost phone and for FMM Samsung account will be used.

Existing operator based solution

AT&T - Popularly known as FamilyMap service which is capable of sending the location data via SMS or email of the family member, this service currently costs around $9.99 per month. Sprint -The Spring Family Locator which currently costs around $5 per month is providing an economically alternative option compared to other operators. It’s accessible through web-enabled browsers and mobile devices. It also provides alerts if the target device doesn't arrive at its pre-assigned destination within the stipulated time.

T-Mobile - T-Mobile provides the T-Mobile Family service. In addition to providing traditional real-time location services, it also provides alert system feature as sprint and week-long history additionally. The current subscription cost is around $10 per month.

Verizon- Verizon currently provides the Verizon Family Locator service on post-paid basis with subscription costs around $10 per month. This service can be accessible via any web-enabled Verizon device. This service also provides alert system service configuration as sprint.

2.3 Track a Cell Phone using Third Party Apps

Another option for tracking a cell phone is to use a third party application. Once we install the application works similar to the major service provider applications by until the utilising the inherent GPS technology on the targeted phone. The following are a few of the popular third party applications available to track cell phones on the market today:

Stealth Genie - Stealth Genie is a commercial mobile phone tracking application popular among the next-generation parents which is used to track their beloved children. This software can be runnable on any Android, Blackberry, or iPhone device and additionally it's capable of providing advanced features such as recording the environment of the user and monitoring abnormalities in both Skype and SMS text conversations

Phone Sheriff-Along with Stealth Genie, Phone Sheriff is a commercial mobile phone tracking application that is designed for both parental and business purposes which is runnable on all Android, Blackberry, Apple, Windows, and Symbian OS devices. In addition to providing real-time location services, it also provides the capability to block phone numbers, monitor text messages, and view all other information located on the targeted phone.

CHAPTER 3

PROPOSED WORK

3.1 Technical Overview: Overall Flow

1. In proposed solution when mobile phone will be switch we will wait for SIM. Initialization and device registration to network. After successful network registration our Algorithm will start.

2. Algorithm will trigger one service and which collect below information. IMEI number, Sim MCC and MNC number, unique number and store these data in database.

3. Then Algorithm will check SIM IMSI number. An international mobile subscriber identity is unique code it’s having 15 digits as mentioned in Global System for Mobile Communications and Universal Mobile Telecommunications System. The IMSI information is stored inside of SIM card.

4. Then Algorithm will check SIM IMSI number of inserted SIM, if its new SIM then it will create one message with having details of IMEI, Unique Number, MCC and MNC and apply RSA algorithm on it with key and appended some identifier above with this message.

```
Single SIM Message Format

MF<SPACE>
Encrypted data using RSA (
<No of SIMs><COLON>
< IMEI Number>< COLON >
<MCC>< COLON >
<MNC>< COLON >
<Encryption Algorithm>< COLON >
)



Dual SIM Message Format

MF<SPACE>
Encrypted data using RSA (
<No of SIMs>< COLON >
< IMEI1 Number>< COLON >
<MCC1>< COLON >
<MNC1>< COLON >
< IMEI2 Number>< COLON >
<MCC2>< COLON >
<MNC2>< COLON >

<Encryption Algorithm>< COLON >
)
```

5. This encrypted message will add one predefine VMN and message has been delivered to RIL to send the message.

3.2 Unique Number

Every mobile phone comes with EMMC for flash memory which having information of Universal CID. EMMC is Embedded Multi Media Card which used as universal low cost data storage and communication media and CID is unique Card Identification register number, which used for card individual number for identification, so unique number is unique code which generated from CID which cannot be edited.

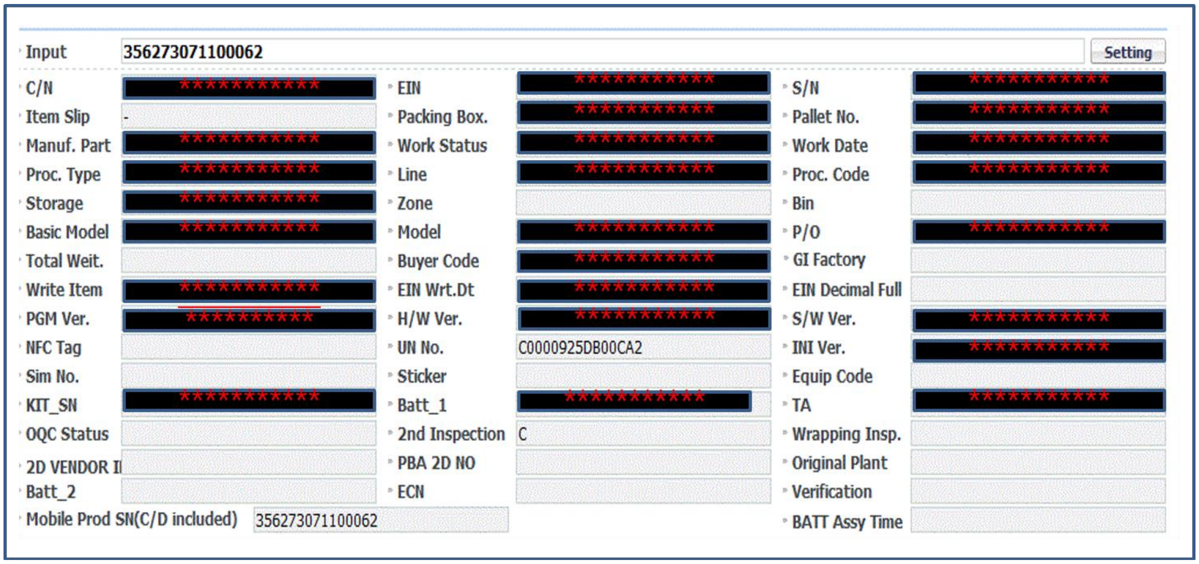
3.3 The Card Identification/ One Time Programmable overview

The Card Identification (CID) register is 128 bits wide. It contains the card identification information which has been used during the card identification phase (Multimedia Card protocol). Every flash or I/O card shall have a unique identification number. Every type of Multimedia Card ROM cards (Refer Jesdec doc JESD84-A43.pdf Pg77).

One Time Programmable (OTP): Programming of the card identification register. This command shall be issued only once. The card contains hardware to prevent this operation after the first programming. Normally this command is reserved for the manufacturer (Refer Jesdec doc JESD84-A43.pdf Pg54 Table 16).

At the time of manufacturing this UN is paired with IMEI/SN and maintained in factory server. In case of any hardware replacement, this EMCC is updated in factory server.

Factory server mapping IMEI and Unique number which updated during IMEI writing in Production



Input 356273071100062

C/N	[redacted]	EIN	[redacted]	S/N	[redacted]
Item Slip	-	Packing Box.	[redacted]	Pallet No.	[redacted]
Manuf. Part	[redacted]	Work Status	[redacted]	Work Date	[redacted]
Proc. Type	[redacted]	Line	[redacted]	Proc. Code	[redacted]
Storage	[redacted]	Zone		Bin	
Basic Model	[redacted]	Model	[redacted]	P/O	[redacted]
Total Weit.		Buyer Code	[redacted]	GI Factory	
Write Item	[redacted]	EIN Wrt.Dt	[redacted]	EIN Decimal Full	
PGM Ver.	[redacted]	H/W Ver.	[redacted]	S/W Ver.	[redacted]
NFC Tag		UN No.	C0000925DB00CA2	INI Ver.	[redacted]
Sim No.		Sticker		Equip Code	
KIT_SN	[redacted]	Batt_1	[redacted]	TA	[redacted]
OQC Status		2nd Inspection	C	Wrapping Insp.	
2D VENDOR II		PBA 2D NO		Original Plant	
Batt_2		ECN		Verification	
Mobile Prod SN(C/D included)	356273071100062			BATT Assy Time	

CHAPTER 4:

REGISTRATION PROCESS

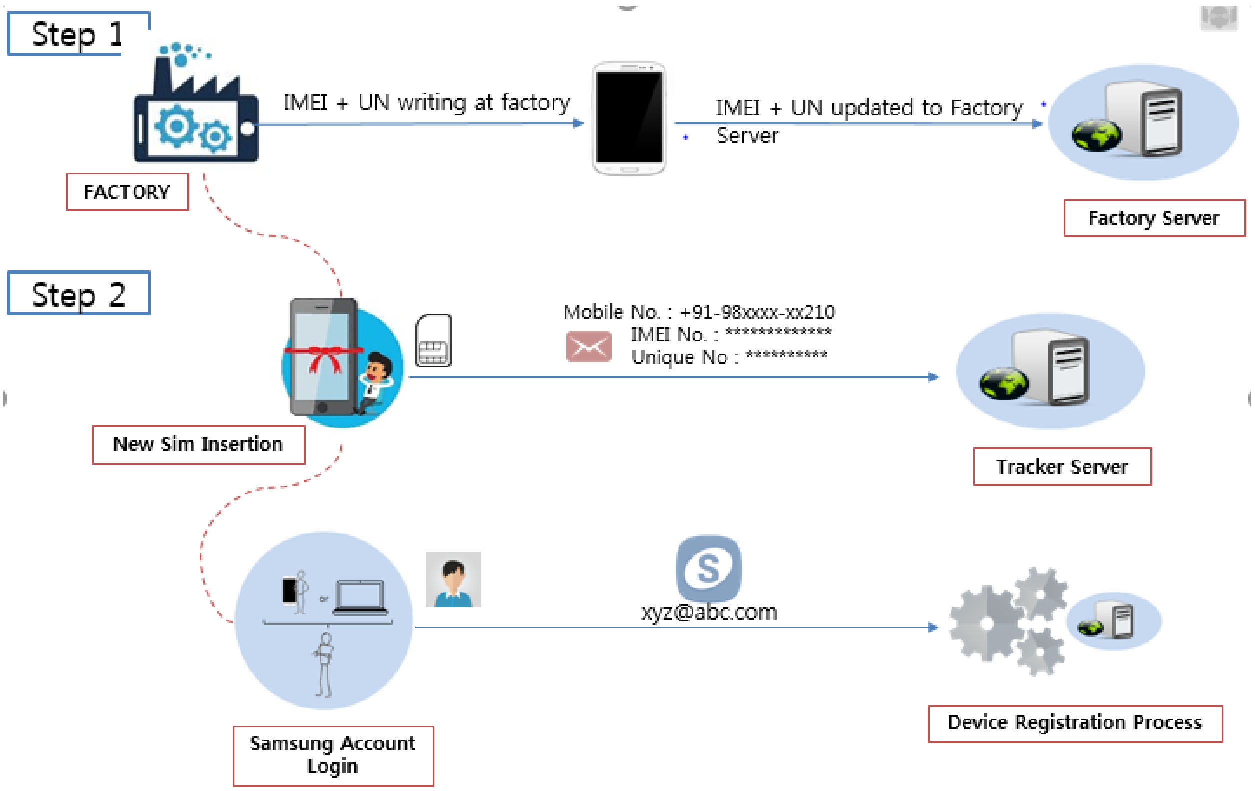
4.1 Technical overview registration process

Registration process can be divided in three parts.

Step 1- New Device registration to Factory server while writing IMEI in production

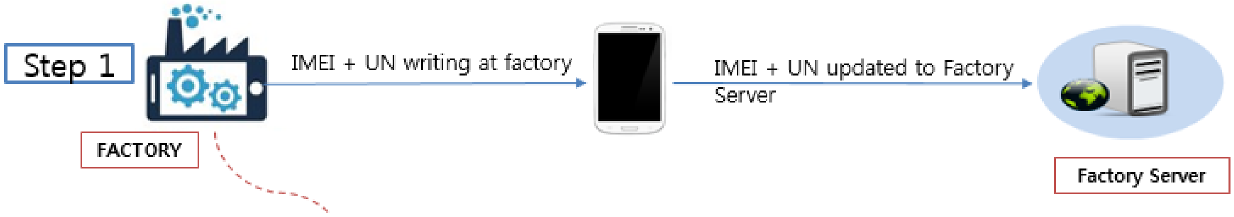
Step 2- Device registration to Tracker sever when user insert new sim in device

Step 3- Onetime registration on Cloud server when user boot the device first time



4.2 Registration Process to Factory Server:

Whenever IMEI writing process done in factory then at that time IMEI number and its mapping to UN will be updated to server. Refer step 1 in below figure. The basic important information of device will send server like IMEI1 Number, Unique number, model Number and Timestamp for Dual sim model we will have two IMEI for single Sim Models IMEI2 will filled with NA.


Step 1
FACTORY
IMEI + UN writing at factory
IMEI + UN updated to Factory Server
Factory Server

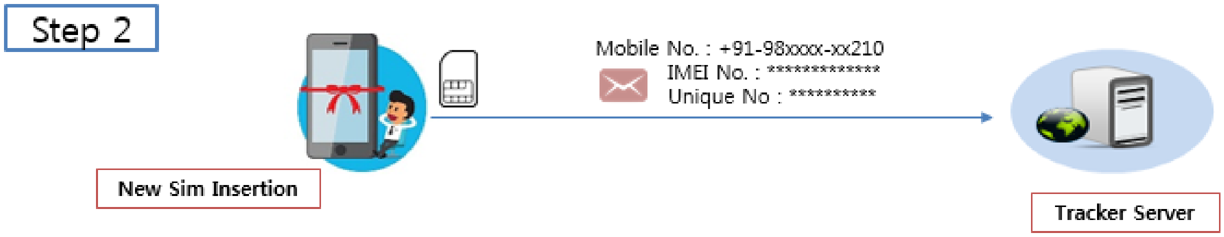
FactoryServerTable Architecture

IMEI1 Number	IMEI2 Number	Unique Number	Model Number	Timestamp
356273071100082	356273071100083	C0000925DB000DC8	G615F	3012181225
356273071100091	NA	C0000925DB000CA2	J710FN	2416171225
356273071100055	356273071100057	D0000425DB000PS2	T385G	1209161329
356273071100069	NA	C0100525DC000CQ3	G611F	2512181220

This FactoryServerTable will be used for mobile cloning detection and lost mobile phone detection when thief will edit the IMEI entry of device somehow. This table keep update whenever any model came in factory for production. After the sale of model if due to any reason ROM not working then service centre use to replace RAM or Motherboard then in that case this table will update so IMEI and unique key mapping will always be maintained. In this table Unique key will work as primary key.

4.3 Registration Process to Tracker Server:

After the IMEI writing process done in factory when device come to shop then sold out at shop now whenever user insert his SIM then first time user registration will be done and in background and one encoded message will be generated form user mobile phone and this encoded message will be sent to tracker server. After receiving encoded message at server Decoding Service will de-code this message and then store the information in database.



UNIQUE_KEY_MASTER_TABLE

IMEI1 Number	IMEI2 Number	Unique Number	Model Number	Timestamp
356283071100082	356267071100083	C0000925GB010DC8	G610F	1312181225
356273071230091	NA	C0000925DB002CA2	J700FN	2316171225
356273781100055	356273034100057	D0000425DB050PS2	T352G	0209161329
356273071145069	NA	C0100525DC007CQ3	G681F	0612181220

In UNIQUE_KEY_MASTER_TABLE Unique Number will work as primary key and foreign key in UNIQUE_KEY_NETWORK_TABLE. IMME2 will marked as NA if its single sim model for dual sim model each row will have to IMEI entry.

UNIQUE_KEY_NETWORK_TABLE

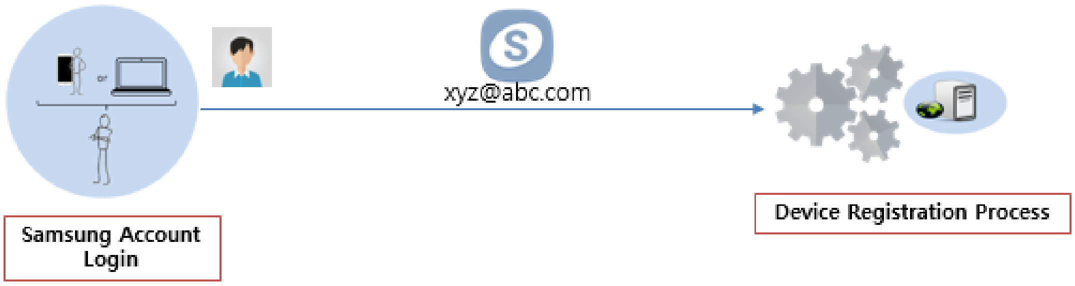
MCC1	MNC1	Mobile number	Unique Number	MCC2	MNC2
404	04	9560733045	C0000995GB010DC8	405	07
405	07	9810863708	C0000925DB902CA2	404	10
405	09	9560733056	D0000425DB055PS2	404	04
404	10	9810863606	C0100525DC006CQ3	404	09

Both table linking will be done using Unique Number. We have kept two pair of MCC and MNC values, one pair of MCC/MNC fetched from sim this provide information of mobile number service provider information and other pair of MCC/MNC provide current network provider of sim. Suppose user A perchance a SIM of O operator in S1 state, thein in this case SIM provided by operator will have MMC/MNC written in SIM which having MCC/MNC information as per current location now he moved to some other country or state where O2 operator provided network service if no network of O network present in that region then in this case MCC/MNC information will be fetch from SIM.

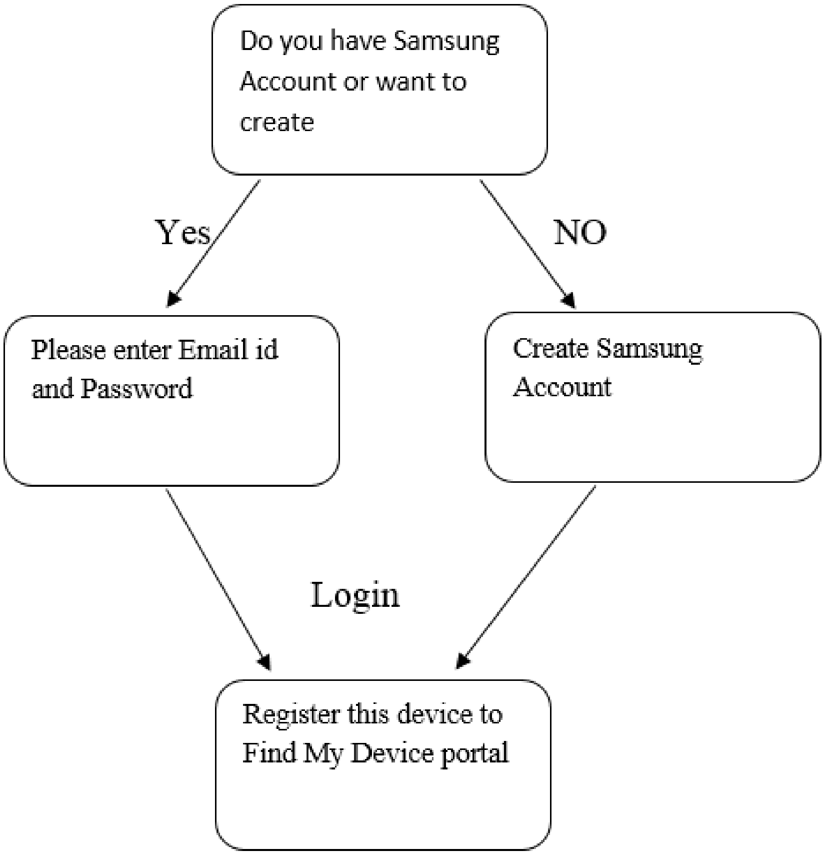
IMEI1 /IMEI2 Number	International Mobile Equipment Identity Number of owner. For dual sim model IMEI1 and IMEI2 both will be updated for single sim IMEI2 will marked as NA.
Unique Number	Its Unique identity of mobile phone this number written in rom once its written it cannot be edited
Contact number	From which number message has been received on Tracker Server
Timestamp	Time at which when registration request has received
MCC1	Its Mobile country code of Sim , this value fetch from sim
MNC2	Its Mobile Network code of Sim , this code value store in sim
MCC2	Its Mobile country code of Sim , this value explain current network MCC value
MNC2	Its Mobile Network code of Sim , this value explain current network MNC value

4.4 Registration Process to FIND_MY_PORTAL

When user boot up his device first time then on set up wizard user has to configure one account if he donot having any Samsung account if having any Samsung account, he can use this account.



If user do not have Samsung account, then he has created the Samsung account if have Samsung account device registration to Find My Mobile portal will be done via existing account. Device unique number, IMEI number will fetch from device and it will be shared to Find My Mobile portal


Do you have Samsung Account or want to create
Yes
NO
Please enter Email id and Password
Create Samsung Account
Login
Register this device to Find My Device portal

FIND_MY_MOBILE Master Table

User ID	Model NO1	Model NO2	Model NO3	Model No...	ModelN0 20
Saurumar.ig	G611	G612	G617	……………..	G518
kumar.ig	S600	G601	G602	………………	G701
vioultumar.ig	G356	G652s	G412s	……………	J415
Rajiv.k2	G612	G618	G672	……………..	J400

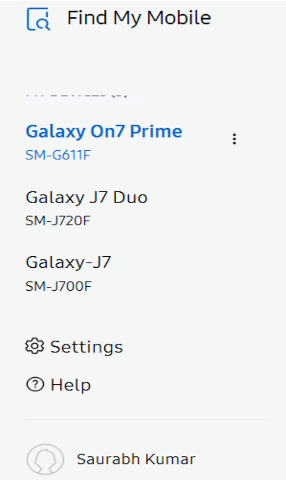
We will keep record of 20 model login by particular Samsung account if user exceed it then first registered record details will be delete and new record will be added in 20th place. It will use FIFO concept User ID work as primary in FIND_MY_MOBILE Master. For particular user cannot have duplicate model number in model list if user use different mobile with same model number and use same Samsung account then new Model details will be updated, and old model detail will removed

MODEL_DETAIL_TABLE

User ID	Model NO	IMEI1	IMEI2	Unique No
Saurabhkumar.ig	G611	356267071100083	356267071100084	C0000925GD000DC7
kumar.ig	S600	356267071105686	356267071105687	C0004525GD000DC6
vioultumar.ig	G356	356267071155678	NA	C0004525GD990DC8
Rajiv.k2	G612	356267071155645	NA	C0004526GD990DC8

4.5 Authentication of Owner:

Before taking any complain from user its authentication is important otherwise someone who is not actual owner of mobile phone miss use it. Authentication will be done using created account on cloud. As we have user data base in FIND_MY_MOBILE Master Table and MODEL_DETAIL_TABLE in Cloud server. After successfully login authentication will be granted.



User can select lost device form this list and mark as lost. Then user has to mention his contact details like email address and contact number on portal for future recovery purpose. This request will be forwarded to tracker server. Tracker server create one data base which will have IMEI Number, Unique Number, Email ID, Contact No, and Timestamp.

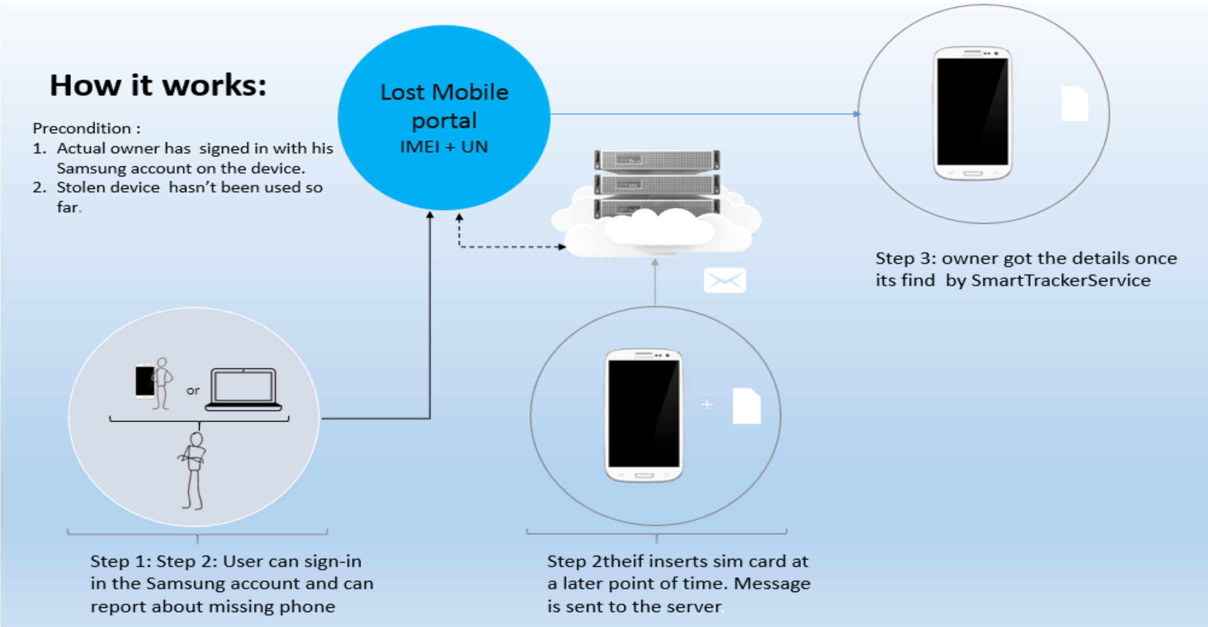
IMEI Number	International Mobile Equipment Identity Number of Lost phone
Email id	Mobile phone Owner Email id, in which our SmartTrackerService will send Auto generate email once this service find the current owner details
Unique Number	Its Unique identity of mobile phone this number written in rom once its written it cannot be edited
Contact number	Owner Current mobile number once our SmartTrackerService find the lost mobile then thief current mobile details will be shared to this number
Timestamp	When user register his request on lost mobile portal, then current date and time will be converted to one time. SmartTrackerService use to monitor if any update received in Tracker server as this time stamp with same Unique number.

On LostPhoneFind Database will be created on Tracker Server. SmartTrackerService will use this database and use to run daily whenever he found less load on server, ideally it will night time as probability of new sim insertion at this will be less.

LostPhoneFind Database Architecture

IMEI Number	Unique Number	Email Id	Contact No	Timestamp
356273071100082	C0000925DB000DC8	Saurabh@gmail.com	9560733045	3012181225
356273071100091	C0000925DB000CA2	rahul@yahoo.com	9560733066	2416171225
356273071100055	D0000425DB000PS2	vipul@samsung.com	9560733088	1209161329
356273071100069	C0100525DC000CQ3	ankur@rediff.com	9570733066	2512181220

4.6 Working of SmartTrackerService:



How it works:

Precondition :

1. Actual owner has signed in with his Samsung account on the device.
2. Stolen device hasn't been used so far.

Step 1: Step 2: User can sign-in in the Samsung account and can report about missing phone

Step 2theif inserts sim card at a later point of time. Message is sent to the server

Step 3: owner got the details once its find by SmartTrackerService

As lost mobile data has been sent to IMEI tracker server, IMEI tracker maintain all lost mobile data and keep checking whether new entry came on IMEI tracker server using UNIQUE_KEY_MASTER_TABLE. If any unique key from LostPhoneFind Database found in UNIQUE_KEY_MASTER_TABLE, then this service returns the current owner details to lost mobile portal and deliver message to actual owner with necessary details.

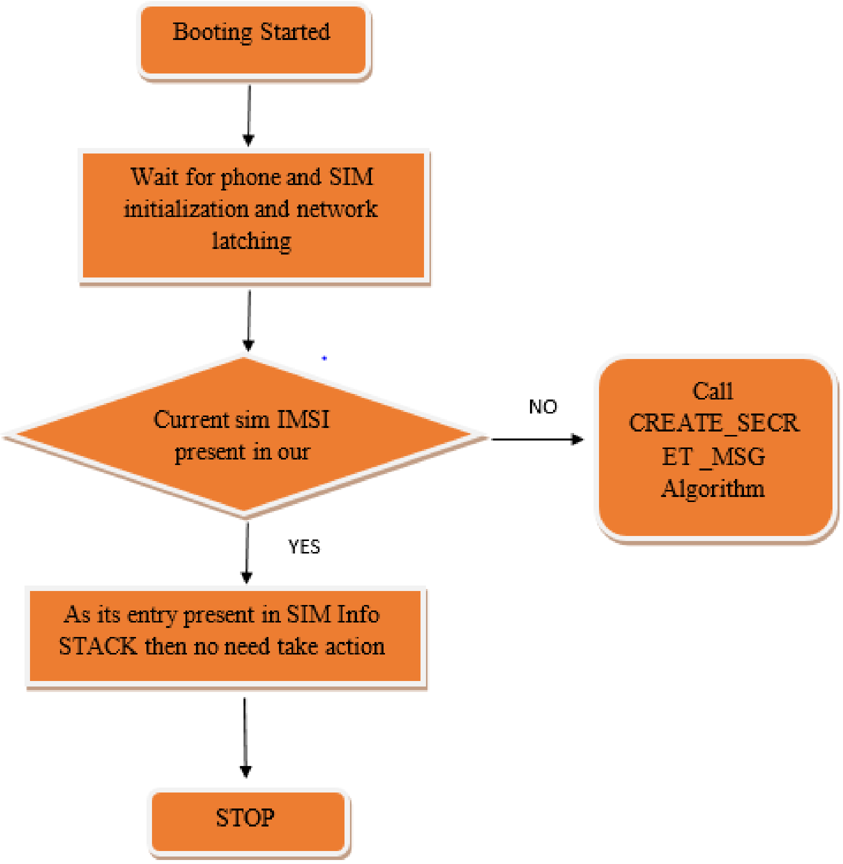
CHAPTER 5

DEVICE INTELLIGENCE

Whenever new sim will insert in mobile phone device intelligence will check whether its new sim or existing sim. If it’s find new sim has been inserted then it collects IMEI Number, Unique Number, and SIM MCC/MNC number and generate Message PDU in background. Then this PDU passed to Encryption algorithm then send secret PDU to Tracker virtual number.

5.1 Device Intelligence: when SIM used before

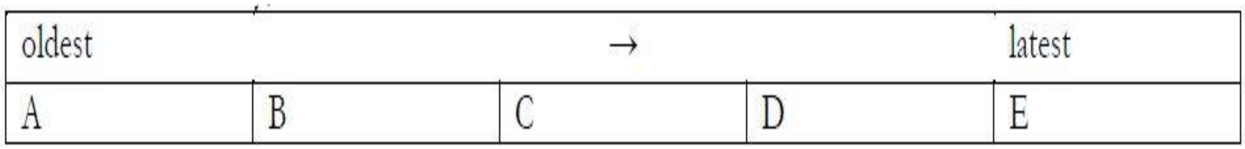
Whenever we insert new SIM we checked IMEI entry in SIM_TABLE_STACK. If the entry not present, then algorithm will follow below flow.


Booting Started
Wait for phone and SIM initialization and network latching
Current sim IMSI present in our
NO
Call CREATE_SECRET _MSG Algorithm
YES
As its entry present in SIM Info STACK then no need take action
STOP

5.2 Technical overview of SIM_TABLE_STACK

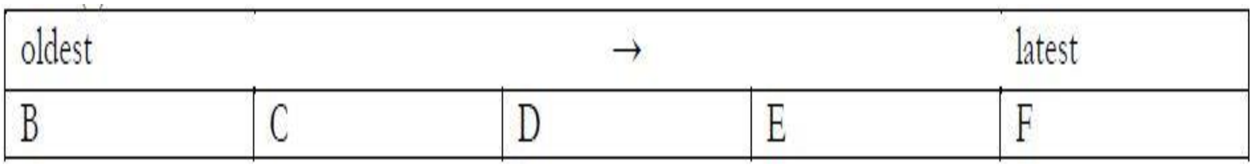
SIM_TABLE_STACK is an array List which remember information of previous IMSI information, Size of SIM_TABLE_STACK set as 5. It is ordered list. When the SIM_TABLE_STACK is full, then oldest entry will be deleted. It means FIFO (First in First Out concept).

(1) If SIM A, B, C, D and E are orderly inserted and secret message is Sent successfully, this consist of SIM_TABLE_STACK is below.



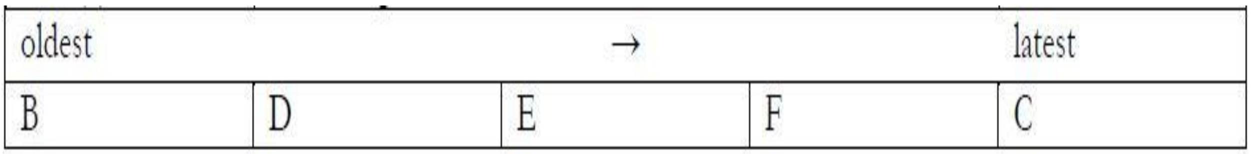
oldest		→		latest
A	B	C	D	E

(2) If SIM F is inserted, the oldest one – A- is deleted.



oldest		→		latest
B	C	D	E	F

3) If SIM C is inserted again, the location of C set as latest one.

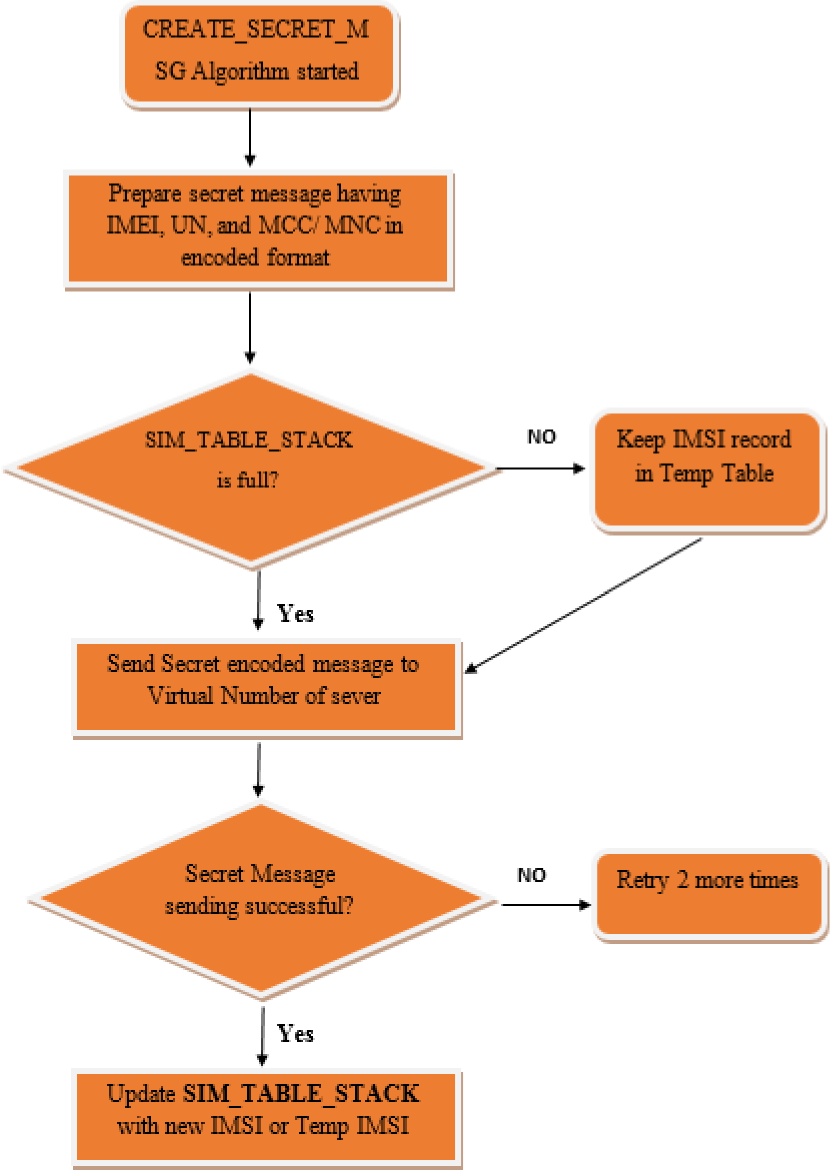


oldest		→		latest
B	D	E	F	C

5.3 Device Intelligence: when New SIM

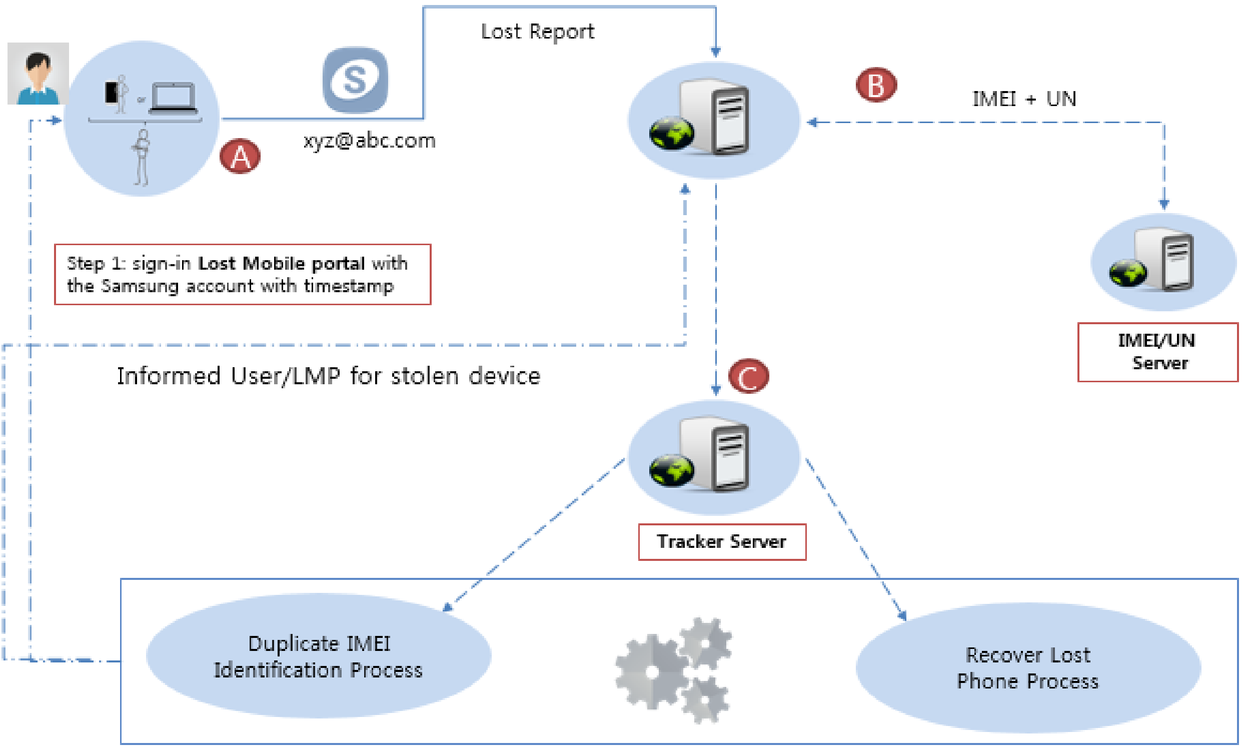
If entry not find in SIM_TABLE_STACK Array list it will be considered as new record, and for new sim Secret message will be created handover to RIL APP to get it deliver.

CREATE_SECRET_MSG Algorithm:


CREATE_SECRET_M
SG Algorithm started
Prepare secret message having IMEI, UN, and MCC/ MNC in encoded format
SIM_TABLE_STACK
is full?
NO
Keep IMSI record in Temp Table
Yes
Send Secret encoded message to Virtual Number of sever
Secret Message sending successful?
NO
Retry 2 more times
Yes
Update SIM_TABLE_STACK with new IMSI or Temp IMSI

5.4 Overall System Design of Lost Mobile Recovery process

As we discussed onetime user registration will be done when user insert sim first time. This registration will be used for tracking his lost phone if it's happen in future. Assume after few month user mobile phone has been snatched or stolen. Below diagram is overall system design architecture of lost mobile tacking and clone mobile detection process.


Lost Report
xyz@abc.com
A
B
IMEI + UN
Step 1: sign-in Lost Mobile portal with the Samsung account with timestamp
IMEI/UN Server
Informed User/LMP for stolen device
C
Tracker Server
Duplicate IMEI Identification Process
Recover Lost Phone Process

User can Track the mobile phone even if IMEI/Binary is Re-flashed

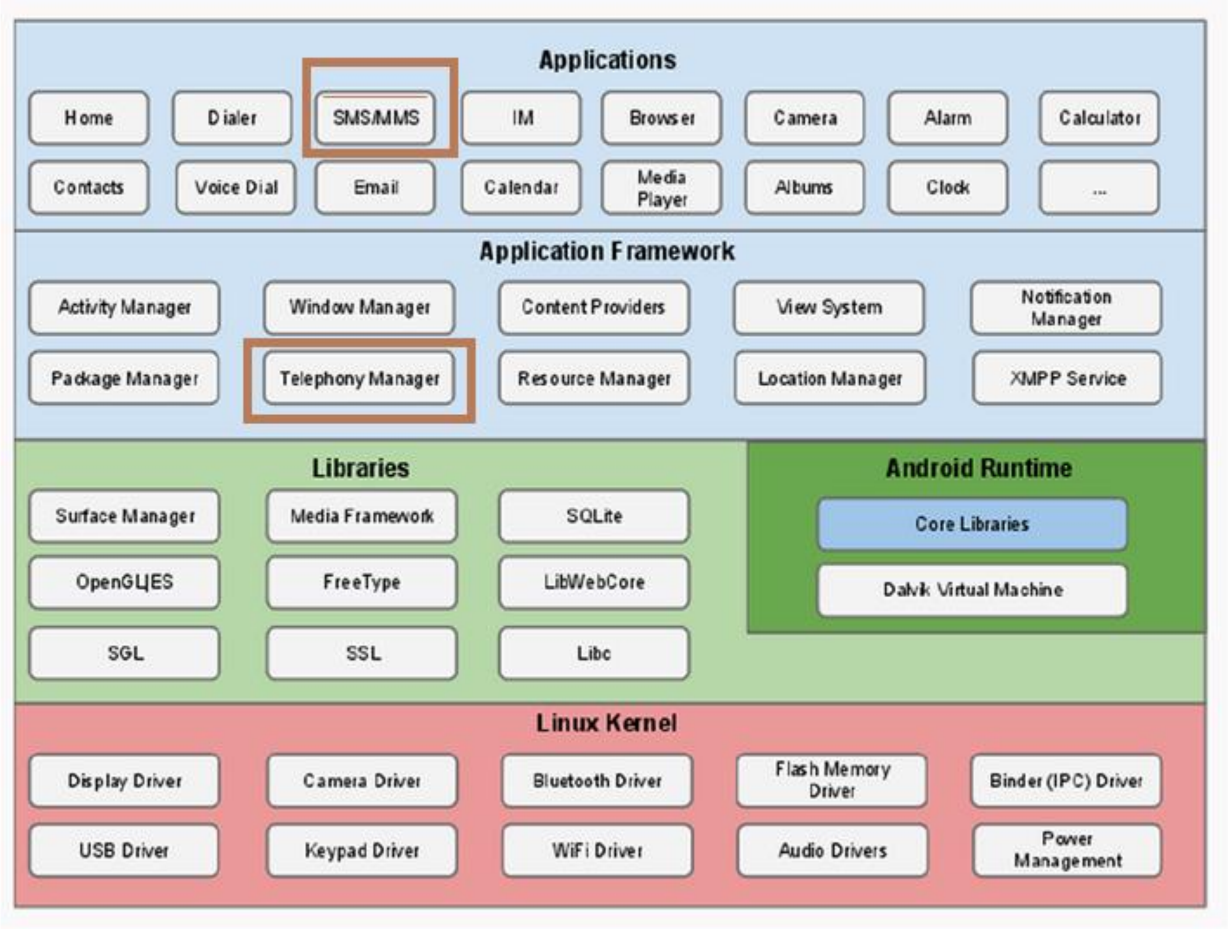
After he lost his mobile phone then our system provide user to report lost phone details after successful authentication his lost mobile complain will be registered. One Tracking service will run on our Tracker server to track the lost phone.

CHAPTER 6

IMPLEMENTATION, USECASE

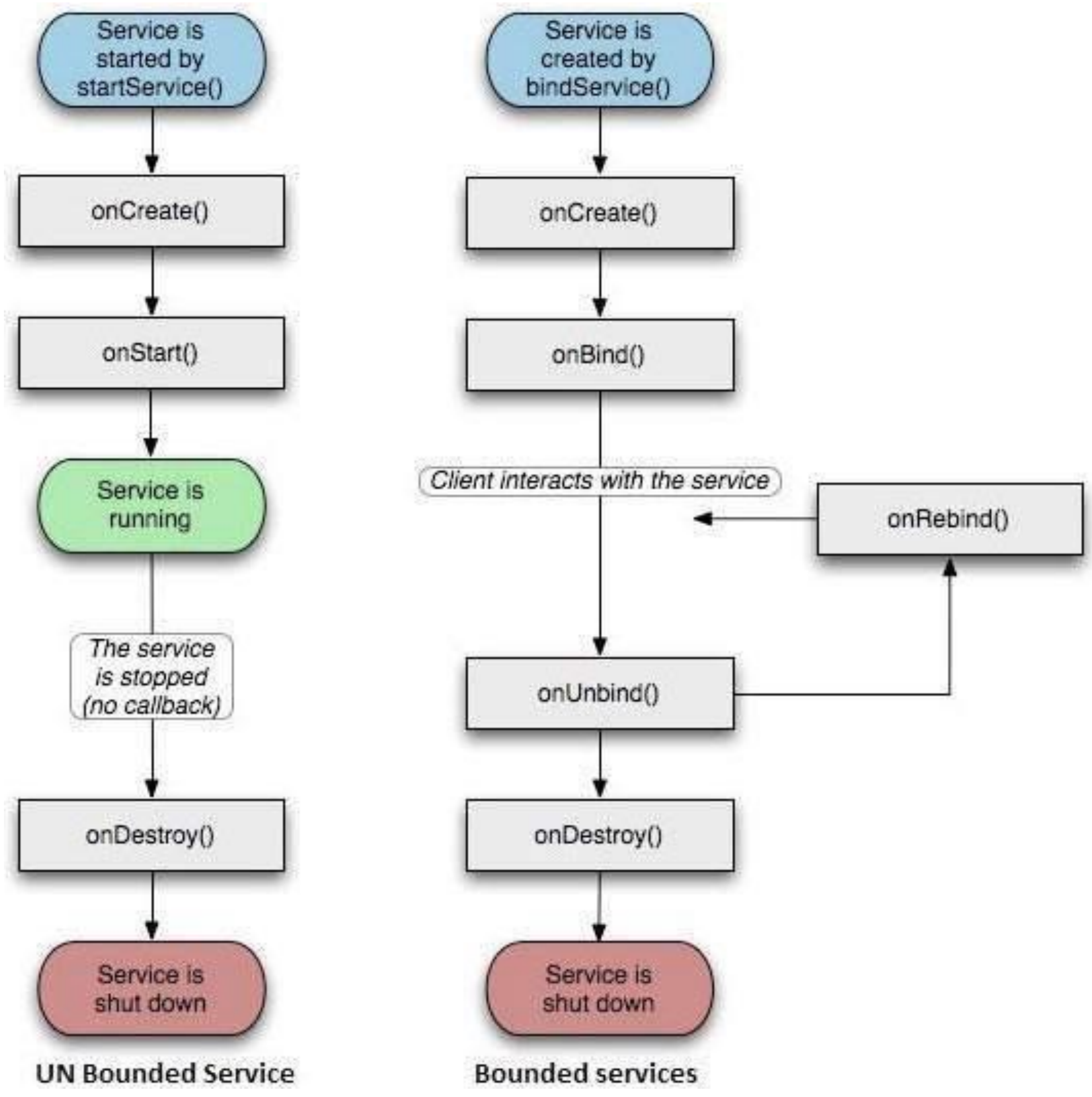
6.1 Implementation

Lost mobile tracking implementation will part OEM software and changes has been two Application, Application Framework Layer. In Application layer changes has been done default message native app. This is system app so user cannot uninstall this app. In Application framework layer changes has been done in Telephony manager.



`

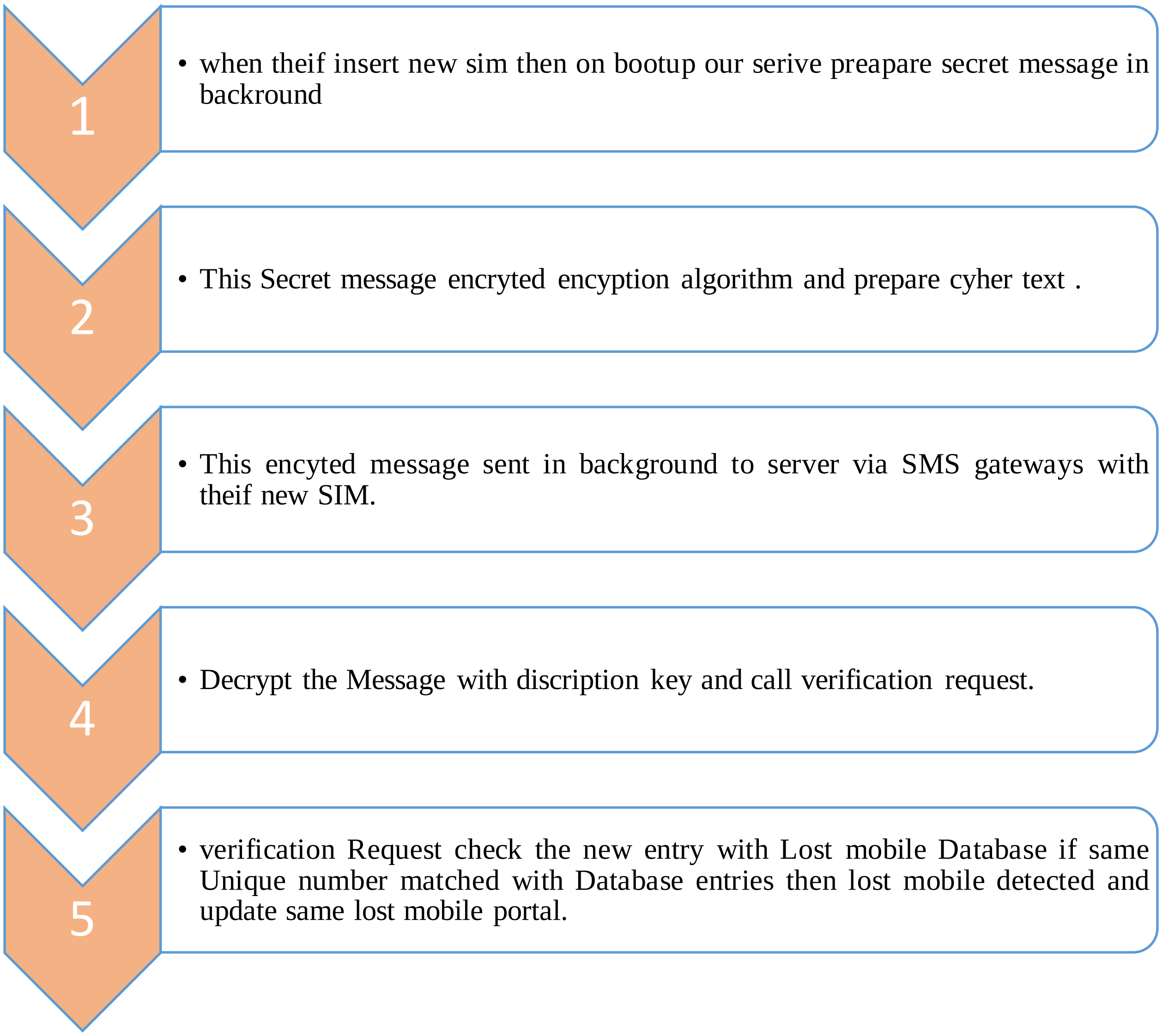
Whenever device is rebooted system sent boot completed broadcast, whenever our application get this broadcast it will trigger Create_Secret_Message service and prepare secret message and encrypt the message and sent to server. Please refer below figure for flow of service in android framework. After performing message sending task service will be destroyed and shut down.



Suppose when our service tried to send message and it’s not delivered due some network issue like low network /zero network, then after some whenever we get network latch broadcast from system then our service will again start to prepare and send the secret message.

6.2 USECASE 1 - Thief Changed the SIM

When our phone is stolen and thief change the sim card, after inserting new sim our algorithms end secret message in background message to server and then its decrypted at server side.



1

- when theif insert new sim then on bootup our serive preapare secret message in backround

2

- This Secret message encryted encyption algorithm and prepare cyher text .

3

- This encyted message sent in background to server via SMS gateways with theif new SIM.

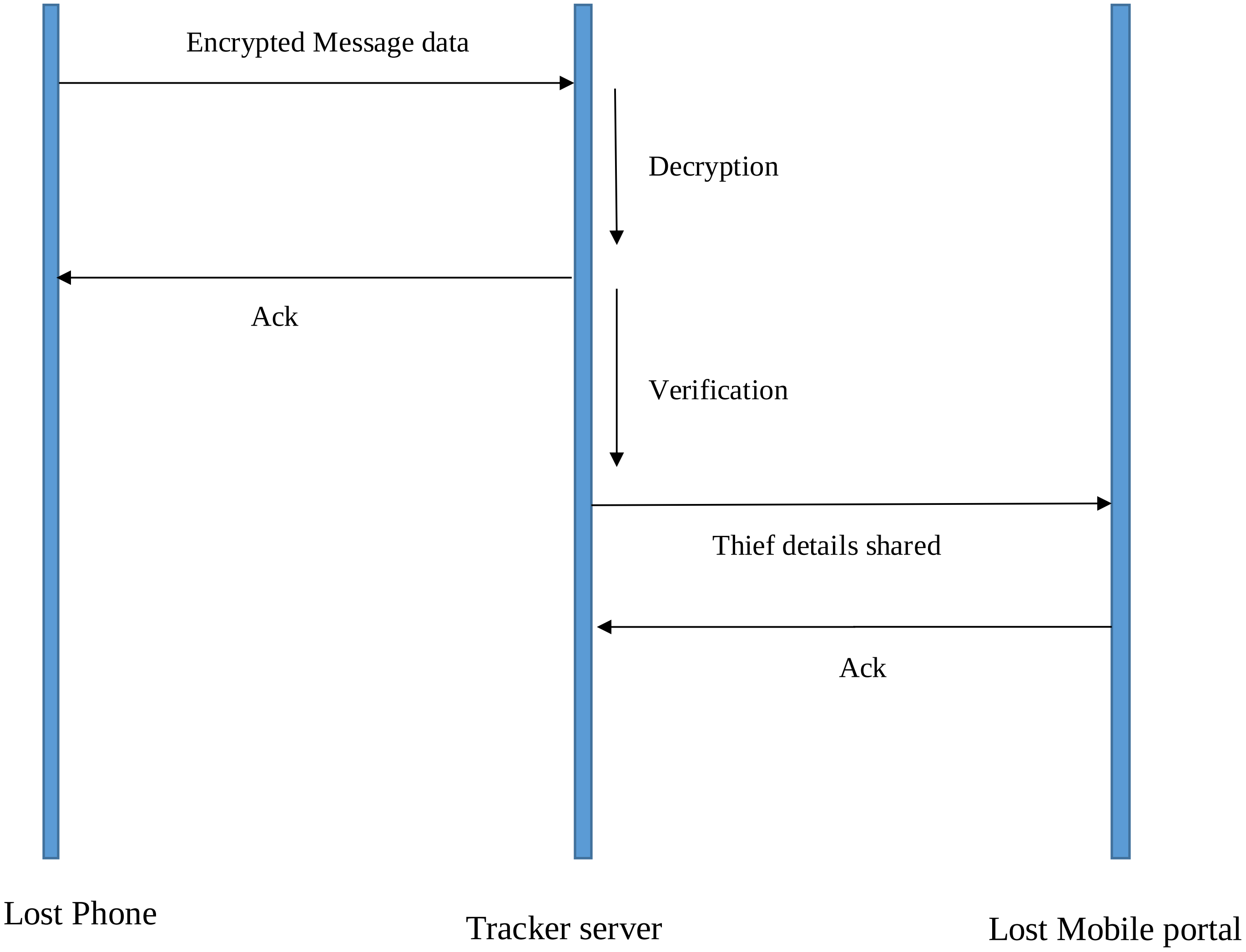
4

- Decrypt the Message with discription key and call verification request.

5

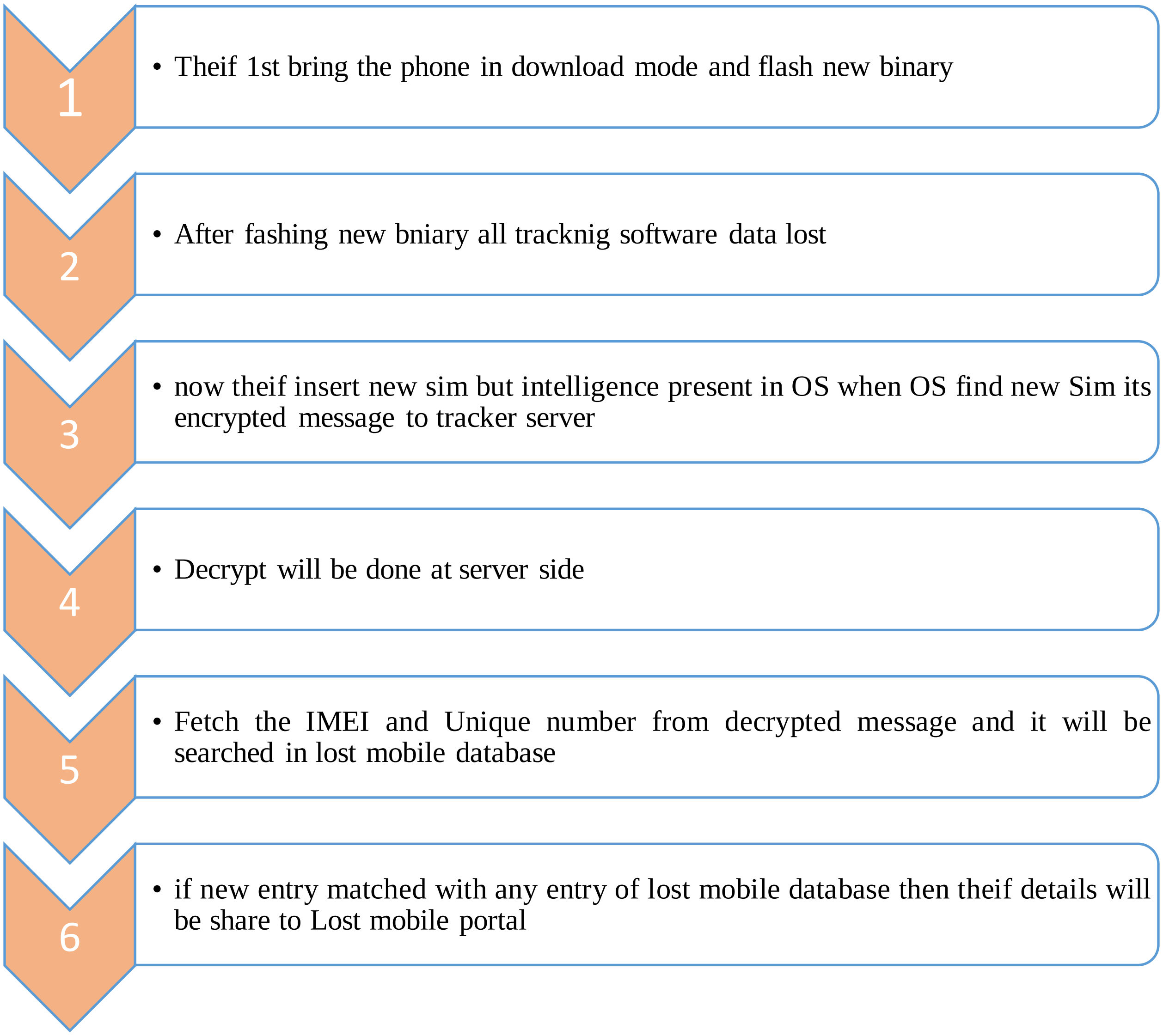
- verification Request check the new entry with Lost mobile Database if same Unique number matched with Database entries then lost mobile detected and update same lost mobile portal.

Naïve thief just changes the sim and insert new sim but in this case almost every tracking software will work like FindMyIPhone of IPhone, FindMyMobile of Samsung but professional 1st wipe out the phone either by flashing new binary or doing master reset. We will cover use case for these in upcoming pages

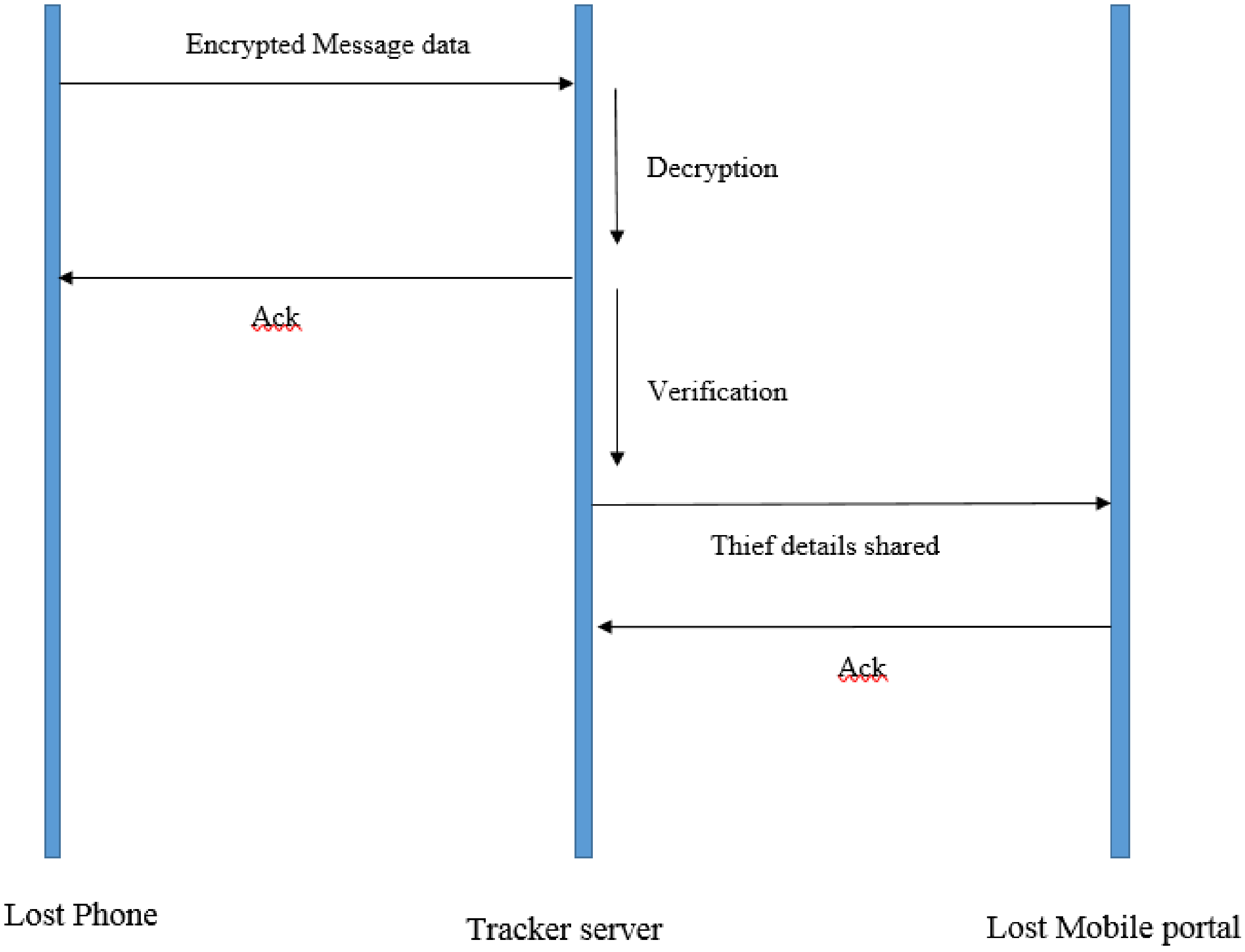


6.3 USECASE 2 - Thief Changed the SIM and Flash New binary

Professional thief is aware of tracking software and their existing loop holes and the use these loopholes to bypass tracking mechanism they bring phone in download mode and the flash new binary. After flashing all tracking install software wiped out and also all stored data will clear from phone but our solution still able to track the phone.

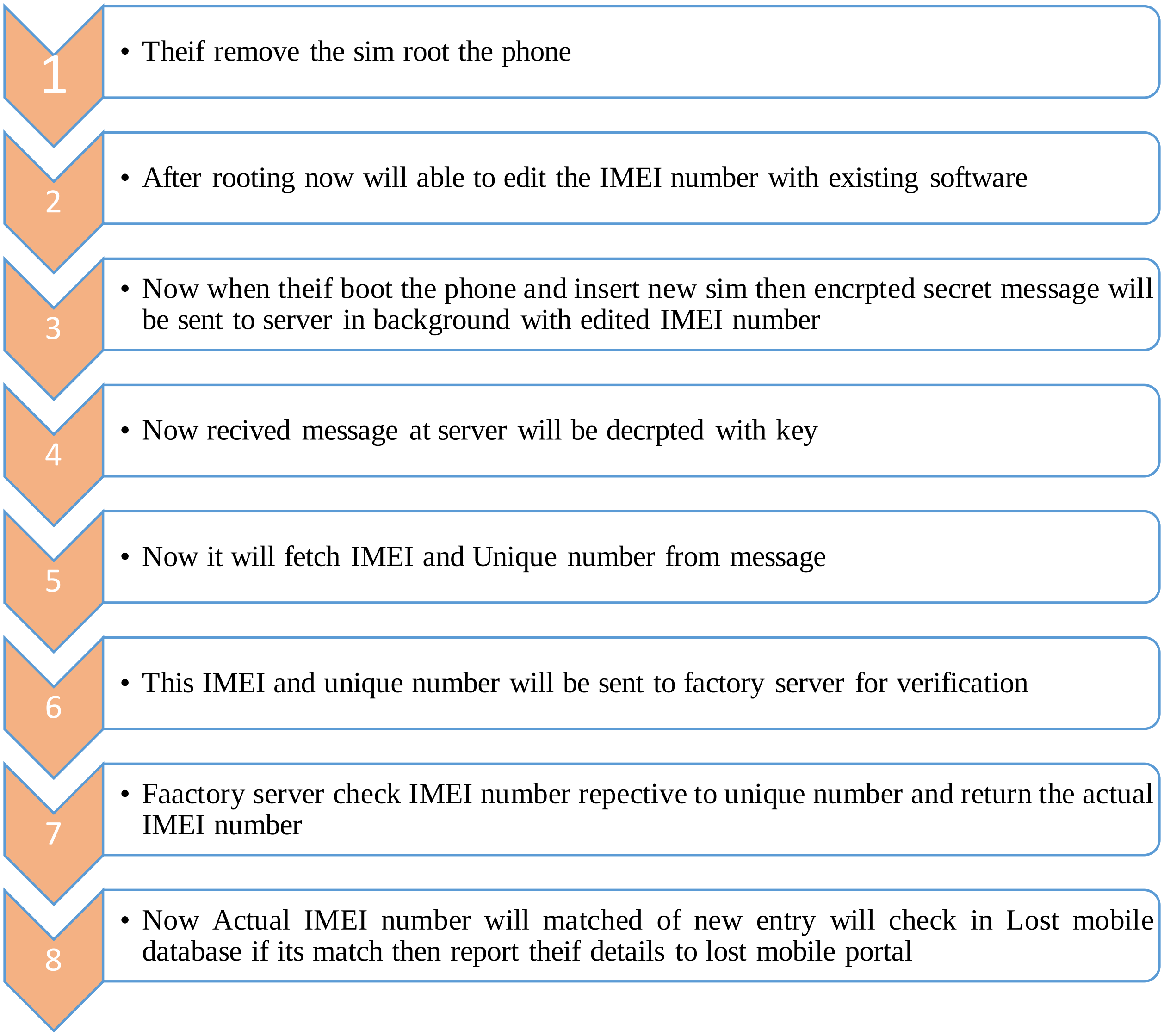


1. Theif 1st bring the phone in download mode and flash new binary
2. After fashing new bniary all tracknig software data lost
3. now theif insert new sim but intelligence present in OS when OS find new Sim its encrypted message to tracker server
4. Decrypt will be done at server side
5. Fetch the IMEI and Unique number from decrypted message and it will be searched in lost mobile database
6. if new entry matched with any entry of lost mobile database then theif details will be share to Lost mobile portal



6.4 USECASE 3 - Thief Changed the SIM and changed the IME

Conceptually IMEI is unique identity of mobile phone and its cannot be edited there are some ways where technical expert thief can root the mobile phone and able to edit the IMEI. Currently all tracking system is based on IMEI, so once it's edited no tracking mechanism will able to detect and track the lost phone. Our proposed solution will still be able to track the phone



1

- Theif remove the sim root the phone

2

- After rooting now will able to edit the IMEI number with existing software

3

- Now when theif boot the phone and insert new sim then encrpted secret message will be sent to server in background with edited IMEI number

4

- Now recived message at server will be decrpted with key

5

- Now it will fetch IMEI and Unique number from message

6

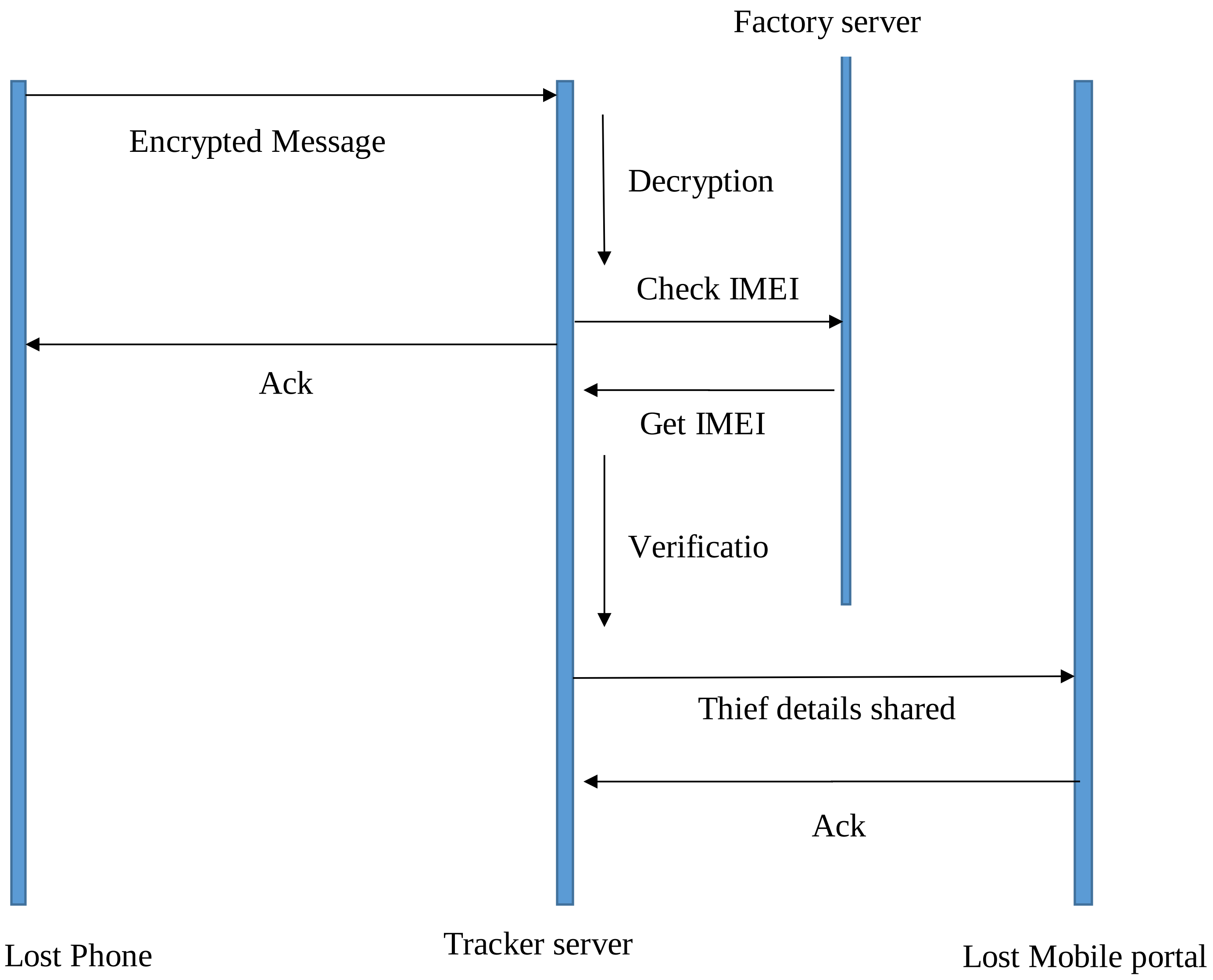
- This IMEI and unique number will be sent to factory server for verification

7

- Faactory server check IMEI number repective to unique number and return the actual IMEI number

8

- Now Actual IMEI number will matched of new entry will check in Lost mobile database if its match then report theif details to lost mobile portal


Factory server
Encrypted Message
Decryption
Check IMEI
Ack
Get IMEI
Verificatio
Thief details shared
Ack
Lost Phone
Tracker server
Lost Mobile portal

REFERENCES

[1] Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).IETF RFC 4186, January 2006. URL https://tools.ietf.org/html/rfc4186.

[2] S. Satya Sri Ambica, P. Padma Priya, Dr.N.Srinivasu, "Sniffer Technology to Detect Lost Mobile ", International Journal ofEngineering Trends & Technology, volume 4,issue4 –April 2013. •

[3] http://www.itpathshala.com/forums/showthread.php?114-Detection-of-lost-mobile-Seminar-reports-amp-ppt-downloads-for-btechstudents&s=f857b08ed3ab10cbccb934bd46895500

[4] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).IETF RFC 4187, January 2006.URL https://tools.ietf.org/html/rfc4187

[5] Cellular Telephone Cloning Final Report.2000, *Economic Crimes Policy Team United States Sentencing Commission* , January 25, 2000

[6] *A. Murphy,2012. The Fraternal Clone Method For Cdma Cell Phones International Journal of Computer Applications Volume 45 No.21, May 2012 [online] Available at : https://www.movzio.com/howto/cell-phone-cloning-guide/*

[7] *Cardina, Donald M., and Anastasios L. Kefalas. "System and method for IMEI detection and alerting." U.S. Patent No.8,126,432. 28 Feb. 2012.*

[8] Gos*den, Paul, et al. "A Uniform Resource Name Namespace for the GSM Association (GSMA) and the International Mobile station Equipment Identity (IMEI)." (2013).*

[9] *iClaried. How to change your iPhone IMEI with ZiPhone (Windows). http://www.iClarified.com/entry/index.php?enid=657*