CLAIMS:

1. A smart IoT device operation method directed to 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 operation method comprises:

a user sending an access request to the server;

the server generating an access instance after the 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 all available communication links, including any cellular or IoT network; and

selecting a lock operation according to the historical determined quality of service at all the communication links at the gateway and at 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 are 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 are 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 are functioning, the access instance and a lock virtual key are 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.

2. The method according to claim 1, wherein, in access scenario A:

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 lock virtual key from the smart gateway device to the smart lock after the user has sent the entry request to the smart gateway device, in order to maintain a highest level of security access; and

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

3. The method according to claim 1, wherein, in access scenario B:

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 the lock virtual key to the smart gateway device after the user has reached the secure site and the user has sent the entry request, and 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.

4. The method according to claim 1, wherein in access scenario C:

polling a current quality of service at 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 from the server, and , after the user has reached the secure site and the user has sent both 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. The method according to claim 1, wherein in access scenario D,

polling a current quality of service of communication links at the smart gateway device and if found by the lock operation access scenario selection module to be defective or the smart gateway device is missing, sending the access instance and the lock virtual key directly to the user device from the server, and 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. The method according to claim 1, wherein in access scenario E,

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

upon access completion, sending lock operation confirmation to the user device and the server after the user 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 the entry request and the access instance to the smart lock, sending the off-line lock virtual key to the smart lock; and

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

8. The method according to claim 6 or 7, further comprises purging the off-line lock virtual key stored in the user device after the system outage is restored, either via a centralized mode or a distributed mode.

9. The method according to any one of claims 2-5, 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 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 scheduled visit date and time have expired.

10. The method according to any one of claims 2-9, keeping records of the IoT device 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 smart IoT devices, which comprises an intrusion detector, an alarm, a temperature and humidity sensor and a fuel level gauge.