

Methods, Medium, IoT Device, Block Chain Platform and IoT System for Recording Transportation Data of Object

FIELD

5 The present disclosure generally relates to the field of Internet of Things (IoT), and particularly to methods, medium, an IoT device, a block chain platform and an IoT system for recording transportation data of an object.

BACKGROUND

10 Currently, with the improved requirements to various kinds of cargoes and the development of logistics transportation network, cold chain has become a popular manner of transportation, especially for some cargoes that were not able or not easy to be transported for a long distance. For example, some fresh foods such as vegetables, fruits and meat and some processed foods such as quick-frozen foods and milk products could be delivered from
15 their places of production even thousands of miles away to local supermarkets or customer's homes through cold chain transportation. Furthermore, some medicines and medical equipments that should be kept in a low temperature may also need to transfer from one place to another through cold chain transportation. The cold chain transportation may be through one of highways, waterways, railways and airways, or may be a composite of
20 multiple different transportation manners. During the whole transportation, including all the procedures of loading and unloading, altering transportation manner or change packaging plants, the object to be transported should be kept at a certain temperature.

 In current cold chain transportation, temperature detection devices are used to detect and record temperatures of respective locations, such as the warehouse at the place of
25 production, the transportation facility (such as the refrigerator car) and the destination (such as the supermarket store or the distribution site).

SUMMARY

 However, since the current temperature detection devices use a common temperature
30 sensor without identification, the finally provided temperature data may have been tampered with. For example, in many refrigerator cars, the temperature detection device is fixed in the compartment and is powered by the vehicle itself. During the long transportation, it is possible for the driver to turn off the power supply to the refrigerator compartment for power saving but keep the reading of the temperature detection device constant. Thus, when the
35 cargo arrives at the destination, a series of constant temperature values that meet the requirements are obtained from the temperature detection device, but in fact, the cargo does

not always stay at that temperature value during the transportation.

Furthermore, in the current temperature detecting and recording process, it is usually only possible to detect the environment temperature at a specific point of each location (such as the warehouse, the transportation facility and the destination) and the temperature of the cargo itself may not be detected in a very close distance.

Further, in the current cold chain transportation, the temperature data is read out from the temperature detection device upon reaching the destination and transmitted to a central database, and thus the data in such a database is easily tampered with and deleted, resulting in unreliable data.

In addition to the cold chain transportation, for the transportation of some other special cargoes, such as fragile items, various data during the transportation of the cargoes should be continuously recorded to ensure that the transportation conditions always meet the requirements.

In view of at least one of the above problems, the present disclosure proposes a method and an IoT device for recording transportation data of an object and an IoT system including such an IoT device.

According to a first aspect of the present disclosure, an IoT device for recording transportation data of an object is provided. The IoT device has been one time programmed with a private key in a manufacturing process of the IoT device. The IoT device includes: at least one sensor configured to detect external environment data of the object during transportation of the object; and a processor configured to receive the data from the sensor and generate a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature generated based on the unique identification number and the data.

According to a second aspect of the present disclosure, a method for recording transportation data of an object is provided. The method includes receiving external environment data of the object detected during transportation of the object from at least one sensor of an IoT device, the IoT device having been one time programmed with a private key in a manufacturing process of the IoT device; and generating a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature generated based on the unique identification number and the data.

According to a third aspect of the present disclosure, a nonvolatile computer readable medium for recording transportation data of an object is provided. The nonvolatile computer readable medium includes computer program codes for receiving external environment data of the object detected during transportation of the object from at least one sensor of an IoT

device, the IoT device having been one time programmed with a private key in a manufacturing process of the IoT device; and computer program codes for generating a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature generated based on the unique identification number and the data.

According to a fourth aspect of the present disclosure, a block chain platform for recording transportation data of an object is provided. The block chain platform includes an underlying block chain; and an application server or a smart contract entity configured to receive a data packet from an IoT device, authenticate the data packet based on a public key of the IoT device and store the data of the data packet to the underlying block chain upon a successful authentication.

According to a fifth aspect of the present disclosure, a method for recording transportation data of an object is provided. The method includes receiving a data packet from an IoT device; authenticating the data packet based on a public key of the IoT device; and storing the data of the data packet to the underlying block chain upon a successful authentication.

According to a sixth aspect of the present disclosure, a nonvolatile computer readable medium for recording transportation data of an object is provided. The nonvolatile computer readable medium includes computer program codes for receiving a data packet from an IoT device; computer program codes for authenticating the data packet based on a public key of the IoT device; and computer program codes for storing the data of the data packet to the underlying block chain upon a successful authentication.

Compared with conventional IoT devices and systems for recording transportation data of an object, the solution of the present disclosure may ensure accurate detecting and recording of the transportation data of the object and may prevent the data from being tampered with.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure will be understood better and other objectives, details, features and advantages of the present disclosure will become more evident from the description of specific embodiments of the disclosure given in conjunction with the following figures, wherein:

Fig.1 illustrates a structure block diagram of the IoT device for recording transportation data of an object according to the present disclosure;

Fig. 2 illustrates a flow chart of a method for recording transportation data of an object according to the present disclosure ;

Fig.3 illustrates a schematic view of the IoT system for recording transportation data of an object according to the present disclosure;

Fig. 4A illustrates a block diagram of the block chain platform according to one embodiment of the present disclosure;

Fig. 4B illustrates a block diagram of the block chain platform according to another embodiment of the present disclosure; and

Fig. 5 illustrates a flow chart of a method for recording transportation data of an object according to the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present disclosure will now be described in more detail in conjunction with accompanying figures. Although embodiments of the present disclosure are shown in the accompanying figures, it should be understood that the present disclosure can be embodied in various ways but not be limited to the embodiments depicted herein. Instead, the embodiments are provided herein to make the disclosure more thorough and complete and convey the scope of the present disclosure to those skilled in the art.

Fig.1 illustrates a structure block diagram of the IoT device 10 for recording transportation data of an object according to the present disclosure. As shown in the Fig. 1, the IoT device 10 includes at least one sensor 12 and a processor 14. The sensor 12 is configured to detect the external environment data of the object during transportation of the object.

The sensor 12 may be any one or combination of several of an environmental sensor, a motion sensor, a gas sensor and a location sensor as described below.

In one implementation, the sensor 12 may be an environmental sensor such as a temperature sensor, a humidity sensor or an air pressure sensor. For example, in the cold chain transportation as described in the background, when transporting fresh foods such as vegetables, fruits or meat and milk products, the temperature and humidity during the transportation is significantly important for the quality of the cargoes. Therefore, the temperature sensor and/or the humidity sensor may be adopted for the sensor 12 to monitor the temperature and/or humidity of the cargoes during the transportation. As another example, some cargoes should be transported under a certain air pressure such as a low air pressure or a high air pressure, in which case the air pressure sensor may be adopted for the sensor 12 to monitor the air pressure during transportation of the cargoes.

In another implementation, the sensor 12 may be a motion sensor (or an inertial sensor) such as a gyroscope, an acceleration sensor or a compass sensor. For example, for some fragile items, the acceleration or shock during the transportation should be monitored,

in which case the acceleration sensor may be adopted for the sensor 12.

In yet another implementation, the gas sensor includes sensors for detecting various gases such as carbon monoxide (CO), carbon dioxide (CO₂), formaldehyde like gases, which may be gas sensors utilizing various principles. For example, to transport some cargoes sensitive to certain gas, a gas sensor for monitoring the concentration of such gas may be adopted for the sensor 12.

Furthermore, the sensor 12 may also be a location sensor such as Global Positioning System (GPS) sensor for detecting the location and trajectory of cargoes during the transportation.

Fig. 2 illustrates a flow chart of a method 100 for recording transportation data of an object according to the present disclosure. The method may be implemented by the processor 14 shown in Fig. 1, for example. The method 100 is described hereinafter in connection with Fig. 1 and Fig. 2.

The processor 14 may be configured to receive the detected external environment data from the sensor 12 (step 102). Unlike conventional IoT devices, the IoT device 10 according to the present disclosure has a unique identification number and is associated with a pair of public key and private key specific for the IoT device 10. Furthermore, the processor 14 is configured to process the data received from the sensor 12 with the private key of the pair of public key and private key to generate a data packet (step 104). The private key may be one time programmed (OTP) to the IoT device 10 within, for example, a memory 17 of the IoT device 10 as shown in Fig. 1, during the production of the IoT device 10. Here, the OTP means programming data on a non-volatile memory where the setting of each bit is locked by a fuse or antifuse. The memory on which the OTP may be performed is one type of read-only memory (ROM) and data may be burned on such a memory only once. Therefore, the data on such a memory is permanent and cannot be changed. By one time programming the private key into the IoT device 10 during the manufacturing process of the IoT device 10, the private key of the IoT device 10 may not be changed anymore during the whole lifecycle of the IoT device 10 and thus the safety of the private key, and therefore the data obtained by the sensor 12, may be ensured. The data packet includes at least the unique identification number of the IoT device 10, the data received from the sensor 12 and a signature generated according to the unique identification number and the data.

In one implementation, the processor 14 may use the public key in the pair of public key and private key as the unique identification number of the IoT device 10. By reusing the public key in the pair of public key and private key as the unique identification number of the IoT device 10, the signaling needed for the platform 20 to identify the IoT device 10 is reduced. In this case, by registering the unique identification number of the IoT device 10

to the block chain platform, the block chain platform may obtain both the unique identification number and the public key of the IoT device 10.

In another implementation, the unique identification number of the IoT device 10 is generated by the processor 14 based on the public key of the pair of public key and private key. For example, the processor 14 may perform a cryptographic Hash operation on the public key and use the result of the Hash operation (the hashed public key) as the unique identification number of the IoT device 10. By separately setting the unique identification number and the public key of the IoT device 10, the public key of the IoT device 10 may be protected and all unique identification numbers of IoT devices provided by a same provider may have a same length if a same Hash operation is used. In this case, the IoT device 10 may transmit its public key to the block chain platform by a registration process, and inform the block chain platform of the used Hash operation, by preconfiguring or signaling separately, for example. Those skilled in the art may understand that the present disclosure is not limited thereto, and the unique identification number of the IoT device 10 may be generated or be assigned in any known or to be developed manners for example, in order for the unique identification number to globally identify the IoT device 10.

In one implementation, the generation of the data packet in step 104 may include the following sub-steps. Firstly, the processor 14 performs a Hash operation on the combination of the unique identification number of the IoT device 10 and the data received from the sensor 12 (sub-step 1042). In contrast to only performing the Hash operation on the detected data, both the unique identification number and the detected data may be protected by performing the Hash operation on both of them. Subsequently, the processor 14 performs an asymmetric encryption on the result of the Hash operation to generate the signature with the private key in the pair of public key and private key (sub-step 1044). Herein, the Hash operation may be any of the general MD4, MD5, SHA-1, SHA-2, SHA-3 or BLAKE2 algorithms. Further, it should be noted that the Hash operation performed by the processor 14 on the unique identification number and the data may be identical to or different from the Hash operation described above for generating the unique identification number of the IoT device 10. Finally, the professor 14 packetizes the unique identification number of the IoT device, the data received from the sensor 12 and the generated signature into a data packet (sub-step 1046).

In one example, the content of the data packet generated by the processor 14 may include the unique identification number of the IoT device 10, the data received from the sensor 12 and the signature generated by the processor 14, while the format of the data packet may be fixed or flexible as described in the following.

Furthermore, the professor 14 is further configured to transmit the generated data

packet to the block chain platform (such as the block chain platform 20 shown in Fig. 3) for storage (step 106). In this regard, the IoT device 10 may further include a communication module 16 that is configured to receive the data packet from the processor 14 and transmit the data packet to the block chain platform for storage. Prior to the transmission of the data packet, the communication module 16 is further configured to register the unique identification number of the IoT device 10 to the block chain platform.

In some cases, it may be desired to read out all the data obtained during the transportation of the object collectively at the destination. For this purpose, the IoT device 10 may be equipped with an offline communication function. In these cases, the communication module 16 may include an offline communication interface that may be used to communicate with a scanner in a near distance communication manner to transmit the data packet generated by the processor 14 to the scanner, which in turn forwards the data packet to the block chain platform. Herein, the near distance communication manner may include at least one of Near Field Communication (NFC), Radio Frequency Identification (RFID) or other known or to be developed near distance communication manners in the art such as WiFi, Bluetooth, and ZIGBEE.

In some cases, it may be desired to monitor all the data during the transportation of the object in real time or substantially real time. For this purpose, the IoT device 10 may be equipped with an online communication function. In these cases, the communication module 16 may include an online communication interface that may be used to connect with a radio access network directly and transmit the data packet generated by the processor 14 to the block chain platform over the radio access network. Herein, the online communication function of the communication module 16 may be implemented by any Radio Access Technology (RAT) known or to be developed in the art.

It may be appreciated by those skilled in the art that whether the communication module 16 is configured to support the online communication or the offline communication or both depends on various factors such as the production cost or the cargoes to be monitored.

In addition to the wireless communication function as described above, the communication module 16 of the IoT device 10 may also support a wired communication function. In this case, the communication module 16 may include a wired communication interface such as a USB interface that transmits the data packet generated by the processor 14 to the block chain platform directly or indirectly through a data cable such as a USB cable.

Furthermore, the IoT device 10 may further include a power supply component 18 which is used to power the IoT device 10. The power supply component 18 may be a battery, for example. Different from conventional detection devices powered outside, it may further

prevent the data obtained by the sensor 12 from being tampered with by powering the IoT device 10 with the power supply component contained in itself.

It may be understood that the IoT device 10 according to the present disclosure may further include some other components relevant to or not relevant to the present solution such as a memory, a transceiver, an antenna, etc., which will not be described in detail herein.

Fig. 3 illustrates an IoT system 1 for recording transportation data of an object according to the present disclosure. As shown in the Fig. 3, in addition to the IoT device 10 described above in connection with the Fig. 1, the IoT system 1 further includes a block chain platform 20. The block chain platform 20 is configured to receive the data packet generated by the processor 14 from the IoT device 10, authenticate the data packet based on the public key of the IoT device 10 and store the data in the data packet upon a successful authentication.

As described above, the format of the data packet may be fixed or flexible. In one implementation, a fixed format of data packet may be used. The following Table 1 shows an exemplary fixed format of the data packet.

Table 1

Unique Identification Number	Data	Signature
------------------------------	------	-----------

Herein, the field of Unique Identification Number indicates the unique identification number of the IoT device 10, the field of Data indicates the data detected by the sensor 12, and the field of Signature indicates the signature generated by the processor 14 according to the unique identification number of the IoT device 10 and the data detected by the sensor 12. It may be understood by those skilled in the art that the fixed format of the data packet is not limited to the specific sequence or form as shown in Table 1, but may adopt other forms that can be conceived by those skilled in the art.

In case of fixed format of data packet, the fixed format may be preconfigured in the IoT device 10 and the block chain platform 20, respectively. For example, respective lengths and sequence of the fields of Unique Identification Number, Data and Signature may be preconfigured.

Fig. 4A illustrates a block diagram of the block chain platform 20 according to one embodiment of the present disclosure. As shown in Fig. 4A, the block chain platform 20 includes an underlying block chain 22 and an application server 24 interfaced with the underlying block chain 22, which may be an application server of the provider for providing service of recording transportation data according to present disclosure.

Fig. 4B illustrates a block diagram of the block chain platform 20 according to another embodiment of the present disclosure. As shown in Fig. 4B, the block chain platform

20 includes an underlying block chain 22 that includes a plurality of block chain nodes 26. In this implementation, a smart contract (such as the smart contract 28 shown in Fig. 4B) dedicated to recording the transportation data may be developed and distributed to the block chain platform 20, for example, to a plurality of block chain nodes 26. Here, the block chain nodes 26 may be regarded as the hosts of the smart contract 28, and are also referred to in the present disclosure as the smart contract entity 28. The smart contract 28 may be developed by a developer of the system 1 or other providers and may be regarded as part of the system 1.

Here, the underlying block chain 22 may be any block chain known in the art or to be developed in the future, including public block chain, private block chain or consortium block chain, which will not be described in detail herein.

Fig. 5 illustrates a flow chart of a method 200 for recording transportation data of an object according to the present disclosure. The method 200 may be implemented by the block chain platform 20. Hereinafter the method 200 will be described in connection with Figs. 4A-4B and Fig. 5.

In step 202, the block chain platform 20 receives the data packet from the IoT device 10. It should be appreciated that the data packet is received in accompanying with the unique identification number of the IoT device 10. Then, the block chain platform determines whether the unique identification number has been registered (step 204). If the unique identification number has been registered (YES in step 204), the block chain platform 20 retrieves the combination of the unique identification number of the IoT device 10 and the data detected by the sensor 12 from the data packet (step 206), and retrieves the signature from the data packet (step 208). Then, the block chain platform 20 performs a same Hash operation on the combination of the unique identification number and the data as the Hash operation performed by the processor 14 to generate the data packet as described above (step 210), and decrypts the signature using the public key of the IoT device 10 (step 212). Subsequently, the block chain platform 20 compares the result of the Hash operation obtained in step 210 and the result of the decryption obtained in step 212 (step 214) and determines whether they are the same (step 216). If they are the same (YES in step 216), which indicates a successful authentication of the data packet, the data in the data packet is stored on the block chain platform 20. Due to the anti-tamper characteristic of the block chain itself, the data on the block chain platform 20 may be safely stored.

Depending on the implementation of the block chain platform, respective steps of the method 200 may be implemented by the application server 24 or the smart contract entity 28 or the combination thereof. For example, steps 202 to 216 of the method 200 may be all performed by the application server 24 shown in Fig. 4A or the smart contract entity 28

shown in Fig. 4B, and then at step 218 the data is stored on the underlying block chain 22. Alternatively, the steps 202, 204, 208 and 212 of the method 200 may be performed by the application server 24 and other steps are performed by the smart contract entity 28. In this case, the block chain platform 20 may be implemented as a combination of that in Fig. 4A and that in Fig. 4B.

In the implementation that the communication module 16 includes an offline communication interface, the IoT system 100 further includes a scanner 30, which may receive the data packet from the IoT device 10 and forward the data packet to the block chain platform 20. Depending on the near distance communication manner supported by the IoT device 10, the scanner 30 should support the same near distance communication manner.

According to the solution of the present disclosure, when the cargo begins to be transported, the IoT device 10 may be powered on and placed together with the cargo (in the package of the cargo, for example). Respective data packets generated by the IoT device 10 during the transportation procedure may be transmitted periodically or aperiodically to the block chain platform 20 at respective locations (such as the warehouse, the transportation facility and the destination) of the whole transportation procedure (in case that the IoT device 10 supports an online communication function), or all the data packets generated during the transportation procedure may be retrieved at once from the IoT device 10 when the cargo reaches the destination and transmitted to the block chain platform 20 (in case that the IoT device 10 supports an offline communication function).

By assigning a unique identification number to the IoT device 10, it may prevent the sensor 12 from being replicated and fake data from being obtained from the replicated sensor.

By one time programming the private key to the IoT device 10 with a programming software, encrypting the data obtained by the sensor 12 with the private key and decrypting the data by the block chain platform 20 with the corresponding public key, the safety of the data transmission may be ensured.

In addition, by uploading the data to the block chain platform and authenticating and storing the data by the block chain platform, the safety of the data storage may be further improved.

In one or more exemplary designs, the functions described by the present disclosure may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium.

The various units of the device described herein may be implemented with discrete hardware components or integrally in a single hardware component such as a processor. For example, the various illustrative logical blocks, modules, and circuits described in

connection with the aspects disclosed herein may be implemented within or performed by a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein.

Those skilled in the art would further appreciate that any of the various illustrative logical blocks, modules, processors, means, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware, computer software, or combinations of both.

The previous description is provided to enable any person skilled in the art to make or use the present disclosure. Various modifications to the present disclosure will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects without departing from the scope of the disclosure. Thus, the present disclosure is not intended to be limited to the examples and designs shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

What is claimed is:

1. An Internet of Things (IoT) device for recording transportation data of an object, the IoT device having been one time programmed with a private key in a manufacturing process of the IoT device, the IoT device comprising:

5 at least one sensor configured to detect external environment data of the object during transportation of the object; and

 a processor configured to receive the data from the at least one sensor and generate a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature
10 generated based on the unique identification number and the data;

 wherein the processor is further configured to:

 perform a Hash operation on a combination of the unique identification number and the data;

 use the private key to perform an asymmetric encryption on the hashed
15 combination of the unique identification number and the data to generate the signature; and

 packetize the unique identification number of the IoT device, the data and the signature into the data packet.

2. The IoT device according to claim 1, wherein the processor is further
20 configured to:

 generate the unique identification number using a public key corresponding to the private key.

3. The IoT device according to claim 2, wherein the processor is further
configured to:

25 perform a Hash operation on the public key and use result of the Hash operation as the unique identification number.

4. The IoT device according to claim 1, wherein the processor is further
configured to:

 use a public key corresponding to the private key as the unique identification

number.

5. The IoT device according to claim 1, wherein the processor is further configured to:

5 register the unique identification number of the IoT device to a block chain platform.

6. The IoT device according to claim 1, wherein the processor is further configured to:

transmit the data packet to a block chain platform.

7. The IoT device according to claim 6, further comprising:

10 a communication module configured to receive the data packet from the processor and transmit the data packet to the block chain platform for storage.

8. The IoT device according to claim 7, wherein the communication module includes an online communication interface, the online communication interface being connected with a radio access network directly and configured to transmit the data packet to the block chain platform over the radio access network.

9. The IoT device according to claim 7, wherein the communication module includes an offline communication interface, the offline communication interface communicating with a scanner in a near distance communication to transmit the data packet to the scanner, the scanner forwarding the data packet to the block chain platform.

10. The IoT device according to claim 9, wherein the near distance communication includes at least one of Near Field Communication (NFC), Radio Frequency Identification (RFID) communication, WiFi communication, Bluetooth communication, and ZIGBEE communication.

11. The IoT device according to claim 7, wherein the communication module includes a wired communication interface, the wired communication interface transmitting the data packet directly or indirectly to the block chain platform through a data cable.

12. The IoT device according to claim 1, wherein the sensor includes at least one

of an environmental sensor, a motion sensor, a gas sensor and a location sensor.

13. The IoT device according to claim 1, further comprising a power supply component for powering the IoT device.

14. A method for recording transportation data of an object, comprising:

5 receiving external environment data of the object detected during transportation of the object from at least one sensor of an Internet of Things (IoT) device, the IoT device having been one time programmed with a private key in a manufacturing process of the IoT device; and

10 generating a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature generated based on the unique identification number and the data;

wherein the generating a data packet includes:

performing a Hash operation on a combination of the unique identification number and the data;

15 using the private key to perform an asymmetric encryption on the hashed combination of the unique identification number and the data to generate the signature; and

packetizing the unique identification number of the IoT device, the data and the signature into the data packet.

20 15. A nonvolatile computer readable medium for recording transportation data of an object, comprising:

computer program codes for receiving external environment data of the object detected during transportation of the object from at least one sensor of an Internet of Things (IoT) device, the IoT device having been one time programmed with a private
25 key in a manufacturing process of the IoT device; and

computer program codes for generating a data packet based on the data using the private key, the data packet including a unique identification number of the IoT device, the data and a signature generated based on the unique identification number and the data;

wherein the computer program codes further include codes for:
performing a Hash operation on a combination of the unique identification number
and the data;
using the private key to perform an asymmetric encryption on the hashed
5 combination of the unique identification number and the data to generate the signature;
and
packetizing the unique identification number of the IoT device, the data and the
signature into the data packet.

10 16. An Internet of Things (IoT) system for recording transportation data of an
object comprising:
the IoT device according to claim 1, and
the block chain platform according to any one of claims 5-13;
wherein the block chain platform comprises an underlying block chain and an
application server or a smart contract entity configured to receive a data packet from
15 the IoT device, authenticate the data packet based on a public key of the IoT device
and store the data of the data package to the underlying block chain upon a successful
authentication.