(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2018 (15.11.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/207123 A1

(51) International Patent Classification:
G08B 13/00 (2006.01) *G06F 21/88* (2013.01)
H04M 1/66 (2006.01)

(21) International Application Number:
PCT/IB2018/053249

(22) International Filing Date:
10 May 2018 (10.05.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201731016467 10 May 2017 (10.05.2017) IN

(72) Inventor; and

(71) Applicant: **AGARWAL, Subham** [IN/IN]; C/o- Everest Carriers, Sevoke Road, Siliguri, District Darjeeling, West Bengal 734001 (IN).

(74) Agent: **KHURANA & KHURANA, ADVOCATES & IP ATTORNEYS**; E-13, UPSIDC, Site-IV, Behind-Grand Venice, Kasna Road, Greater Noida, National Capital Region, Uttar Pradesh 201310 (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

WO 2018/207123 A1

(54) Title: TRACKING AND LOCATING LOST, MISPLACED AND STOLEN MOBILE DEVICES USING ANTI-THEFT TECHNOLOGY

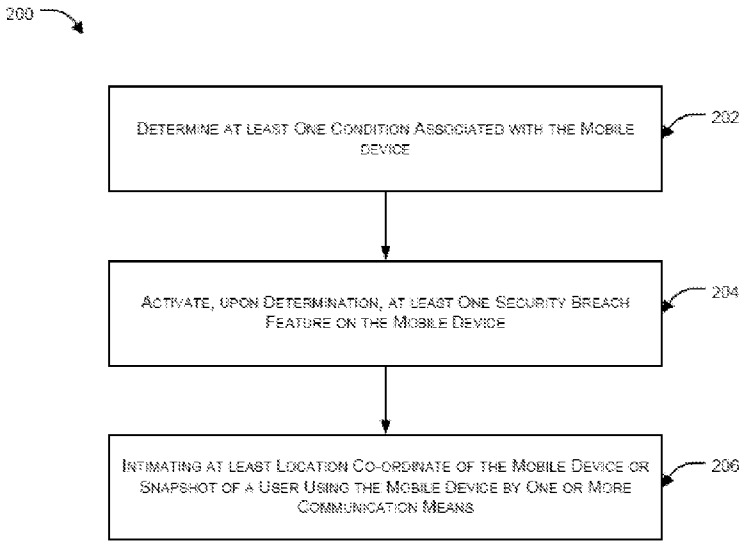

FIG. 2

(57) Abstract: The present disclosure provides a mechanism that protect against any kind of irrelevant or unwanted infringements of the highest order. The mechanism is an anti-theft software application along with non-detachable chip which has inbuilt non-removable SIM card connected with the software application installed internally. The chip can be installed externally installed inside the mobile device which is designed to track cellular devices with extreme accuracy/pin point precision. In an embodiment, the present disclosure guarantees total security by providing snapshots, recording live audio and video, procuring GPS location and the phone number of the new SIM card inserted by sending required SMS to the lost device after which activation lock is turned ON automatically. Activation lock makes it impossible to use or sell the mobile devices, such as but not limited to, iPhone, iPad, iPod touch, Apple Watch, laptops, Android, BlackBerry and Windows smartphones.

[Continued on next page]

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

TRACKING AND LOCATING LOST, MISPLACED AND STOLEN MOBILE DEVICES USING ANTI-THEFT TECHNOLOGY

TECHNICAL FIELD

The present disclosures relate to the field of mobile device tracking. More particularly, the present disclosure relates to tracking lost, misplaced and stolen mobile devices using anti-theft technologies.

BACKGROUND

Background description includes information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

Presently, mobile telephones and devices, particularly those based upon the global system for mobile communications (GSM) standard, contain an electronic module commonly known as a subscriber identity module (SIM). The SIM uniquely identifies a subscriber and is used to store data to be used by the mobile device, and may also contain appropriate authentication functions. In addition to the SIM, the mobile device is identified using an equipment identifier known as an internal mobile equipment identity (IMEI).

In general, the mobile phone tracking is the ascertaining of the position or location of a mobile phone, whether stationary or moving. Localization may occur either via multilateration (MLAT) of radio signals between (several) cell towers of the network and the phone, or simply via GPS. To locate a mobile phone using multilateration of radio signals, it must emit at least the roaming signal to contact the next nearby antenna tower, but the process does not require an active call. The global system for mobile communications (GSM) is based on the phone's signal strength to nearby antenna masts. Mobile positioning may include location-based services that disclose the actual coordinates of a mobile phone, which is a technology used by telecommunication companies to approximate the location of a mobile phone, and thereby also its user.

The technology of locating is based on measuring power levels and antenna patterns and uses the concept that a powered mobile phone always communicates

wirelessly with one of the closest base stations, so knowledge of the location of the base station implies the cell phone is nearby. Advanced systems determine the sector in which the mobile phone is located and roughly estimate also the distance to the base station. Further approximation can be done by interpolating signals between adjacent antenna towers. Qualified services may achieve a precision of down to 50 meters in urban areas where mobile traffic and density of antenna towers (base stations) is sufficiently high. Rural and desolate areas may see miles between base stations and therefore determine locations less precisely. GSM localization uses multilateration to determine the location of GSM mobile phones, or dedicated trackers, usually with the intent to locate the user.

Presently, location of a mobile phone can be determined in a number of ways. Few of the ways includes but are not limited to Network-based location determination as discussed in US 5519760, Handset-based location determination, SIM-based location determination, Wi-Fi location determination, Hybrid location determination.

In current GSM based systems, for example, subscribers are typically identified using data contained in the SIM, rather than the IMEI. The SIM is typically removable and may be utilized in different mobile devices. Conventional GSM based systems allow a user to insert their SIM card into any mobile device. Malicious individuals have recognized that a stolen mobile device may be used with a different, legally obtained SIM card. A typical scenario is where an inexpensive mobile device is purchased to obtain a legitimate SIM card. The SIM card is then removed from the legitimate device and inserted into a stolen device. The stolen device is typically much more elaborate and expensive than the legitimate device. Since the network will identify the device using the legitimate SIM, rather than the IMEI of the stolen device, the user may be able to operate the stolen mobile device with impunity.

When no sim is inserted the device gets connected to WiFi service providers like Jio net, true WiFi, etc., which helps us to stay connected on the road without a sim card and is installed everywhere in the district after which all the security measures can be triggered.

When the battery from the device is removed or device is switched off,we can connect to the non-detachable chip installed externally inside the device which

controls the device functionalities like triggering power off-power on, connects to true wifi , etc . The chip also has non-removable 4G/5G sim installed in it to take security action with the device using SMS system or app and access data like GPS location, power on-power off the device, turn internet on/off, and other desirable actions.

In case the chip is removed by any means, mobile app installed inside the software will help retrieve the device.

Installment of the chip is not limited to device but also to products like keys, document carrier, wallet, vaults and other valuable products.

The externally installed non-detachable 4g simcard chip connected with the enkrypto app installed internally also provides onboard diagnostics (OBD) of the mobile device in which it is installed.

Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

With the advancement of technology, various techniques have been devised to track / detect lost, misplaced and stolen mobile devices. For example, one technique is a Chipolo device which enables you to find your belongings by sound see them on a map or use community search to recover lost items. When your Chipolo tracking device is within the 200-feet Bluetooth range, it will play a loud tune until you find it. When you need to locate your phone, just double press any of your Chipolo tracking devices to make your lost phone ring – even if it's on silent. However, the Chipolo requires a continuous Bluetooth connectivity. Another technique is TrackR bravo which is coin-sized Bluetooth tracker that can attach to anything. Using Bluetooth low energy (BLE) which is like Bluetooth used commonly except that it consumes very low power. An application is provided by the device manufacturer i.e., TrackR. The handset can sense the TrackR up to a distance of 10Metres which is standard for BLE.

Another technique is McAfee Mobile Security, which is similar to Android Device Manager, made for android devices. The McAfee Mobile Security application takes PHOTO (Selfie) on typing the PIN incorrectly 3 times. Similarly, Android Device Manager is an ANTI-THEFT application for android which helps to locate the device using the internet services of the device. After syncing Google accounts, simply type "find my phone" in google.com. Also, there

are many more similar types of patent and non-patent literature that discusses new and advance techniques for tracking lost, misplaced and stolen mobile devices.

However, the existing techniques like Cerberus, Mobile tracker anti-theft app, Where's My Droid, find iPhone, Lost android, Prey, and the like anti-theft applications in the domain/are of technology has certain limitations as thief can easily bypass the security by a force shutdown the phone and then formatting the phone. Also, the SIM card form the phone can be removed after which most of the existing anti-theft applications stops reading the data and then the thief can format the phone. Furthermore, the thief after hacking the phones can uninstall the existing anti-theft applications after which they become completely incompatible. Thus, the existing anti-theft applications are not legitimate.

Furthermore, the existing techniques of patent application filed previously such as CN101764887B and other applications in the domain are not foolproof solutions for tracking lost, misplaced and stolen mobile devices but have achieved considerable success by disabling a stolen device so that it no longer functions within the network. However, there is an increasing desire and demand to not only disables stolen devices, but to track such devices so that they may be recovered by the authorities and the perpetrators brought to justice. Further, there still exists a scope of an improvement in the existing techniques for tracking lost, misplaced and stolen to not only efficiently mitigate the demand and desire but also to economically solve the issues of tracking in terms of time and cost required for the same.

Hence there is a need in the art for a system and method that can efficiently and economically track lost, misplaced and stolen mobile devices.

SUMMARY

The present disclosures relate to the field of mobile device tracking. More particularly, the present disclosure relates to tracking lost, misplaced and stolen mobile devices using anti-theft technologies.

Accordingly, an aspect of the present disclosure relates to a mobile device with anti-theft functionality.

In an aspect, the mobile device can include one or more processors. In another aspect, the mobile device can include a condition determining engine to control

the one or more processors to determine at least one condition associated with said mobile device, said at least one condition being selected from whether the mobile device is lost, whether the mobile device is misplaced, whether the mobile device is stolen, or whether the mobile device is tampered. In another aspect, the mobile device can include a security breach engine to control the one or more processors to activate, upon detection of said at least one condition, at least one security breach feature pre-configured at a hardware level or at an operating system (OS) level on the mobile device to operate as said anti-theft functionality.

In an aspect, at least one condition can be determined based at least on any or combination of an attempt to insert a new SIM card in the mobile device, insertion of a new SIM card in the mobile device, removal of an existing SIM card from the mobile device, failure of multiple login attempts, and generation of different noises around the mobile device.

In an aspect, at least one condition can include a corresponding security breach feature determined based on pre-defined rules or criteria preset by an authenticated user.

In an aspect, at least one security breach feature can be activated automatically.

In an aspect, at least one security breach feature can be adapted to activate one or more functionalities and/or sensors of said mobile device to retrieve information from nearby proximity of the mobile device and/or locality of the mobile device.

In an aspect, mobile device can include a transceiver to control the one or more processors to transmit, upon activation of said at least one security breach feature, at least a location co-ordinate of the mobile device or at least a snapshot of a user using the mobile device in real-time or at a fixed interval of time.

In an aspect, at least one security breach feature can be adapted to activate, upon activation of said at least one security breach feature, one or more authentication mechanisms to forbid at least one of formatting, power off/forced shutdown, notification access, uninstallation of installed software applications, rebooting, trigger factory reset of the mobile device.

In an aspect, at least one security breach feature can be adapted to activate, upon activation of said at least one security breach feature, one or more authentication mechanisms to forbid at least one of formatting, power off/forced shutdown,

notification access, uninstallation of installed software applications, rebooting, trigger factory reset of the mobile device.

In an aspect, mobile device can include a transceiver to control the one or more processors to receive, upon activation of said at least one security breach feature, one or more messages from remote location to activate one or more in-built functionality of said mobile device, said in-built is selected form a Bluetooth, a Wi-Fi, or a data connectivity.

In an aspect, mobile device can include an alarming device to control the one or more processors to play, upon activation of said at least one security breach feature and upon detection of an authenticated user in nearby proximity, a unique sound pre-defined for said mobile device.

In an aspect, mobile device can include a fake shutdown functionality to control the one or more processors to enter, upon activation of said at least one security breach feature and upon an attempt to force shutdown, into a simulated power OFF mode (a.k.a fake power off) in which the mobile device screen/modem is OFF but a chipset said mobile device is ON with limited capabilities.

In an aspect, the mobile device can include an alarming non-detachable chip installed externally to the mobile device and communicably connected with one or more applications installed internally inside the mobile device adapted to generate on-board diagnostics (OBD) data associated with the mobile device to activate said at least one security breach feature.

In an aspect, said mobile device can include a non-detachable chip having a transceiver. The chip can be externally connected to the mobile device and is configured to connect with one or more applications installed inside said mobile device. In another aspect, the one or more applications installed in said mobile device can generate at least on-board diagnostics (OBD) data associated with the mobile device. Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

Various objects, features, aspects and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are included to provide a further understanding of the present disclosure, and are incorporated in and constitute a part of this specification. The drawings illustrate exemplary embodiments of the present disclosure and, together with the description, serve to explain the principles of the present disclosure.

The diagrams are for illustration only, which thus is not a limitation of the present disclosure, and wherein:

FIGs. 1A-B illustrates exemplary functional modules of the proposed system, in accordance with an exemplary embodiment of the present disclosure.

FIG. 2 illustrates an exemplary method of working of the proposed system, in accordance with an exemplary embodiment of the present disclosure.

FIG. 3 illustrates an exemplary working of the proposed system, in accordance with an embodiment of the present disclosure.

FIG. 4A-4B illustrates exemplary options presented by a mobile device when configured with the proposed invention, in accordance with an embodiment of the present disclosure.

FIG. 5 illustrates an exemplary working of the proposed system, in accordance with an exemplary embodiment of the present disclosure.

DETAILED DESCRIPTION

The following is a detailed description of embodiments of the disclosure depicted in the accompanying drawings. The embodiments are in such detail as to clearly communicate the disclosure. However, the amount of detail offered is not intended to limit the anticipated variations of embodiments; on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present disclosure as defined by the appended claims.

Various terms as used herein are shown below. To the extent a term used in a claim is not defined below, it should be given the broadest definition persons in the pertinent art have given that term as reflected in printed publications and issued patents at the time of filing.

The present disclosures relate to the field of mobile device tracking. More particularly, the present disclosure relates to tracking lost, misplaced and stolen mobile devices using anti-theft technologies.

Existing techniques for tracking lost, misplaced and stolen mobile devices have achieved considerable success by disabling a stolen device so that it no longer functions within the network. However, there is an increasing desire and demand to not only disables stolen devices, but to track such devices so that they may be recovered by the authorities and the perpetrators brought to justice. Further, there still exists a scope of an improvement in the existing techniques for tracking lost, misplaced and stolen to not only efficiently mitigate the demand and desire but also to economically solve the issues of tracking in terms of time and cost required for the same.

Hence there is a need in the art for a system and method that can efficiently and economically track lost, misplaced and stolen mobile devices.

Accordingly, in an embodiment the present disclosure provides a mechanism that protect against any kind of irrelevant or unwanted infringements of the highest order. The mechanism is an anti-theft software application designed to track cellular devices with extreme accuracy/pin point precision.

In an embodiment, the present disclosure ensures that the user of the mobile device remains at utmost ease, when their mobile devices are lost/misplaced/stolen.

In an embodiment, the present disclosure guarantees total security by providing snapshots, recording live audio and video, procuring GPS location and the phone number of the new SIM card inserted by sending required SMS to the lost device after which activation lock is turned ON automatically. Activation lock makes it impossible to use or sell the mobile devices, such as but not limited to, iPhone, iPad, iPod touch, Apple Watch, Samsung gear, laptops, Android, BlackBerry, Windows smartphones, electronic wearable and accessories.

In an embodiment, the present disclosure can be implemented as a mobile based application therefore it can be classified under the IT and communication sector.

In an embodiment, the concept and nature of the present disclosure is based on an anti-theft tracking mobile application that provides complete and enhanced state -of -the- act tracking technology which is adapted to procure a lost device.

In an embodiment, the anti-theft mechanism of the present disclosure is a SIM removal protection system. The present disclosure has an enhanced security feature that uses the unique IMSI NO of the new SIM card inserted to generate the 10-digit phone number which is sent to optional number as an SMS.

In an embodiment, the anti-theft mechanism of the present disclosure has a security breach feature which turns on the video, take photo, frequent locations of the lost (options can be edited) cellular device which is shared with the optional number or user account when the SIM is removed without the user's permission. The security breached feature is turned ON until the new SIM is inserted after the user can control the lost cellular device with the new SIM card number which is sent to optional number as an SMS or uploaded to the user account.

In an embodiment, when no SIM card is inserted, the device can be connected to Wi-Fi service providers like Jio net, true Wi-Fi, etc. which helps us to stay connected on the road without a SIM card and is installed everywhere in the district after which all the security measures can be triggered.

In an embodiment, when the battery from the device is removed or device is switched off, the device can connect to the non-detachable chip installed externally inside the device which controls the device functionalities like triggering power off-power on, connects to true Wi-Fi, etc. The chip also has unremovable SIM installed in it to take security action with the device using SMS system or app and access data like GPS location, power on-power off, turn internet on/off, etc. In case the chip is removed by any means, mobile app installed inside the software will help retrieve the device. Installment of the chip is not limited to device but also to products like keys, document carrier, wallet, vaults etc. The externally installed non-detachable 4g SIM card chip connected with the enkrypto app installed internally also provides onboard diagnostics (OBD) of the mobile device in which it is installed. Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

In an embodiment, the anti-theft mechanism of the present disclosure works with SMS system. The present disclosure does not require Bluetooth or internet connectivity for tracking. Tracking is made possible by using, IMEI, MLAT towers, GSM towers, internet service providers like Jio Net, True Wi-Fi, etc.,

GPS system or location services of the device calculate fields like MOBILE COUNTRY CODE (MCC), MOBILE NETWORK CODE (MNC), LOCATION AREA CODE (LAC) and CELL ID simultaneously to determine precise location which sends the coordinate to the optional number as an SMS which can be opened with Google maps, and various other methods.

In an embodiment, the anti-theft mechanism of the present disclosure works with a non-detachable chip which includes a non-removable SIM with internet data, which can be installed in the device which has access to security functions and access to keys like power ON/OFF the device remotely in case the SIM card is removed.

In an embodiment, the anti-theft mechanism of the present disclosure works even if the battery from the device is removed, SIM card is removed or the device is powered off as the installed chip containing 4G/5G/Verizon/AT&T etc. SIM card can be tracked and will perform required security function.

In an embodiment, the anti-theft mechanism of the present disclosure the device gets connected to the on road Wi-Fi service provided by internet service providers like Jio net, True Wi-Fi, etc. to access the device remotely incase the SIM card is removed until new SIM card is installed.

In an embodiment, the anti-theft mechanism of the present disclosure provides an area to switch on Bluetooth/Wi-Fi/4g/etc. of the lost cellular device via sending sms to the lost cellular device or through user account for more accuracy and precision location when near to the device.

In an embodiment, the anti-theft mechanism of the present disclosure is a face recognition system. Since Google maps are accurate to 50m it is necessary to obtain the images of the person in possession of the lost cellular device. Highly advanced feature of present disclosure detects a face, takes snapshots (selfie), play loud alarm when near to the device, etc. and send it to optional number as an SMS and even uploads in the user account. Also with a highly advanced connectivity (Bluetooth/GSM towers/Wi-Fi/etc.) with the lost cellular device maps accuracy of the location can be made more precise. (Approx. 5-15m). In an exemplary embodiment, an alert is preferably unique to the device, such that the device can be acoustically identified. For example, the user of the phone may have recorded a message to be played in the event that the alert signal is transmitted to it. Such a

message may be audible, such as, “Hey! This is Alex’s phone. I'm lost. Please take me to me owner!” As well as a deterrent to being kept by an unauthorized owner, people known to the owner who are in hearing distance will be able to identify the phone and perhaps retrieve it and return it to the owner.

In an embodiment, the anti-theft mechanism of the present disclosure is a is based on an anti-theft tracking mobile application that provides complete and enhanced state -of -the- act tracking technology which is adapted to procure a lost device. For example- A map view in the application or system to track and locate family friends and relatives by typing in their phone number or email address and make video call , phone calls, etc. and chat with them by sharing photos, docs. And texts.

In an embodiment, the anti-theft mechanism of the present disclosure includes password security to power off/factory reset/reboot/uninstall. The major drawback with existing application is that anybody can power off/factory reset/reboot the cellular device after which it is not possible to track the cellular device. The present disclosure enables user to activate password in the form of finger print, pattern or numbers before switching off /factory reset/reboot/uninstall the device. So it will not be possible to switch off/factories reset / reboot/uninstall a cellular device until and unless you provide your finger print, pattern or numbers, etc.

In an embodiment, the anti-theft mechanism of the present disclosure is allocated with a cloud space. The cloud space will also be provided to backup data automatically when connected to internet services. Default time will be (12:00am - 4:00am).So the important data can be backup remotely in case of emergency quickly.

In an embodiment, the anti-theft mechanism of the present disclosure has a travel/crowd mode. The travel/crowd mode directly turns on crowd mode with help of SIRI/voice over /notification bar/control centre/menu bar. Also when events are connected to calendar, mechanism sends you a push notification 5 mins before the event (can be edited) to turn on the crowd mode. Helps to protect device in crowded areas by making sound in case the device is swiftly taken out from the pocket.

In an embodiment, the anti-theft mechanism of the present disclosure provides the user end to end ENCRYPTION of the user's data along with a TWO FACTOR VERIFICATION and AUTHORISTATION.

In an embodiment, the anti-theft mechanism of the present disclosure provides a mechanism to lock/unlock other applications installed in the cellular device through finger print, password, pattern, etc.

In an embodiment, the anti-theft mechanism of the present disclosure can directly file an FIR or register a complaint to authorities. The present disclosure provides a platform to file an FIR directly from the application with the help of internet if battery dies or when it is not possible to track the cellular device due to any unavoidable circumstances.

In an embodiment, the anti-theft mechanism of the present disclosure provides an option to choose between different INSURANCE providers and also provides an area where the user can look up on the reviews of the existing insurance service providers companies. In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism where you can connect with your relatives, friends and family and can see their existing location, share your location, track family/friends/relatives, and share texts and documents, etc. In an exemplary embodiment, the anti-theft mechanism of the present disclosure has a mechanism where mobile's location can save in a user account in case if the mobile is switch-off forcefully.

In an embodiment, the system can assist to save back up files remotely. In an exemplary embodiment, back up files can save to DROPBOX, GOOGLE DRIVE, application or ENKRYPTO CLOUD. In another exemplary embodiment, the backup files can save into a new device.

In an exemplary embodiment, the system can connect with another mobile application such as related with banking application or payment app to connect with wallets, keys, vault, valuables, etc.

In an exemplary embodiment, the system can save location history after every 15 (sec) on the device, so user can retrieve it from the web dashboard. In another exemplary embodiment, the system can track each second location after the lost mode is turned on, which automatically turns on GPS and lock it with a password.

In an exemplary embodiment, the anti-theft mechanism of the present disclosure has a mechanism where the device can perform fake shut down. For example- The lock screen can perform a fake shutdown by holding power off button; phone cannot be usable for 30 sec.

In an exemplary embodiment, the anti-theft mechanism of the present disclosure has a mechanism where the device can block power menu. For example- if the user activate block power menu then the power key cannot work so thief cannot acres the power key without password.

In an exemplary embodiment, the anti-theft mechanism of the present disclosure has a mechanism where the device can block status bar. For example- If user activate block status bar then the status cannot expand in the lock screen.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to delete or clear the application or confidential documents. In an exemplary embodiment, chat maybe deleted with a time period set by the user if wanted or otherwise the chat may be deleted within default time limit such as 24 hours.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism which can survive hard factory reset which saves the application in root folder and asks security permissions to access it.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to save the frequent location of the device automatically which can be accessed from the app data.

In an embodiment, the anti-theft mechanism of the present disclosure user can HIDE the application and can access it by typing a phone number and asks security permission before accessing the application.

In an embodiment, the anti-theft mechanism of the present disclosure asks security permission to connect the device with the computer or debugging the device.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to be protected from 3rd party Software Development Kit (SDK) like android debug bridge, etc.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism asks security permission while making any changes in the root folder of the device.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to make the device faster by providing options clean unwanted data from the device and clear cache, etc.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to provide one simple one touch technique to root the device without making any major changes in the STOCK ROM or slowing down the processor.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to show a map view in the application or system to track and locate family friends and relatives by typing in their phone number or email address and make video call , phone calls, etc. and chat with them by sharing photos, docs. And texts.

In an embodiment, the anti-theft mechanism of the present disclosure the application can be downloaded in .apk, .doc, .ipa, .dmg, etc. format in variable devices.

In an embodiment, the anti-theft mechanism of the present disclosures has a mechanism to look other application using face ID, fingerprint and other security measures.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism which saves devices location while user makes an attempt to power off the device

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to create rules by creating event, adding conditions and then select actions based on the conditions to personalize the application.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to customize auto task, to take actions automatically in case any of the desired security measure is breached.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to save backup of the different devices in the enkrypto cloud and re install backup, merge back up, etc. into a new device.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to ask security permission before uninstalling the application from the device.

In an embodiment, the anti-theft mechanism of the present disclosure has a mechanism to capture photo or image or video automatically. In an exemplary embodiment, the anti-theft mechanism can capture image or picture when the user dismisses the application message. In another exemplary embodiment, once photo uploaded to the cloud, email and sms, the system or application can disable all the functions keys of the device. In another exemplary embodiment, the application or system can capture image when user tries to opens a message after lost mode is turned on. The application can ask password before opening message. In another exemplary embodiment, the application can set the number of consecutive failed unlock attempts after which the application can capture image. In another exemplary embodiment, the application can capture image after user unlocks the device after lost mode is turned on. In another exemplary embodiment, the application can capture image when SIM is removed from the device. In another exemplary embodiment, when the user enters wrong password after pre-defined or pre-determined attempts then the system can click photo, saves current GPS location.

In an embodiment, the anti-theft mechanism of the present disclosure has inbuilt Nano-technology chip stitched secretly with products like wallets, keys, vault, valuables, etc. connected with the application to help track back their valuables if lost , misplaced or stolen.

In an embodiment, the anti-theft mechanism of the present disclosure includes an attractive user interface in the market along with browser extension for the easy and user friendly interface for the people.

FIG. 1A illustrates exemplary functional modules of the proposed system, in accordance with an exemplary embodiment of the present disclosure. In an embodiment, the proposed system, the anti-theft mechanism 100 includes a determination module 102, an activation module 104, and an intimation module 106.

In an embodiment, the determination module 102 is configured to determine at least one condition associated with the mobile device. The condition associated

with the mobile device, can include but is not limited to, lost, misplaced and stolen mobile device.

In an exemplary embodiment, the condition associated with the mobile device can be ascertained based on any of the existing mechanisms that may include but are not limited to, insertions of new SIM card in the mobile device, or removal of the existing SIM card from the mobile device, multiple login attempts failure, various different noises around the mobile device, and the like.

In an embodiment, the activation module 104 is configured to upon determining the condition stated above, activate at least one security breach feature on the mobile device.

In an exemplary embodiment, the security breach feature can be pre-configure or pre-defined feature of the mobile device. In another exemplary embodiment, the security breach feature can be a software application which get triggered automatically or manually based upon determining the condition stated above.

In an exemplary embodiment, the security breach feature can activate any of the existing sensors such as accelerometer sensors, GPS, audio sensors to listen the nearby proximity of the mobile device and locality of the mobile device when the device is lost, misplaced and stolen.

In an embodiment, the intimation module 106, upon activating the security breach feature, is configured to intimate at least location co-ordinate of the mobile device or snapshot of a user using the mobile device by one or more communication means.

In an exemplary embodiment, the location co-ordinate and the snapshot can be intimated to the owner by any of the existing communication means. In an example, the communication means can include but are not limited to, SMS on the alternate number pre-stored/pre-configured, e-mail, location co-ordinates of the mobile device which can be opened on the Google map like application easily, and the like. In an exemplary embodiment, if the user mobile phone stolen in the market and theft tries to change SIM then, the mobile device captures video/photo and transmits GPS location to an registered e-mail address or to a registered phone number or to an optional number pre-stored along with SIM information.

In an embodiment, the anti-theft mechanism enables to provide finger print, password or pattern before format / wipe out the existing data in the mobile

device once the aforementioned condition is determined. Such formatting/wiping of the data can be user pre-defined or can be activated remotely by the owner at any point of time. In an embodiment, the device can include a location module, such as a GPS, D-GPS or an A-GPS module, or some other module capable of performing location determination or assisting with it. The locating module may be a component or module separate from the memory. There may be one, two or more locating modules, each operating on a different principle or one acting as a backup for another. In an embodiment, the anti-theft mechanism enables power alarm, play sound, send text messages to friends or relatives, once the aforementioned condition is determined.

FIG. 1B illustrates exemplary functional modules of the proposed mobile device, in accordance with an exemplary embodiment of the present disclosure. In one embodiment, the proposed mobile device 150 may include at least one processor 152, an input/output (I/O) interface 154, and a memory 156. The at least one processor 152 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the at least one processor 152 is configured to fetch and execute computer-readable instructions stored in the memory 156.The I/O interface 154 may include a variety of software and hardware interfaces, for example, a web interface, a graphical user interface, and the like. The I/O interface 154 may allow the proposed mobile device 150 to interact with a user directly. Further, the I/O interface 154 may enable the proposed mobile device 150 to communicate with other computing devices, such as web servers and external data servers (not shown). The I/O interface 154 can facilitate multiple communications within a wide variety of networks and protocol types, including wired networks, for example, LAN, cable, etc., and wireless networks, such as WLAN, cellular, or satellite. The I/O interface 154 may include one or more ports for connecting a number of devices to one another or to another server.

The memory 156 may include any computer-readable medium known in the art including, for example, volatile memory, such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile

memory, such as read only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes. The memory 156 may include modules, routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. In one implementation, the memory 206 may include a transceiver 158, a condition determining engine 160, a security breach engine 162, and an alarming device 164.

In an aspect, the transceiver 158 can control the one or more processors to transmit, upon activation of said at least one security breach feature, at least a location co-ordinate of the mobile device or at least a snapshot of a user using the mobile device in real-time or at a fixed interval of time. In another aspect, the transceiver 158 can control the one or more processors to receive, upon activation of said at least one security breach feature, one or more messages from remote location to activate one or more in-built functionality of said mobile device, said in-built is selected form a Bluetooth, a Wi-Fi, or a data connectivity.

In an aspect, the condition determining engine 160 can control the one or more processors to determine at least one condition associated with said mobile device, said at least one condition being selected from whether the mobile device is lost, whether the mobile device is misplaced, whether the mobile device is stolen, or whether the mobile device is tampered.

In an aspect, the security breach engine 162 can control the one or more processors to activate, upon detection of said at least one condition, at least one security breach feature on the mobile device to operate as said anti-theft functionality, wherein said at least one security breach feature is a pre-configured hardware level feature or an operating system (OS) level feature of the mobile device.

In an aspect, the alarming device 164 can be adapted to generate, upon activation of said at least one security breach feature and upon detection of an authenticated user in a nearby proximity of said mobile device, a unique alarming sound, said unique alarming sound is pre-defined by the authenticated user for said mobile device. In an exemplary embodiment, user forgot mobile phone in the bus while travelling and theft or unauthorized user try to access the mobile phone. The user or authorized user remember the mobile device and visit bus as soon as the

authorized user reach nearby or proximate location then it starts alarm or notify the authorized user by audible message.

In an exemplary embodiment, all the data generated/transmitted/ received by any of the modules residing in mobile device 150 may be stored in data 166. The data 166 may be a storage device.

FIG. 2 illustrates an exemplary method of working of the proposed system, in accordance with an exemplary embodiment of the present disclosure. The method 200 may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, functions, etc., that perform particular functions or implement particular abstract data types. The method 200 may also be practiced in a distributed computing environment where functions are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, computer executable instructions may be located in both local and remote computer storage media, including memory storage devices.

The order in which the method 200 is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method 200 or alternate methods. Additionally, individual blocks may be deleted from the method 200 without departing from the spirit and scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof. However, for ease of explanation, in the embodiments described below, the method 200 may be considered to be implemented in the above described anti-theft mechanism 100.

At block 202, the anti-theft mechanism determines at least one condition associated with the mobile device. In an exemplary embodiment, the condition associated with the mobile device can be ascertained based on any of the existing mechanisms that may include but are not limited to, insertions of new SIM card in the mobile device, or removal of the existing SIM card from the mobile device, multiple login attempts failure, various different noises around the mobile device, and the like.

At block 204, the anti-theft mechanism activates, upon determination, at least one security breach feature on the mobile device. In an exemplary embodiment, the security breach feature can be pre-configured or pre-defined feature of the mobile device. In another exemplary embodiment, the security breach feature can be a software application which get triggered automatically or manually based upon determining the condition stated above.

In an exemplary embodiment, the security breach feature can activate any of the existing sensors such as accelerometer sensors, GPS, audio sensors to listen the nearby proximity of the mobile device and locality of the mobile device when the device is lost, misplaced and stolen.

At block 206, the anti-theft mechanism intimates at least location co-ordinate of the mobile device or snapshot of a user using the mobile device by one or more communication means.

In an exemplary embodiment, the location co-ordinate and the snapshot can be intimated to the owner by any of the existing communication means. In an example, the communication means can include but are not limited to, SMS on the alternate number pre-stored/pre-configured, e-mail, location co-ordinates of the mobile device which can be opened on the Google map like application easily, and the like.

In an embodiment, the anti-theft mechanism enables to provide finger print, password or pattern before format / wipe out the existing data in the mobile device once the aforementioned condition is determined. Such formatting/wiping of the data can be user pre-defined or can be activated remotely by the owner at any point of time.

In an embodiment, the anti-theft mechanism enables power alarm, play sound, send text messages to friends or relatives, once the aforementioned condition is determined.

FIG. 3 illustrates an exemplary working 300 of the proposed system, in accordance with an embodiment of the present disclosure. In an embodiment, as shown in FIG. 3, the mobile device 302 can be installed with an anti-theft mechanism application. The anti-theft mechanism application determines at least one condition say SIM change detection 306 associated with the mobile device. The condition associated with the mobile device, can include but is not limited to,

lost, misplaced and stolen mobile device. Upon such detection, the mobile device can automatically enable camera feature of the phone to take snapshot 308 of the user handling the phone or transmit the current location 310 associated with the phone. The snapshot of the user and/or the location of the phone can be transmitted by any of the existing communication means which may be pre-configured with the phone. In an example, the communication means may include but are not limited to by sending email 312a and/or by sending the messages 312b.

In an exemplary embodiment, upon such detection of the condition, the authenticated user (owner) is notified of the same by any of the existing communication means (say message 304) basis of which the owner can take corrective measure by remotely wiping out the data 314 associated with the phone.

FIGs. 4A-4B illustrates exemplary options presented by a mobile device when configured with the proposed invention, in accordance with an embodiment of the present disclosure.

In an embodiment, as shown in FIG 4A. the mobile device when configured with the proposed invention automatically is enabled with various options 400, that may be selected from but are not limited to, enable/disable data/WIFI/roaming/ Bluetooth, record audio, when find option is used by a registered a device location is shown on Google maps, pass code to power off/notification bar/uninstall/force shutdown /reboot /factory reset, get call/SMS log, SIM information can be transmitted, detect through IMEI/MLAT tower/Bluetooth//JIONET tower/WIFI/SMS/GPS, lock code/unlock device, lock/unlock other application, alarm with text, launch FIR, claim insurance, speak message, make device call number with speaker, start shell, capture photograph, recharge SIM, capture video, capture screen shot/ screen recording, backup device/ SD card 12:00AM-04:00AM (default: can be edited) so that SD card device can be erased anytime, get device information (battery, radius within 50m etc. periodic location, time graph of location (location from 1:00pm to 5:00pm) (default: can be edited), travel/crowd mode.

In an exemplary embodiment, the mobile device, when configured with the proposed invention, loses, misplaced and stolen, the mobile device can

automatically perform various functions, such as but not limited to, specifically: remotely erase iPhone or mobile and take backup in applications user account. In another exemplary embodiment, the anti-theft functionality of mobile device can erase lost device remotely by SMS or user account.

In an exemplary embodiment, the system or anti-theft security system can restore backup in any new device or multiple device from cloud or network.

In an exemplary embodiment, the system can lock or password locks for important folders which can be opened with 3rd party while debugging, etc. In another exemplary embodiment, the system can lock the banking application or social media applications or important applications.

In an embodiment, as shown in FIG 4B. the mobile device, when configured with the proposed invention, loses, misplaced and stolen, the mobile device can automatically perform various functions 450, such as but not limited to, specifically:

i. when a SIM change is detected, the mobile device captures video/photo and transmits GPS location to an registered e-mail address or to a registered phone number or to an optional number pre-stored along with SIM information;

ii. when a password to uninstaller is being feed, the mobile device captures video/photo and transmits GPS location to an registered e-mail address or to a registered phone number or to an optional number pre-stored;

iii. can enable/disable data/WIFI;

iv. can maintain location time graph; of frequent location

v. when factory reset/ reboot detection/ force shutdown detected, the mobile device captures video/photo and transmits GPS location to an registered e-mail address or to a registered phone number or to an optional number pre-stored along with SIM information;

vi. Send/trigger alarm with message;

vii. can backup data at the cloud, for example, backup data (12:am-4:00am), (default: can be edited)and can erase data;

viii. when jionet tower detected automatically connects and upload to cloud account;

ix. can be changed from normal mode to travel mode;

x. can make device call a number, can automatically change remote lock/unlock/ status bar/power/ application;

xi. when no SIM detected, WIFI/Bluetooth/GPS/ MLAT notification;

xii. Can claim insurance/ launch FIR, and other SOS systems.

xiii. Can provide password /finger print/ pattern for shutdown as well as for formatting / rebooting the device.

xiv. Can automatically take video along with GPS locations once SIM card is removed and stores to the cloud which can be accessed remotely.

xv. Can provide password / finger print/ pattern for uninstalling the application.

xvi. Can automatically get connected to telecom services such as but not limited to JIO NET which provides free WIFI services in and around the city so that application comes on-line easily.

xvii. Can provide end to end data encryption.

xviii. Can provide a place to lock /unlock other applications in the device like whatsapp photo message and the like.

xix. Can be triggered using IMEI of the phone.

xx. can include an inbuilt Nanotechnology SIM installed which can be connected to the application and which will be stitched with items like Wallet, Files, Keys, Mobile covers, and the like.

xxi. Can communicate with the nearby mobile signal tracking towers to find the locations of the device.

xxii. Can utilize inbuilt mechanisms such as WIFI and/or Bluetooth for tracking using the MAC address.

xxiii. Can generate a time graph based on the events and can share the same over the network.

xxiv. Can provide a browser extension for providing user friendly experience.

FIG. 5 illustrates an exemplary working of the proposed system, in accordance with an exemplary embodiment of the present disclosure in which the non detachable nano-technology chip with non removable 4G/5G sim card is installed (fixed) inside the device which helps to track the device in case the device goes through hard factory reset, debugged using SDK tools like Android Debug Bridge , battery is removed , sim card is removed and not installed and other like

conditions. Furthermore the chip can access power ON/OFF keys of the device and directly syncs with ENKRYPTO app to take any desired security actions.

In an embodiment, the anti-theft mechanism of the present disclosure can be implemented in the form of a non-detachable chip which includes a non-removable SIM with internet data, which can be installed in the device which has access to security functions and access to keys like power ON/OFF the device remotely in case the SIM card is removed.

In an embodiment, the anti-theft mechanism of the present disclosure works even if the battery from the device is removed, SIM card is removed or the device is powered off as the installed chip containing 4G/5G/Verizon/AT&T etc. SIM card can be tracked and will perform required security function.

In an embodiment, when no SIM card is inserted, the device can be connected to Wi-Fi service providers like Jio net, true Wi-Fi, etc. which helps us to stay connected on the road without a SIM card and is installed everywhere in the district after which all the security measures can be triggered.

In an embodiment, when the battery from the device is removed or device is switched off, the device can connect to the non-detachable chip installed externally inside the device which controls the device functionalities like triggering power off-power on, connects to true Wi-Fi, etc. The chip also has unremovable SIM installed in it to take security action with the device using SMS system or app and access data like GPS location, power on-power off, turn internet on/off, etc. In case the chip is removed by any means, mobile app installed inside the software will help retrieve the device. Installment of the chip is not limited to device but also to products like keys, document carrier, wallet, vaults etc. The externally installed non-detachable 4g SIM card chip connected with the enkrypto app installed internally also provides onboard diagnostics (OBD) of the mobile device in which it is installed. Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

In an exemplary embodiment, the anti-theft mechanism of the present disclosure enables protects against any kind of irrelevant or unwanted infringements of the highest order such as phone discharges or battery removed or other desirable action.

Referring again to FIG. 5, In an aspect, the mobile device can include an alarming non-detachable chip installed externally to the mobile device and communicably connected with one or more applications installed internally inside the mobile device adapted to generate on-board diagnostics (OBD) data associated with the mobile device to activate said at least one security breach feature.

In an aspect, said mobile device can include a non-detachable chip having a transceiver. The chip can be externally connected to the mobile device and is configured to connect with one or more applications installed inside said mobile device. In another aspect, the one or more applications installed in said mobile device can generate at least on-board diagnostics (OBD) data associated with the mobile device. Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

While the foregoing describes various embodiments of the invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. The scope of the invention is determined by the claims that follow. The invention is not limited to the described embodiments, versions or examples, which are included to enable a person having ordinary skill in the art to make and use the invention when combined with information and knowledge available to the person having ordinary skill in the art.

ADVANTAGES OF THE INVENTION

a. The present disclosure provides an anti-theft technology or mechanism.

b. The present disclosure provides an anti-theft technology for tracking lost, misplaced and stolen mobile devices, wallets, vaults, gadgets, valuables, etc.

c. The present disclosure provides a mechanism that protect against any kind of irrelevant or unwanted infringements of the highest order.

d. The present disclosure is an anti-theft software application designed to track cellular devices with extreme accuracy/pin point precision.

e. When no sim is inserted , the device gets connected to the online wifi service providers like Jio net , true wifi , etc after which all the security measures can be triggered.

f. When the battery from the device is removed or device is switched off,we can connect to the non-detachable chip installed externally inside the device

which controls the device functionalities like triggering power off-power on, connects to true wifi, etc . The chip also has non removable sim installed in it to take security action with the device using SMS system or app and access data like GPS location, power on-power off, turn internet on/off, and other desired actions.

g. The externally installed non-detachable 4g simcard chip connected with the enkrypto app installed internally also provides onboard diagnostics (OBD) of the mobile device in which it is installed.

h. Installment of the chip is not limited to device but also to products like keys, document carrier, wallet, vaults and other valuables.

i. Further it will survive a hard and soft factory reset and will ask for a security measure to connect any usb to the device or debug the device.

j. The present disclosure provides a mechanism that guarantees total security by providing snapshots, recording live audio and video, procuring GPS location and the phone number of the new SIM card inserted by sending required SMS to the lost device after which activation lock is turned ON automatically.

I Claim:

1. A mobile device with anti-theft functionality comprising:

one or more processors;

a condition determining engine to control the one or more processors to determine at least one condition associated with said mobile device, said at least one condition being selected from whether the mobile device is lost, whether the mobile device is misplaced, whether the mobile device is stolen, or whether the mobile device is tampered;

a security breach engine to control the one or more processors to activate, upon detection of said at least one condition, at least one security breach feature pre-configured at a hardware level or at an operating system (OS) level on the mobile device to operate as said anti-theft functionality.

2. The mobile device as claimed in claim 1, wherein said at least one condition is determined based at least on any or combination of an attempt to insert a new SIM card in the mobile device, insertion of a new SIM card in the mobile device, removal of an existing SIM card from the mobile device, failure of multiple login attempts, and generation of different noises around the mobile device.

3. The mobile device as claimed in claim 1, wherein said at least one condition comprises a corresponding security breach feature determined based on pre-defined rules or criteria preset by an authenticated user.

4. The mobile device as claimed in claim 1, wherein at least one security breach feature is activated automatically.

5. The mobile device as claimed in claim 1, wherein said at least one security breach feature is adapted to activate one or more functionalities and/or sensors of said mobile device to retrieve information from nearby proximity of the mobile device and/or locality of the mobile device.

6. The mobile device as claimed in claim 1, wherein said mobile device comprises a transceiver to control the one or more processors to transmit, upon activation of said at least one security breach feature, at least a location co-ordinate of the mobile device or at least a snapshot of a user using the mobile device in real-time or at a fixed interval of time.

7. The mobile device as claimed in claim 1, wherein

said at least one security breach feature is adapted to activate, upon activation of said at least one security breach feature, one or more authentication mechanisms to forbid at least one of formatting, power off/forced shutdown, notification access, uninstallation of installed software applications, rebooting, trigger factory reset of the mobile device, triggering hard factory reset , accessing root folder, trying to connect to computer via USB ,trying to connect to any 3rd party Software Development Kit (SDK) like android debug bridge; or

said at least one security breach feature is adapted to activate, upon activation of said at least one security breach feature, one or more data formatting mechanisms to automatically format one or more pre-defined data stored in the mobile device.

8. The mobile device as claimed in claim 1, wherein said mobile device comprises a transceiver to control the one or more processors to receive, upon activation of said at least one security breach feature, one or more messages from remote location to activate one or more in-built functionality of said mobile device, said in-built is selected form a Bluetooth, a Wi-Fi, or a data connectivity.

9. The mobile device as claimed in claim 1, wherein said mobile device comprises an alarming device to control the one or more processors to play, upon activation of said at least one security breach feature and upon detection of an authenticated user in nearby proximity, a unique sound pre-defined for said mobile device.

10. The mobile device as claimed in claim 1, wherein said mobile device comprises a fake shutdown functionality to control the one or more processors to

enter, upon activation of said at least one security breach feature and upon an attempt to force shutdown, into a simulated power OFF mode (a.k.a fake power off) in which the mobile device screen/modem is OFF or battery is removed but a nano-technology chipset said mobile device is ON with non removable sim card installed inside the nano technology chip to take security action with the device using SMS system or app and access data like GPS location, power on-power off, turn internet on/off and other desired actions.

11. The mobile device as claimed in claim 1, wherein said mobile device comprises a non-detachable chip having a transceiver, wherein said chip is externally connected to said mobile device and is configured to connect with one or more applications installed inside said mobile device.

12. The mobile device as claimed in claim 11, wherein said one or more applications installed in said mobile device are adapted to generate at least on-board diagnostics (OBD) data associated with the mobile device.

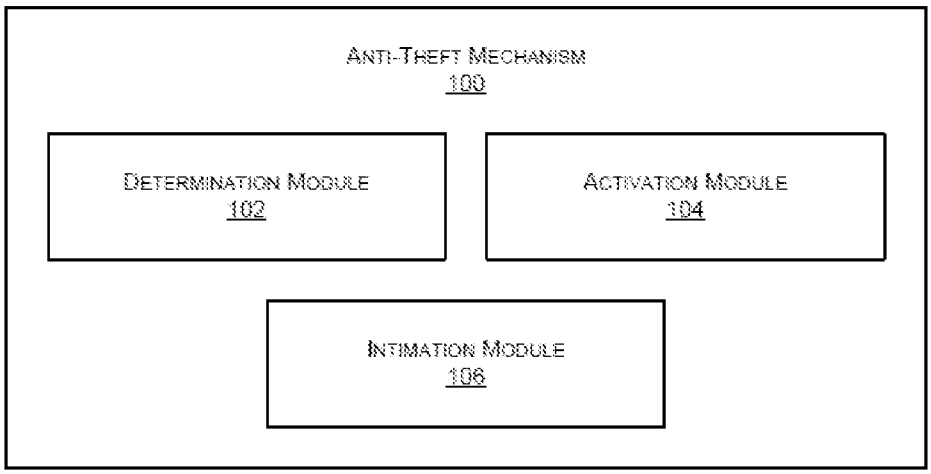
ANTI-THEFT MECHANISM
100
DETERMINATION MODULE
102
ACTIVATION MODULE
104
INTIMATION MODULE
106

FIG. 1A

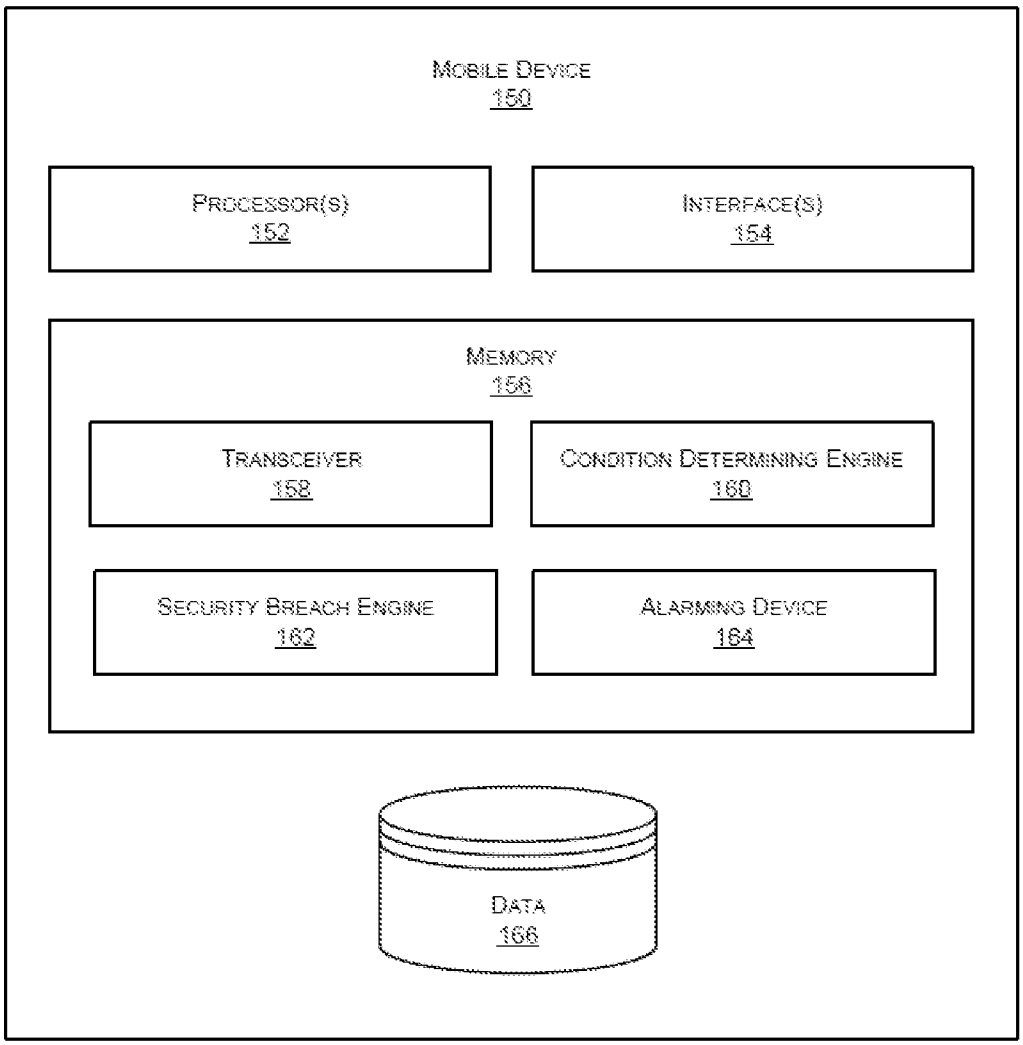
MOBILE DEVICE
150
PROCESSOR(S)
152
INTERFACE(S)
154
MEMORY
156
TRANSCEIVER
158
CONDITION DETERMINING ENGINE
160
SECURITY BREACH ENGINE
162
ALARMING DEVICE
164
DATA
166

FIG. 1B

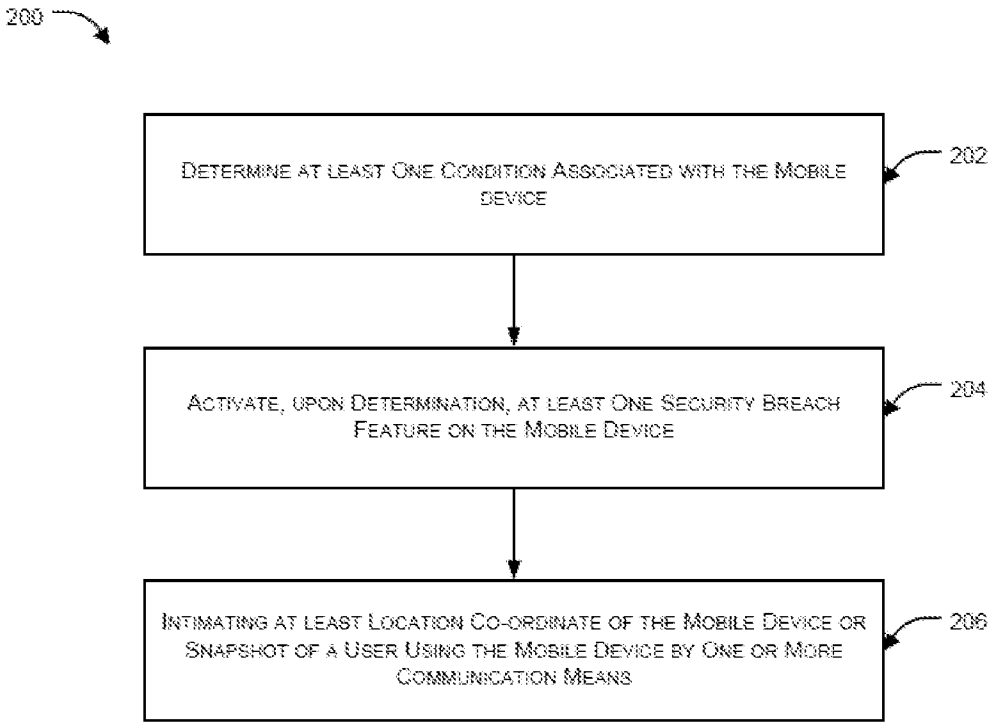
200
Determine at least One Condition Associated with the Mobile device
202
Activate, upon Determination, at least One Security Breach Feature on the Mobile Device
204
Intimating at least Location Co-ordinate of the Mobile Device or Snapshot of a User Using the Mobile Device by One or More Communication Means
206

FIG. 2

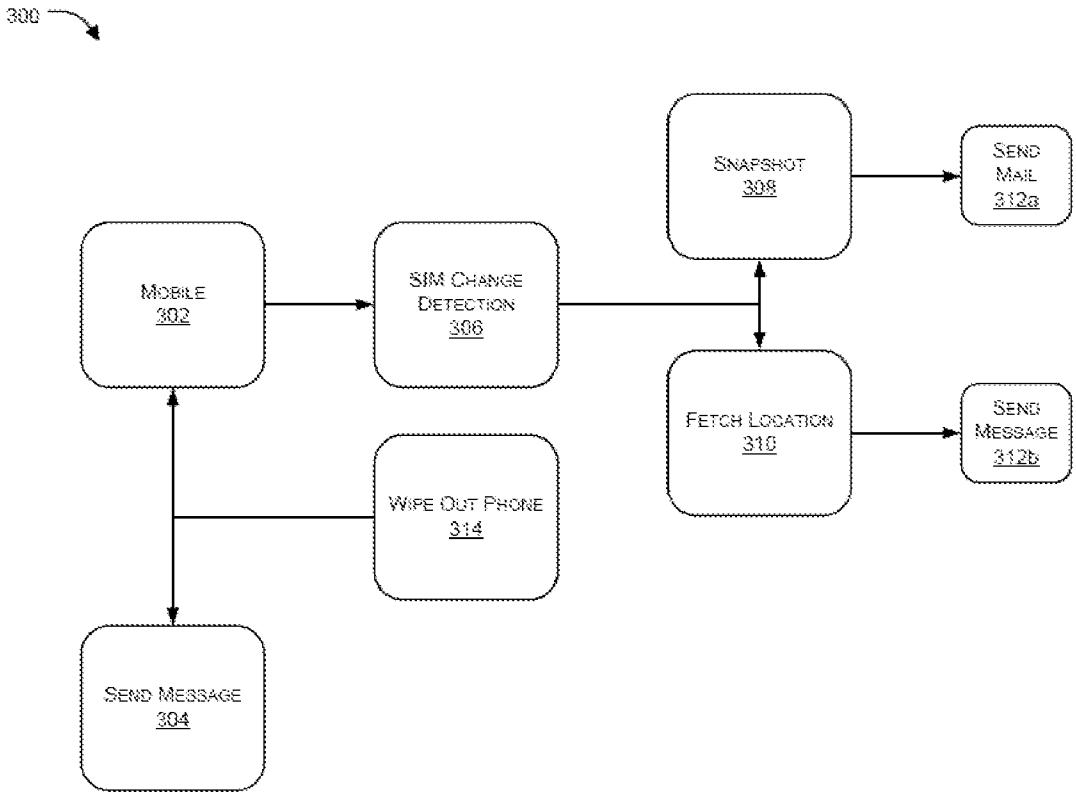
300
Mobile
302
SIM Change
Detection
306
Snapshot
308
Send
Mail
312a
Fetch Location
310
Send
Message
312b
Wipe Out Phone
314
Send Message
304

FIG. 3

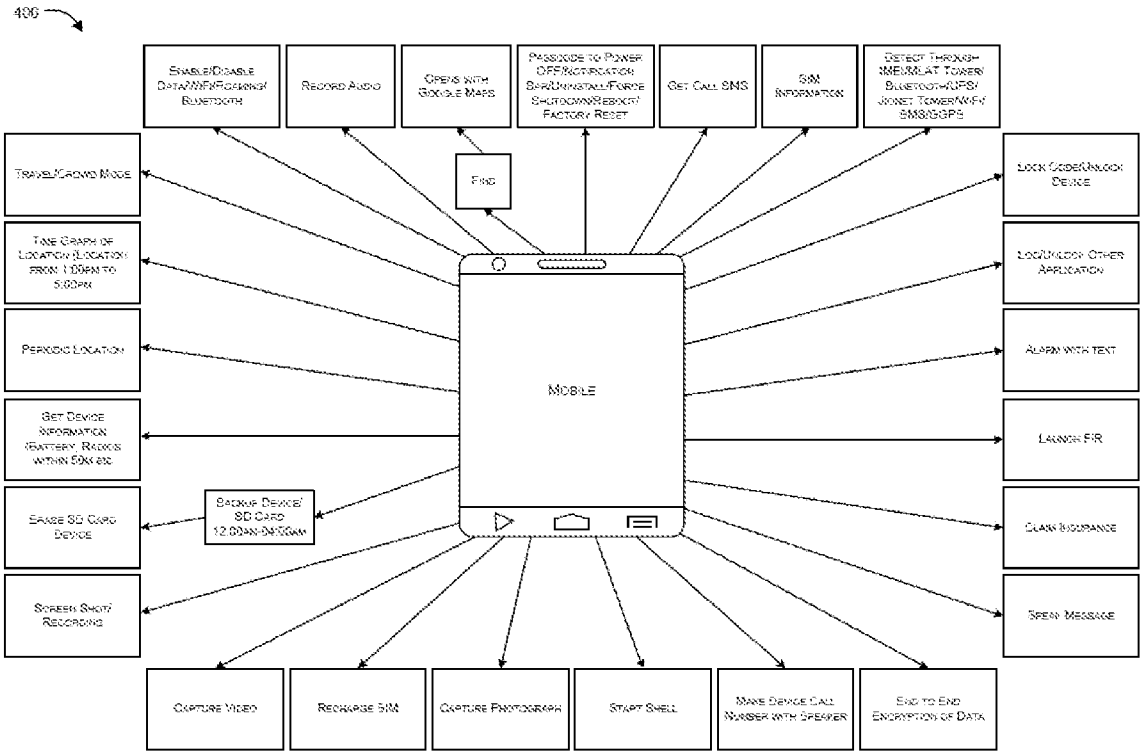
400
Enable/Disable Data/WiFi/Tethering/ Bluetooth
Record Audio
Opens with Google Maps
Passkode to Power OFF/Notification Bar/Uninstall/Force Shutdown/Reboot/ Factory Reset
Get Call SMS
SIM Information
Detect Through IMEI/IMSI/AT Tower/ Bluetooth/GPS/ Joinet Tower/Wi-Fi SMS/GGPS
Travel/Ground Mode
Find
Lock Code/Unlock Device
Take Graph of Location (Location) from 1:00PM to 5:00PM
Lock/Unlock Other Application
Periodic Location
Alarm with text
Get Device Information (Battery, Radios within 50M etc
Launch FIR
Erase SD Card Device
Backup Device/ SD Card 12.00AM-04:00AM
Claim Insurance
Screen Shot/ Recording
Speak Message
Capture Video
Recharge SIM
Capture Photograph
Start Shell
Make Device Call Number with Speaker
End to End Encryption of Data
MOBILE

FIG. 4A

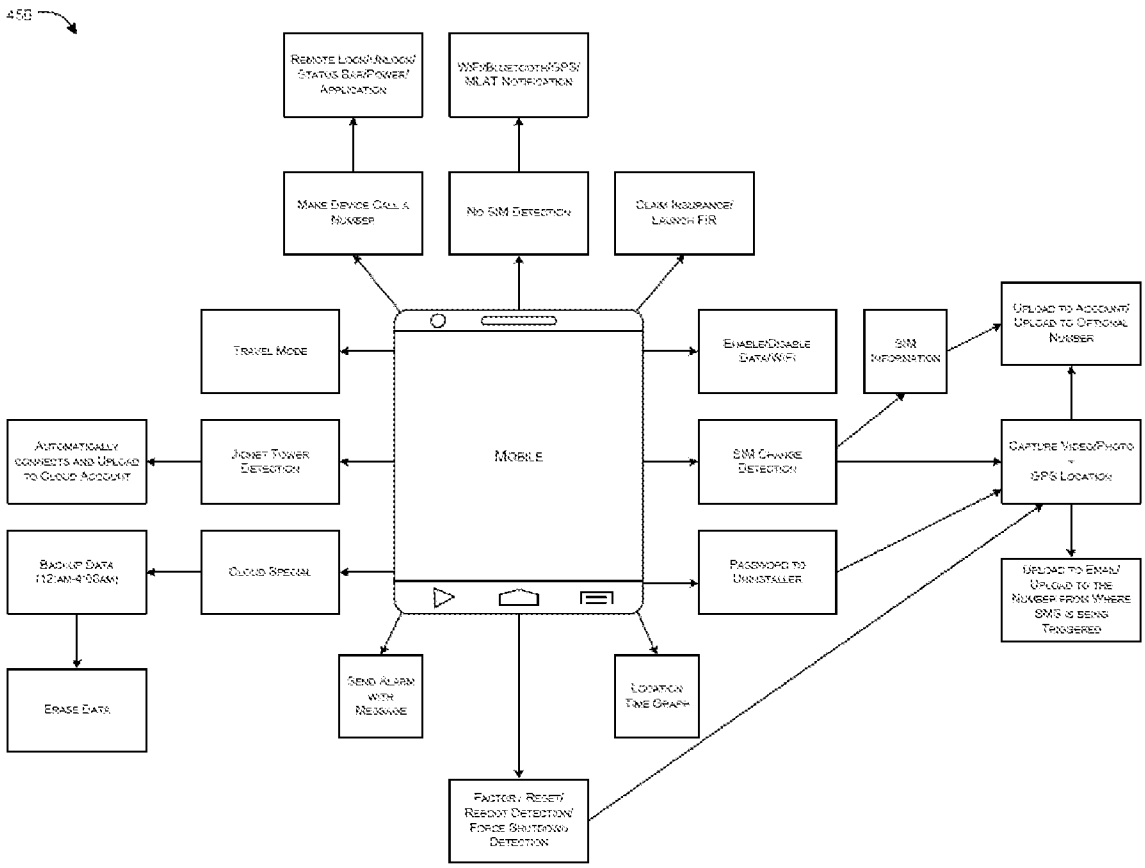
450
Remote Lock/Unlock/ Status Bar/Power/ Application
WiFi/Bluetooth/GPS/ MLAT Notification
Make Device Call a Number
No SIM Detection
Claim Insurance/ Launch FIR
Travel Mode
Enable/Disable Data/WiFi
SIM Information
Upload to Account/ Upload to Official Number
Automatically connects and Upload to Cloud Account
Jionet Power Detection
Mobile
SIM Change Detection
Capture Video/Photo + GPS Location
Backup Data (12am-4:00am)
Cloud Special
Password to Uninstaller
Upload to Email/ Upload to the Number from Where SMS is being Triggered
Erase Data
Send Alarm with Message
Location Time Graph
Factory Reset/ Reboot Detection/ Force Shutdown Detection

FIG. 4B

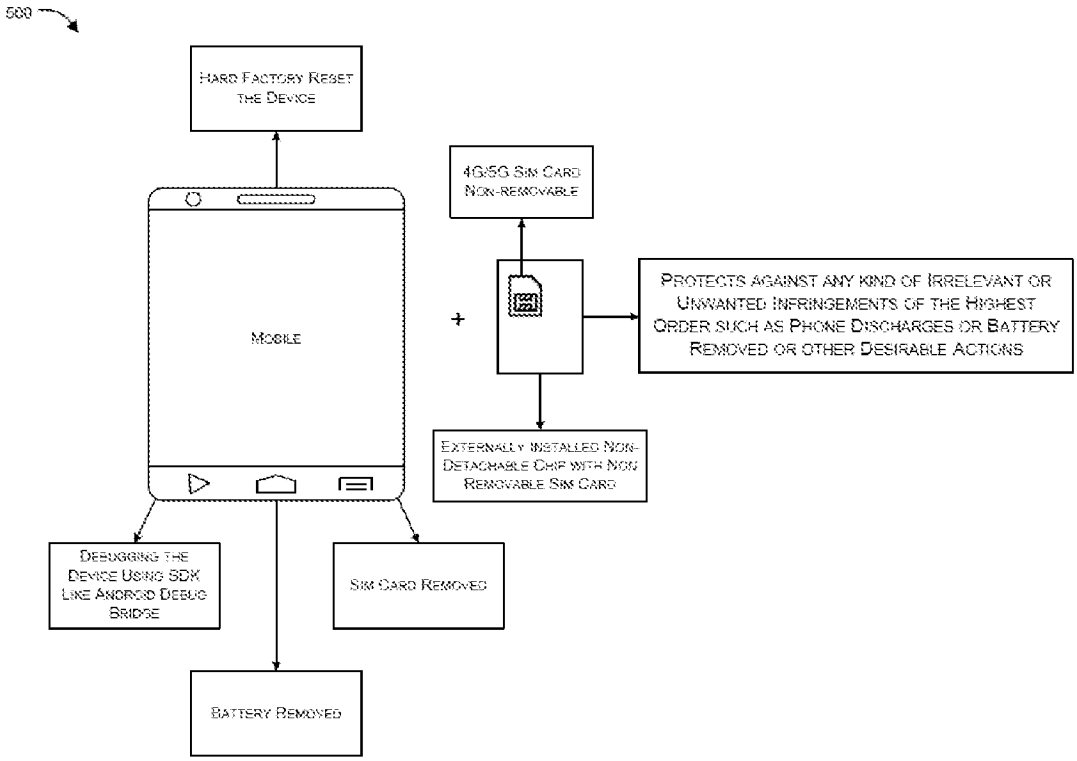
500
Hard Factory Reset the Device
4G/5G Sim Card Non-Removable
Mobile
+
Protects against any kind of Irrelevant or Unwanted Infringements of the Highest Order such as Phone Discharges or Battery Removed or other Desirable Actions
Externally Installed Non-Detachable Chip with Non Removable Sim Card
Debugging the Device Using SDK Like Android Debug Bridge
Sim Card Removed
Battery Removed

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2018/053249

A. CLASSIFICATION OF SUBJECT MATTER
G08B13/00,H04M1/66,G06F21/88 Version=2018.01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G08B, H04M, G06F, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases- TotalPatent One, IPO Internal Database
Searched Terms- stolen mobile, security breach, SIM, snapshot, sound

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0323115 A1 (BROADCOM CORPORATION), 30/10/2014 (30, OCTOBER 2014) abstract, paragraph [0039]-[0040]	1-12
Y	WO 2015077947 A1 (REN, MING), 04/06/2015 (04, JUNE 2015) paragraphs [0006]-[0017]	1-5, 8, 11, 12
Y	US 20080076459 A1 (SAMSUNG ELECTRONICS CO. LTD.), 27/03/2008, (27, MARCH 2008) paragraph [0011]	6
Y	CN 104182707 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.), 03/12/2014 (03, DECEMBER 2014) paragraphs [0027], [0029] and [0036]	7
Y	US 20120188064 A1 (LOOKOUT. INC., A CALIFORNIA CORPORATION), 26/07/2012 (26, JULY 2012) paragraphs [0090]-[0099]	9
Y	CN 104780279 A (SHANGHAI FEIXUN COMMUNICATION CO. LTD), 15/07/2015 (15, JULY 2015) abstract	10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21-08-2018	21-08-2018
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Nikhil Katiyar Telephone No. +91-1125300200