

**SECURITY SYSTEM AND METHOD FOR DATA COMMUNICATION
CONCERNING INTERNET OF THINGS (IoT)**

Field of the Invention

[0001] The present invention relates to Internet of Things (IoT), specifically the
5 present invention relates the secured communication of the IoT devices and its backend
system and method therefor.

Background

[0002] In today's increasingly interconnected world, secure communication
between devices and systems is of paramount importance. As more critical operations
10 and sensitive data are transmitted wirelessly between devices, ensuring the integrity and
confidentiality of this data is essential to prevent unauthorized access and breaches.
However, despite advances in communication technologies, the standard encryption
methods employed by many equipment manufacturers have become increasingly
vulnerable to sophisticated attacks. Cybercriminals and malicious entities now possess
15 the tools to intercept and hijack data, exploiting weaknesses in conventional security
protocols. This poses significant risks, particularly in applications that require high levels
of data security, such as power distribution networks, financial systems, and IoT
infrastructures.

[0003] Existing encryption mechanisms often fail to provide adequate protection,
20 leaving transmitted data exposed to man-in-the-middle attacks, data tampering, and
unauthorized decryption. As a result, there is an urgent need for improved security
measures that can ensure end-to-end encryption and safeguard communications, even in
the face of evolving cyber threats.

[0004] Traditionally, electrical consumption was measured using analogue meters that required manual reading by utility personnel. This method was labour-intensive, prone to human error, and lacked the ability to provide real-time data. Consequently, utility companies faced challenges in accurate billing, timely detection of outages, and efficient energy management.

[0005] The advent of digital smart meters has revolutionized the way electrical consumption is monitored and managed. Smart meters provide numerous advantages over traditional meters, including real-time monitoring, enhanced accuracy, and the ability to support dynamic pricing models. These meters measure various parameters such as energy consumption, voltage levels, and current, providing valuable data to both consumers and utility providers. However, to fully leverage the capabilities of smart meters, efficient communication between individual meters and the backend system center is essential.

[0006] Various communication technologies have been developed to facilitate the transmission of data from smart meters to backend system. Radio Frequency (RF) mesh networks use low-power radio signals to create a mesh topology where each meter acts as a node that can relay data. This decentralized approach ensures robustness and reliability, as data can take multiple paths to reach the backend system center. Despite its advantages, RF mesh networks can be limited by range and interference issues, particularly in densely populated areas.

[0007] Meters equipped with communication modems can directly send data to the backend system center via existing data network infrastructure. Despite the advancements in communication technologies, several challenges persist in the efficient

and reliable transmission of data between smart meters and backend system centers. Data security and privacy are paramount, requiring robust encryption and authentication mechanisms to prevent unauthorized access and data breaches. High-density urban areas with numerous meters can experience network congestion, leading to delays in data transmission and potential data loss. As the number of smart meters increases, the communication infrastructure must scale to handle the increased data volume without compromising performance.

[0008] In view of these challenges, the present invention aims to provide an improved method and system for data communication between individual power distribution grid meters and a backend system center. The invention seeks to enhance data security, reduce network congestion, ensure scalability, and improve the reliability of data transmission. By introducing innovative communication protocols and architectures, the invention aims to optimize the performance and efficiency of smart meter communication systems, thereby supporting the effective management and monitoring of power distribution grids.

Summary

[0009] In one aspect of the present invention, there is provided a secure device adapted for power grid metering network having a plurality of power meters and a power grid metering backend system. The secure device comprises a communication module having a socket for locally connecting to the power grid meters or the power grid backend system, as a gateway to transmit data over a communication network; a microprocessor acts as a control unit for the secure device and handling the data flow; an FPGA chip operationally encrypting/decrypting the data; a secure element for handling key

diversification for encrypting/decrypting the data by FPGA chip. The secure device is connected locally to the power grid meters and power grid metering backend system, operationally, encrypting/decrypting data transmitting through the communication network, such that the data is end-to-end encrypted across the power grid metering network by the secure device.

[0010] In one embodiment, the secure element is certified by Common Criteria (CC) or Federal Information Processing Standards (FIPS).

[0011] In another embodiment, the secure device of Claim 1, wherein the secure device further comprises an admin authenticator for access authentication to the secure device. It is possible that the admin authenticator is in a card form having its own secure element embedded therein. It is also possible that the admin authenticator is integrated on the secure device in a form of biometric scanner/sensor. The admin authenticator may be deployed remotely from the secure device.

[0012] In another aspect of the present invention, there is further provided a power grid metering network having a plurality of power grid meters connected to a power grid metering backend system via a communication network. The communication network can be wired or wireless network. The power grid metering network comprises the aforesaid secure devices. These secure devices are connected locally and directly to the power grid meter such that data passes through the secure device before transmitting to the communication network, and another secure device connected directly before the power grid metering backend system.

[0013] In yet another aspect, there is provided a method for providing additional encryption/decryption for a power grid metering network over a communication network. The method comprises adding secured devices to the power grid metering

network having power grid meters and power grid metering backend system connected through a communication network; activating secured elements of the secured devices; encrypting data from power grid meter through the secured devices; transmitting the encrypted data to the power grid metering backend system through the communication
5 network; and decrypting the encrypted by the secured devices for processing by the power grid metering backend system. The data transmitted through the communication network is end-to-end encrypted by the secure devices. These devices offer enhanced protection against unauthorized access by employing advanced encryption standards.

[0014] In one embodiment, the end-to-end encryption is done by the aforesaid
10 security device.

[0015] In yet another aspect, there is provided an Internet of Things (IoT) network for transmitting data over the IoT network. The network comprises an IoT device adapted to communicate to a IoT backend; a communication module having a socket for locally connecting to the power grid meters or the power grid backend system,
15 as a gateway to transmit data over a communication network; a microprocessor acts as a control unit for the secure device and handling the data flow; an FPGA chip operationally encrypting/decrypting the data; a secure element for handling key diversification for encrypting/decrypting the data by FPGA chip. The secure device is connected locally to the IoT devices and the IoT backend system, operationally, encrypting/decrypting data
20 transmitting through the communication network, such that the data is end-to-end encrypted across the power grid metering network by the secure device.

[0016] In one embodiment, the secure element is certified by Common Criteria (CC) or Federal Information Processing Standards (FIPS).

[0017] In another embodiment, the secure device further comprises an admin authenticator for access authentication to the secure device. It is possible that the admin authenticator is in a card form having its own secure element embedded therein. Alternatively, the admin authenticator can be integrated on the secure device in a form of biometric scanner/sensor. Yet another possibility, the admin authenticator may be deployed remotely from the secure device.

[0018] In a further aspect of the present invention, there is provided an IoT network having a plurality of IoT devices connected to an IoT backend system via a communication network. The IoT network comprises the aforesaid secure device. The secure device is connected locally and directly to the IoT devices such that data passes through the secure device before transmitting to the communication network, and another secure device connected directly before the IoT backend system.

[0019] Yet a further aspect of the present invention, there is provided a method for providing additional encryption/decryption for a IoT network over a communication network. The method comprises adding secured devices to the IoT network having IoT devices and an IoT backend system connected through the communication network; activating secured elements of the secured devices; encrypting data from IoT devices through the secured devices; transmitting the encrypted data to the IoT backend system through the communication network; and decrypting the encrypted by the secured devices for processing by the IoT backend system. Data transmitted through the communication network is end-to-end encrypted by the secure devices, wherein these devices offer enhanced protection against unauthorized access by employing advanced encryption standards.

[0020] In another embodiment, the end-to-end encryption is done by the aforesaid security device.

Brief Description of the Drawings

5 [0021] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0022] FIG. 1 illustrates a block diagram of a secured smart power grid metering system in accordance with an embodiment of the present invention;

[0023] FIG. 2 illustrates a secured smart power grid metering network in accordance with an alternative embodiment of the present invention;

[0024] FIG. 3 illustrates a process flow a secured smart power grid metering network in accordance with an embodiment of the present invention;

[0025] FIG. 4 illustrates a schematic diagram of the EV charging network having secured devices of FIG. 1 in accordance with an embodiment of the present invention;

15 [0026] FIG. 5 illustrates a block diagram of a secure device in accordance with an alternative embodiment of the present invention; and

[0027] FIG. 6 illustrates an Internet of Things (IoT) device integrated with a secured element in accordance with an embodiment of the present invention.

[0028] These devices offer enhanced protection against unauthorized access by
20 employing advanced encryption standards.

Detailed Description

[0029] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0030] FIG. 1 illustrates a block diagram of a secured transmission system for power grid metering network **100** in accordance with an embodiment of the present invention. The power grid metering network **100** comprises a plurality of power meters **110** connected to a power grid metering backend system **120** through a communication network **150**. Each of the power grid meter is locally connected with an secured device **182** for encrypting/decrypting data to be transmitted through the communication network **150**. The communication network **150** can be a private data network dedicated for the power grid metering network, or a public data network or cloud network. The power grid metering network **100** further comprises a backend system secured device **184** locally connected directly to the power grid metering backend system **120** for decrypting data transmitted across the communication network **150**.

[0031] In this application, the power grid metering backend system **120** or simply backend system for a power grid metering infrastructure is a critical component that manages, processes, and analyses data received from individual power meters. One of its primary functions is data collection and aggregation. The backend system may

continuously collects real-time data from power meters, including energy consumption, voltage, current, and power quality parameters. This data is then compiled from numerous meters for consolidated reporting and analysis, ensuring a comprehensive view of the power grid's status and performance. The backend system processes and
5 analyses the collected data to compute energy usage, facilitating accurate billing. It may also perform pattern analysis to identify trends, peak usage times, and potential inefficiencies. Anomaly detection capabilities allow the system to identify unusual patterns or discrepancies that may indicate meter tampering, fraud, or malfunction, enabling prompt intervention. Hence, billing and customer management are seamlessly
10 integrated into the backend system allowing automated billing functions. Additionally, the system can send alerts and notifications to customers regarding usage, billing cycles, and detected anomalies, enhancing customer service and transparency. Security and compliance are paramount concerns for the backend system. It implements robust security measures to protect data from unauthorized access and cyber threats.
15 Furthermore, the backend system ensures that data management practices comply with industry regulations and standards, maintaining the integrity and legality of operations.

[0032] The secured devices **182** and the backend system secured device **184**, each comprises a certified secured element adopted to encrypt/decrypt data transmitting through the communication network **150**. The certified secured element must at least be
20 certified under the Common Criteria (CC) and/or Federal Information Processing Standards (FIPS) certifications. It is well understood to a skilled person that CC and FIPS certifications are security standards used to evaluate the security features of a device or system, including the smart chip, also known as a secure element. These certifications evaluate a range of security features, such as access control, authentication,

secure boot, and key management, to ensure that the device or system is designed and implemented securely.

[0033] The communication network **150** can be any data communication network, wired and/or wireless, which include local area network (LAN) or wide area network (WAN). In another embodiment, it can also be a mobile communication network.

[0034] In one embodiment, the secured devices **182**, **184** are adapted as a plug-and-play devices. The secured devices **182**, **184** may adopt connectors compatible with the data communication network **150**, such as the Power over Ethernet (PoE), Coax, RJ45 etc.

[0035] In another embodiment, the secured devices **182**, **184** may be adopted as integral part of the power meters and backend system.

[0036] For avoidance of doubt, the secured element in this description refers to security module that is designed to provide secure storage and processing of sensitive data, such as cryptographic keys, certificates, and passwords. They are microchips embedded in a device and it is designed to provide a secure execution environment for sensitive operations, such as authentication, encryption, and decryption, and is often used in applications that require a high level of security, such as mobile payments, digital identity, and secure communications. Further, it offers a range of security features, such as secure boot, hardware-based encryption, and secure storage of cryptographic keys. These features help to protect the secured element from physical and logical attacks, such as side-channel attacks, brute-force attacks, and tampering. Secured elements are often

certified by independent organizations, such as the Common Criteria (CC) or Federal Information Processing Standards (FIPS), to ensure that they meet specific security requirements. These certifications provide assurance to users and customers that the secured element has undergone rigorous testing and evaluation to ensure that it meets a
5 high level of security.

[0037] The secure element is hardware based solution for securing data at the transport layer. The solution can be a plug-and-play system that can be customized and upgraded according to the owner's requirement and fully controlled by the owner because it can be separately fabricated and configured without affecting the power
10 meters. The owner may manage the entire power meters and the security thereof remotely and securely. The use of separate encryption and decryption devices provides end-to-end encryption of data transmitting over the network. Further, such external devices having the secured element can be added to existing power meters. With this additions, the data transmissions over the power metering network can be secured, even
15 against manufacturers of the power metering system.

[0038] FIG. 2 illustrates a secured transmission system for power grid metering network 200 in accordance with an alternative embodiment of the present invention. Similarly, the power grid metering network 200 comprises a plurality of power meters 210 connected to a power grid metering backend system 220 through a communication
20 network 250. Each of the power meters relates to a secured device 282 for encrypting/decrypting data to be transmitted through the communication network 250. The power grid metering network 200 further comprises a backend system secured

device **284** connected directly to the power grid metering backend system **220** for decrypting data received from the communication network **250**.

[0039] The secured devices **282, 284**, each comprises a secured element therein, for encrypting/decrypting data channelled into the secured devices **282, 284**. The secured smart power grid metering network **200** further comprises admin authenticators **292**. The admin authenticators **292** adapted and personalised to the users carrying the admin authenticators **292**. In one embodiment, the admin authenticators carry the user biometrics and/or passwords for authentication. The authentication is needed to operate and manage the secured devices **282, 284**. That realises a two-factors authentication (2FA) to activate and operate the secured devices **282, 284** for added security to the secured smart power grid metering network **200**. Accordingly, in order to access the secured elements at upstream and downstream, authentication is required through the admin authenticator **292**. In a desired embodiments, the admin authenticators **292** also comprises a secured elements that work in conjunction with the secured devices **282, 284**. The secured devices **282, 284** may further comprise a reader that operationally perform verification and authentication of the admin authenticators **292**. The reader may equip with wired or wireless means for reading the admin authenticators **292**. In one embodiment, the admin authenticator can be in a form of card that store the admin user authentication details. In another embodiment, the admin authenticator can be integrated on the secured devices **282, 284** in a form of biometric scanner/sensor, whereby authorised personnel can accessed the secure elements **282,284** for maintenance with their registered biometric information.

[0040] With the reader equipped on the secured devices **282**, **284**, the secured devices **282**, **284** can be activated at first used through the admin authenticators **292**, and any subsequent maintenance shall require the admin authenticators **292** to access the secured devices **282**, **284**. Accordingly, without the admin authenticators **292**,
5 unauthorised personnel will not be able to access the secured devices due to the highly secured elements embedded in the admin authenticators **292**. And even with the presence of the admin authenticators **292**, one will require an authentication factor, such as password, biometric identification, to prove identity of the person holding the admin authenticator **292**.

10 [0041] The admin authenticators **292** may be a handheld device having the secured element. In another embodiment, the admin authenticators **292** may be in a form of smart-chip/card, or tokens having a secured element that can be easily carried around. In one embodiment, the secured devices **282**, **284** may further comprise biometric reader and/or password keypad.

15 [0042] The authentication process involves the use of biometric authentication, such as fingerprint recognition or facial recognition in conjunction with the encrypted credentials to offer multi-layers security measures to ensure that only authorized personal can access the secured devices **282,284**.

[0043] It is well recognized that the secured elements certified under CC and/or
20 FIPS are highly secured. One reason for this is that these secured elements are designed with specific functionality and isolation with a limited number of commands that are strictly controlled and regulated, i.e. limited attack surface. This ensures that only authorized users can access the secured devices and perform the necessary operations.

Additionally, the limited number of usable commands also makes it more difficult for attackers to exploit vulnerabilities in the secured element, as there are fewer avenues for them to exploit. This limited functionality makes secured elements highly secure and provides a strong defence against a wide range of threats. Overall, secured elements that

5 have been certified under CC or FIPS are an essential component of modern security architectures and provide a crucial layer of protection for sensitive data and applications.

[0044] In another embodiment, the secured devices 282 can only be accessed through the remote authentication from through the secure device 284, which is usually managed by the central office. These devices offer enhanced protection against

10 unauthorized access by employing advanced encryption standards.

[0045] FIG. 3 illustrates a process flow for a power grid metering network in accordance with an embodiment of the present invention. The process comprises adding secured devices to a power grid metering network at step 302; activating secured elements of the secured devices at step 304; encrypting data from power meters through

15 the secured devices at step 306; transporting the encrypted data to the power grid metering network through the communication network at step 308; and decrypting the encrypted by the secured devices for processing by the power grid metering backend system 312. It is to be noted that the data communication over the communication network is bidirectional. All power meters can retrieve information from the power grid

20 metering backend system, and vise versa.

[0046] At the step 302, the secured devices are added to each power meter and the backend system of the power grid metering network. Each of the secured devices comprises secured elements for securing at least encryption keys. Each of the secured

devices can be fabricated as external or add-on devices to the power grid metering network. At the step **304**, each of the secure elements shall be activated on first used by authorized administrators. The authorized administrators are usually authorized personnel from the operator or owner of the power grid metering network. Only those
5 activated secure elements can be used for encrypting/decrypting the data.

[0047] At the step **306**, all data transmitted through the power grid metering network is encrypted by the secure element of the secured device with the encryption keys. At the step **308**, the encrypted data is transmitted to the power grid metering network through the communication network. It is to be noted and understood that when
10 the encrypted data travels over the communication network, which may include external network, such as internet, the encrypted data is only decryptable by the keys of the intended recipient. In the present case, the encrypted data is decryptable only by the secured device connected to the backend system (i.e. intended recipient). At the step **312**, when the secured device receives the encrypted data from the respective power
15 meter having a secured device connected thereto, it decrypts the encryption of the encrypted data then feeds the decrypted data to the power grid metering backend system for further processing and storing the data.

[0048] **FIG. 4** illustrates a schematic diagram of the power grid metering network **100** having secured devices of **FIG. 1** in accordance with an embodiment of the
20 present invention. As shown, the secured devices **182** and **184** comprises a communication module **402**, a microprocessor **404** and a secured element **406**. The secured devices **182** are provided at each power meter at the upstream side, and the secured device **184** is provided at the downstream side such that data from the upstream

sides are encrypted before travelling across the network and decrypted by the secured device at the downstream secured device. The communication module **402** provides communication ports for interfacing the power meter and the power grid metering backend system with the communication network **150**. Data transmitted through the secured devices is being processed by the microprocessor **404** to encrypt/decrypt data with the keys possessed by the secured elements **406**. In effect, data **410** from the power meters **110** are encrypted/decrypted by the secured device **182**. The encrypted data **420** is then transmitted to the metering backend system **120** through the network **150**. Without the secured device **184**, the encrypted data **420** would be meaningless to the power grid metering backend system **120**. Therefore, the secured device **184** is connected to the metering backend system **120** to decrypt the encrypted data **420**. The decrypted data **430** may then process and store on the power grid metering backend system **120**.

[0049] In one embodiment, data processing is done by the microprocessor **404** in conjunction with the secured elements **406** to encrypt/decrypt the data for enhanced security.

[0050] The present invention offers an additional, self-managed, point-to-point hardware-based encryption to secure the data over the network at transport layer.

[0051] In another embodiment, the communication module may comprise a wireless communication means, i.e. antenna, GSM module, WIFI module, or Bluetooth module and/or the like.

[0052] FIG. 5 illustrates a block diagram of a secure device 500 in accordance with an alternative embodiment of the present invention. The secure device 500 comprises a microprocessor 502, a FPGA Chip 504, a secure element 506, an ethernet transceiver 508 and an RJ46 socket 509. These devices offer enhanced protection against
5 unauthorized access by employing advanced encryption standards.

[0053] The microprocessor 502 acts as the control unit, managing data flow, high-level tasks, and etc., while also handling communication protocols for the ethernet transceiver 508. It hands over the data to the FPGA chip 504 for performing computationally intensive encryption or decryption tasks. The FPGA chip 504 works in
10 conjunction with the secure element 506 that handles key diversification, ensuring that encryption keys are unique and secure. This secure element 506 operationally generates or stores cryptographic keys, making it difficult for unauthorized parties to gain access. After the FPGA chip 504, aided by the secure element 506, completes the encryption or decryption, the microprocessor 502 performs additional tasks such as appending
15 metadata, error checking, or routing the encrypted data to its destination. The microprocessor can also dynamically reconfigure the FPGA to switch between different algorithms as needed and manage other security measures.

[0054] It is well understood to a skilled person that the microprocessor 502 or the server/computer can be compromised by hacker or insider leak. Hence, the data
20 in/out through the RJ45 socket 509 then the ethernet transceiver 508 is hardware encrypted/decrypted by the FPGA chip 504. During the encryption/decryption, the FPGA chip 504 obtained keys from the secure element 506 where key diversification is

carry out. So without the key, the data would be meaningless to any hacker or intruder who obtained them.

[0055] With the secure device 500 added to the upstream (i.e. power meters) and downstream (i.e. power grid metering backend system) of the power grid metering network, the data transmitted through the communication network can be encrypted/decrypted through the secured device 500.

[0056] In an alternative embodiment, the Secure Element (SE) collaborates with the Field-Programmable Gate Array (FPGA) chip to automatically validate the digital signatures of all received packets, including ICMP echo requests commonly known as "ping" packets. If the digital signature of an incoming packet does not align with the cryptographic computation performed internally by the SE, the packet is deemed to be invalid. Consequently, the SE discards this packet without issuing any response, effectively rendering the device unresponsive to unauthorized ping requests, and making its IP address invisible to potential attackers.

[0057] The above embodiments described in the context of power metering networks. The inventor of the present invention found out that it is equally applicable to other environments where secure data transmission is critical, such as Internet of Things (IoT) devices. IoT systems typically involve the collection, processing, and wireless transmission of data from various sensors and actuators. In these systems, data security is paramount to prevent unauthorized access or interception during transmission. The invention's secure communication mechanism, including the integration of a secured element for data encryption, ensures that IoT devices can transmit sensitive information

over wireless networks without compromising data integrity or privacy, thereby extending the benefits of the invention to a wide range of IoT applications.

[0058] **FIG. 6** illustrates a block diagram of an Internet of Things (IoT) device **600** having a secure communication system in accordance with an embodiment of the present invention. The IoT device **600** comprises sensors/actuators **602**, a processor/controller **604**, and an IoT communication module **606**. In traditional configurations, the IoT communication module **606** facilitates direct wireless communication with a network **608**, transmitting data over various wireless communication standards such as Wi-Fi, Bluetooth, or cellular networks (4G/5G). However, in such traditional systems, the transmitted data may be vulnerable to interception or hijacking during transmission, posing significant security risks.

[0059] To address these concerns, the present invention introduces a Secured Element and Communication Module **610**, which replaces the traditional IoT communication module **606**. This secure module **610** ensures that all data processed by the processor/controller **604** is encrypted prior to transmission, thereby enhancing the security of the IoT device **600**. The secured element integrated within the module **610** is responsible for encrypting the data using advanced cryptographic techniques, ensuring that even if the data is intercepted during transmission, it remains protected and unintelligible to unauthorized entities.

[0060] The sensors/actuators **602** gather data from the external environment, which is then processed by the processor/controller **604**. Instead of being directly transmitted via the conventional IoT communication module **606**, the processed data is routed through a secured communication pathway. The processor/controller **604** sends

the processed data to the Secured Element and Communication Module **610**, which first encrypts the data and then transmits it wirelessly through a secure communication channel. This secure communication can utilize standard wireless protocols but ensures that all transmitted data is encrypted and safe from interception or unauthorized access.

5 **[0061]** As mentioned above, the secured element is adopted as a core component of the present invention due to its widely recognized robustness and high level of security. Secured elements are specifically designed and certified to provide a tamper-resistant environment for storing sensitive data, such as cryptographic keys, and executing security-related functions. Unlike traditional software-based encryption
10 methods, secured elements operate in a hardware-based, isolated environment, making them virtually unbreachable by external attacks. This level of security is bolstered by stringent certifications such as Common Criteria (CC) or Federal Information Processing Standards (FIPS), ensuring that the secured element meets the highest security standards. By integrating a secured element into the IoT communication module, the present
15 invention ensures that data is encrypted and protected at the hardware level, making unauthorized access or decryption by adversaries exceedingly difficult, even if the communication is intercepted during transmission.

[0062] Embodiments of the present invention aims to perform a hardware encryption to the data before travelling in the air. While the IoT device **600** may already
20 have its own encryption/decryption provided by the original manufacturer, it is known to the skilled person that ordinary state of the art encryption method, hardware or software, still vulnerable to breach attached for the reason provided above. The secured element of the secured element and communication module **610** ensures that data that

leaves the communication module of the secured element and the communication module **610** is encrypted. Regardless of whether the data (encrypted) is transmitted through a router **608** or service provider, data remains encrypted until it is decrypted at the intended backend system (not shown). Even if an adversary attempts to hijack the communication, they will be unable to access the actual data due to the robust encryption provided by the secured element.

[0063] In one embodiment, this secure communication system can be integrated either during the initial manufacturing of the IoT device or, in another embodiment, retrofitted as an add-on kit, providing flexibility in implementation. In either embodiment, the inventor proposes to abandon the IoT communication module **606**, and replace the same with the secured element and communication module **610**. It is desired that the secured element and communication module **610**, in one embodiment, to be provided as one unit to ensure the compatibility between the secure element and the communication module. This also ensures that any legacy IoT systems can also benefit from the enhanced security features provided by this invention.

[0064] In the case whereby the secure element and communication module **610** is incorporated at initial manufacturing of the IoT device **600**, in one embodiment, the IoT **600** may be fabricated with the sensors/actuators **602**, the processor/controller **604** and the secured element and communication module **610** as one unifying device, i.e. pre-fabricated as one device. In another embodiment, the IoT **600** is prefabricated with only the sensors/actuators **602** and processor/controller **604**, with a interfacing port. The secured element and communication module **610** is pre-fabricated as a separate device

with a corresponding interfacing port, such that when in use, the secured element and communication module **610** is attached to the IoT **600** through the interfacing port.

[0065] In yet another embodiment, the secure element and communication module is fabricated as one modification kit. Users may perform the necessary manual modifications to any existing or legacy IoT devices to cut off their existing communication module **606** from the device and replace the same with the secure element and communication module **610** kit for performing the required encryption and transmission of the IoT device **600**.

[0066] This innovative solution significantly enhances the security of IoT devices by ensuring that all data transmitted from the device is encrypted, thus protecting sensitive information from unauthorized access, even in cases where the transmission is intercepted.

[0067] As described above, a person skill in the art would recognise that the secure element and the communication module **610** is equally applicable to FIG. 1 to FIG. 5. Specifically, the power meters **110** of FIG. 1 and **210** of FIG. 2 can be replaced by IoT devices and the backend system **120** of FIG. 1 and **220** of FIG 2 can be substituted with corresponding IoT backend system. In other words, the embodiments depicted in FIG. 1 to FIG. 5 are applicable for IoT devices with minimal modifications, with the exceptions IoT usually transmits through wireless means, such as Wi-Fi, 5G, or other wireless network, rather than the wired network as described in the previous figures.

[0068] It should be understood that the present invention is not limited to the specific embodiments described herein. The use of the secured element and

communication module is broadly applicable across various technologies beyond the disclosed examples. Any system or device requiring secure data transmission between upstream and downstream components can benefit from the integration of such secured elements. For example, is also applicable on CCTV network, EV charging network, EV

5 charging network to take advantages of the inventive ideas to protect the data network integrity, ensuring that transmitted information remains safeguarded from unauthorized access or interception, without departing from the scope of the invention.

Claims

1. An Internet of Things (IoT) network for transmitting data over the IoT network,
the network comprising:
- an IoT device adapted to communicate to a IoT backend;
 - 5 a communication module having a socket for locally connecting to the IoT
devices or the IoT backend system, as a gateway to transmit data over a communication
network;
 - a microprocessor acts as a control unit for the secure device and handling the data
flow;
 - 10 an FPGA chip operationally encrypting/decrypting the data;
 - a secure element for handling key diversification for encrypting/decrypting the
data by FPGA chip;
 - wherein the secure device is connected locally to the IoT devices and the IoT
backend system, operationally, encrypting/decrypting data transmitting through the
15 communication network, such that the data is end-to-end encrypted across the IoT
network by the secure device.
2. The secure device of Claim 1, wherein the secure element is certified by Common
Criteria (CC) or Federal Information Processing Standards (FIPS).
- 20
3. The secure device of Claim 1, wherein the secure device further comprises an
admin authenticator for access authentication to the secure device.

4. The secure device of Claim 3, wherein the admin authenticator is in a card form having its own secure element embedded therein.
5. The secure device of Claim 3, wherein the admin authenticator is integrated on
5 the secure device in a form of biometric scanner/sensor.
6. The secure device of Claim 3, wherein the admin authenticator is deployed remotely from the secure device.
- 10 7. An IoT network having a plurality of IoT devices connected to an IoT backend system via a communication network, the IoT network comprising:
a secure device of any one of the Claims 1- 6,
wherein the secure device is connected locally and directly to the IoT devices such that data passes through the secure device before transmitting to the communication
15 network, and another secure device connected directly before the IoT backend system.
8. A method for providing additional encryption/decryption for a IoT network over a communication network, the method comprising:
adding secured devices to the IoT network having IoT devices and an IoT
20 backend system connected through the communication network;
activating secured elements of the secured devices;
encrypting data from IoT devices through the secured devices;
transmitting the encrypted data to the IoT backend system through the communication network; and

decrypting the encrypted by the secured devices for processing by the IoT backend system,

wherein data transmitted through the communication network is end-to-end encrypted by the secure devices, wherein these devices offer enhanced protection against
5 unauthorized access by employing advanced encryption standards.

9. The method of Claim 8, wherein the end-to-end encryption is done by the security device in accordance with any one of claim 1-6.