

(43) International Publication Date
28 January 2016 (28.01.2016)(51) International Patent Classification:
G06Q 50/28 (2012.01)(21) International Application Number:
PCT/MY2015/050069(22) International Filing Date:
10 July 2015 (10.07.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2014702049 24 July 2014 (24.07.2014) MY(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology
Park Malaysia, Kuala Lumpur, 57000 (MY).(72) Inventors: **AB MANAN, Jamalul-lail**; c/o MIMOS Ber-
had, Technology Park Malaysia, 57000 Kuala Lumpur
(MY). **MUBARAK, Mohd Faizal**; c/o MIMOS Berhad,
Technology Park Malaysia, 57000 Kuala Lumpur (MY).(74) Agent: **CHUAH, Jern Ern**; Advanz Fidelis Sdn Bhd,
Suite 609, Block D, Phileo Damansara 1, No 9 Jalan 16/11,
Petaling Jaya, Selangor, 46350 (MY).(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, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,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, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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 the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: SYSTEM AND METHOD FOR SECURE TRACKING OF INTERNET OF THINGS BASED GOODS IN SUPPLY CHAIN SYSTEM

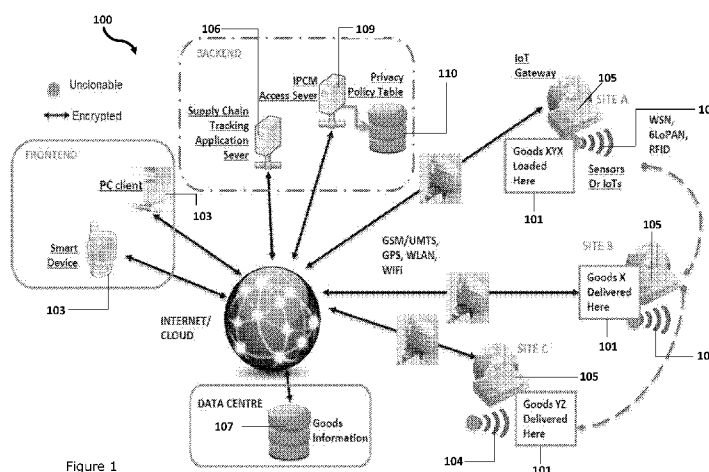


Figure 1

(57) Abstract: A supply chain is a sequence of processes associated with production and distribution of goods. Security and privacy of these processes in a supply chain is of utmost importance besides the delivery of goods to its destination. Disclosed herein is a system (100) and method for managing the security and privacy of the tracking of goods in a supply chain achieved through the steps of setting up supply chain tracking system, registering the goods, storing goods information and then retrieving goods information. Such security and privacy operations are carried out through verification and authentication of the users and client devices (103).

SYSTEM AND METHOD FOR SECURE TRACKING OF INTERNET OF THINGS BASED GOODS IN SUPPLY CHAIN SYSTEM

TECHNICAL FIELD OF THE INVENTION

5

The invention relates to supply chain system and in particular secure tracking of goods in a supply chain system.

BACKGROUND OF THE INVENTION

10

A supply chain is a sequence of processes associated with production and distribution of goods. With advancement of technology, supply chain systems are driven in the direction of integrating Internet of Things (IoT) into supply chain system components. The IoT enables real time automatic data transfer of physical items over an internet network without the need for human-to-human or human-to-computer interaction. The benefits of IoT in a supply chain system allow monitoring of goods information such as availability, capacity, inventory and more importantly tracking the location of goods. The real time availability of these data allows improved decision planning, service optimization and resource allocation. In a supply chain system, getting goods delivered safely and securely to the intended destination is as crucial as in getting goods to the right place at the right time.

25

However, supply chain systems are highly vulnerable as they comprise many different system components, large quantities of goods and huge amount of information. Therefore, focus is placed on assessing and mitigating risks associated with physical vulnerabilities such as piracy, counterfeiting, theft, terrorism and weather-related disruptions. Another issue faced in supply chain system is credentials of participants in the supply chain. Failure to properly securing information transfer from participant to participant in the supply chain network can result in abuse of information obtained.

30

In view of the abovementioned security threats, several methods have been

developed to provide a secure tracking of goods in a supply chain system.

International patent publication number WO 2004090778 A1 discloses a method of secured supply chain management and control comprising provision and verification of security of shipment of goods. The method disclosed is performed by tracking goods by means of interfacing with multiple information system, standard security devices such as physical fencing and visual monitoring such as CCTV systems. This method identifies the security aspects of examination of goods, recording of inspection, a secured storage system and audit reporting, without disclosure on information privacy.

US patent number 8,332,656 B2 discloses a system and method for decoding and reading Radio-Frequency (RF) tags of collection of goods. The system and method disclosed encompasses enhancements to the security of the supply chain by using RF tags as a means of tracking goods in a supply chain. There were no mention however on security or privacy when registering goods in a supply chain, when storing information of goods in the database or retrieving information of goods upon user queries.

A research paper entitled "End-to-End Transport Security in the IP-Based Internet of Things" (Brachmann et al, 2012) addresses security protection for IoT based goods with end-to-end protection by using either Hypertext Transfer Protocol (HTTP) and Transport Layer Security (TLS) or Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS) by proposing mapping between TLS and DTLS. The article further discloses security attacks that lead to resource exhaustion and optimized end-to-end security at the application process. However, the research paper only discusses online or over the internet security protection for internet of things based goods. There were no mention of physical security of the goods in a supply chain system.

In terms of security protection to IoT based goods in a supply chain, the existing systems and methods have their limitations. Therefore, it is an aim of

this present invention to provide a system and method that is capable of secure tracking of goods in a supply chain system.

SUMMARY OF THE PRESENT INVENTION

5

The present invention aims to provide a secure system and method for tracking of internet of things based goods in a supply chain by at least a client device.

10 It is an object of the present invention to provide a system and method for prioritizing information, wherein the information gathered from sensors bounded to internet of things based goods are first divided into categories, classified based on risks and then tracked or monitored via Global Positioning System (GPS).

15

It is a further object of the present invention to provide partner trust management, wherein goods are managed between partners at different stages in a supply chain using platform integrity verification mechanism.

20 It is a further object of the present invention to prevent duplication of goods by means of attaching a physical unclonable function embedded sensor to the internet of things based goods.

It is a further object of the present invention to share information securely over
25 the supply chain, wherein completeness of goods delivery is based on goods arrival to the destination with no security breach. A privacy policy is implemented between partners on accessibility of information such as real time tracking of goods.

30 It is a further object of the present invention to provide a secured and trusted infrastructure in the supply chain, wherein the security and privacy of information related to internet of things based goods are guaranteed from being cloned, replaced or hijacked.

Ultimately, the present invention relates to a system for tracking internet of things based goods in a supply chain by at least a client device. The system comprises a plurality of sensors for detecting internet of things based goods in said supply chain, a plurality of gateways for receiving and identifying values of said plurality of sensors, at least a tracking server for tracking information and location of said goods in said supply chain and at least a supply chain database for storing said internet of things based goods information for retrieval by at least a client device. The abovementioned plurality of sensors is embedded with a physical unclonable function for preventing duplication. Furthermore, the system comprises at least a privacy access server connected to a privacy policy module for managing the access rights of said at least a client device.

The present invention further relates to a method for tracking internet of things based goods in a supply chain by at least a client device. The method comprises the steps of setting up said supply chain, registering said internet of things based goods in said supply chain, storing information of said internet of things based goods in a supply chain database wherein said information is obtained by initiating queries to said plurality of gateways and retrieving information of said internet of things based goods upon user queries. The step of setting up said supply chain further comprises the steps of registration of said at least a client device and users of said at least a client device to at least a privacy access server, and set up of access rights for said at least a client device in said at least a privacy access server. Furthermore, the step of registering said internet of things based goods in said supply chain comprises attaching a sensor embedded with a physical unclonable function and storing information of said internet of things based goods in said at least a privacy access server.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a system for securely tracking internet of things based goods in a supply chain according to the present invention.

Figure 2 illustrates a process workflow for setting up the supply chain
5 according to the present invention.

Figure 3 illustrates a process workflow for registering internet of things based goods information according to the present invention.

10 Figure 4 illustrates a process workflow for storing internet of things based goods information according to the present invention.

Figure 5 illustrates a process workflow for retrieving information of said internet of things based goods upon user queries according to the present
15 invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

The above mentioned and other features and objects of this invention will
20 become more apparent and better understood by reference to the following detailed description. It should be understood that the detailed description made known below is not intended to be exhaustive or limit the invention to the precise form disclosed as the invention may assume various alternative forms. On the contrary, the detailed description covers all the relevant
25 modifications and alterations made to the present invention, unless the claims expressly state otherwise.

Referring to Figure 1, illustrated is one embodiment of a system (100) for securely tracking internet of things based goods (101) in a supply chain,
30 wherein the system (100) comprises at least a client device (103), a plurality of sensors (104) for detecting internet of things based goods (101) in a supply chain, a plurality of gateways (105) for receiving and identifying values of said plurality of sensors (104), at least a tracking server (106) for tracking

information and location of said goods in a supply chain and at least a supply chain database (107) for storing said internet of things based goods (101) information for retrieval by at least a client device (103). These system (100) components are interlinked over a computing network such as the internet or
5 a computing cloud system.

Source of initialization of the entire system (100) depends on said a plurality of sensors (104) for detecting internet of things based goods (101) in a supply chain, wherein the sensors (104) emit information of the goods on a real time
10 basis to the supply chain system. The information emitted are received by said a plurality of gateways (105) which in turn sends said information to the computing network. A user using a client device (103) is able to track information of goods (101) at any desired point in said supply chain through the tracking server (106). As the tracking server (106) is connected to said at
15 least a supply chain database (107), a registered user is able to obtain real time information of his or her goods via an online web application. A client device (103) takes the form of a personal computer, a mobile device, a tablet or a technical device accessible to a web browser over the internet.

20 The abovementioned plurality of sensors (104) is embedded with a physical unclonable function (PUF) to prevent duplication. PUF is a complex physical system with mapping of inputs and corresponding outputs that cannot be predicted or reproduced even given the exact manufacturing process used to produce it. Therefore, PUF demonstrates resiliency against side channel,
25 physical and software attacks. This technology that is primarily implemented in smartcards due to its secure nature will give internet of things based goods (101) the security needed to prevent duplication, piracy or counterfeiting.

A key feature in the system (100) for providing tracking security in a supply
30 chain is through at least a privacy access server (109) connected to a privacy policy module (110). The herein mentioned privacy policy module (110) comprises at least a list of registered client devices (103) and a list of said plurality of gateways (105) labelled with access rights for said at least a client

device (103). Hence, said privacy policy module (110) manages the access rights and computes the abovementioned list based on selection of access rights by said users.

- 5 During the initial setup stage, the users have to specify and agree with the level of access rights to be stored in the privacy policy module (110). Depending on the access rights which have been set into the privacy policy module (110), a user using said at least a client device (103) has means to access said plurality of gateways (105) through means of a user authentication. Therefore, the users have much needed control over his or her private information. Generally, the process of accessing information of internet of things based goods (101) is performed in said privacy access server (109) according to said privacy policy module (110).
- 10
- 15 The system (100) for tracking internet of things based goods (101) in a supply chain is further secured by means of encrypted information transfer between said plurality of sensors (104), said plurality of gateways (105), said at least a privacy access server (109), said at least a tracking server (106) and said at least a supply chain database (107). The end-to-end interlinking between system (100) components by means of encrypted information ensures secured communication. Due to the importance of information transfer in the system (100), various types of encryption are implemented such as whole disk encryption referring to the encryption of an entire physical disk, supply chain database (107) integrated encryption wherein data is encrypted as it is written, network transit encryption whereby encrypting information while in transit on a network, wireless networks encryption that only encrypts information between the client device (103) and wireless access point, et cetera.
- 20
- 25

- 30 In the same context, any of said a plurality of sensors (104), said a plurality of gateways (105), said at least a privacy access server (109), said at least a tracking server (106) and said at least a supply chain database (107) in a supply chain system are evaluated for trustworthiness through a platform validation module, also known as trusted platform module. This platform

validation module is effectively a crypto processor designed to provide hardware with security by integrating cryptographic keys into devices. Further compounding to the benefits mentioned above, the platform validation module includes capabilities such as remote attestation, binding, data sealing using
5 secret endorsement key.

In particular, a method for tracking internet of things based goods (101) in a supply chain by at least a client device (103) according to the present invention involves four main sub divisional methods, that is one for setting up
10 said supply chain, registering said internet of things based goods (101) in said supply chain, storing information of said internet of things based goods (101) in a supply chain database (107) wherein said information is obtained by initiating queries to said plurality of gateways (105) and another for retrieving information of said internet of things based goods (101) upon user queries.
15 The entire process flow for traffic violation detection will be further elaborated in the following descriptions.

The method of setting up said supply chain further comprises the steps of registration of said at least a client device (103) and users of said at least a
20 client device (103) to at least a privacy access server (109), and set up of access rights for said at least a client device (103) in said at least a privacy access server (109).

Referring now to Figure 2, illustrated is a process workflow of a method for
25 setting up said supply chain in accordance with the present invention, wherein the method of setting up said supply chain is initialized by setting up user authentication system for user access to supply chain tracking system (SCTS) (201), followed by setting up mutual platform integrity verification between all machines in the SCTS via trusted platform module within said supply chain
30 including IoT gateways (105), servers, and at least a client device (103) (202). After of which at least a client device (103) is registered to the privacy access server (109) connected to said privacy policy module (110) also known as information privacy control module (IPCM) (203). Once client devices (103)

are registered, all users are registered to the supply chain database (107), including user identification, user passwords and information of user's goods (204). Ensuing that, user selections for access rights are set up in the privacy access server (109) and saved into the privacy policy module (110) (205). The
5 privacy policy module (110) sets up access rights for client device (103) to access mobile IoT gateway (105) based on user privacy access rights (206). These information of user selected access rights sets up a secure connection for client access to a selected IoT gateway (105)(207). To ensure proper set up of said supply chain, the SCTS is set up to execute challenge respond with
10 a test unit IoT gateway (105) to review capability of to make on-line IoT reading (208).

A process workflow of a method for registering IoT based goods (101) information is shown in Figure 3. Registering said IoT based goods (101) in
15 said supply chain comprises attaching a sensor (104) embedded with a physical unclonable function and storing information of said IoT based goods (101) in said at least a privacy access server (109) (301). The information mentioned herewith comprises user identification (userid), user selected privacy access, goods information and IoT identification (iotid), which will be
20 further stored in privacy policy module (302).

Figure 4 of the drawings shows schematically a flowchart of a method for storing IoT based goods (101) information. Storing information of said IoT based goods (101) in a supply chain database (107) wherein said information
25 is obtained by initiating queries to said plurality of gateways (105). These queries contain information registered with the supply chain tracking system such as gateway (105) identification (gwid), iotid, sensor (104) identification (sid) (401). When the gateway (105) receives these information, the privacy access server (109) will acknowledge that the gwid and iotid are valid before
30 sending the goods information including gwid, iotid, sid and goods location (gloc) to the supply chain tracking system (402). The goods information is identified and stored in the supply chain database (107), wherein said goods information are classified according to said privacy policy module (110) (403).

Referring to Figure 5, illustrated is a process workflow of a method for retrieving information of said internet of things based goods (101) upon user queries. To retrieve information goods, a registered user has to log on to the web application of the supply chain tracking system for validation of the user authentication (501). After which said web application will initiate mutual platform integrity verification in order to verify that the user is trusted (502). In addition to that, said supply chain database (107) certifies both user and client device (103) are registered (503). These are the security features implemented by the present invention before a user is able to query the supply chain tracking system about the location of his or her goods (504). The supply chain tracking system confirms the user access based on the status keyed in the privacy policy module (110) and sends the respective accessible information about the user's goods location to the user (505). Therefore, in essence retrieval of information of said internet of things based goods (101) is performed via a web application which requires authentication of said users and validation of said client device (103)

The invention described herein is susceptible to variations, modifications and/or additions other than those specifically described and it is to be understood that the invention includes all such variations, modifications and/or additions which fall within the scope of the following claims.

CLAIMS

1. A system (100) for tracking internet of things based goods (101) in a supply chain by at least a client device (103), comprising:

5 a plurality of sensors (104) for detecting said internet of things based goods (101) in said supply chain;

 a plurality of gateways (105) for receiving and identifying values of said plurality of sensors (104);

10 at least a tracking server (106) for tracking information and location of said goods in said supply chain; and

 at least a supply chain database (107) for storing said internet of things based goods (101) information for retrieval by at least a client device (103);

15 characterized in that said a plurality of sensors (104) are embedded with a physical unclonable function for preventing duplication; and

 said system (100) further comprises at least a privacy access server (109) connected to a privacy policy module (110) for managing access rights for said at least a client device (103).

20

2. A system (100) of claim 1, wherein said privacy policy module (110) comprises at least a list of registered client devices (103) and a list of said plurality of gateways (105) which is labelled with access rights for said at least a client device (103).

25

3. A system (100) of claim 1, wherein said at least a client device (103) is provided access to said plurality of gateways (105) as controlled by said privacy access server (109) according to said privacy policy module (110).

30

4. A system (100) of claim 1, wherein said plurality of sensors (104), said plurality of gateways (105), said at least a privacy access server (109),

said at least a tracking server (106) and said at least a supply chain database (107) are interlinked with encrypted information to ensure secured communication.

- 5 5. A system (100) of claim 1, wherein any one or any combination of said a plurality of sensors (104), said a plurality of gateways (105), said at least a privacy access server (109), said at least a tracking server (106) and said at least a supply chain database (107) are evaluated for trustworthiness through a platform validation module.

10

6. A method for tracking internet of things based goods (101) in a supply chain by at least a client device (103) comprising the steps of:

 setting up said supply chain (201);

 registering said internet of things based goods (101) in said

15

supply chain;

 storing information of said internet of things based goods (101)

in a supply chain database (107) wherein said information is

obtained by initiating queries to said plurality of gateways (105)

(401); and

20

 retrieving information of said internet of things based goods (101) upon user queries;

 characterized in that the step of setting up said supply chain comprising the steps of registering said at least a client device (103)

and users of said at least a client device (103) to at least a privacy

25

access server (109) (204), and setting up of access rights for said at least a client device (103) in said at least a privacy access server (109) (205); and

 registering said internet of things based goods (101) in said

supply chain comprises attaching a sensor (104) embedded with a

30

physical unclonable function and storing information of said internet of things based goods (101) in said at least a privacy access server (109) (301).

7. The method of claims 6, wherein setting up said supply chain further comprises setting up mutual platform integrity verification via trusted platform module within said supply chain.
- 5 8. The method of claim 6, wherein information of said goods stored in said supply chain database (107) are classified according to said privacy policy module (110) (402).
- 10 9. The method of claim 6, wherein said queries are verified in terms of user and client device (103) registration status and information of goods retrieved in response to said queries is provided according to said access rights as set up in said at least a privacy access server (109) (505).
- 15 10. The method of claim 6, wherein retrieving of information of said internet of things based goods (101) upon user queries is performed via a web application which requires authentication of said users and validation of said client device (103).

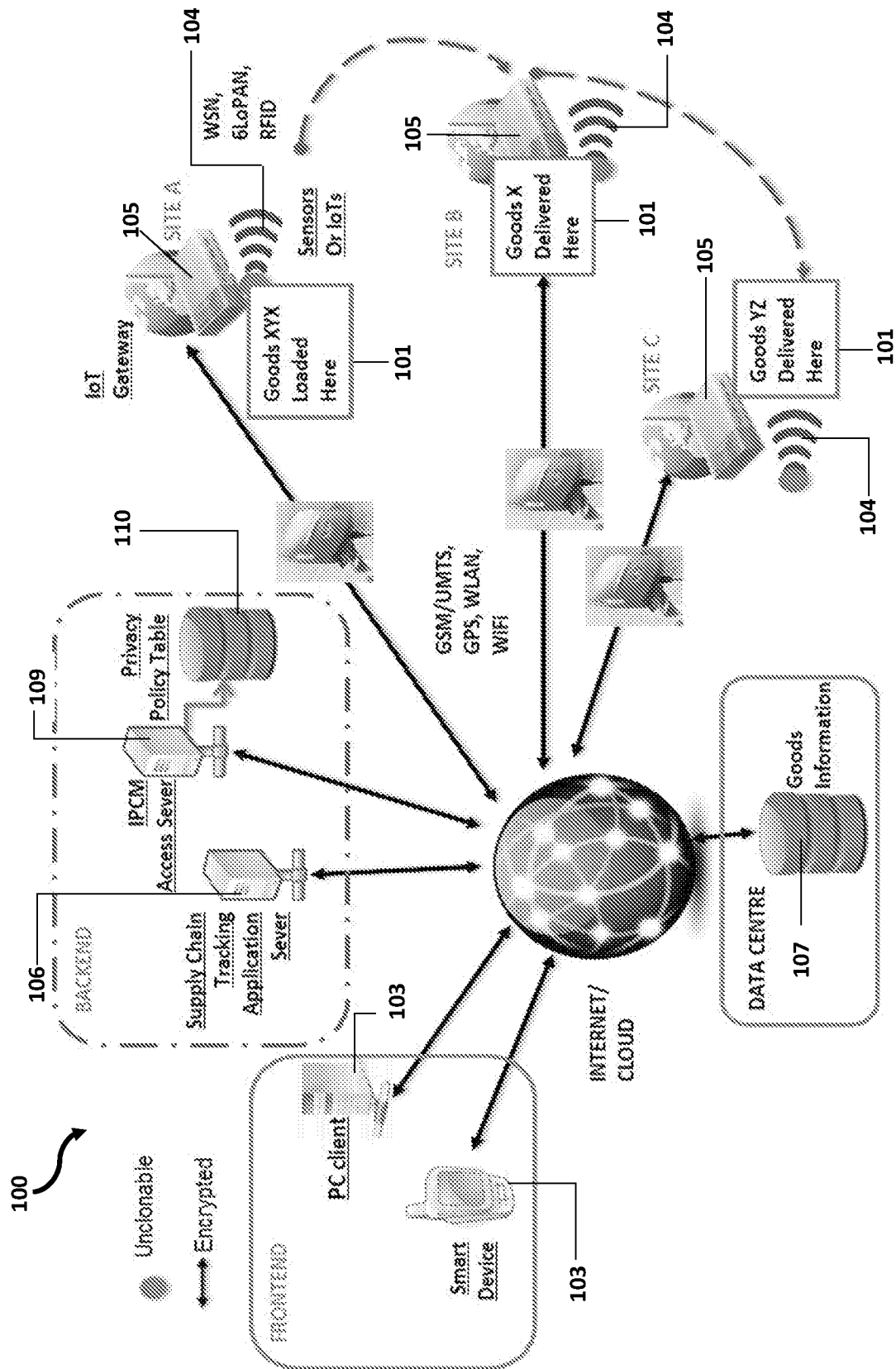


Figure 1

2/4

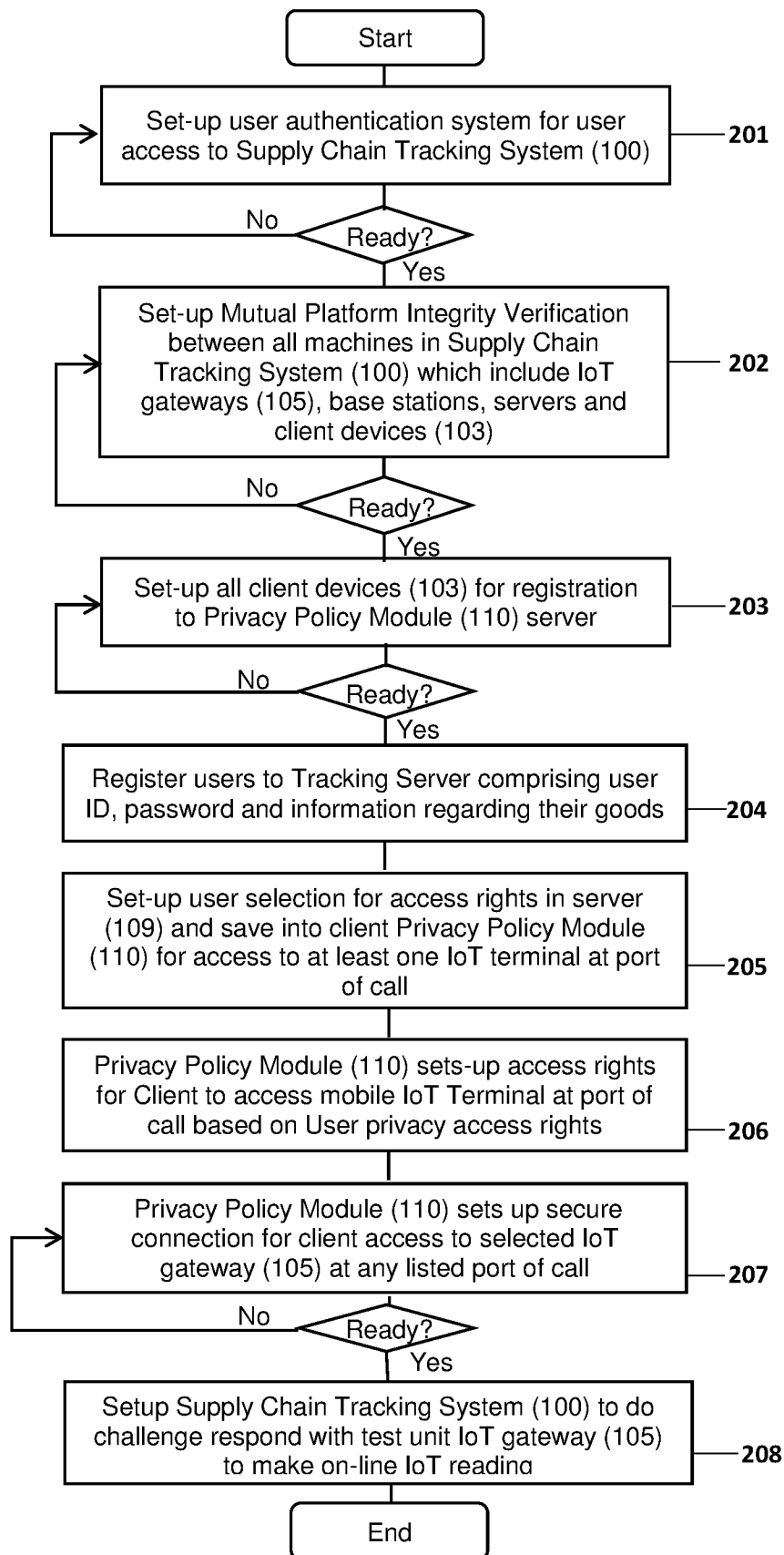


Figure 2

3/4

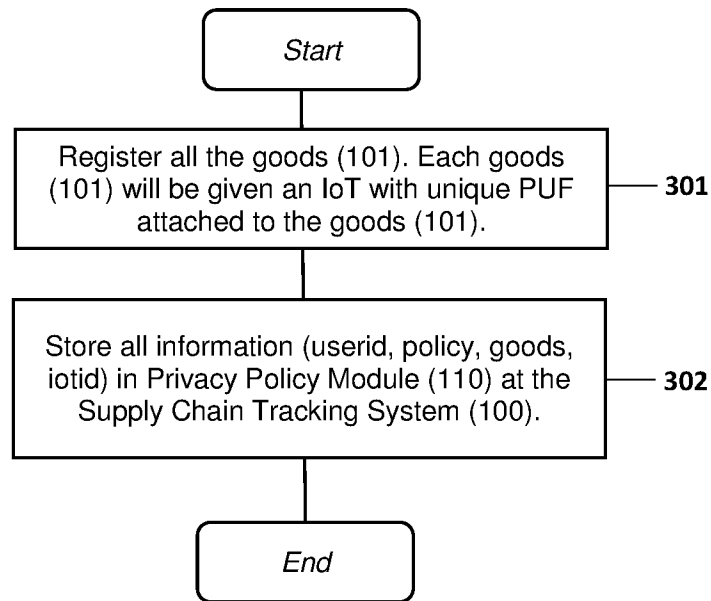


Figure 3

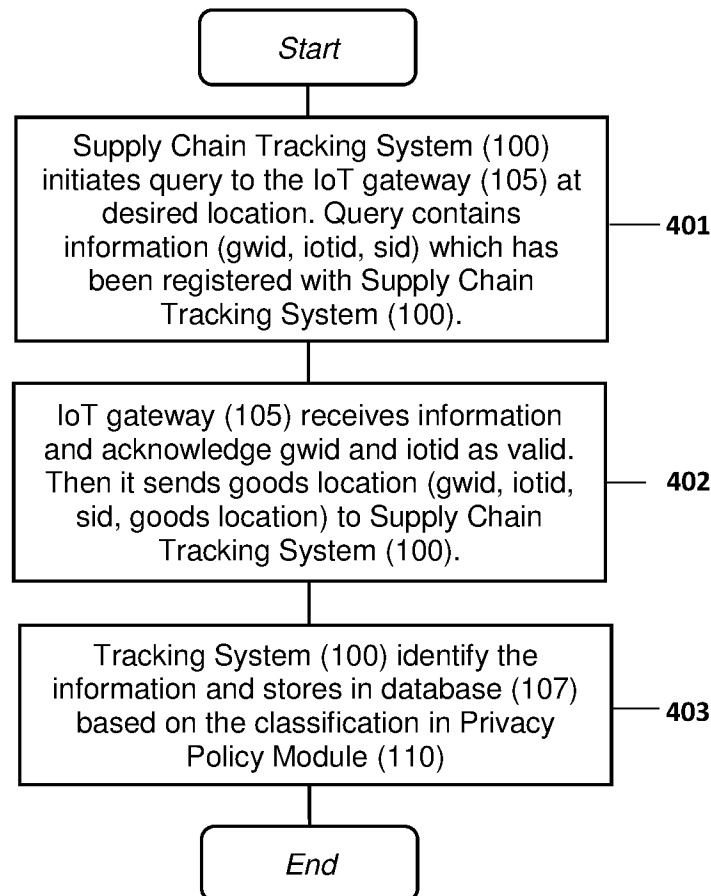


Figure 4

4/4

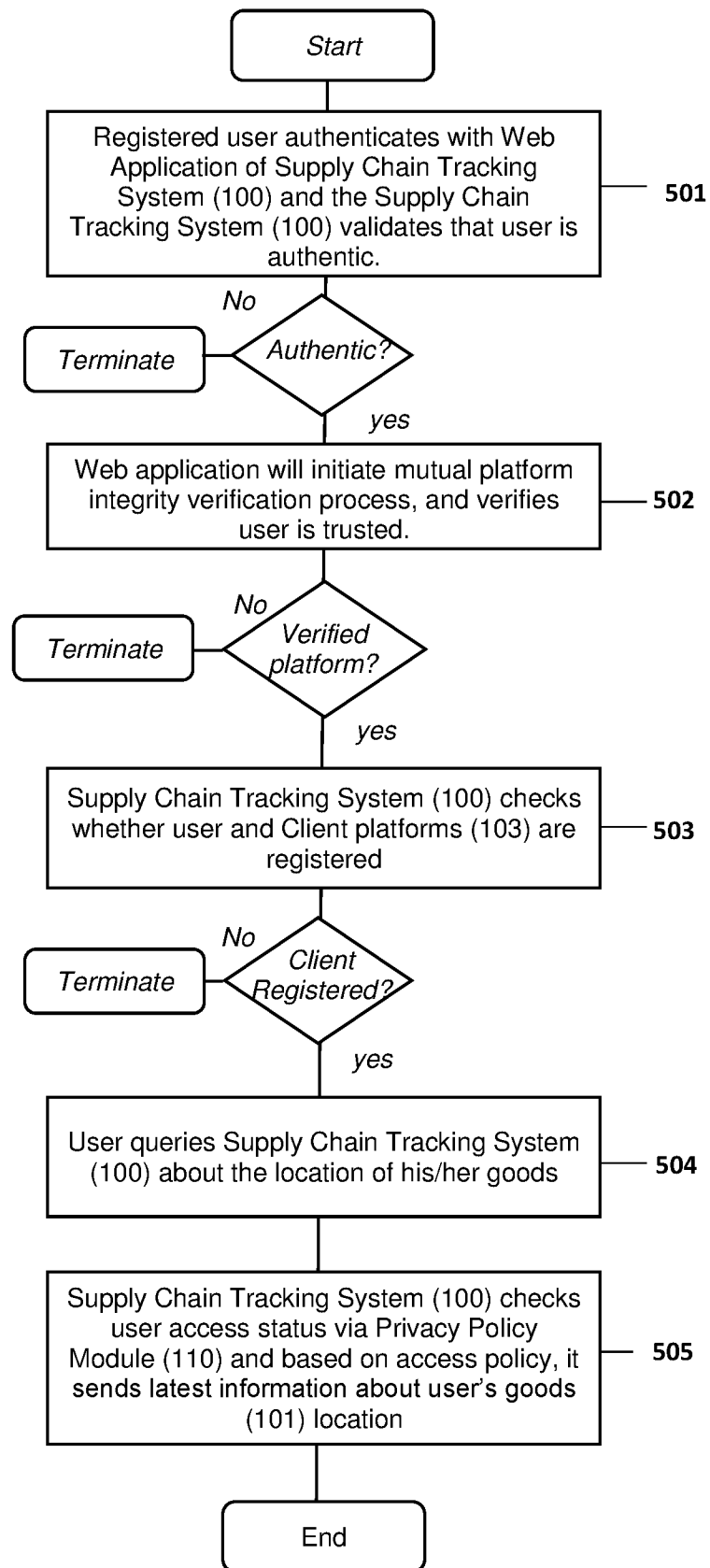


Figure 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/MY2015/050069

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06Q50/28 (2012.01) i

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)

Int.Cl. G06Q50/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2015
 Registered utility model specifications of Japan 1996-2015
 Published registered utility model applications of Japan 1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013/0277425 A1 (ZORTAG Inc.) 2013.10.24, paragraphs [0052], [0075]-[0100] (Family: none)	1-10
Y	US 2010/0019026 A1 (HOCHFIELD Barry) 2010.01.28, paragraphs [0056]-[0104] & JP 2009-532792 A & WO 2007/128966 A1 & EP 2011061 A1	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“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

12.11.2015

Date of mailing of the international search report

24.11.2015

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

MIYACHI, Masato

Telephone No. +81-3-3581-1101 Ext. 3562

5L

3796