

Smart Padlock and Securing or Tracking An Asset

Field of Invention

[001] The present invention relates to smart padlocks, systems for operating the smart padlocks and securing or tracking an asset. In particular, the operating system relates to a low power Internet of Things (IoT) technology (for example, hosted on a narrow band-IoT network).

Background

[002] We now live in a world of electronic devices and inter-connectivity, and IoT technology is considered the enabler to allow all electronic devices to be connected, in the forms of machine-to-people and machine-to-machine communications. The key challenges to adopting IoT technology include: device cost, battery life, security, scalability, system coverage and so on.

[003] The mass market for IoT is huge and diverse. This disclosure also concerns securing and tracking assets, or in general, asset management; often, assets are kept in controlled accessible areas and this disclosure relates to smart or electronic padlocks for securing assets in these controlled areas, which may be immobile or mobile. Chinese patent publication CN105336029 discloses an IoT based intelligent lock system and method. A user can unlock the lock through a RF card, a Bluetooth terminal or an application program installed on a smartphone.

[004] In another approach, US patent publication US20160049032 discloses a keyless padlock that is operable using a unique identification code.

[005] Despite development of the above electronic locks, there exists a need for other padlocks that have other features and advantages over the existing prior art.

Summary

[006] The following presents a simplified summary to provide a basic understanding of the present invention. This summary is not an extensive overview of the invention, and is not intended to identify key features of the invention. Rather, it is to present some of the inventive concepts of this invention in a generalised form as a prelude to the detailed description that is to follow.

[007] The present invention seeks to provide smart padlocks and systems for operating them. The smart padlocks are used to secure controlled access sites at some installations; the smart padlocks can also be used to secure, track and locate goods or assets stored in shipping containers or delivery trucks. It is also possible to secure, track and locate mobile assets, such as, bicycles.

[008] In one embodiment, the present invention provides a smart padlock as defined in claims 1-10; the present invention also provides a system for operating the smart padlocks or smart padlocks and sensors as defined in claims 11-24.

[009] In another embodiment, the present invention provides a method for securing, tracking and locating goods or assets stored in secure enclosures, which include shipping containers and delivery trucks, as defined in claims 25-27.

Brief Description of the Drawings

[0010] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0011] FIG. 1A illustrates a system for implementing a smart padlock and an accompanying lock management software using a gateway according to an embodiment of the present invention; FIG. 1B illustrates a system for implementing a smart padlock and an accompanying lock management software using a low power gateway according to another embodiment; while FIG. 1C illustrates a system for implementing a smart padlock/sensors

and an accompanying lock/sensors management software according to another embodiment; FIG. 1D illustrates a system for implementing a smart padlock according to another embodiment; FIG. 1E illustrates a user interface used in the lock management software, whilst FIG. 1F illustrates a user interface used in an associated mobile device;

[0012] FIG. 2A illustrates steps involved in registering administrators, users and padlock identities before using the above lock management software; Table 1A illustrates some administration personnel involved in operating the lock management software; and Table 1B illustrates some of the users and padlocks data stored in the database; FIG. 2B illustrates steps involved in operating the smart padlock according to the system shown in FIG. 1A; FIG. 2C illustrates steps involved in operating the smart padlock according to the system shown in FIG. 1B, whilst FIG. 2D illustrates steps involved in operating the smart padlock according to the system shown in FIG. 1D;

[0013] FIGs. 3A-3C illustrate a configuration of the above smart padlock without use of a physical key; and FIGs. 3D-3E illustrate another smart padlock for use with a portable key; and

[0014] FIGs. 4A-4B illustrate use of smart padlock tracking, monitoring and locating of mobile goods or assets in secure containers; and FIG. 4C illustrates a map showing locations of some smart padlocks.

Detailed Description

[0015] One or more specific and alternative embodiments of the present invention will now be described with reference to the attached drawings. It shall be apparent to one skilled in the art, however, that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals or series of numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0016] FIG. 1A shows a lock system 100 for implementing a smart padlock 110, 110a, 110b and an accompanying lock management software 200 using a known gateway 10 according

to an embodiment of the present invention. The known gateway 10 may be an internet, LTE and/or cellular network, whilst in FIGs. 1B and 1C, another lock system 1000, 1000a is operable through a low power gateway 12 (such as, a LoRa (low power long range), a LPWA (low power wide area), LTE-M or Sigfox network) using the same or another version of the lock management software 200a, and in FIG. 1D, another lock system 2000 is operable through a narrow-band IoT network 14 using the same or another version of the lock management software 200b.

[0017] In FIG. 1A, the smart padlock 110, 110a, 110b are used to secure a controlled access site 180, such as a telco station or a public utility substation. These controlled access sites may not be manned round the clock but require regular maintenance, asset management and so on. These controlled access sites thus require a system for operating these smart padlocks, which may be configured as a shackle padlock 110 or a sliding bolt padlock 110a. As shown in FIG. 1A, a server 20 and a database 21 are connected to the known gateway 10, and a workstation 30 at a command centre is then connected to the server 20. Operable inside the workstation 30 is the lock management software 200. It is possible that there is a plurality of workstations and some workstations may be connected to the server 20 indirectly through the gateway 10. In use, a user carries a mobile device 40 and visits the controlled access site 180. The mobile device 40 operates a mobile application 300 and connects the smart padlock 110, 110a to the lock management software 200 via the gateway 10. FIGs. 1E and 1F illustrate user interfaces of the lock management software 200, 200a-200b and mobile application 300.

[0018] Before using the above lock system 100, the lock management software 200, 200a, 200b is prepared, in a process 250 shown in FIG. 2A, by installing the lock system and lock management software, in step 260, registering administrators and users (in steps 265 and 270) and recording the media access control (MAC) addresses of mobile devices 40 for use by the respective users in the database 21; also during registration, categories of security access/permission into the controlled site 180 are defined, for example, with managers being permitted to access all sites and some other users are restricted to predefined areas. It is possible that the controlled access site 180 has more than one level of security access; for example, in the telco station, within the premises secured with a smart padlock, another smart padlock may secure an inner area having a higher level of security, for eg., that for

housing a power generator and standby batteries; the power generator and standby batteries are portable assets which are often targets for thieves. It is also possible to register a group of users with privileged access for a relatively long period of access; for example, a cleaning contractor may visit a site 180 without having to make prior request, and the cleaners may be given privileged access to a plurality of sites located in a predefined region. In step 275, the smart padlocks at all the sites 180 are also registered. In step 280, a decision is made whether any new user, administrator, padlock or site is to be registered. If the decision in step 280 is positive, the process reverts back to step 265; if the decision in step 280 is negative, the process connects, in step 285, with users on site and/or directly with the each of the padlocks and at the same time, logging all the administration, user and padlock activities in the database 21. A decision is made in step 290 whether there is a scheduled maintenance; if there is no maintenance, the process reverts to step 265; if there is a shut down for maintenance, the process issues a notice before the process 250 ends at step 295. Table 1A shows some of the corporate administration data stored in the database 21, whilst Table 1B shows some of the users and padlocks data.

[0019] FIG. 2B shows a process 400 of operating smart padlock 110, 110a, 110b with the mobile application 300. The process 400 illustrated in FIG. 2B is highly simplified. In step 405, the user starts the mobile application 300 on the mobile device 40. In one embodiment, in step 410, the user sends a request for access and in response, the lock management software 200 captures the media access address (MAC) of the mobile device 40, an administrator approves the request and sends a softkey to the user account in step 422; at the site, the user logs in to the user account and retrieves the softkey. The user also turns on the Bluetooth application in the mobile device 40, in step 430; the Bluetooth application searches for the smart padlock 110, 110a, 110b that is within range, synchronises with the smart padlock by frequency hopping, decrypts the softkey and authenticates the user. A decision is made in step 435 whether the decryption and authentication steps are successful. Once authentication, decryption and synchronization are successful, in step 450, the smart padlock 40 becomes unlocked for a predetermined duration according to the request made. If the decision in step 435 is negative, the mobile application 300 sends an alert to the administrator and the lock usage history is updated. In another embodiment, an administrator has scheduled a user to visit a site and informed the user carrying a registered mobile device 40. As in the above embodiment, upon reaching the site, the user logs in to

one's account, retrieves the softkey, turns on the device Bluetooth and allows the mobile device to synchronise, decrypt and authenticate to unlock the smart padlock 110, 110a, 110b for a predetermined duration. In step 455, a decision is made whether the user has completed the task. If the user has completed a task, the user puts the padlock back in the original position and locks the smart padlock 110, 110a, 110b via the mobile application 300; after communication between the mobile device and the smart padlock is established, a lock sensor 122 inside the padlock sends out a locked signal and the lock management software 200 updates the state of the smart padlock 110, 110a and the process ends in step 480. All the communication and access history of the smart padlock are captured in the database 21; records in the database 21 allow the owner of the padlock system 100 to analyse the database, for example, for preventive maintenance or for any investigation. In step 455, if a task duration exceeds the predetermined access duration, the user makes an additional request in step 460 and another softkey is generated and communicated to unlock the smart padlock 110, 110a, 110b. If the task is completed, and after the lock open duration has elapsed but the padlock is not returned to the original position, the mobile application 300 sends an alert to the user. In an embodiment, the smart padlock 110, 110a, 110b has a camera 156; the camera 156 is activated when the lock open duration has elapsed and an administrator at a workstation at the command centre can determine whether the padlock is returned to the original position and is locked. Whilst Bluetooth communication between the mobile device 40 and the smart padlock 110, 110a, 110b has been described, the present invention is also applicable when the mobile device 40 is configured with other type of near field (NF) communication with the smart padlock 110, 110a, 110b. The present invention is implementable using current technology of an internet, cellular or LTE gateway 10.

[0020] Referring back, FIG. 1B shows the lock system 1000 in which a LP gateway 12 is provided by a low power wide area or long range network, such as, LoRa, LPWAN, LTE-M or Sigfox. The LP gateway 12 may coexist with the above gateway 10. As in the above system 100, this lock system 1000 includes a server 200 connected to both the LP gateway 12 and gateway 10, and a workstation 30 at a command centre running a version of a lock management software 200a. The gateway 10 serves the mobile device 40, which allows communication with the smart padlock 110, 110a, 110b. In use, the smart padlock 110, 110a, 110b is connected to the lock management software 200a via the LP gateway 12,

whilst the mobile device 40 runs a mobile application 300, communicates with the smart padlock via near field NF communication (such as, Bluetooth) and with the lock management software 200a via the gateway 10.

[0021] FIG. 1C shows a locks/sensors system 1000a according to another embodiment. In the locks/sensors system 1000a, a sense hub 1100 is located close to the padlocks 110 and sensors 111 near a work site; some of these sensors 111 may include proximity sensors, door lock sensors 111, temperature sensors 111a, humidity sensors 111b, fuel tank sensors, security cameras, and so on. Some of these locks and sensors are equipped with LPWAN modules and are able to connect with the lock/sensor management software 200b through the LPWAN (using Sigfox, LoRa, NB-IoT); other locks and sensors are equipped with Bluetooth modules and are able to connect with the lock/sensor management software 200b through the sense hub 1100; for eg. information on the padlocks and sensors is collected by the sense hub 1100 and relayed to the remote command centre via the LPWA gateway; in the same manner, commands are sent from the command centre through the sense hub 1100 to the padlocks, security cameras, etc. Preferably, the range of communication between the padlocks, sensors, cameras, etc and sense hub 1100 is substantially about 1-50m, whilst the range of the LPWA communication is substantially about 1-10 km.

[0022] The use of the sense hub 1100 is useful as the smart padlocks 110, sensors 111, etc. are limited in sizes (for eg., to accommodate an antenna dipole for longer range communication) or the signal power from the smart padlocks 110 or sensors 111 may be low. When there is a plurality of smart padlocks and sensors, there are cost and productivity advantages to provide a sense hub for communication with the command centre. In addition, the numbers of padlocks and sensors are scalable. Each sense hub 1100 has a hardware portion and a software portion. The hardware portion includes electronics for Bluetooth, LoRa, NB-IoT and/or Sigfox communication, whilst the software includes web client and mobile client applications. Another advantage of using the sense hub is that data that passed through the sense hub can be used for data mining and analytics; for eg., the web client can be used to perform predictive, prescriptive, diagnostic and AI analyses. When a few smart padlocks or sensors are deployed onsite or a few padlocks or sensors are deployed on a shipping container, truck, motorbike or bicycle (which is on the move), the

padlocks or sensors may communicate directly with the command centre through the LPWAN gateway.

[0023] FIG. 2C shows a process 500 of operating the smart padlock with the mobile application 300 using the above lock system 1000, 1000a and LPWA gateway 12. In step 510, the user starts the mobile application 300 on the mobile device 40. In one embodiment, the user sends a request, in step 520, to access a site 180 and in response, the lock management software 200a captures the media access address (MAC) of the mobile device 40, an administrator approves the request, in step 522, and the system sends a softkey directly to the padlock, in step 524. In another embodiment, a scheduled visit is arranged by an administrator and a softkey is sent directly to the padlock. At the site, the user logs in to one's account and turns on the device Bluetooth, in step 530; the Bluetooth application searches for the smart padlock 110, 110a, 110b that is within range, synchronises with the smart padlock by frequency hopping, decrypts the softkey and authenticates the user. A decision is made in step 535 whether the synchronization, decryption and authentication steps are successful. If authentication, decryption and synchronization between the mobile device 40 and the smart padlock 110, 110a, 110b are successfully established, the smart padlock becomes unlocked for a predetermined duration, in step 550. If the decision in step 535 is negative, the mobile application 300 sends an alert to the administrator and the lock usage history is updated. In step 555, a decision is made whether the user has completed the task. If the user has completed a task, the user puts the padlock back in the original position and locks the smart padlock 110, 110a, 110b via the mobile application 300; after communication between the mobile device and the smart padlock is established, the lock sensor 122 inside the padlock sends out a locked signal and the lock management software 200a updates the state of the smart padlock 110, 110a, 110b and the process ends in step 580. In step 555, if a task duration exceeds the predetermined access duration, the user makes an additional request in step 560 and another softkey is generated and communicated to unlock the smart padlock 110, 110a, 110b. If the task is completed, and after the lock open duration has elapsed and the padlock is not returned to the original position, the mobile application 300 sends an alert to the user; the user is responsible to ensure that the process ends successfully with step 580. As in the above embodiment, the smart padlock 110, 110a, 110b may have a camera 156; the camera 156 can be activated when the lock open duration has elapsed, and an administrator at a workstation at the command centre can

determine whether the padlock is returned to the original position and is locked. In another embodiment (not shown in the figure), when technology is mature and the mobile device is enabled for LP communication, then the gateway 10 becomes redundant.

[0024] Referring back, FIG. 1D shows the lock system 2000 in which a gateway 14 is provided by a narrow band IoT (NB-IoT) network. As in the above embodiments, this lock system 2000 includes a server 20 connected to the NB-IoT gateway 14 and a workstation 30 at the command centre running a version of the lock management software 200b. As shown in FIG. 1D, some padlocks 110, 110a, etc. and sensors 111 may communicate with the NB-IoT gateway 14 through an IoT hub 2100. This IoT hub 2100 is similar in functions with the above sense hub 1100, which connects a plurality of smart padlocks 110 and sensors 111 with the command centre but now through the NB-IoT gateway 14. The cost and productivity advantages of the IoT hub 2100 are also similar to those of the sense hub 1100. Also, the numbers of smart padlocks and sensors in use become scalable. The smart padlock 110, 110a, 110b may include a touch sensor 150, a vibration sensor 152, a fingerprint scanner 154 or a camera 156 (as seen in FIG. 3A or 3B).

[0025] FIG. 2D shows a process 600 for operating the smart padlock using the NB-IoT gateway 14. The process starts at step 605 and, in step 620, a user makes a request to access a site via a mobile device 40 (such as a smartphone) or by contacting an administrator at the command centre. In step 622, the user receives an approval and, in step 624, a softkey is sent directly to the smart padlock 110, 110a at the site. At the site, the user touches the smart padlock 110, 110a, 110b and the touch sensor 150 or vibration sensor 152 responds by waking up the smart padlock 110, 110a, 110b from a sleep mode, and activates the fingerprint sensor 154, in step 630. After the fingerprint sensor 154 detects and captures a fingerprint scan, the padlock decrypts the softkey generated by the lock management software 200b and authenticates the biometric identity with the identity registered in the database 21. A decision is made in step 635 whether the decryption and authentication processes are successful. If decryption of the softkey and authentication of the biometric identity are positive, a signal is sent, in step 650, to unlock the smart padlock 110, 110a, 110b for a predetermined duration to allow the user to carry out a task. If the decision in step 635 is negative, the lock management software 200b sends an alert to the administrator. In step 655, completion of the task is checked. If the task is not completed

within the duration requested, the user makes an additional request or contacts the administrator for assistance, in step 660. If the task is completed, in step 670, a check is whether the padlock has been returned to the original location and locked. If the decision is negative, the lock management software sends an alert to the user, for example on the mobile device or another device at the site. If the decision in step 670 is positive, the process ends at step 680. In another embodiment, a scheduled visit is arranged by an administrator and the user visits the site to carry out the assigned task. As in the above embodiment, when the smart padlock is equipped with a camera 156, the check in step 670 can be visually verified. In yet another embodiment, the fingerprint scanner function is located on the mobile device (instead of on the smart padlock).

[0026] The lock system 2000 is advantageous because the padlock 110, 110a, 110b can be tracked and monitored at the command centre or at any workstation by an administrator. In the event when an external force is applied on the smart padlock, the lock sensor 122 or vibration sensor 152 may sense an intrusion or attempted intrusion and the smart padlock would send an intrusion alert to the site manager or administrator. When a mobile device 40 is used at the site where the smart padlock is used, the lock system 100, 1000, 2000 also captures the GPS coordinates of the mobile device 40 as the location of the smart padlock; in this way, locations of all the deployed smart padlocks can be located and monitored at the command centre on a regional map; in addition, the locations of nearby deployed smart padlocks can also be visually seen on a regional map on each mobile device 40. FIG. 4C displays a map with some neighbouring smart padlocks on the mobile application 300.

[0027] FIG. 3A shows a configuration of the above smart padlock 110. The smart padlock 110 has a shackle 112 and body 120. Inside the body, there is a lock sensor 122, an actuator 124 and electric terminals 126. The lock sensor 122 determines whether the padlock is locked or unlocked. The actuator 124 activates the locking mechanism, while the electric terminals 126 provide the electric signal and power to the lock sensor 122 and actuator 124. The body 120 is metallic and provides an integral strength to the smart padlock. At a lower side of the smart padlock, there is a removable housing 130. FIG. 3B shows the housing 130 is connected to the body 120 by a screw 128 and a pin 129. The screw 129 is accessible through the opening for the shackle end only when the smart padlock is unlocked. The housing 130 is made of a non-metal and protects a circuit board 131, an electronic chip 133,

an antenna dipole 134 and a battery 135, amongst other components, being connected to the circuit board. FIG. 3C shows a schematic of the chip 133 being mounted on the circuit board 131 and in electric connection with the antenna dipole 134. The circuit board 131 is also connected to contacts 136 matching the electric terminals 126 and a micro-B socket 140. The micro-B socket provides for an interface with an external power source, for eg. during an emergency or when the battery 135 power is too low. Preferably, the smart padlock 110 is sealed for immersion proof according to IP68 rating.

[0028] In one embodiment, the electronic chip 133 and antenna dipole 134 are configured for near field communication, such as, Bluetooth; in another embodiment, the chip 133 and antenna 134 are configured for LPWA, LoRa and/or LTE-M network communication; in yet another embodiment, the electronic chip 133 and antenna dipole 134 are configured for NB-IoT network communication. In the latter embodiment, the circuit board 131 is also connected to a touch sensor 150 and/or a vibration sensor 152. In another variation of the latter embodiment, the circuit board 131 is also connected to a fingerprint scanner 154. In yet another variation, the circuit board 131 is also connected to a camera 156.

[0029] FIG. 3D shows a smart padlock 110b according to another embodiment. As in the above embodiment, the smart padlock 110b has a lock body 120 and a shackle 112 but requires a portable key 160 to be brought to a site for locking and unlocking. The portable key 160 includes a circuit board 131, an electronic chip 133, an antenna dipole 134, a battery 135 and other electric components, as in the above embodiment. However, the electrical contacts are located in a plug 162 portion on the portable key and match with the terminals located in a receiving socket 127. FIG. 3E shows an external view of the portable key 160. In another embodiment of the portable key, the circuit board 131 is also connected to a touch sensor 150 or a fingerprint scanner 154.

[0030] In the above embodiment, the smart padlocks 110, 110a, 110b have been described for use on fixed installations. It is possible that the smart padlocks 110, 110a, 110b are also suitable for use on mobile installations, such as, on shipping containers or delivery trucks in which goods or assets in transit are kept secure with padlocks, as shown in FIGs. 4A and 4B. These smart padlocks can also be used on bicycles. With these smart padlocks 110,

110a, 110b, these shipping containers, delivery trucks, bicycles, motorbikes, etc. can be tracked and located as part of secure goods delivery and asset management.

[0031] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the present invention. For eg., the housings 130 with NB-IoT network communication can be configured as standalone trackers for further tracking of goods or assets while in transit, both within a country or across international borders.

CLAIMS:

1. A smart padlock comprising:
 - a body, a shackle or a locking pin and a set of electric terminals;
 - a housing that is removably connected to the body, with the housing including a set of electric contacts matching the set of electric terminals on the body, a circuit board, an electronic chip, an antenna dipole and a battery;
 - wherein, after a softkey has been received by the antenna dipole, and the softkey is decrypted and authenticated inside the electronic chip, an output signal is sent to the set of electric terminals to unlock the smart padlock.
2. The smart padlock according to claim 1, wherein the electronic chip and antenna dipole are operable for near field NF communication, including Bluetooth.
3. The smart padlock according to claim 1, wherein the electronic chip and antenna dipole are operable for LPWA, LoRa, LTE-M or Sigfox communication.
4. The smart padlock according to claim 1, wherein the electronic chip and antenna dipole are operable for NB-IoT communication.
5. The smart padlock according to claim 4, further comprising a touch sensor and/or a vibration sensor to wakeup the electronic chip from a sleep mode to an operational state.
6. The smart padlock according to claim 5, further comprising a fingerprint scanner to capture a fingerprint for authentication inside the electronic chip.
7. The smart padlock according to any one of the preceding claims, wherein the housing is configured as a standalone portable key, with the portable key being configured with a matching micro-B port for supplying emergency power or for emergency operation of the smart padlock.
8. The smart padlock according to any one of the preceding claims, further comprising a micro-B port for connection with an external power source for supplying emergency power.

9. The smart padlock according to any one of the preceding claims is used for controlling access into an area or nested area(s) at a fixed installation.

10. The smart padlock according to any one of claims 1-8 is used for securing, tracking or locating goods or assets in a shipping container or a delivery truck or for securing, tracking and locating mobile assets, including bicycles or motorbikes.

11. A padlock operating system comprising:

a gateway;

a server and a database connected to the gateway;

a workstation at a command centre being connected to the server, with the workstation operating a lock management software;

a mobile device registered for communicating with the server and workstation via the gateway; and

a smart padlock in near field communication with the mobile device;

so that, upon retrieving a softkey generated by the lock management software and turning on the near field communication between the smart padlock and the mobile device, the softkey is decrypted and authenticated inside the smart padlock, and in response to positive authentication, a signal is outputted to unlock the smart padlock for a predetermined duration.

12. The system according to claim 11, wherein the gateway is the internet, cellular or LTE network.

13. The system according to claim 11 or 12, wherein the mobile device operates a mobile application for requesting a softkey and the mobile device is identified by a media access address (MAC) associated with the mobile device.

14. A padlock and sensor operating system comprising:

a low power (LP) gateway, including a wide area (LPWA), long range (LoRa), LTE-M or Sigfox network;

a server and a database connected to the LP gateway;

a workstation at a command centre being connected to the server, with the workstation operating a lock/sensor management software; and

a smart padlock or sensor registered for communicating with the server and workstation via the LP gateway;

so that, after positive authentication, a signal is outputted to unlock the smart padlock for a predetermined duration.

15. The system according to claim 14, further comprising a sense hub for connecting a plurality of smart padlocks or sensors at a site through the LP gateway.

16. The system according to claim 14 or 15, further comprising:

a mobile device registered for communicating with the server and workstation via the internet, cellular, LTE or LP gateway; and

after the smart padlock receives a softkey generated by the lock management software and a user turning on the near field communication between the smart padlock and the mobile device, the softkey is decrypted and authenticated inside the smart padlock

17. A smart padlock or sensor operating system comprising:

a narrow-band IoT (NB-IoT) gateway;

a server and a database connected to the NB-IoT gateway;

a workstation at a command centre being connected to the server, with the workstation operating a lock management software; and

a smart padlock or sensor registered for communicating with the server and workstation via the NB-IoT gateway, with the smart padlock having a touch or vibration sensor;

so that, after the smart padlock receives a softkey generated by the lock management software and a user scans one's fingerprint, the softkey is decrypted and authenticated inside the smart padlock, and in response to positive authentication, a signal is outputted to unlock the smart padlock for a predetermined duration.

18. The smart padlock operating system according to claim 17, wherein the touch or vibration sensor wakes the smart lock from a sleep mode to an active mode.

19. The smart padlock operating system according to claim 17 or 18, wherein the vibration sensor is operable to detect an intrusion and to send an alert to the command centre.
20. The smart padlock operating system according to any one of claims 17-19, wherein the smart padlock further comprises a fingerprint scanner or a camera.
21. The smart padlock operating system according to any one of claims 17-20, further comprising a mobile device registered for communicating with the server and workstation via the internet, cellular, LTE or LP gateway.
22. The smart padlock operating system according to claim 21, wherein the fingerprint scanner is located on the mobile device (instead of on the smart padlock).
23. The smart padlock operating system according to any one of claims 17-22, further comprising an IoT hub for connecting a plurality of smart padlocks or sensors at a site through the NB-IoT gateway.
24. A smart padlock code for operating the lock system or lock/sensor system according to claims 11-23, wherein the code is recorded on a computer readable medium.
25. A method of securing, tracking and locating goods or an asset, the method comprising:
 - securing the goods or the asset located in a controlled access area or in a mobile enclosure using a smart padlock;
 - remotely generating a softkey for opening the smart padlock from a lock management software, sending the softkey to the smart padlock via a gateway and allowing the smart padlock to unlock for a predetermined duration after the softkey is decrypted by a user and the user identity is authenticated;
 - tracking a state and time of unlocking of the smart padlock; and
 - sending an alert if the predetermined duration of unlocking has expired or if the smart padlock is tampered with.

26. The method according to claim 25, wherein the goods or asset is tracked or located by using the GPS of the associated smart padlock.

27. The method according to claim 25 or 26, wherein the gateway includes one of the following or any combination: IoT, LPWA, LoRa, LTE, LTE-M, Sigfox, internet and cellular network.