

Smart IoT End Devices Supervised By A Gateway Device and Secure Methods of Operation

Related Patent Applications

[001] This patent application is a continuation-in-part (CIP) of the US patent application no. 16/764,005 or PCT/SG2018/050579 entitled “Gateway Device For IoT Sensors Or Actuators” filed on 27 November 2018.

Field of Invention

[002] The present invention relates to smart IoT end devices system supervised by a smart gateway device and secure methods of operation for a user access to a secure site. This secure operation methods serve critical infrastructure assets located at secure sites with 24-hours, 7-days-a-week supervision at low data cost and high security; even when quality of service of a low-power wide-area network (LPWAN) used by the system has deteriorated or the gateway device has failed, the smart IoT devices remain operable or to maintain security at the secure sites. Operation of these smart IoT devices is especially useful where the secure sites are distributed across a wide geographical region.

Background

[003] Assets, being valuable, are usually located in secure areas, invariably under locks or padlocks and keys. Smart locks and padlocks are also sought to secure sites of critical installations, such as, telecommunication stations, in which entry access is controlled and monitored 24-hours, 7-days-a-week. Smart locks offer compelling benefits over conventional, mechanical locks. In a secure system, these smart locks provide improved security, with enhanced efficiency and lower operating costs, especially when these secure sites are located over a wide geographical region. With smart lock implementation, travelling time to and forth to collect and to return physical keys from an operations centre is eliminated by providing virtual keys to authorized users; further, the operations centre or a server connected to the operations centre can be managed remotely, for eg., via a tablet or smartphone from another office or from home; apart from travel time and operational

efficiency, there are also real health and safety benefits by cutting down on travelling. Also, data collected on smart lock operations can be analyzed to improve operation, to improve security, for trouble-shooting, and so on; these are some advantages for organizations managing thousands of distributed assets or sites.

[004] To attain the highest security standards demanded for such critical infrastructure assets at a secure site, these smart locks need to be supervised or monitored continuously 24x7. In a conventional telco environment using 3G/4G/5G, such a demand requires substantial device power and is thus expensive to operate. Low-power wide-area networks (LPWANs) are now sought to provide 24x7 supervision or monitoring at low data transmission cost and low power consumption. However, building LPWAN capability into large numbers of smart locks is operationally problematic and expensive. An efficient approach to solving this problem is to provide on-site LPWAN gateway devices that communicate in long-range (LR) directly with the operations centres and/or associated server, preferably in real-time, over a LPWAN network, as is disclosed by Applicant in patent application nos. PCT/SG2018/050579 and 10201708266U in Singapore; these gateway devices then supervise or communicate over short-range (SR), (for example, via Bluetooth) centrally with the other smart IoT devices; these smart IoT devices include smart locks and other accompanying smart sensors or actuators, intrusion alarms, motion sensors, security cameras, smoke detectors, and so on; some of these sensors may monitor temperatures of equipment, oil or gas levels of generators, and so on. Utilising a gateway architecture for smart IoT devices' operations means only a single LPWAN subscription is required at a secure site.

[005] The most secure mode of operation of the above smart IoT devices is for the smart gateway device to be operational continuously 24x7 and for every transaction to be conducted in real-time and recorded in the server. However, despite LPWAN networks being designed for high reliability, there will be occasional network outages. There will also be times when the gateway devices fail or possibility of the gateway devices being stolen; yet during such network or gateway device failure, at least the smart locks must remain operational. It can thus be seen that there exists a need to provide secure methods for operating these smart locks or smart IoT devices at all times, be it during normal routine operation or during partial or complete system outage.

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 secure methods or modes for operating smart IoT devices located at critical infrastructure secure sites, which are located over a wide geographical region. At each secure site, the smart IoT devices are supervised by a smart gateway device; the gateway device is centrally located so that it is in short-range (SR) communication with the smart IoT devices and in long-range (LR) communication with an operations centre or a server through a low-power wide-area network (LPWAN). One of the smart IoT devices is a smart lock, which is operable to control access to the secure site; to ensure high security at the secure site, the system's method of transmitting virtual keys and authentication credentials are provided that allow the system to operate in a highly secure manner during normal routine operation and during partial or complete system outage or gateway device failure.

[008] In one embodiment, the present invention provides a smart IoT device operating and monitoring system comprising: a server; an artificial intelligence (AI) module connected to the server; a low-power, wide-area network (LPWAN); a smart lock configured as one of various smart IoT device for controlling a user entry to a secure site; and a smart gateway device supervising the smart lock and the various smart IoT devices located at the secure site; wherein the server, the LPWAN, the smart gateway device, the smart lock/smart IoT devices are in sequential communication links, so that the smart lock and IoT devices operations are monitored continuously 24-hours, 7-days, with a lock operation access scenario selection being controllable by the AI module according to a determined quality of service at the communication links, any cellular communication link and at any other communication link (including an IoT network) that is available at the secure site.

[009] In another embodiment, the present invention provides a method for operating the above smart IoT lock system, with the method comprising: generating an access instance after an access request to the secure site has been approved, where the access instance comprises a user identity, smart lock identity, a scheduled date and time of visit to the secure site; determining a quality of service by the AI module, with the AI module comprising a pre-selection module and a lock operation access scenario selection module, with the pre-selection module determining a historical quality of service of the LPWAN link and the lock operation access scenario selection module determining a current quality of service of all available communication links (including any cellular or IoT network, and any failure of the gateway device or the server); and selecting a lock operation (from so-called access scenarios A-E) according to the determined quality of service at all communication links at the gateway and at the user device.

[0010] Preferably, the user device operates a user application and has communication links to the smart lock, the gateway or the server through the LPWAN, a telco or IoT network. User access includes an approval in the form of an access instance. Also, preferably, the AI module includes a pre-selection module and an access scenario selection module. In one embodiment, the master module is connected to the server whilst a slave module is connected to the gateway device.

[0011] The preselection module determines a historical quality of service of the LPWAN links, whilst the access scenario selection module determines a current quality of service of all communication links available at the secure site.

[0012] Depending on findings of the preselection and access scenario selections modules, the access instance and lock virtual key are sent to the gateway device, the smart lock or the user device application according to any one of access scenarios A-E with differing levels of security as defined in claims 6-11 or 17-21.

[0013] Preferably, during lock operation, the scheduled visit date and time comprised in the access instance are verified against a RTC reference associated with the server, the gateway or the smart lock. A device key manager residing in the server is operable to register, create, remove, renew or update and monitor all the lock virtual keys and to manage sending of the lock virtual keys in coordination with the access scenario selection

module; the device key manager can operate in a centralized mode or a distributed mode depending on whether the server is functioning in real-time.

Brief Description of the Drawings

[0014] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0015] FIG. 1 illustrates a system architecture for implementing smart IoT devices' operations via a gateway device, a LPWAN and a server according to an embodiment of the present invention;

[0016] FIG. 2 illustrates the above smart IoT device operating under a normal routine or scheduled real-time operation with the server, with the IoT device being exemplified by a smart lock and a virtual key being sent to a smart lock during scheduled lock operation;

[0017] FIG. 3 illustrates the above smart lock operating under a scheduled real-time operation with the server with the virtual key being sent to the gateway device in advance of scheduled lock operation;

[0018] FIG. 4 illustrates the above smart lock operation under a scheduled real-time operation with the server with the virtual key being sent to the gateway device in advance of scheduled lock operation, after which the long-range (LR) communication at the gateway device failed;

[0019] FIG. 5 illustrates the above smart lock operation under a scheduled real-time operation with the server with the virtual key being sent to the gateway device in advance of scheduled lock operation, after which both the long-range (LR) and short-range (SR) communications at the gateway device failed; and

[0020] FIG. 6 illustrates the above smart lock operation during a system outage or after the gateway device has failed and the server is updated after lock operation.

Detailed Description

[0021] 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 present invention. For ease of reference, common reference numerals or series of numerals will be used throughout the drawings when referring to the same or similar features common to the drawings.

[0022] FIG. 1 shows an architecture of a secure system 100 for operating smart IoT devices 500 located at an infrastructure site or a secure site. As seen from FIG. 1, the secure system 100 includes a smart gateway device 400 in long-range (LR) communication with a server 200 through a low-power wide-area network (LPWAN) 300; the smart gateway device 400 in turn supervises some smart IoT devices 500, 502, etc. via short-range (SR) communication. An authorized user is able to link up in SR communication with both the smart IoT devices 500, 502, etc. and the gateway device 400. In addition, the server 200 is in cellular communication link 20 with the authorized user device 600 via a telco cellular system 10 or via a co-existing IoT network 302 (such as, SigFox, LoRA, etc.) that may be available at the secure site. As shown, an Operations Centre 201 is linked up in communication with the server 200, whilst the server is supported by a database 202. The Operations Centre 201 is also provided with access rights to records in the database 202, for eg. during protracted communication outage. Connected to the server 200 is an artificial intelligence (AI) module 204 to help control the secure methods or modes of operation of the secure system 100; in another embodiment, an AI module 404 is alternatively connected to the smart gateway device 400; it is also possible that the AI modules are connected to both the server 200 and smart gateway 400, such that the AI module 204 connected to the server is operable as a “master” whilst the AI module 404 is operable on a “slave” relationship. The LPWAN 300 may be configured variously on a SigFox, Lora, NBIoT or similar platform; it is possible the LPWAN 300 and IoT network 302 may share network access or cooperate with one another to provide geographically wide coverage.

[0023] These smart IoT devices 500 include smart lock or padlocks 502 or door locks 504, sensors (such as, temperature and humidity sensors 508, oil or gas level gauges 510, proximity sensors, motion sensors 506, cameras, etc.) or actuators (such as, an intrusion alarm 507). The secure system 100 is now described with a smart lock 502 being used as an example of the smart IoT device 500 together with the AI module 204 connected to the server 200 for ease of illustration, with the following modes of secure operation and security levels:

[0024] Scheduled routine operation with the server and gateway device in real-time communication, where a virtual key is sent to the gateway device only during scheduled lock operation (Access Scenario A): This is the most secure mode of operation and security attributes, including virtual keys, lock identity and site identity, are managed and controlled by the Operations Centre 201, and are stored within the server 200, 202 in real-time. In this secure and real-time mode, operations of all the IoT devices 500, 502, 504, etc. and the gateway device 400 are monitored at the Operations Centre 201 and transactions involved are recorded in the server 200, 202. In other words, communication links in the secure system 100 are in real-time, the gateway device 400 is fully operational and status of the IoT devices 500, 502, 504, etc. are continuously monitored 24x7.

[0025] FIG. 2 illustrates a cycle of process steps of a user requesting access to a secure site, opening a lock 502 to enter the secure site, operating the lock 502 to secure the site after scheduled tasks have been completed, with all communication links being in real-time and status of the IoT devices are recorded in the server 200, 202 as under access scenario A. Referring to FIG. 2, in step 1010, the user requests site access in advance of a scheduled site visit or an appointment using user device 600 application and the access request is sent to the server 200 and the Operations Centre 201; in one embodiment, the access request includes the site identity, and date and time of visit. The access request may be sent in real-time through the LPWAN 300, the IoT network 302, the telco cellular network 10 or the gateway 400, via the user device 600 application, by SMS, email, phone call to an automated application operating in the server 200 or a phone call to the Operations Centre 201. After receipt of the access request, the Operations Centre 201 or the automated application in the server reviews the access request; if approval to access the secure site is granted, the approval is sent, in step 1020, from the Operations Centre 201 to the server

200 in the form of an access instance; the access instance contains the user identity, lock identity, gateway identity, and scheduled date and time of visit. This approved access instance is stored in the server 200, 202 for verification of future entry requests when the registered user attends to the secure site. In addition, in step 1020, the mobile user device 600 is informed of the approved access instance has been created or granted.

[0026] In step 1021, an Access Scenario Pre-selection is made by the AI module 204 considering historical performance of the quality of service of the gateway LR and SR communication links as well as user device 600 connectivity at the location (via the telco cellular network 10 and IoT network 302) and identity of the user who has sent the access request (identity of the user, for e.g. in FIG. 6, off-line virtual keys may be issued only to trusted employees). The artificial intelligence (AI) module 204 connected to the server 200 then makes autonomous access pre-selection decision based on Table 1 below. This access pre-selection in step 1021 thus affects the method of secure operation of the system 100:

[0027] Table 1: Access scenarios A-E pre-selection based on historical performance of communication links with the server 200:

Access Scenario	Mode of Operation	Preferred or Non-preferred operation method	Gateway Long Range + Short Range communications operational performance satisfactory?	Gateway Long Range performance not satisfactory + Short Range communications operational performance satisfactory?	Gateway Long Range + Short Range communications operational performance not satisfactory or not installed?	User Device Application connectivity via Telco or IoT network non-operational at Lock location?
A	On-Line	Preferred	True	False	False	False
B	On-Line	Preferred	False	True	False	False
C ¹	On-Line	Preferred	False	True	False	False
D	On-Line	Non- Preferred	False	False	True	False
E	Off-Line	Non- Preferred	False	False	True	True

[0028] In this specific case, as quality of service is highly reliable, access scenario A has been selected. The historical quality of service of the gateway LR and SR communication links, user device 600 connectivity at the lock location and identity of the user determine the access scenario pre-selection.

[0029] As scheduled, the user attends to the secure site, in step 1030, and logs in to the system 100 with the user device 600 application; in the process, the user identity, user

¹ Note in Access Scenario pre-selection inputs for both scenarios B and C are identical, it is only in the later step 1050 where actual scenario selection occurs does implementation differs.

device identity, lock identity and system password are verified. Initially, the user device 600 application verifies the user identity, user device identity, user device password and system password with user credentials registered in the user device 600 application. At this stage, the authorized user wakes up communication link 520 with the smart lock 502, and the user device 600 application verifies current status and quality of the LPWAN network 300, both SR and LR communications links as well as any other connectivity the user device 600 may support (such as the IoT network 302, which may include SigFox, LoRA, etc.). Once the verification processes are completed, the user device 600 application sends an entry request containing the user identity, user device identity, user system password, lock identity, gateway identity, the communication links quality and status back to the server 200, in step 1030; information is sent either via the LPWAN 300 or cellular communication network 10 or the gateway 400, or the IoT network 302 (e.g. SigFox, LoRA, etc.) depending on operation of these communication links and networks as well as the preferred operation mode the system is configured as. In response, in step 1040, the server 200 authenticates the user credentials from the entry request with the approved access instance registered in the server 200; once the user and site access credentials (including the smart lock and gateway identities) are verified to be true, the server 200 further verifies the scheduled date and time of visit with the server's real-time clock reference (server RTC). If all credential verifications at the server 200 are true, the server 200 gathers identity of the gateway device 400 associated with the smart lock 502 and the AI module 204 interrogates current quality of service and status of the gateway 300 LR and SR communication links as well as user device connectivity in step 1050.

[0030] The current quality of communication service, status of the gateway LR and SR communication links, and user device 600 connectivity at the site location determine the access scenario selection in Table 2, as follow:

[0031] Table 2: Access Method selection using current QoS and status of gateway links and user device connectivity at site location and site configuration:

Access Method Selected	Gateway Installed for associated smart Lock (Gateway registered in Server)?	Long-Range Communication Gateway Intact?	Short-Range Communication Gateway Intact?	Mobile Devices Communication to Server via LPWAN network or Gateway possible at location?	Mobile Devices Communication to Server via Telco or IoT Network possible at location?	Virtual Keys pre-loaded in Gateway?
A	Yes	Yes	Yes		Yes	
A	Yes	Yes	Yes	Yes	No	
B	Yes	Yes	Yes		Yes	Yes

B	Yes	Yes	Yes	Yes	No	Yes
C	Yes	No	Yes		Yes	Yes
C	Yes	No	Yes	Yes	No	Yes
D	Yes	No	No		Yes	
D	Yes	No	No	Yes	No	
D	Yes	Yes	No		Yes	
D	Yes	Yes	No	Yes	No	
D	No				Yes	
D	No			Yes	No	
E	Yes	No	No		No	
E	No			No	No	

The artificial intelligence module 204 connected to the server 200 then makes autonomous access decision based on the current quality of service of the LR and SR communication links, user device connectivity as well as site configuration according to Table 2.

[0032] In step 1050, the AI module 204 queries the LR and SR communication links at the gateway device 400, user device 600 communication links, whether the secure site is gateway equipped, state of any pre-loaded virtual keys in any associated gateway as well as presence of the smart lock 502 with values in truth Table 2 and decides on access scenario A to operate the system 100.

[0033] In response to granting of access scenario A, a virtual key for opening the smart lock 502 is sent, in step 1060, together with the access instance, to both the gateway device 400 and the smart lock 502 via the LR, the SR communication links and the LPWAN 300; sending the virtual key only during scheduled site visit ensures the highest security level of this system 100. In step 1070, the user opens the lock 502 and gains entry to the secure site; this triggers a change of state of a sensor in the smart lock 502 from “locked” to “unlock” and the status change of the lock is sent, in step 1080, to both the gateway device 400 and the server 200; the server then updates the records of the user identity, lock identity, date and time of entry to the secure site. Following step 1080, step 1090 hand-shakes by sending a lock operation confirmation message to the user device 600 application. Once the authorized user has completed the scheduled tasks at the secure site, and before leaving the secure site, operates the lock 502 to lock-up the site, in step 1095, the sensor in the lock sends a “locked status” to both the gateway device 400 and the server 200, and the records of site entry in the server 200 are then updated and the access request made may be indicated as “done”; the cycle of processing ends with the server 200 sending a confirmation of “locked” status at the secure site to the user device 600 application, in step 1096. These transactions performed by the above steps are in real-time and the records are

kept for a predetermined period of time, for example, for data analytics or trouble-shooting. When a user needs access to the secure site to perform some tasks and makes another access request, the above secure system 100 cycles through the process steps 1010 – 1096 again to ensure that only an authorized user can enter the secure site and security demanded at the site is continuously monitored 24x7.

[0034] Scheduled routine operation with the server and gateway device in real-time communication and the virtual key is being sent in advance to the gateway device (Access Scenario B): In this access scenario B, the current quality of service of the LR communication link has dropped, say from 99% to 90%, and the AI module 204 connected to the server 200 is programmed to pre-select access scenario B, in step 1021, basing on truth Table 1. To overcome this deficiency, in step 1022, the virtual key and the access instance (containing the user identity, lock identity, gateway device identity, and scheduled date and time of visit) are now sent in advance of the scheduled visit directly to the gateway device 400, as shown in FIG. 3; as will be understood, sending the virtual key and access instance to the gateway device 400 in advance of the scheduled visit still ensures a high security but at a level lower than for Access Scenario A. As in Access Scenario A, all communication links remain in real-time and the status of the smart lock 502 are recorded in the server 200, 202. Following step 1022, in step 1024, confirmation of receipt of the virtual key and access instance are sent from the gateway device 400 to the server 200. Process steps 1010, 1020 and 1021 for requesting access, access approval and access pre-selection are identical to those described under access scenario A and will not be described again.

[0035] As shown in FIG. 3, the authorized user attends to the site visit, and steps 1030, 1040 and step 1050 are executed identically to those described under access scenario A and therefore will not be described again.

[0036] Within access scenario selection step 1050, as in access scenario A, the AI module 204 polls the current quality of service of the various communication links and finds that the LR communication link at the gateway 400 which historically was deficient is currently still intact with sufficient quality and thus selects access scenario B; following which, in step 1061, after credential verifications, the server 200 sends an authorization to the gateway device 400 to issue the virtual key and the access instance to the smart lock 502.

The user at the secure site turns on the user device 600 application and sends a “lock open” command to the smart lock 502, in step 1070; the smart lock sensor responds, in step 1080, and step 1090 handshakes lock “open” operation with the user device application. After the authorized user has completed the scheduled tasks and locked up the secure site, in step 1095, the lock sensor sends a “locked” status to both the gateway device 400 and the server 200, and records of site entry in the server 200 are then updated and the access request is updated to “done”; the cycle of processing ends with the server 200 sending a confirmation of “locked” status at the secure site to the user device 600 application, in step 1096.

[0037] Scheduled routine operation with the server and gateway device in real-time communication and after virtual key has been sent in advance to the gateway device, the LR link failed (Access Scenario C): This access scenario C is a progression from the previous access scenario B, in that the LR communication link is historically deficient and after the virtual key and access instance to open the smart lock 502 had been sent to the gateway device 400 in advance of the site visit and the entry request, the LR communication link at the gateway failed. FIG. 4 illustrates the process steps involved in access scenario C.

[0038] Steps 1010, 1020, 1021, 1022, 1024, 1030 and 1040 are as described above and will not be described again. In step 1050, the AI module 204 interrogates current quality of service of the various communication links and finds that LR communication link has deteriorated; subsequently, during user and entry request authentications, the LR communication link is either non-functional or functioning but at a lower quality and reliability than in access scenario B; thus, in step 1050, with the LR communication link having failed or deteriorated (as shown in truth Table 2), the system 100 progresses to execute step 1062 by the server 200 sending the access instance to the user device 600 application according to access scenario C. The user device 600 application then sends, in step 1063, the user identity and the lock identity to the gateway device 400 via the SR communication link; in the gateway device 400, the user and the lock identities are verified against the approved access instance stored in the gateway 400 and the entry date and time are checked against the gateway RTC, in step 1064; once these verifications are true, the gateway device 400 sends the virtual key, in step 1065, to the registered smart lock 502. In step 1070, the authorized user attends to the site and opens the smart lock 502 to enter the secure site. The sensor in the smart lock 502 responds, in step 1072, by sending a changed

status to the gateway device 400 via the SR communication link; the gateway device 400, then, confirms the lock “open” operation in step 1073 and, in step 1080, the lock “open” status is sent to the server 200 from the user device 600 application (for eg. via the LPWAN 300, the telco cellular or the IoT network, given that the LR communication link at the gateway 400 has failed or has deteriorated performance); the server 200 then updates records of the user identity, lock identity, and the date and time of entry to the secure site; in step 1090, a lock “open” confirmation message is sent from the server 200 to the user device 600 application. After user has completed the scheduled tasks and locked up the secure site, in step 1095, the lock sensor sends a “locked” status to both the gateway device 400 and the server 200, and the records of site entry in the server 200 are then updated and the access request is updated to “done”; the cycle of processing ends with the server 200 sending a confirmation of “locked” status, in step 1096, at the secure site to the user device 600 application.

[0039] In access scenario C, the virtual key and access instance being sent to the gateway device 400 in advance of the scheduled visit still ensures a high security but at a level lower than for access scenario A, even after the LR communication link at the gateway 400 has failed or deteriorated. As in access scenarios A and B, all communication transactions remain in real-time and the status of the smart lock 502 is monitored continuously.

[0040] Scheduled routine operation between the server and user device application in real-time and after the virtual key to the lock has been sent to the gateway device, both the LR and SR link at the gateway device failed or deteriorated (Access Scenario D): As in the above processes, steps 1010, 1020, 1021, 1022 and 1024 involve user requesting access to a secure site and after verification and approval, an access instance and lock virtual key are sent to the gateway 400 in advanced of the scheduled visit. In step 1030, the authorized user attends to the secure site, turns on the user device 600 application and sends an entry request to the server 200 via the LPWAN 300, the telco cellular 10 or the IoT 302 network; in response, in step 1040, the server 200 authenticates the user credentials from the entry request with the credentials registered in the server 200; once the user identity and the access instance are verified to be true, the server 200 further verifies the entry date and time with the server’s real time clock (server RTC) reference. If all credential verifications at the server 200 are true, the server gathers identity of the gateway device 400 associated with the smart lock 502 and interrogates states of operation of the

gateway LR and SR, user device communication and presence of the smart lock 502, in access scenario selection step 1050. So, in step 1050, the AI module 204 detects that the gateway device 400 has failed and/or missing, and thus selects access scenario D based on the truth Table 2.

[0041] As shown in FIG. 5, in step 1066, the virtual key and the access instance are sent from the server 200 to the user device 600 application as well as instructions to use access scenario D; in response, in step 1067, the virtual key and the access instance are sent to the registered smart lock 502 and, in step 1068, the access instance, and access date and time are verified against the smart lock RTC. Once the access instance is determined to be true, the lock is unlocked, in step 1070. An “open” status of the smart lock 502 is sent back to the user device 600 application, in step 1075. The lock “open” status is also sent to the server 200, in step 1080, via the LPWAN 300, the telco cellular 10 or IoT 302 network; in response, the server 200 then updates records of the user identity, lock identity, date and time of entry at the secure site and, in step 1090, a lock “open” confirmation message is sent from the server 200 to the user device 600 application. After user has completed the scheduled tasks and locked up the secure site, in step 1095, the lock sensor sends a “locked” status to the server 200; the records of site entry are then updated in the server 200 and the access request is updated to “done”; the cycle of processing ends with the server 200 sending a confirmation of “locked” status, in step 1096, at the secure site to the user device 600 application. In access scenario D, even when the gateway device 400 has failed or missing after the access request has been approved, all the process steps are still monitored in real-time and security at the secure site is still maintained.

[0042] Operation of the system 100 not in real-time (Access Scenario E): FIG. 6 shows the system 100 operations under access scenario E. In access scenario E, after a user has requested access to a secure site and approval has been granted, as in steps 1010 and 1020, the server 200, the LPWAN 300 and the gateway device 400 failed. A predetermined period after the access approval has been granted and the AI module 204 has failed to respond or has sent out an alert, the Operations Centre 201 generates an off-line virtual key for the registered smart lock 502, in step 1026, by activating an off-line subroutine application, and, in step 1027, the virtual key and access instance are sent to the user device 600 application in advance of the site visit, via the telco cellular 10 or the IoT network 302. Upon receipt of the virtual key and access instance by the user device 600

application, a confirmation message is sent, in step 1028, to the Operations Centre 201. After the authorized user has reached the secure site, and turns on the user device 600 application and sends, in step 1030, an entry request and a lock “open” command to the registered smart lock 502; in a following step, step 1065, the virtual key and access instance are sent to the registered lock 502. As shown in FIG. 6, after the user identity, the lock identity and the access instance verification against the lock RTC are established to be true or valid, and the user sends a “lock open” command to open the smart lock 502, in step 1070, and gain entry to the secure site. The sensor in the smart lock 502 then responds, in step 1075, with an “unlock” status to the user device 600 application. After the user has completed the scheduled tasks and locked up the secure site, in steps 1076 and 1077, the lock sensor sends a “locked” status update, in step 1079, to the user device 600 application. After the server 200 operation has been restored, the user device 600 application connects up with the server 200, in step 1080, and, in step 1090, the server 200 acknowledges to the user device 600 application of successful upload; the server 200 follows up by updating records of site visit and changing the access request status as “done”; the above system 100 of cycle of processing ends, and the server 200 waits for the next cycle of a user making another access request.

[0043] In a variation of the above, it is possible that in access scenario E, the server 200 remains operational after performing steps 1010 and 1020; in this variation, the server 200 is programmed to generate an off-line virtual key for the registered smart lock 502 and to send the virtual key and access instance to the user device 600 application in advance of the site visit, via the telco cellular 10 or the IoT network 302. The following steps from 1028 to 1090 are then executed to complete the above system 100 operation cycle under access scenario E.

[0044] In the above description, the access scenarios A-E are operational in terms of differing security levels. Access scenario A is the most secure lock operation where the lock virtual keys and the access instances are stored within the server 200 until the registered user has reached the secure site and sent a “lock open” command from the user device application; effectively, all control and decision making are done from the Operations Centre 201 and the server 200 in real-time at all times, the gateway device 400, the IoT devices 500, 502, etc. are monitored and their operation statuses are stored in the

server 200; the term “in real time” means that the server 200 and the Operations Centre 201 know the status of the smart locks 502 in real-time. In addition, the lock virtual key is sent to the gateway only during the scheduled date and time defined in the access instance, thus making the system very secure.

[0045] Access scenario B would be selected by the AI module 204 if the LR communication with the gateway device 400 has a history of deteriorated performance. This is to ensure that if during the scheduled access should the LR communications again failed or deteriorated, then since the lock virtual key and access instance have been received by the gateway device 400, the smart lock 502 can still be operated as per access scenario B. In this specific case when the user attends to the secure site and the LR communications is found to be reliable, the AI module 204 would choose to use access scenario B. Effectively, lock operation is still controlled from the Operations Centre 201 or server 200 in real-time before the authorized user visits the secure site defined in the access instance.

[0046] Access scenario C is a progression from access scenario B where the LR communication at the gateway 400 failed or deteriorated after receipt of the lock virtual key and access instance in the gateway 400. When the truth Table 2 is found to be true, the AI module 204 selects access scenario C, the gateway 400 is then approved to send the virtual key it contains to the registered smart lock 502. All the lock operations remain in real-time (albeit, via cellular 10, the LPWAN 300 communication link or the IoT network 302 with the server 200).

[0047] Access scenario D is a progression from access scenario C where the gateway 400 failed or deteriorated (e.g. no LR and SR communication links) after gateway 400 receipt of the lock virtual key and access instance; access scenario D can also happen where the gateway 400 is missing or stolen after gateway 400 receipt of the lock virtual key and access instance. When the truth Table 2 is found to be true, the AI module 204 selects access scenario D and the lock virtual key and the access instance are sent directly to the user device 600 application, and all the lock operations remain in real-time (albeit, via cellular 10, the LPWAN 300 communication or the IoT network 302 with the server 200).

[0048] Access scenario E happens after an access request has been sent to both the server 200 and the Operations Centre 201 via the telco cellular 10, the LPWAN 300, or IoT network 302, and the system 100 responds with an approval, after which all the LPWAN 300, the telco cellular 10 and the network 302 links failed. The AI module 204 detects failure of all the LPWAN 300, the telco cellular and the IoT network links, and then selects access scenario E for emergency lock operation by generating an off-line virtual key and access instance; these off-line virtual key and access instance are sent to the user device 600 application after this emergency situation has occurred. After the user attends to the associated secure site and makes an entry request, the smart lock 502 responds appropriately. After the site visit, all the lock operations are loaded to the server 200 from the user device 600 application once any communication link to the system 100 is restored and the user device 600 application is re-connected to the server 200.

[0049] Under access scenario E, the lock's off-line virtual key and access instance are sent to the user device 600 application, but the server 200 or the Operations Centre 201 is unable to monitor status of the IoT devices 500, in particular the smart lock 502, until the user device 600 is logged-in to the system 100 again; this creates a security concern in that the user device 600 can be stolen or the user becomes rogue and security at the relevant secure site may thus be compromised; to address this security issue, in one embodiment, access scenario E may be reserved only for users who are trusted employees. To ensure that security at the secure site is not compromised in any manner, the above system 100 has a purge routine to purge all the virtual off-line keys and access instances that had expired and are stored in the gateway device 400 and smart IoT devices 500, 502, etc. In another embodiment, it is possible that the virtual off-line keys are re-authorized in the trusted employees' user device 600 for use only during an emergency situation when there is a protracted system (the LPWAN 300, the telco cellular 10 or the IoT network 302) outage; such re-authorization process can be done by a dynamic key management process, either via a centralized mode or a distributed mode by an IoT device key manager that is operable in the server 200. In the centralized mode, the off-line virtual keys are changed or renewed only when the user visits the relevant secure site and makes an entry request; with this centralized mode, the smart locks 502 are woken-up from a sleep mode for access entry so as to conserve battery power. In the distributed mode, the off-line virtual keys are changed or renewed in a progressive manner after the system 100 has been restored from an outage.

These changes or renewal of the off-line virtual keys are performed transparently from the users.

[0050] Records of the smart IoT operations are stored in the server 200 for a predetermined period of time to allow the system to perform operational data analytics or to investigate any past incident. These records containing the access instances are controlled by the server real-time clock reference (server RTC).

[0051] In addition, each of the smart gateway device and the IoT devices 500, 502, etc. has its own real-time clock reference (namely, gateway RTC, smart lock RTC, intrusion alarm RTC, etc.). These device RTCs are programmed to purge the virtual keys and the access instances once the scheduled time and date had expired; if the scheduled date and time have not expired, the virtual keys can be renewed or recycled by the device key manager.

[0052] 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 example, in the description, we describe a user making an access request from one's device application. Alternatively, it is possible that the system 100 is automated, site visits are scheduled by the Operations Centre 201 and the access instances are notified to the authorized users at their user devices. Alternatively, it is also possible that an unregistered user makes a voice call to the Operations Centre 201 and once the user identity is verified (for example, via video), an access instance can be sent to the user device application. For added security, each of the secure site is also supervised by a motion sensor 506 and an intrusion alarm 507. Whilst a smart lock has been used in the above description, the system 100 is also used to monitor the various smart IoT devices 500 deploy at the secure site; for example, the door lock 504 is used to send status and date/time of door opening or closing to the server 200; the temperature and humidity sensor 508 is used to monitor the environmental conditions, and the fuel level gauge 510 is used to monitor the fuel level at an associated generator set.

CLAIMS:

1. A smart IoT device operating and monitoring system comprising:
 - a server;
 - an artificial intelligence (AI) module connected to the server;
 - a low-power, wide-area network (LPWAN);
 - a smart lock configured as one of various smart IoT device for controlling a user entry to a secure site; and
 - a smart gateway device supervising the smart lock and the various smart IoT devices located at the secure site;

wherein the server, the LPWAN, the smart gateway device, the smart lock/smart IoT devices are in sequential communication links, so that the smart lock and IoT devices operations are monitored continuously 24-hours, 7-days, with a lock operation access scenario selection being controllable by the AI module according to a determined quality of service at the communication links, any cellular communication link and at any other communication link (including an IoT network) that is available at the secure site.
2. The system according to claim 1, further comprising a user device with communication links to the smart lock, the gateway and the LPWAN, or through a telco cellular or any other available communication link (including the IoT network) to the server, wherein the user device is operable with a user device application.
3. The system according to claim 2, wherein controlling the user access to the secure site comprises obtaining an approval for access to the secure site, where the approval comprises an access instance, which contains the user identity, the smart lock identity, the gateway identity and scheduled date and time of visit, is sent to the user device application.
4. The system according to any one of claims 1-3, wherein the AI module comprises a pre-selection module and a lock operation access scenario selection module, with the pre-selection module determining a historical quality of service of the LPWAN link and the lock operation access scenario selection module determining a current quality of service of all the available communication links (including any failure of the gateway device or the server) at the secure site.

5. The system according to any one of claims 1-4, where the AI module comprises a master module connected to the server and a slave module connected to the gateway device.
6. The system according to claim 4 or 5, wherein, when the preselection and the lock operation access scenario selection modules determine that the server and the gateway device are functioning reliably, the access instance and a lock virtual key are sent to the gateway device (in so-called access scenarios A) after a user has reached the secure site and sent an entry request, in order to maintain a highest level of security.
7. The system according to claim 6, further comprising the user device application connecting with the server and being authenticated by the server, before the access instance and the lock virtual key are sent to the smart lock for user entry to the secure site.
8. The system according to claim 4 or 5, wherein, after the preselection and the lock operation access scenario selection modules determine that the server and the gateway device are functioning but the gateway device has a history of deteriorated reliability, the access instance and a virtual key are sent to the gateway device (in so-called access scenario B) after a user has made an access request to the secure site, an access approval has been given and prior to the user reaching the secure site or making an entry request.
9. The system according to claim 4 or 5, wherein, after the preselection and the lock operation access scenario selection modules determine that the server and the gateway device are functioning, the access instance and the lock virtual key are sent to the gateway device, and a LR communication link between the gateway device and the server is later found to be unreliable by the lock operation access scenario selection module (in so-called access scenario C), the server sends the access instance directly to the user device application for user entry to the secure site after the user has made an access request to the secure site, an access approval has been given and prior to the user reaching the secure site or making an entry request.
10. The system according to claim 4 or 5, wherein, after the preselection and the lock operation access scenario selection modules determine that the server and the gateway

device are functioning, the access instance and the lock virtual key are sent to the gateway, after which the gateway device is found by the lock operation access scenario selection module to be defective or absent (in so-called access scenario D), the server then sends the access instance and the lock virtual key directly to the user device application for user entry to the secure site after the user has made an access request to the secure site, an access approval has been given and prior to the user reaching the secure site or making an entry request.

11. The system according to claim 4 or 5, wherein, after the gateway device and all available communication links are found to be out of working order due to an outage, an off-line lock virtual key is created at an operations centre connected to the server or at the server and the off-line lock virtual key is then sent directly to the user device application for user entry to the secure site (in so-called access scenario E) after a user has made an access request to the secure site, an access approval has been given and prior to the user reaching the secure site or making an entry request.

12. The system according to claim 11, wherein the off-line virtual key is kept in the user device of only trusted employees and the off-line virtual key is dynamically changed or renewed after the communication link outage has been restored.

13. The system according to any one of claims 6-12, wherein the scheduled visit date and time comprised in the access instance are verified against a real-time clock reference (RTC) associated with the server, the gateway or the smart lock after the user has sent a “lock open” command from the user device application to the lock and before lock “open” operation is granted, and after the user has locked up the secure site after the scheduled visit, the respective RTC is used to purge the access instance from the server, the gateway device or the smart lock after the scheduled visit date and time have expired.

14. The system according to any one of claims 6-13, further comprising a device key manager residing in the server, wherein the device key manager is operable to register/create/remove, renew, update and monitor all the lock virtual keys, and to manage distribution of the lock virtual keys in coordination with the access scenario selection in the AI module.

15. The system according to claim 14, wherein the device key manager is operable either in a centralized mode (when the server is functioning in real-time) or in a distributed mode (when the server is non-functioning in real-time).

16. A smart IoT lock system comprising a server, an artificial intelligence (AI) module connectable to the server, a low-power wide-area network (LPWAN), a smart gateway device located in a secure site, and a smart lock for controlling a user entry to the secure site, such that the server, the LPWAN, the smart gateway device and the smart lock are in sequential communication links, so that the smart IoT lock operation method comprises:

generating an access instance after an access request to the secure site has been approved, where the access instance comprises a user identity, smart lock identity, a scheduled date and time of visit to the secure site;

determining a quality of service by the AI module, with the AI module comprising a pre-selection module and a lock operation access scenario selection module, with the pre-selection module determining a historical quality of service of the LPWAN link and the lock operation access scenario selection module determining a current quality of service of all available communication links (including any cellular or IoT network, and any failure of the gateway device or the server); and

selecting a lock operation (from so-called access scenarios A-E) according to the determined quality of service at all communication links at the gateway and at the user device.

17. The method according to claim 16, wherein, in access scenario A:

after the preselection module determining that the server and the gateway device are functioning reliably; and

polling a quality of service of the communication links at the server, the gateway device and the smart lock, and if all the communication links are found to be reliable, sending an access instance and a lock virtual key to the gateway device after a user has reached the secure site and user has sent an entry request, in order to maintain a highest level of security.

18. The method according to claims 16, wherein, in access scenario B:

after the preselection module determining that the server and the gateway device are functioning but the gateway device has a history of deteriorated reliability; and

polling a quality of service of the communication links at the server, the gateway device and the smart lock, and if all the communication links are found to be reliable, sending the access instance and a virtual key to the gateway device after the user has made an access request to the secure site, an access approval has been given, and prior to the user reaching the secure site or making an entry request.

19. The method according to claim 16, wherein in access scenario C:

after the preselection module determining that the server and the gateway device are functioning; and

polling a quality of service at a LR communication link between the gateway device and the server, and if found to be unreliable by the lock operation access scenario selection module, sending the access instance directly to the user device application from the server, after the user has made an access request to the secure site, an access approval has been given, and prior to the user reaching the secure site or making an entry request.

20. The method according to claim 16, wherein in access scenario D,

after the preselection and the lock operation access scenario selection modules determining that the server and the gateway device are functioning, sending the access instance and the lock virtual key to the gateway; and

polling a quality of service of communication links at the gateway device and if found by the lock operation access scenario selection module to be defective or the gateway device is missing, sending the access instance and the lock virtual key directly to the user device application from the server after the user has made an access request to the secure site and an access approval has been given, and prior to the user reaching the secure site and making an entry request.

21. The method according to claim 16, wherein in access scenario E,

after the gateway device and all available communication links are found to be out of working order due to an outage, creating an off-line lock virtual key at an operations centre connected to the server or at the server and sending the off-line lock virtual key

directly to the user device application, prior to the user reaching the secure site or making an entry request.

22. The method according to claim 21, further comprises renewing or recycling the off-line virtual key stored in the user device after the system outage is restored, either via a centralized mode or a distributed mode.

23. The method according to any one of claims 17-22, further comprises:

verifying the scheduled visit date and time comprised in the access instance against a real-time clock reference (RTC) associated with the server, the gateway or the smart lock after the user has sent a “lock open” command from the user device application to the lock and before lock “open” operation is granted; and

purging the access instance from the server, the gateway device or the smart lock after the respective RTCs have expired.

24. The method according to any one of claims 17-23, keeping records of the lock operations in the server for a predetermined period of time for data analytics or for investigative tracing.