



(51) International Patent Classification:
H04L 9/40 (2022.01)

(21) International Application Number:
PCT/IB2021/060739

(22) International Filing Date:
19 November 2021 (19.11.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **ABB SCHWEIZ AG** [CH/CH]; Brugger
Strasse 66, CH-5400 Baden (CH).

(72) Inventors: **TT, Mini**; 40, Yash Classic Enclave, Kalyan
Nagar, Karnataka, Bangalore 560043 (IN). **SABU, Bo-
by**; Kochupurackal, Paingottoor, Kothamangalam, Kerala

686671 (IN). **VS, Adhin**; Vellachalil (H), Sasimala post,
Pulpally, Kerala 673579 (IN).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,
KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,
NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: METHOD FOR VERIFYING IDENTITY OF INDUSTRIAL DEVICE, AN INDUSTRIAL DEVICE AND A COM-
PUTING SYSTEM

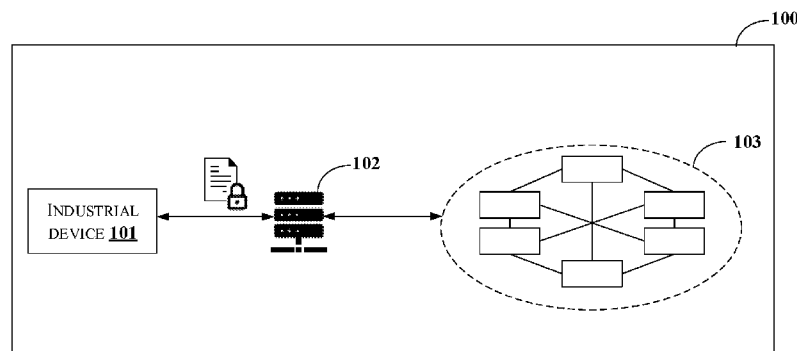


FIGURE 1A

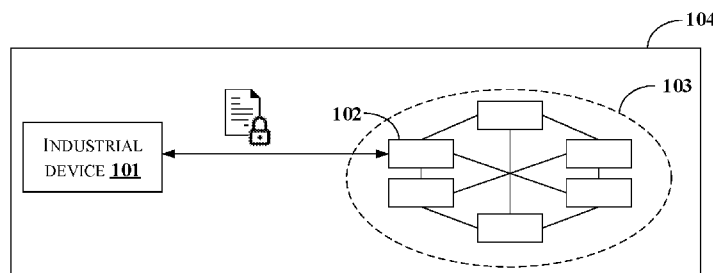


FIGURE 1B

(57) Abstract: The present disclosure relates to a method, an industrial device (101), and a computing system (102) for verifying identity of the industrial device (101). The method comprises obtaining an encryption key associated with an identity information of the industrial device (101). The identity information is stored in the industrial device (101). Further, the method comprises generating a digital signature for measurement data of the industrial device (101), using the encryption key, to obtain signed measurement data. Furthermore, the method comprises transmitting the signed measurement data, to a computing system (102). The computing system (102) receives the signed measurement data from the industrial device (101). Further, the computing system verifies the signed measurement data, based on identity information of the industrial device (101) stored in the computing system (102).

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

- *with international search report (Art. 21(3))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

TITLE: “METHOD FOR VERIFYING IDENTITY OF INDUSTRIAL DEVICE, AN INDUSTRIAL DEVICE AND A COMPUTING SYSTEM”

TECHNICAL FIELD

[001] The present disclosure generally relates to industrial devices. More particularly, the present disclosure relates to a method, an industrial device, and a computing system for verifying identity of the industrial device.

BACKGROUND

[002] An industrial plant comprises multiple industrial devices. The industrial devices generally include measurement devices that are used to measure values of parameters such as temperature, pressure, flow, level, and the like. The measurement devices transmit the measured values (also termed as measurement data) to a system for storing, processing, analysis, and the like. Certain measurement data needs to be secured and transmitted to the system without being tampered. An example of the measurement data can include emission values of the industrial plant in an application of emission monitoring. The emission values may be transmitted periodically to regulatory bodies. It is essential that such measurement data is not tampered. Hence, various techniques are used to secure the measurement data. For example, the industrial device may transmit the measurement data to the regulatory bodies over a blockchain network. Other applications include, for example, custody transfer, verification, and the like.

[003] It is equally necessary to ensure that data integrity is maintained when the measurement data is transmitted from the industrial device to the system. In order to establish the data integrity, authenticity of the industrial device also needs to be ensured. Identity of the device is a key factor in establishing authenticity. The traceability of the measurement data and the authenticity of the industrial device has to be ensured. In conventional systems, there is no mechanism to verify the identity of the industrial device. The authenticity of the measurement data is not ensured when received at an edge device and further at the blockchain network. Hence, there is a need for a system that overcomes one or more limitations of the above-described systems.

[004] The information disclosed in this background of the disclosure section is only for enhancement of understanding of the general background of the invention and should not be

taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

SUMMARY

[005] In an embodiment, the present disclosure discloses a method for verifying identity of an industrial device. The method comprises obtaining an encryption key associated with an identity information of the industrial device. The identity information is stored in the industrial device. Further, the method comprises generating a digital signature for measurement data of the industrial device, using the encryption key, to obtain signed measurement data. Furthermore, the method comprises transmitting the signed measurement data, to a computing system. The authenticity of the digital signature is verified using the identity information stored in the computing system, thereby verifying the identity of the industrial device.

[006] In an embodiment, the present disclosure discloses an industrial device comprising a sensing unit, a communication interface, and a processor. The processor is configured to obtain an encryption key associated with an identity information of the industrial device. The identity information is stored in the industrial device. Further, the processor is configured to generate a digital signature for measurement data of the industrial device, using the encryption key, to obtain signed measurement data. Furthermore, the processor is configured to transmit the signed measurement data, to a computing system. The authenticity of the digital signature is verified using the identity information stored in the computing system, thereby verifying the identity of the industrial device.

[007] In an embodiment, the present disclosure discloses a computing system for verifying identity of an industrial device. The computing system comprises a communication interface, one or more processors, and a memory. The one or more processors are configured to receive signed measurement data from the industrial device. The signed measurement data is measurement data of the industrial device associated with a digital signature. Further, the one or more processors are configured to verify the signed measurement data, based on identity information of the industrial device stored in the computing system, thereby verifying the identity of the industrial device.

[008] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further

aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

[009] The novel features and characteristics of the disclosure are set forth in the appended claims. The disclosure itself, however, as well as a preferred mode of use, further objectives, and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying figures. One or more embodiments are now described, by way of example only, with reference to the accompanying figures wherein like reference numerals represent like elements and in which:

[0010] Figures 1A and 1B illustrate an exemplary environment for verifying identity of an industrial device, in accordance with some embodiments of the present disclosure;

[0011] Figure 2 illustrates an internal architecture of an industrial device, in accordance with some embodiments of the present disclosure;

[0012] Figure 3 shows an exemplary flow chart illustrating method steps for verifying identity of an industrial device, in accordance with some embodiments of the present disclosure;

[0013] Figure 4 shows exemplary illustration for verifying identity of an industrial device, in accordance with some embodiments of the present disclosure;

[0014] Figure 5 illustrates an internal architecture of a computing system for verifying identity of the industrial device, in accordance with some embodiments of the present disclosure;

[0015] Figure 6 shows an exemplary flow chart illustrating method steps for verifying identity of an industrial device, in accordance with some embodiments of the present disclosure;

[0016] Figure 7 shows exemplary illustration for verifying identity of an industrial device, in accordance with embodiments of the present disclosure; and

[0017] Figure 8 shows a block diagram of a general-purpose computing system for verifying identity of an industrial device, in accordance with embodiments of the present disclosure.

[0018] It should be appreciated by those skilled in the art that any block diagram herein represents conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and executed by a computer or processor, whether or not such computer or processor is explicitly shown.

DETAILED DESCRIPTION

[0019] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0020] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternatives falling within the scope of the disclosure.

[0021] The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a system or apparatus preceded by "comprises... a" does not, without more constraints, preclude the existence of other elements or additional elements in the system or apparatus.

[0022] Embodiments of the present disclosure relate to a method, an industrial device, and a computing system for verifying identity of the industrial device. Identity information of the industrial device is generally stored in the industrial device. A device certificate including the identity information is stored in the computing system. Further, when a measurement is made by the industrial device, measurement data is digitally signed and transmitted to the computing system. Digital signature is generated based on an encrypted key which is associated with the identity information. The computing system receives the digitally signed measurement data and verifies the authenticity of the industrial device using the already stored device certificate

which includes the identity information. The traceability of the measurement data from the point of measurement is achieved, which ensures data integrity across data flow path from the industrial device to other systems.

[0023] Figure 1A illustrates an exemplary environment 100 for verifying identity of an industrial device, in accordance with some embodiments of the present disclosure. The exemplary environment 100 comprises an industrial device 101, a computing system 102, and a blockchain network 103. The industrial device 101 may be part of an industrial plant or a process plant comprising multiple industrial devices. The industrial device 101 may be used to measure values of one or more parameters such as temperature, pressure, force, and the like. For example, the industrial device 101 may be a gas analyzer, a flowmeter, a level transmitter, a positioner, a pressure transmitter, a temperature sensor, and the like. In a non-limiting embodiment, the industrial device 101 may also include actuators, such as motors, generators, and electronic components such as drive, circuit breakers. In an embodiment, the industrial device 101 may transmit the measured values (also termed as measurement data) to the computing system 102. The computing system 102 may perform pre-processing, post-processing, analysis of the measurement data, and the like. For example, the computing system 102 may be an edge device. The computing system 102 may be a computing device such as a laptop computer, a desktop computer, a Personal Computer (PC), a notebook, a smartphone, a tablet, e-book readers, a server, a network server, a cloud-based server, router, and the like. Further, the computing system 102 may transmit the measurement data to a blockchain server over the blockchain network 103. The blockchain network 103 is a digital ledger used to record data transactions across multiple computer systems securely. The blockchain network 103 comprises a plurality of servers (also referred as the blockchain servers). Each of the plurality of servers may be a computing entity such as a computer or a server. The plurality of servers may be accessed by a plurality of entities to store, monitor, analyze and control operations of the industrial plant in general. For example, the plurality of entities may be end customer organization, service organization, vendor organization, channel partner organization, integrator organization, control system organization, and the like. The computing system 102 may transmit the measurement data to a server among the plurality of servers in the blockchain network 103. In an example, the computing system 102 may perform pre-processing of the measurement data. Further, the computing system 102 may transmit the measurement data to the server for further processing of the measurement data, analysis of the measurement data for diagnosis of the industrial device 101, and the like. In another example, the computing system

102 may perform pre-processing and analysis of the measurement data. Further, the computing system 102 may transmit measurement data to the server for further analysis of the measurement data. In another embodiment, the computing system 102 may be a server in the blockchain network 103. An exemplary environment 104 for this embodiment is shown in Figure 1B. The industrial device 101 may transmit the measurement data directly to the server for processing, analysis, storing and the like.

[0024] Typically, when the industrial device 101 is manufactured, device information is provided to the industrial device 101. The device information is unique to each industrial device 101. Further, identity information is generated and stored during configuration of the industrial device 101 in the industrial plant or the process plant. The identity information comprises the device information associated with the industrial device 101 and an encryption key. For example, a key pair having a private key and public key is generated. The private key may be stored in the industrial device 101. The public key may be included in the identity information. Further, the identity information may be transmitted to the computing system 102. For example, the identity information may be transmitted during a handshaking process between the industrial device 101 and the computing system 102. The computing system 102 may store the identity information for future verification of the industrial device 101. The industrial device 101 obtains the encryption key when measurement data is generated in the industrial device 101. Further, the industrial device 101 generates a digital signature for the measurement data of the industrial device 101. The digital signature is generated using the encryption key. The measurement data associated with the digital signature is known as signed measurement data, in the present disclosure. Further, the industrial device 101 transmits the signed measurement data to the computing system 102. The computing system 102 receives the signed measurement data from the industrial device 101. Further, the computing system 102 verifies the signed measurement data using the identity information stored in the computing system 102.

[0025] Figure 2 illustrates an internal architecture of the industrial device 101, in accordance with some embodiments of the present disclosure. The industrial device 101 may comprise a sensing unit 201, a processor 202, and a communication interface 203. The sensing unit 201 may be an input device that provides an output signal with respect to a physical quantity (input). The sensing unit 201 may be a sensor. For example, the sensing unit 201 may be a temperature sensor, a flow sensor, a gas sensor, a pressure sensor, and the like. The sensing unit 201 may

sense the input from an environment (the industrial plant). Further, the sensing unit 201 may output the measurement data. For example, the measurement data may include temperature values, pressure values, concentration of gases, and the like.

[0026] The processor 202 may be configured to receive the measurement data from the sensing unit 201. In an embodiment, the processor 202 may be a secure cryptoprocessor. The secure cryptoprocessor is a dedicated computer-on-a-chip or microprocessor for carrying out cryptographic operations. The cryptoprocessor is embedded in a packaging with multiple physical security measures, which gives it a degree of tamper resistance. For example, the secure cryptoprocessor may be a Hardware Security Module (HSM). The HSM contains one or more secure cryptoprocessor chips. The cryptoprocessor does not reveal keys or executable instructions on a bus, except in encrypted form, and zeros keys by attempts at probing or scanning. The crypto chip(s) may also be potted in the hardware security module with other processors and memory chips that store and process encrypted data. Any attempt to remove the potting will cause the keys in the cryptoprocessor chip to be zeroed. In another embodiment, the processor 202 may be part of a computing device with trusted computing. The computing device may be associated with a cryptographic chip for enabling a secure environment. For example, the cryptographic chip may be a Trusted Platform Module (TPM). The TPM is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. In one embodiment, the industrial device 101 may include a plurality of processors. For example, a general-purpose processor may be used to obtain the measurement data from the sensing unit 201 and process the measurement data. Further, the industrial device 101 can include the secure cryptoprocessor storing the identity information and the encryption keys. The secure cryptoprocessor receives the measurement data from the general-purpose processor. Further, the secure cryptoprocessor digitally signs the measurement data using the encryption keys and provides the digitally signed measurement data back to the general-purpose processor for transmitting to the computing system 102. In some embodiments, the tasks of the general-purpose processor and the secure cryptoprocessor can be performed by a single processor. A person skilled in the art will appreciate that the industrial device 101 can have different types of processors/ controllers, and all such scope is envisaged by the present disclosure.

[0027] The processor 202 is configured to obtain the encryption key associated with the identity information of the industrial device 101. The identity information may comprise device

information associated with the industrial device 101 and a public key associated with the encryption key. The encryption key may be a private key. The encryption key may be securely stored in the secure cryptoprocessor. The secure cryptoprocessor may be communicatively coupled to a dedicated memory. The encryption key may be stored in the dedicated memory. The identity information of the industrial device 101 may be stored outside the dedicated memory. For example, the identity information may be stored in a memory of the computing device, when the processor 202 is part of the computing device with trusted computing.

[0028] Further, the processor 202 may be configured to generate the digital signature for the measurement data of the industrial device 101, using the encryption key, to obtain signed measurement data. The digital signature is generated using the private key stored in the secure cryptoprocessor. Furthermore, the processor 202 is configured to transmit the signed measurement data, to the computing system 102. The processor 202 may transmit the signed measurement data via the communication interface 203 over a communication network. The communication interface 203 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. The communication interface 203 may employ connection protocols include, but not limited to, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0029] Figure 3 shows an exemplary flow chart illustrating method steps for verifying identity of the industrial device 101, in accordance with some embodiments of the present disclosure. As illustrated in Figure 3, the method 300 may comprise one or more steps. The method 300 may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform particular functions or implement particular abstract data types.

[0030] The order in which the method 300 is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the scope of the subject matter described herein. Furthermore, the

method can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0031] At step 301, the industrial device 101 obtains the encryption key associated with the identity information of the industrial device 101. In an embodiment, the encryption key is the private key. As the encryption key is used for authenticating the industrial device 101, the private key among the keypair including the private key and public key is obtained. The identity information may comprise device information associated with the industrial device 101 and the public key associated with the encryption key. In an embodiment, the private key and the public key may be generated during manufacturing process within the industrial device 101. Also, the device information such as a unique ID for the device, device name, device model and make, and such details may be generated during the manufacturing process and stored in the industrial device 101. The private key and the public key may be generated using a public key algorithm, such as RSA (Rivest-Shamir-Adleman) technique. A person skilled in the art will appreciate that any methods other than the above-mentioned technique may be used to generate a key-pair (the private key and the public key). The private key and the public key are mathematically linked with each other. The private key and the public key may be transmitted securely to an issuing entity. The issuing entity may be a certificate authority. The certification authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by named subject of the certificate. This allows other parties to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. For example, the digital certificate may be in a X.509 format. The issuing entity may transmit the digital certificate, upon receiving the private key and the public key from the industrial device 101. In another embodiment, the private key and the public key may be provided by the issuing entity. The digital certificate is termed as the identity information in the present description. The identity information may comprise device information such as device identification (ID), issuing entity ID, manufacturer ID, validity period of the digital certificate, and the like. Further, the identity information may comprise the public key. The identity information may be stored in a memory of the industrial device 101. The private key may be securely stored in the dedicated memory associated with the secure cryptoprocessor. Referring to example 400 of Figure 4, the industrial device 101 is a gas analyzer. The sensing unit 201 may measure concentration of gases in the industrial plant. At step 1, the sensing unit 201 may provide the measurement data to the secure cryptoprocessor 202. At step 2, the secure cryptoprocessor 202

may obtain the encryption key securely stored in a dedicated memory 401 associated with the secure cryptoprocessor 202.

[0032] Referring back to Figure 3, at step 302, the industrial device 101 generates the digital signature for the measurement data of the industrial device 101. The industrial device 101 generates the digital signature using the encryption key. The encryption key is the private key. Firstly, the measurement data is hashed using known cryptographic hashing functions such as SHA-256, SHA-512, and the like. The hashed data is encrypted using the private key which is termed as the digital signature. This is also referred as the signed measurement data in the present description. The digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature identifies that the message was created by a known sender (authentication), and that the message was not altered in transit. The digital signature may be generated using a digital signature technique such as Elliptic curve (EC) cryptography, RSA technique, and the like. Elliptic curve cryptography uses one-way hash functions and point multiplication to compute points on an elliptic curve. A person skilled in the art will appreciate that any known methods other than the above-mentioned techniques may be used to generate the digital signature using the encryption key. Referring again to the example 400 of Figure 4, at step 3, the secure cryptoprocessor generates the digital signature for the measurement data using the encryption key, to obtain the signed measurement data.

[0033] Referring back to Figure 3, at step 303, the industrial device 101 transmits the signed measurement data, to the computing system 102. The industrial device 101 may transmit the signed measurement data via the communication interface 203. In an embodiment, the computing system 102 is an edge device. The signed measurement data may be transmitted to the blockchain network 103 for processing, analysis, and the like, via the edge device. In another embodiment, the computing system 102 is a server in the blockchain network 103. The signed measurement data may be transmitted directly from the industrial device 101 to the blockchain network 103. The computing system 102 may verify the authenticity of the digital signature is using the identity information stored in the computing system 102, thereby verifying the identity of the industrial device 101. Referring again to the example 400 of Figure 4, at step 4, the secure cryptoprocessor 202 transmits the signed measurement data to the computing system 102. In an example, the server may be associated with a regulatory authority which monitors whether

emission level of the industrial plant is exceeding above a permitted limit. The server may receive the signed measurement data comprising values of concentration of gases.

[0034] Figure 5 illustrates an internal architecture of the computing system 102 for verifying the identity of the industrial device 101, in accordance with some embodiments of the present disclosure. The computing system 102 may comprise one or more processors 501, a memory 502, and a communication interface 503. Only one processor is shown in Figure 5, for illustrative purposes only, and should not be considered as limiting. In some embodiments, the memory 502 may be communicatively coupled to the one or more processors 501. The memory 502 stores instructions executable by the one or more processors 501. The one or more processors 501 may comprise at least one data processor for executing program components for executing user or system-generated requests. The memory 502 may be communicatively coupled to the one or more processors 501. The memory 502 stores instructions, executable by the one or more processors 501, which, on execution, may cause the one or more processors 501 to verify the identity of the industrial device 101. The one or more processors 501 may be configured to receive the signed measurement data from the industrial device 101, via the communication interface 503 over a communication network. The communication interface 503 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. The communication interface 503 may employ connection protocols include, but not limited to, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. Further, the one or more processors 501 may be configured to verify the signed measurement data, based on the identity information of the industrial device 101 stored in the computing system 102.

[0035] Figure 6 shows an exemplary flow chart illustrating method steps for verifying identity of the industrial device 101, in accordance with some embodiments of the present disclosure. As illustrated in Figure 6, the method 600 may comprise one or more steps. The method 600 may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data

structures, procedures, modules, and functions, which perform particular functions or implement particular abstract data types.

[0036] The order in which the method 600 is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0037] At step 601, the computing system 102 receives the signed measurement data from the industrial device 101. In an embodiment, the computing system 102 receives the identity information from the industrial device 101 during handshaking process between the industrial device 101 and the computing system 102. The identity information is the certificate associated with the industrial device 101 comprising the device information and the public key associated with the encryption key. The computing system 102 uses the identity information to verify the identity of the industrial device 101 every time the measurement data is received from the industrial device 101. In another embodiment, the computing system 102 may request the industrial device 101 for the identity information when required by the computing system 102 during further communication between the industrial device 101 and the computing system 102. The computing system 102 may receive the signed measurement data i.e., the measurement data of the industrial device 101 associated with the digital signature. The signed measurement data may be received via the communication interface 503 over the communication network. Referring to example 700 of Figure 7, at step A refers to handshaking process between the industrial device 101 and the computing system 102. At step A, the identity information of the industrial device 101 is received by the computing system 102. Step A is a one-time process between the industrial device 101 and the computing system 102. At step 1, the computing system 102 receives the signed measurement data from the industrial device 101. In an embodiment, the identity information may be shared with the plurality of servers. Therefore, when the digitally signed measurement data is shared with the plurality of servers, each of the plurality of servers can verify the authenticity of the industrial device 101.

[0038] At step 602, the computing system 102 verifies the signed measurement data, based on the identity information of the industrial device 101. The identity information is stored in the computing system 102. The computing system 102 may retrieve the public key from the identity

information of the industrial device 101. Further, the computing system 102 may be configured to decrypt the signed measurement data using the public key. The public key corresponds to the private key used to generate the digital signature for the measurement data. The computing system 102 may perform the decryption using a technique used to generate the digital signature. For example, the RSA technique may be used by the industrial device 101 to generate the digital signature. The computing system 102 may decrypt the signed measurement data using the RSA technique. A successful decryption identifies that the signed measurement data is received from a valid source (the industrial device 101). The decryption fails when the signed measurement data is tampered and received from other source. Referring to the example 700 of Figure 7, at step 2, the computing system 102 retrieves the public key from the memory 502 associated with the computing system 102. At step 3, the computing system 102 verifies the signed measurement data by decrypting the signed measurement data using the public key. Referring to the example stated in paragraph 33 of the present description, the authenticity of the signed measurement data can be validated by the regulatory authority and identity of the industrial device 101 can be verified. Hence, there is a trust that the signed measurement data is received from valid industrial device 101 and data integrity is ensured.

[0039] In an embodiment, the computing system 102 may transmit the measurement data of the industrial device 101 with or without the digital signature to other computing systems. In an example, the computing system 102 may transmit the measurement data to a regulatory authority. The measurement data may be transmitted with the digital signature, so that the regulatory authority may verify the identity of industrial device 101. In another example, the computing system 102 may transmit the measurement data of the industrial device 101 associated with a company X to a company Y. The company Y may require the measurement data of the industrial device 101 for documentation purpose. The company Y need not know specific industrial device 101 of the company X providing the measurement data. In such cases, the identity of the industrial device 101 may be hidden. Hence, the present invention provides methods to provide the signed measurement data when the identity of the industrial device 101 has to be verified.

COMPUTER SYSTEM

[0040] Figure 8 illustrates a block diagram of an exemplary computer system 800 for implementing embodiments consistent with the present disclosure. In an embodiment, the computer system 800 may be used to implement the computing system 102. Thus, the computer

system 800 may be used to verify the identity of the industrial device 101. The computer system 800 may comprise a Central Processing Unit 802 (also referred as “CPU” or “processor”). The processor 802 may comprise at least one data processor. The processor 802 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0041] The processor 802 may be disposed in communication with one or more input/output (I/O) devices (not shown) via I/O interface 801. The I/O interface 801 may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, RCA, stereo, IEEE (Institute of Electrical and Electronics Engineers) -1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

[0042] Using the I/O interface 801, the computer system 800 may communicate with one or more I/O devices. For example, the input device 810 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output device 811 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, Plasma display panel (PDP), Organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0043] The processor 802 may be disposed in communication with the communication network 809 via a network interface 803. The network interface 803 may communicate with the communication network 809. The network interface 803 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 809 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. The network interface 803 may employ connection protocols include, but not limited to, direct connect, Ethernet (e.g., twisted pair 10/100/1000

Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0044] The communication network 809 includes, but is not limited to, a direct interconnection, an e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi, and such. The first network and the second network may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the first network and the second network may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0045] In some embodiments, the processor 802 may be disposed in communication with a memory 805 (e.g., RAM, ROM, etc. not shown in Figure 8) via a storage interface 804. The storage interface 804 may connect to memory 805 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as serial advanced technology attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fiber channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0046] The memory 805 may store a collection of program or database components, including, without limitation, user interface 806, an operating system 807, web browser 808 etc. In some embodiments, computer system 800 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle ® or Sybase®.

[0047] The operating system 807 may facilitate resource management and operation of the computer system 800. Examples of operating systems include, without limitation, APPLE MACINTOSH^R OS X, UNIX^R, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTIONTM (BSD), FREEBSDTM, NETBSDTM, OPENBSDTM, etc.), LINUX DISTRIBUTIONSTM (E.G., RED HATTM, UBUNTUTM, KUBUNTUTM, etc.), IBMTM

OS/2, MICROSOFTTM WINDOWSTM (XPTM, VISTATM/7/8, 10 etc.), APPLE^R IOSTM, GOOGLE^R ANDROIDTM, BLACKBERRY^R OS, or the like.

[0048] In some embodiments, the computer system 800 may implement the web browser 808 stored program component. The web browser 808 may be a hypertext viewing application, for example MICROSOFT^R INTERNET EXPLORERTM, GOOGLE^R CHROME^{TM0}, MOZILLA^R FIREFOXTM, APPLE^R SAFARITM, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 808 may utilize facilities such as AJAXTM, DHTMLTM, ADOBE^R FLASHTM, JAVASCRIPTTM, JAVATM, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 800 may implement a mail server (not shown in Figure) stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASPTM, ACTIVEXTM, ANSITM C++/C#, MICROSOFT^R, .NETTM, CGI SCRIPTSTM, JAVATM, JAVASCRIPTTM, PERLTM, PHPTM, PYTHONTM, WEBOBJECTSTM, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), MICROSOFT^R exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system 800 may implement a mail client stored program component. The mail client (not shown in Figure) may be a mail viewing application, such as APPLE^R MAILTM, MICROSOFT^R ENTOURAGETM, MICROSOFT^R OUTLOOKTM, MOZILLA^R THUNDERBIRDTM, etc.

[0049] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc Read-Only Memory (CD ROMs), Digital Video Disc (DVDs), flash drives, disks, and any other known physical storage media.

[0050] Embodiments of the present disclosure allows verification of authenticity of the digital signature for verifying the identity of the industrial device. The traceability of the measurement data from the point of measurement is achieved, which ensures data integrity across data flow path from the industrial device to other systems.

[0051] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0052] The terms "including", "comprising", "having" and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0053] The enumerated listing of items does not imply that any or all of the items are mutually exclusive, unless expressly specified otherwise. The terms "a", "an" and "the" mean "one or more", unless expressly specified otherwise.

[0054] A description of an embodiment with several components in communication with each other does not imply that all such components are required. On the contrary a variety of optional components are described to illustrate the wide variety of possible embodiments of the invention.

[0055] When a single device or article is described herein, it will be readily apparent that more than one device/article (whether or not they cooperate) may be used in place of a single device/article. Similarly, where more than one device or article is described herein (whether or not they cooperate), it will be readily apparent that a single device/article may be used in place of the more than one device or article or a different number of devices/articles may be used instead of the shown number of devices or programs. The functionality and/or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality/features. Thus, other embodiments of the invention need not include the device itself.

[0056] The illustrated operations of Figures 3 and 5 show certain events occurring in a certain order. In alternative embodiments, certain operations may be performed in a different order, modified, or removed. Moreover, steps may be added to the above-described logic and still conform to the described embodiments. Further, operations described herein may occur

sequentially or certain operations may be processed in parallel. Yet further, operations may be performed by a single processing unit or by distributed processing units.

[0057] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based here on. Accordingly, the disclosure of the embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

[0058] While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope being indicated by the following claims.

Referral Numerals:

Referral number	Description
100	Exemplary environment
101	Industrial device
102	Computing system
103	Blockchain network
104	Exemplary environment
201	Sensing unit
202	Processor
203	Communication interface
400	Example
401	Memory
501	Processor
502	Memory
503	Communication Interface
700	Example
800	Computer system
801	I/O interface

802	Processor
803	Network interface
804	Storage interface
805	Memory
806	User interface
807	Operating system
808	Web browser
809	Communication network
810	Input device
811	Output device

We claim:

1. A method for verifying identity of an industrial device (101), the method comprising:
 - obtaining, by a processor (202), an encryption key associated with an identity information of the industrial device (101), wherein the identity information is stored in the industrial device (101);
 - generating, by the processor (202), a digital signature for measurement data of the industrial device (101), using the encryption key, to obtain signed measurement data; and
 - transmitting, by the processor (202), the signed measurement data, to a computing system (102), wherein authenticity of the digital signature is verified using the identity information stored in the computing system (102), thereby verifying the identity of the industrial device (101).
2. The method of claim 1, wherein the measurement data of the industrial device (101) is received from a sensing unit (201) associated with the industrial device (101).
3. The method of claim 1, wherein the encryption key is a private key.
4. The method of claim 1, wherein the identity information comprises device information associated with the industrial device (101) and a public key associated with the encryption key.
5. The method of claim 1, wherein the identity information is transmitted to the computing system (102) during handshaking process between the industrial device (101) and the computing system (102).
6. An industrial device (101) comprising:
 - a sensing unit (201);
 - a communication interface (203); and
 - a processor (202), configured to:
 - obtain an encryption key associated with an identity information of the industrial device (101), wherein the identity information is stored in the industrial device (101);
 - generate a digital signature for measurement data of the industrial device (101), using the encryption key, to obtain signed measurement data; and

transmit the signed measurement data, to a computing system (102), wherein authenticity of the digital signature is verified using the identity information stored in the computing system (102), thereby verifying the identity of the industrial device (101).

7. The industrial device (101) of claim 6, wherein the processor (202) is configured to receive the measurement data of the industrial device (101) from the sensing unit (201) associated with the industrial device (101).
8. The industrial device (101) of claim 6, wherein the encryption key is a private key.
9. The industrial device (101) of claim 6, wherein the identity information comprises device information associated with the industrial device (101) and a public key associated with the encryption key.
10. The industrial device (101) of claim 6, wherein the processor (202) transmits the identity information to the computing system (102) during handshaking process between the industrial device (101) and the computing system (102).
11. A computing system (102) for verifying identity of an industrial device (101), the computing system (102) comprising:
 - a communication interface (503);
 - one or more processors (501);
 - a memory (502) storing processor-executable instructions, which, on execution, cause the one or more processors (501) to:
 - receive signed measurement data from the industrial device (101), wherein the signed measurement data is measurement data of the industrial device (101) associated with a digital signature; and
 - verify the signed measurement data, based on identity information of the industrial device (101) stored in the computing system (102), thereby verifying the identity of the industrial device (101).
12. The computing system (102) of claim 11, wherein the identity information comprises device information associated with the industrial device (101) and a public key associated with the industrial device (101).

13. The computing system (102) of claim 11, wherein the one or more processors (501) verifies the signed measurement data by decrypting the signed measurement data using a public key corresponding to a private key, wherein the private key is used to generate the digital signature for the measurement data.
14. The computing system (102) of claim 11, wherein the one or more processors (501) receive the identity information from the industrial device (101) during handshaking process between the industrial device (101) and the computing system (102).
15. The computing system (102) of claim 11, wherein the computing system (102) is one of, an edge device and a server in a blockchain network (103), associated with the industrial device (101).

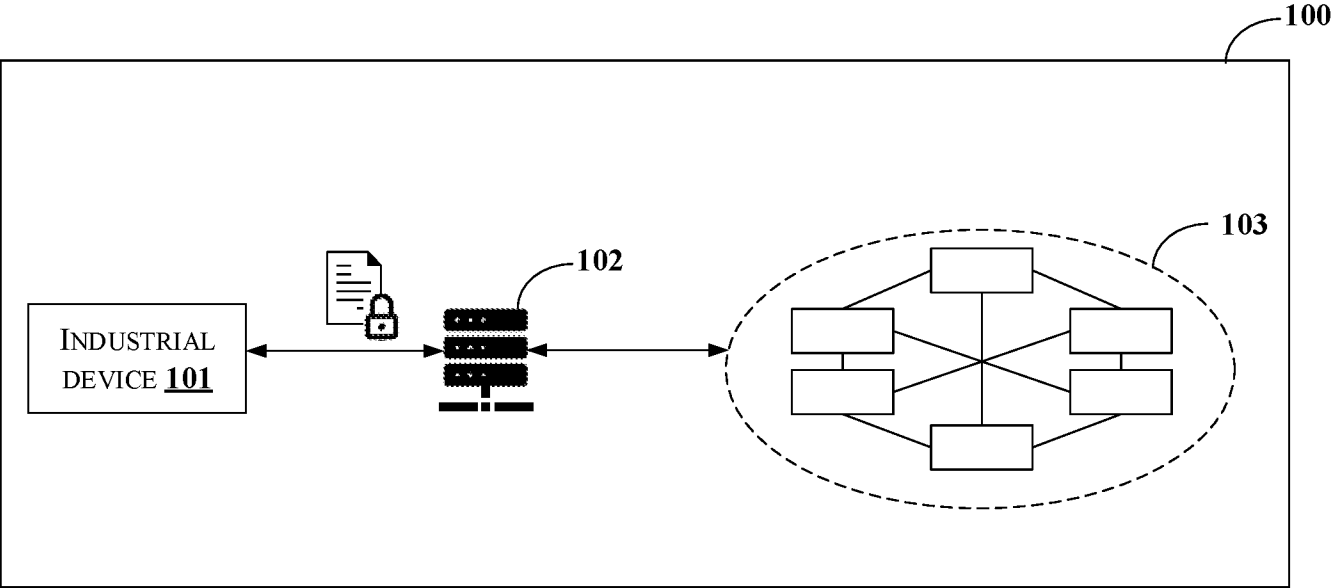


FIGURE 1A

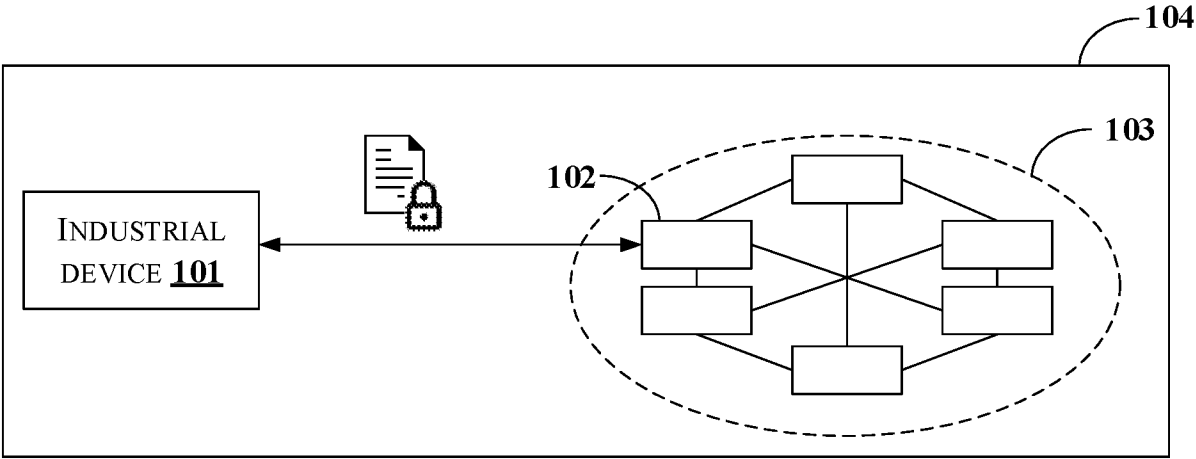


FIGURE 1B

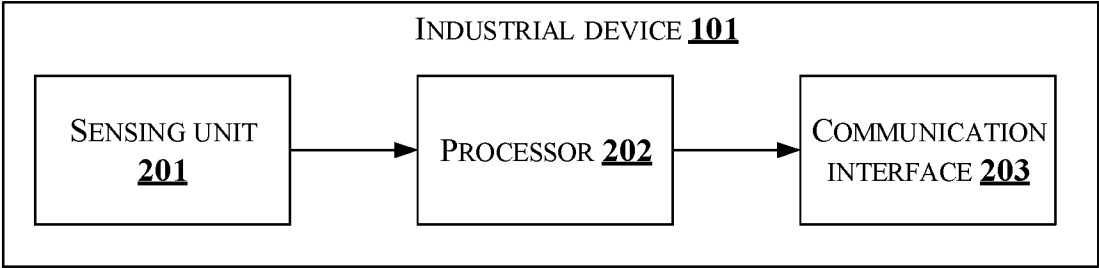


FIGURE 2

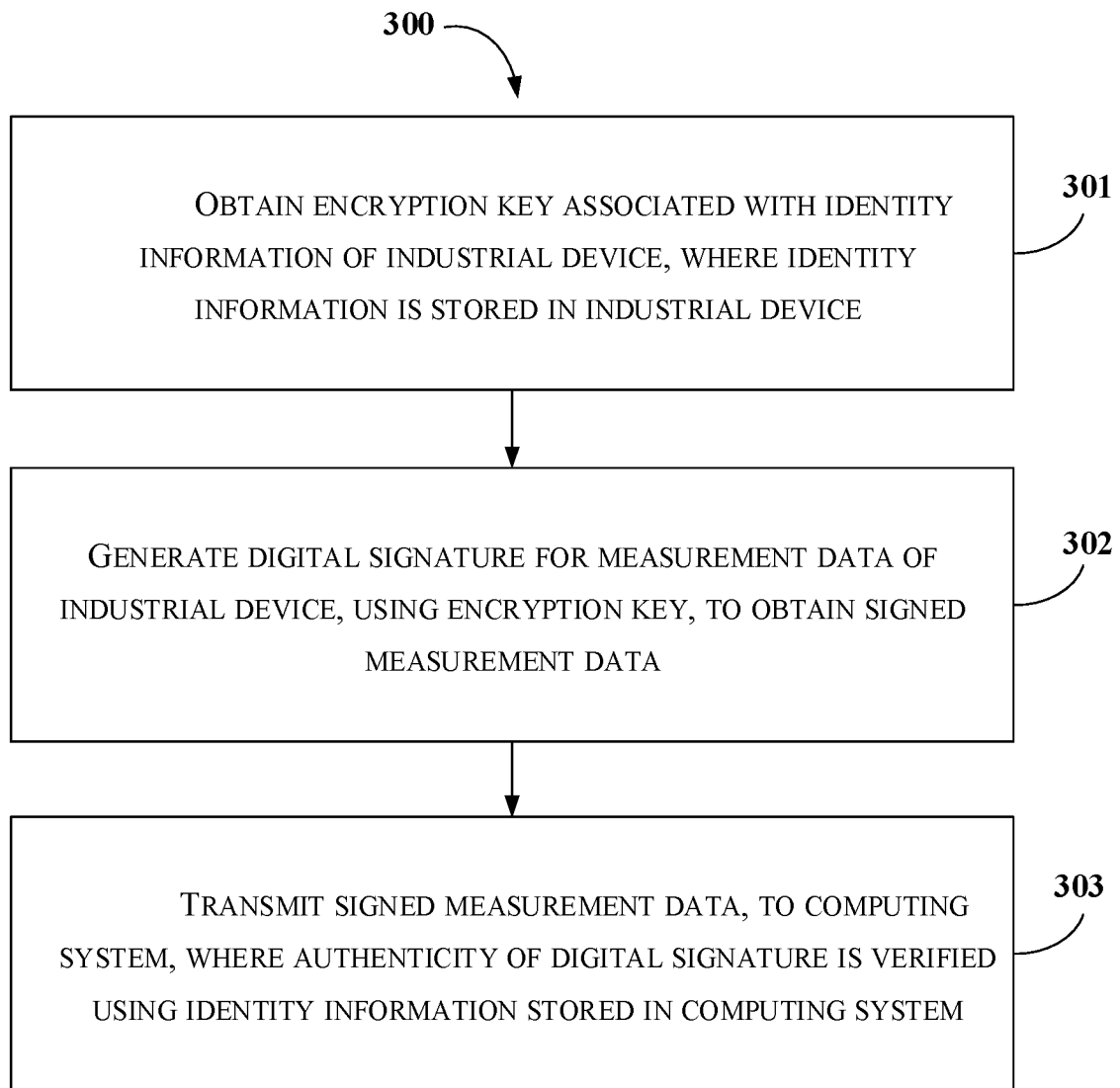


FIGURE 3

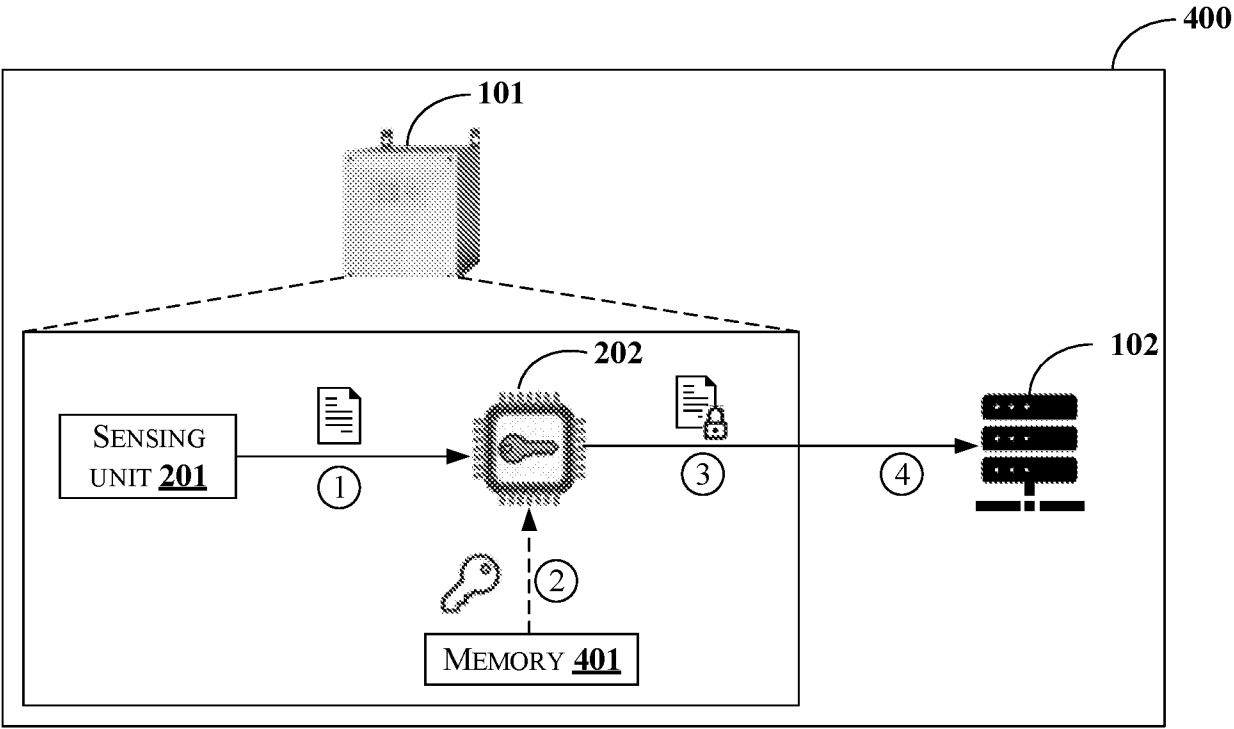


FIGURE 4

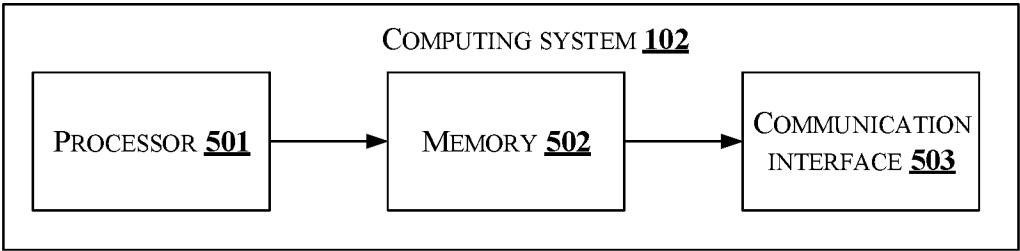


FIGURE 5

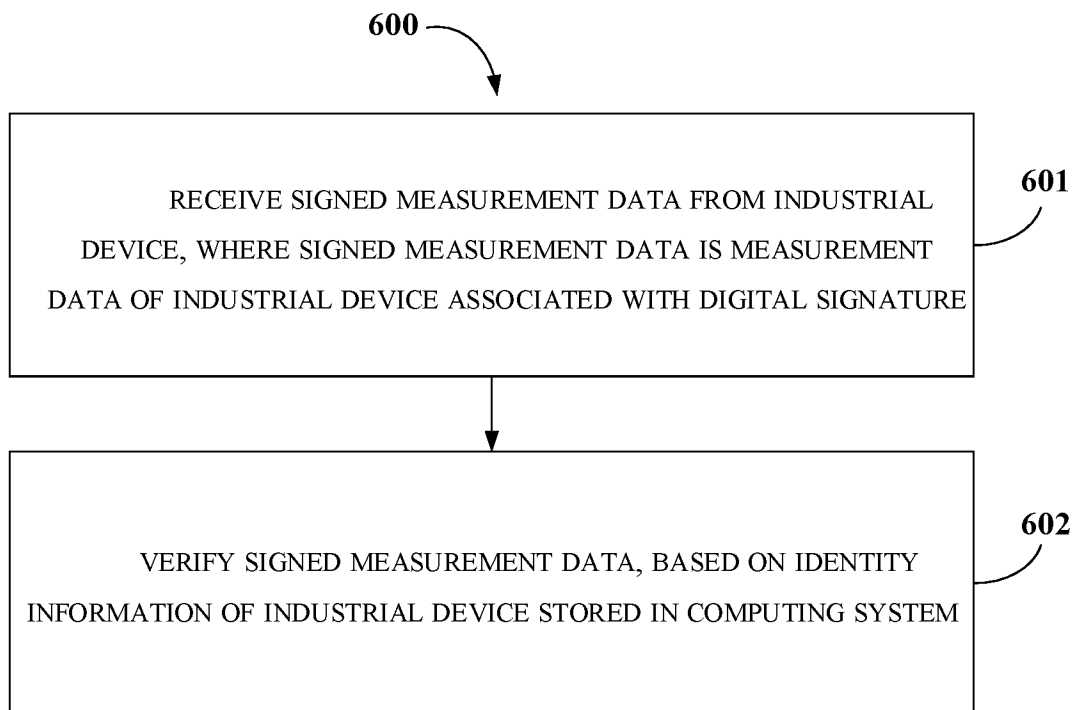


FIGURE 6

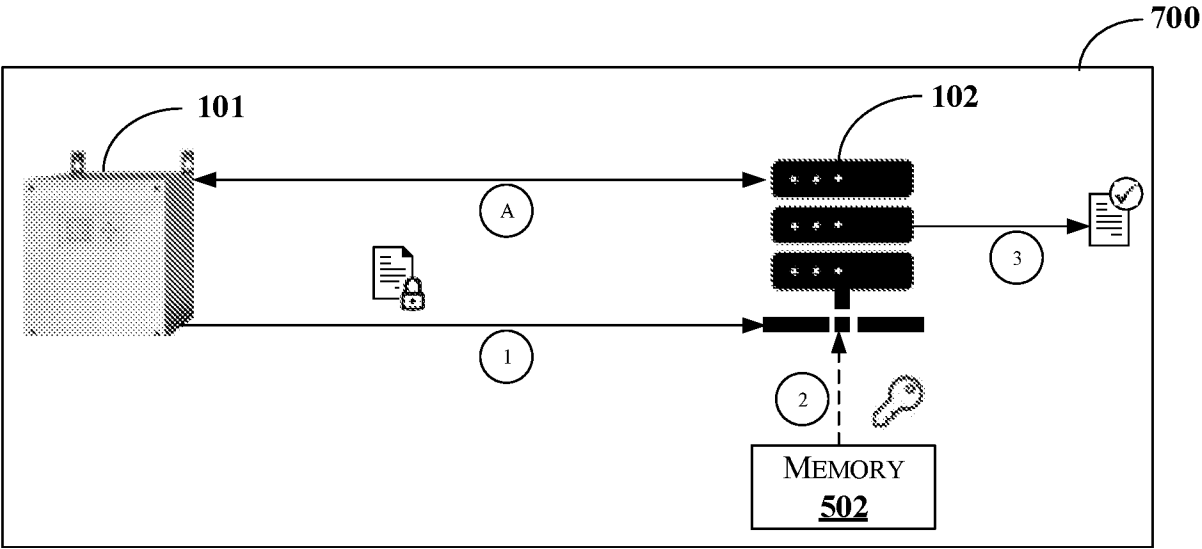


FIGURE 7

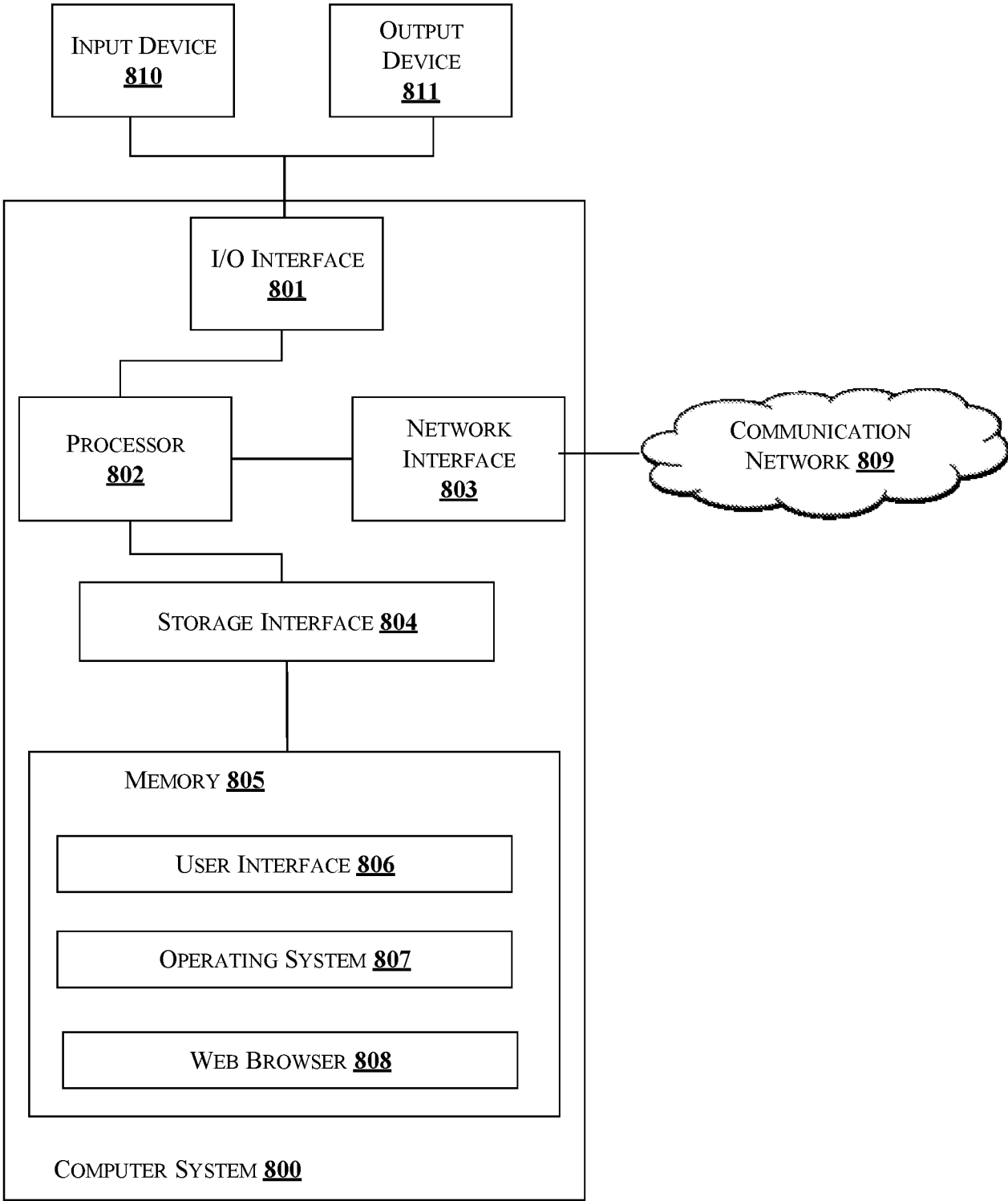


FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2021/060739

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/40 ADD.				
According to International Patent Classification (IPC) or to both national classification and IPC				
B. FIELDS SEARCHED				
Minimum documentation searched (classification system followed by classification symbols) H04L				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data				
C. DOCUMENTS CONSIDERED TO BE RELEVANT				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	US 2021/083883 A1 (DITTMANN GERO [CH] ET AL) 18 March 2021 (2021-03-18) abstract paragraph [0023] paragraph [0026] paragraph [0035] paragraph [0040] paragraph [0046] - paragraph [0049] paragraph [0054] - paragraph [0059] figures 1, 3 -----	1-15		
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.				
* Special categories of cited documents :				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; border: none;"> "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed </td> <td style="width: 50%; vertical-align: top; border: none;"> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family </td> </tr> </table>			"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family			
Date of the actual completion of the international search	Date of mailing of the international search report			
29 June 2022	07/07/2022			
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Poppe, Fabrice			

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2021/060739

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021083883	A1	18-03-2021	NONE