

SYSTEM AND METHOD FOR ESTABLISHING SECURE COMMUNICATION

FIELD OF THE INVENTION

- 5 The present invention relates to the field of data network communications and in particular, the establishment of secured communication for providing connectivity between communication devices.

BACKGROUND TO THE INVENTION

- As the market and ecosystem of users, devices, Internet of Things (IoT) and number of
10 mobile transactions grows, security threats will increase concomitantly, and large-scale security breaches will become more imminent. A related problem is how one can securely register a device so that only authorised devices are registered in the network. While these IoT devices and gateway devices provide a lot of valuable information, the lack of an easy and secure way for data collection and transportation would prove to be of limited use in
15 establishing communication.

Furthermore, when communicating with multiple other entities, the management of various credentials could be complex and resource consuming. This could be particularly unfavourable in a resource-constrained environment, such as IoT ecosystem where up to a billion devices (e.g. sensors, and actuators) are connected to the ecosystem.

- 20 Due to the interconnectivity of devices via the Internet or network and the scale of such IoT ecosystems, security remains one of the main concerns in the adoption of IoT technologies. Each device in the ecosystem could be a potential entry point to hackers accessing business-critical information or personal data. The advent of big data and big security breaches have only further compounded consumer's concerns about the security and trustworthiness of a
25 distributed heterogeneous IoT system.

As a result, there is a need for a system and method for managing secure communication to overcome at least in part some of the aforementioned disadvantages. In particular, to provide a system and a method for managing secure communication remotely between

communication devices for providing secure and centralised management of devices and data gathered/collected.

SUMMARY OF THE INVENTION

Throughout this document, unless otherwise indicated to the contrary, the terms,
5 “comprising”, “consisting of”, and the like, are to be construed as non-exhaustive, or in another words, as meaning “meaning but not limited to”.

Security and scalability are essential considerations for adopting an Internet of Things (IoT) system. In some instances, aggregating the massive amount of data between the sensors and actuators that are connected to the system and processing to enable processing of these data.
10 In highly-dispersed IoT environments, the management, and security of these sensors and actuators are critical for mass deployment. In addition, each of these IoT devices may have requirements for different protocols, translating and transferring data between systems of different communications protocols.

Advantageously, the present invention provides a central device management solution that
15 integrates with various platforms and protocols for secure device enrolment and authentication, thereby supporting and authenticating the numerous connected devices. Embodiments of the invention are advantageously for providing centralised solution to enrol, manage, orchestrate and monitor all devices and data gathered from these devices. Further embodiments provide gateway devices that are equipped with strong wireless
20 backhaul support, thereby enabling the easy yet secure collection and transportation of IoT device data.

In accordance with a first aspect of the present invention, there is provided a method for managing secure communication remotely in a network comprising:

- authorizing a gateway for communicating with a server based on a unique identifier;
- 25 providing a credential token associated with the gateway for use in communications between the gateway and the server;
- authorizing a device for communicating with the server based on a generated key associated with the device, wherein the device is coupled to the gateway;

accessing data from the device based on the key for communicating between the device and the server; and

managing the communication between the device and the server remotely.

Preferably, generating the unique identifier comprising:

- 5 receiving an encrypted data from the gateway;
 decrypting the encrypted data;

 validating and storing decrypted data; and

 generating the unique identifier based on the validated data.

Preferably, a plurality of devices couple to the gateway.

- 10 Preferably, the server is in communication with a plurality of gateway.

Preferably, the server comprises a pool of the unique identifiers.

Preferably, the coupling of the device and the gateway is provided by physical ports or wireless communication.

Preferably, the gateway is encrypted.

- 15 Preferably, creating and storing a decryption key associated with the gateway that is accessible to the server.

Preferably, the gateway requests the server for issuance of a new credential token if the credential token is inactive.

- 20 Preferably, the unique identifier of the gateway is generated from MAC address and product ID.

In accordance with a second aspect of the present invention, there is provided a system for managing secure communication remotely between a device coupled to a gateway and a server, comprising:

- the server comprising:
25 a processor;

a network module configured to authorize a gateway based on a unique identifier;
provide a credential token associated with the gateway that is authorized for
communicating with the gateway; generate a key for the device that is authorized to
communicate with the server; and manage communication between the server and a
5 device coupled to the gateway; and

the gateway comprising:
a processor;
a communication interface for receiving and sending data from the device; and
10 a network module configured to provide the unique identifier for communicating
with the server; receive the credential token for communicating with the server; and
authorize the device for communicating with the server;

wherein the server, the gateway, connects to the device, obtains data from the device
15 and sends the data to the server via the communication interface to manage the data
received from the device remotely.

Preferably, the server comprises a pool of the unique identifiers.

Preferably, the server is in communication with a plurality of gateway.

Preferably, the device is coupled to the gateway by physical ports or wireless
20 communication.

Preferably, wherein the gateway is encrypted.

Preferably, the gateway is configured to create and store a decryption key that is accessible
to the server device.

Preferably, the gateway requests the server for issuance of a new credential token if the
25 credential token is inactive.

Preferably, the unique identifier of the gateway is generated from MAC address and product
ID.

Preferably, the system is configured for adopting and integrating by the server and/or the
one or more devices.

Preferably, the system is configured to provide centralized management of the one or more devices remotely.

Preferably, a network communication means is configured to allow transmission between the server and the device.

- 5 The embodiments of the present invention have at least the following advantages:
1. According to embodiments, there is provided a secure and centralized means for device enrolment and authentication to ensure all devices that are connected are authenticated, making every data in the network trusted and secure. Furthermore, device enrolment and authentication are easy to use and does not require re-
10 registration with the system admin.
 2. According to embodiments, there is provided an overall device management system, for supporting centrally all devices connected via the gateway, including secure device enrolment, registration and authorisation for end user devices which are
15 connected to the gateway, thereby ensuring secure communication between the system entities. The system enables remote controlling of these end user devices by sending commands to the gateway device.
 3. According to embodiments, there is provided a system for easy integration with
20 Internet of Things (IoT) devices, which allows interoperability to securely gather/transfer data and is advantageous for convenient connection to the network. Furthermore, the system supports multiple device types, from gateways, sensors, servers, and network equipment.

Other aspects and advantages of the invention will become apparent to those skilled in the
25 art from a review of the ensuing description, which proceeds with reference to the following illustrative drawings of various embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of illustrative example only, with reference to the accompanying drawings, of which:

Figure 1 is a block diagram of the system for managing secure communication remotely for providing connectivity between communication devices in accordance with an embodiment of the present invention.

Figure 2 is architectural diagram depicting the software structure of the data management
5 device in the system of Figure 1.

Figure 3 is a flow chart depicting steps for registering a gateway device with the data management device.

Figure 4 is a block diagram depicting the developments for data encryption prior to device registration.

10 Figure 5 is a flow chart depicting steps for authorizing a sub-device to manage secure communication in the network.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing
15 particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

The use of the singular forms “a”, “an”, and “the” include both singular and plural referents
20 unless the context clearly indicates otherwise.

The use of “or”, “/” means “and/or” unless stated otherwise. Furthermore, the use of the terms “including” and “having” as well as other forms of those terms, such as “includes”, “included”, “has”, and “have” are not limiting.

The use of the term “wirelessly” includes 3G, 4G, 5G, Wi-Fi, and any other kinds of wireless
25 connection.

The use of the term “sub-device” includes any device that can connect wirelessly to a network and have the ability to transmit data e.g. IoT devices. Sub device sub devices may be heterogeneous devices relative to operation and or communications protocols.

In accordance with an aspect of the present invention, there is provided a system 100 for managing secure communication remotely between communication devices. The system 100 comprises a data management device 102 and a gateway device 104. The data management device 102 is connected to the gateway device 104 via a communication means.

5 The data management device 102, the gateway device 104 and the sub-devices 106 interconnect to enable transfer of data between the devices via the communication means (see Figure 1).

The system 100 is directed towards an upstream to downstream data integration and technology solution that advantageously provides ease of integration of gateway devices 104, which is capable of supporting a wide range of machine to machine protocols, supports a variety of standard network protocols, along with strong wireless backhaul support make it easy to collect and transport the IoT device data. Furthermore, the system 100 provides a central device enrolment and authentication by ensuring that all connected devices 106 are authenticated.

15 Referring to Figure 2, there is provided the architectural diagram of the data management device 102 supporting a network of devices and applications in accordance to an embodiment of the present invention. A plurality of devices and IoT applications may have connection to a communication network.

The gateway 104 (or provided as a computerized gateway device) is adapted to be in communication with one or more sub-devices 106 such as sensors, wireless communication devices having sensor or data for transmission onto a larger network. The gateway device 104 may receive data from the sub-devices 106. The gateway device 104 comprises a communication interface for interfacing with the sub-devices 104 and protocols to gather and/or transfer data which may be analysed and processed for further operations. The gateway 104 comprises a processor to process messages from sub-devices 106 in a network. The gateway 104 enables various components of a distributed system to communicate. The gateway device 104 enables interoperability between applications and protocols that run on different operating systems.

The gateway device 104 is adapted to receive data from sub-devices 106 according to several different protocols. When the sub-device 106 pushes data to the gateway device 106, the gateway device 104 may access a device 106 and fetch characterization data from the sub-device 106. Characterization data describes protocol specific workflow, interface type etc.

which may be required for the sub device 106 and application communicating to the gateway 104. The gateway 104 may observe a request/response to fetch or retrieve data from each accessible device 106. The gateway 104 gathers data and transmits to destination through an embedded middleware, providing technology integration for platform and protocol support.

5 Advantageously, the gateway 104 enables scaling efficiently and rapidly to support devices 106 while keeping costs relatively low.

The gateway device 106 routes data to the data management module 102. The data management module 102 receives data received over the network from registered gateway devices 106. The data management module 102 receives and manages the data. The data

10 management module 102 may receive data from devices 106 according to several different protocols. The data management module 102 comprises a multi-protocol middleware platform to gather and integrate the data. The data management module 102 comprises a processor to process the data. In an example, data may be processed and analysed by transporting securely to an IoT platform cloud. The data management module 102 may

15 enable this data readily available for any type of processing, for example, through Machine-to-Machine (M2M) and application interfaces that support configuration management, device status management, ID management and device authentication.

In another embodiment, the data management module 102 unifies all IoT applications by providing a unified communication channel with support of different device types such as

20 sensors, PLC and machinery equipment for support Machine-to-Machine (M2M) interface.

In a further embodiment, the data management module 102 supervises and safeguards data from security threats. The data management module 102 implements real-time service level agreement (SLA) management for all gateway devices 104 and sub-devices 106 that are

25 connected to the network. The data management module 102 comprises a data gathering platform that provides for potential for software growth in managing and processing distributed data. The data management module 102 may enable secure delivery of both structured and unstructured data. The data management module 102 may store any type of data without restrictions on data structure or format.

30 In one example, the data management module enables internet-connected devices 106 to the Cloud and allows applications in the Cloud to interact with the internet-connected devices. The devices report their state by publishing messages in JSON format on MQTT topic.

When a message is published on an MQTT topic, the message is sent to the server MQTT broker, which is responsible for sending all messages published on an MQTT topic to all devices subscribed to that topic. The devices can also report the DDS protocol.

5 The communication between a device and the data management module is protected through the use of x.509 certificates, which is advantageously widely accepted in Internet applications. The data management module provides a certificate for the device. When the device is deactivated, the data management module may revoke a certificate of that device. The device will be disconnected to MQTT broker.

10 In accordance with another aspect of the present invention, there is provided a method for managing secure communication between communication devices for providing connectivity and management of devices thereof. The method comprises central device enrolment, registration, authentication and authorization. The method includes the following steps:

15 **Step 1:** Device registration, wherein credentials are presented from the gateway device 104 to the data management module 102.

Step 2: The data management module authorizes the gateway device 104 when the proper credentials are presented. If the proper credentials are not presented, authorization is not enabled by the data management module 102.

20 **Step 3:** An authorized gateway device 104 registers other sub-devices 106 that are connected to the network, so as to enable 2-way communication between the data management module 102 and the gateway device 104 securely.

Device Registration

Referring to Figure 3, device registration is carried out centrally with the data management module, in which the gateway device that wishes to communicate securely with the data management module carries out a registration request to the data management module 302.

The gateway registers with the data management module by providing a Device ID. Using the Device ID, the gateway sends the encrypted data to the server through REST API 302. The data management module decrypts the Device ID 304. The Device ID is a combination of MAC and Product ID. The API server validates Device ID with its database to determine

whether there is an existing Device ID 306. If there is an existing Device ID, the server retrieves a token from the database for the gateway 308. If there is no existing Device ID in the database, the server may show an error 310 but may nonetheless generate a token for the gateway device. The gateway device receives and stores the Device ID and token 312.

- 5 The Device ID is combined MAC address, product ID, a static deviceID key is generated based on the following (Figure 4):

- ~ Step 1: a string of 16 bytes, DeviceId_1
 - ~ Product ID: SkyLab device identifier, a string of 10 bytes
 - ~ Mac Address: the hardware address of first Ethernet interface, string of 6 bytes
- ~ Step 2: encrypt (DeviceId_1) = DeviceId_2, a string of 44 bytes base on AES algorithms, and encode base64
- ~ Step 3: encode DeviceId(2) => final DeviceID (mix of DeviceId(2) and 3 last bytes of Mac address and combine with the encrypt key version)

- 15 The gateway device sends the encrypted data to the server through REST API.

The server decrypts the data, verifies and stores all decrypted information such as: product_id, MAC address. In addition, the server generates a unique device identifier and token in response to the agent. The gateway may use this token for authentication when calling the REST API on the server through https. The server uses Json Web Token (jwt).

- 20 Using the approaches above, the registration capability enables identification of devices that are deployed in the network, for device registration, maintenance, scalability, and other functions.

Device Authorization

Referring to Figure 5, communication between the data management module and the device
25 may be carried out via X.509 certificate. This is to confirm the gateway can communicate
with the data management module. If there is no certificate, the gateway may request Device
certificate API for X.509 certificate through HTTPS 302. In response to the request, the

Device certificate may be issued by PKI server as part of the authorization/authentication process 304/306.

Once authorized, the data management module issues the certificate 304. The certificate may be delivered to the gateway via REST API protocol over HTTPS. The certificate may also
5 protect the communication between an authorized sub-device and the data management module, which advantageously enables only trusted devices to communicate and send data.

Upon successful authentication, the authorized gateway may register for sub-devices that are already connected. In other embodiments, the gateway may register other new sub-devices that request connection.

10 For a sub-device that wishes to communicate with the data management module, the gateway obtains and checks for a X.509 certificate 308. If there is there is a valid certificate, secure communication may be established between the sub-device and the data management module. If there is no certificate of the device, the gateway makes a request for a certificate
15 certificate to determine if the certificate is issued; and check the validity/expiry of the certificate.

When a sub-device is deactivated, the data management module may revoke a certificate of that device. The device will then be disconnected to MQTT broker. In the case of certificate expiry or revocation, the gateway may request for issuance of a new certificate from the data
20 management module.

In other embodiments, authorization may be carried out manually or automatically when the gateway makes a registration request to the data management module. In some instances, security association for an application may be configured by a user. For manual authorization involving a user, the gateway awaits authorization. In this case, the user may
25 obtain a generated QR code which may be authorized by the server. Upon obtaining authorization, the data management module may issue x.509 certificate for the gateway.

Data Visualization

An authorized gateway device may push data that has been collected from registered sub-devices to a platform on the data management module for visualizing the data. For example,

the data management module may comprise a web portal for visualising the transmitted data. This advantageously enables pipelining and processing of the data from the devices.

Device Management

5 The system provides support to many types of devices, from sensors to gateways to servers and network equipment to enable central management of connected devices remotely and securely. Advantageously, the system provides interoperability between systems and can support scalability to build a device ecosystem.

10 The data management module also enables control of the gateway remotely, for example: send command (lock, unlock, restart, etc.), set configuration, update firmware, etc. A user of the data management system may lock devices that have compromised security. Locked devices will not be accessible to the gateway command-line interface (CLI). For example, settings may be configured to lock the device automatically after three failed attempts to login to the gateway or other back up functions. Advantageously, user permissions and device auditing may be achieved efficiently and conveniently.

15 The data management module enables deactivating end user devices remotely. Devices may be deactivated to prevent devices from sending data to the server, or for further processing. A user may be informed and can deactivate a device from the data management module in the event where abnormal data or behaviour may be observed.

20 The gateway may be encrypted for security. This prevents theft of data, in the event where parts of the gateway device be missing. In this case, a passphrase for decryption may be used. This passphrase may be randomly generated when the gateway device is first installed.

The working environment of the gateway device may be encrypted. Encryption may be carried out using binary files, libraries, log files, configuration files, and the like to ensure security of files during transmission.

25 It would be further appreciated that although the invention covers individual embodiments, it also includes combinations of the embodiments discussed. For example, the features described in one embodiment is not being mutually exclusive to a feature described in another embodiment, and may be combined to form yet further embodiments of the invention.

30