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).~~

1~~16~~. A smart IoT ~~lock system~~device operating method 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 IoT device including 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 device ~~lock~~ operation method comprises:

generating an access instance after an access request to the secure site has been approved, wherein the access instance comprises a user identity, gateway 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 historical determined quality of service at all the communication links at the gateway and at ~~the~~a user device, from the following scenarios:

scenario A, wherein the server and the smart gateway device are functioning reliably, the access instance and a lock virtual key are sent only after the user has reached the secure site and sent an entry request to the server; or

scenario B, wherein the server and the smart gateway device are functioning but the smart gateway device has a history of deteriorated reliability, the access instance and a lock virtual key have been sent to the smart gateway device; or

scenario C, wherein the server and the smart gateway device are functioning, the access instance and a lock virtual key have been sent to the smart gateway device, and a long range (LR) communication link between the server and the smart gateway device is later found to be unreliable by the lock operation access scenario selection module; or

scenario D, wherein the server and the smart gateway device (400) are functioning, the access instance and a lock virtual key have been sent to the smart gateway device, after

which the smart gateway device is found to be defective or absent by the lock operation access scenario selection module; or

scenario E, wherein after the smart gateway device and all the available communication links thereto are found to be out of working order due to an outage or non existent.

217. The method according to claim 116, wherein, in access scenario A:

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

polling a current quality of service of the communication links at the server, the smart gateway device, the user device and the smart lock by the lock operation access scenario selection module, and if all the communication links are found to be reliable, sending ~~an~~the access instance and ~~a~~the lock virtual key to the gateway device after a user has made an access request to the secure site, and an access approval has been given, and after ~~a~~the user has reached the secure site and the user has sent an entry request, sending the lock virtual key from the smart gateway device to the smart lock, in order to maintain a highest level of security access; and

upon access completion, sending lock operation confirmation to the server.

318. The method according to claim~~s 16~~ 1, 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 current quality of service of the communication links at the server, the smart gateway device, the user device and the smart lock by the lock operation access scenario selection module, and if all the communication links are found to be reliable, sending the access instance and ~~a~~the virtual key to the smart gateway device after ~~the~~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~~ after the user has reached the secure site and the user has sent an entry request, sending the lock virtual key from the smart gateway device to the smart lock; and

upon access completion, sending lock operation confirmation to the server.

419. The method according to claim 116, wherein in access scenario C:

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

polling a current quality of service at ~~a~~the LR communication link between the smart gateway device and the server by the lock operation access scenario selection module, 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~~, after the user has reached the secure site and the user has sent the user and lock identities to the smart gateway device, sending the lock virtual key from the smart gateway device to the smart lock; and

upon access completion, sending lock operation confirmation to the gateway, the user device and the server.

5~~2~~0. The method according to claim 1~~1~~6, 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 current 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~~ after the user has reached the secure site and the user device has sent the access instance to the smart lock, sending the lock virtual key to the smart lock; and

upon access completion, sending lock operation confirmation to the user device and the server.

6~~2~~1. The method according to claim 1~~1~~6, 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~~and after the user has reached the secure site and the user device has sent an

entry request and the access instance to the smart lock, sending the lock virtual key to the smart lock; and

upon access completion, sending lock operation confirmation to the user device and the server after the use device obtains connectivity to the server.

7. The method according to claim 1, wherein in access scenario E,

creating an off-line lock virtual key by the AI module and sending the off-line lock virtual key directly to the user device, and after the user has reached the secure site and the user device has sent an entry request and the access instance to the smart lock, sending the lock virtual key to the smart lock; and

upon access completion, sending lock operation confirmation to the user device and the server after the use device obtains connectivity to the server.

8~~22~~. The method according to claim 6 or 7~~21~~, further comprises ~~renewing or recyclingpurging~~ 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.

9~~23~~. The method according to any one of claims 2-5~~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 smart gateway device or the smart lock after the user has sent a “lock open” command from the user device ~~application~~ to the smart lock and before lock “open” operation is granted; and

purging the access instance from the server, the smart gateway device or the smart lock after the respective ~~RTCs~~scheduled visit date and time have expired.

10~~24~~. The method according to any one of claims 2-9~~17-23~~, keeping records of the IoT device~~lock~~ operations in the server for a predetermined period of time for data analytics or for investigative tracing.

11. The method according to any one of the preceding claims, further comprises:

maintaining the IoT devices, which comprises an intrusion detector, an alarm, a temperature and humidity sensor and a fuel level gauge.