(12)Indian Patent Application

---

(21) Application Number: 202241015263

(22) Filing Date: 19/03/2022 (43) Publication Date: 22/09/2023

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): Pramanik, Sudip

(51) International Classifications: H04L 29/06 H04L 29/08 G06F 8/65 G06F 8/61 H04W 12/06

(54) Title: SYSTEM AND METHOD OF UPDATING AN ASSET

(57) Abstract: A method and a system for updating an asset is disclosed. The method may include receiving an asset identification (ID) associated with an asset from the asset, via a charging station and authenticating the asset ID based on one or more authentication parameters. The method may further include identifying an associated server from a plurality of servers based on the asset ID. The associated server is to provide an update package associated with the asset. The method may further include upon authenticating the asset ID and identifying the associated server, requesting the associated server for an update package associated with the asset, and establishing a secure communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

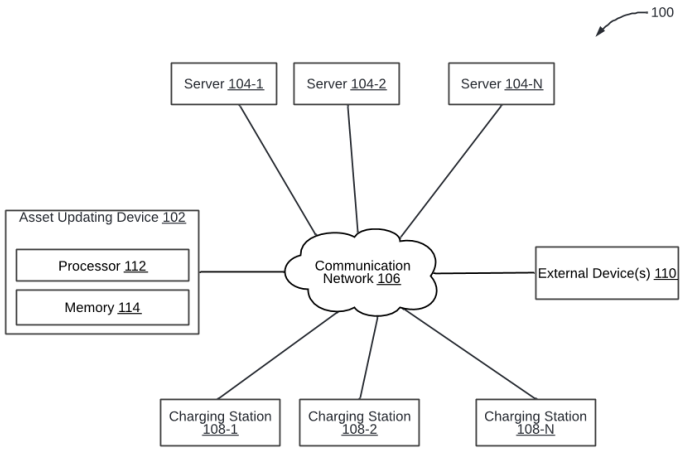



FIG. 1

# FORM 2

THE PATENTS ACT 1970
(39 OF 1970)
&
The Patent Rules, 2003
Complete Specification
(See Section 10 and Rule 13)

**1. TITLE OF THE INVENTION**

**SYSTEM AND METHOD OF UPDATING AN ASSET**

**2. APPLICANT(S)**

| | | |
|---|---|---|
| (a) NAME | : | **L&T TECHNOLOGY SERVICES LIMITED** |
| (b) NATIONALITY | : | **INDIAN** |
| (c) ADDRESS | : | **DLF IT SEZ Park, 2nd Floor – Block 3, 1/124, Mount Poonamallee Road, Ramapuram, Chennai – 600 089, INDIA.** |

**3. PREAMBLE TO THE DESCRIPTION**

**COMPLETE**

The following specification particularly describes the invention and the manner in which it is to be performed.

## DESCRIPTION

### Technical Field

**[001]** This disclosure relates generally to updating an asset, and more particularly to a system and method of updating an electronic control unit software of an electric vehicle.

## BACKGROUND

**[002]** Presently, the auto industry is moving into software-defined architecture. For software updates for Electronic Control Unit (ECU) of the vehicles, Software-Over-The-Air (SOTA)-based and Firmware-Over-The-Air (FOTA)-based techniques are used. These SOTA-based and FOTA-based techniques allow connecting to the Original Equipment Manufacturer (OEM) servers to download and install the update pack.

**[003]** Although, these over-the-air (OTA)-based techniques allow OEMs to upgrade numerous systems at once; however, deploying an OTA-based system poses challenges for car manufacturers in terms of safety, security, and reliable connectivity. This is mainly because these connections are based on communication over wireless channels which are prone to various online security threats. Moreover, the SOTA-based and FOTA-based techniques face challenges in software update verification and authentication.

**[004]** Therefore, there is a need for improved method and system for management of large-scale ECU software updates, while ensuring safe and secure data exchange and protection against unauthorized device access and online threats.

## SUMMARY OF THE INVENTION

**[005]** In an embodiment, a system for updating an asset is disclosed. The system may include a processor and a computer-readable medium communicatively coupled to the processor, wherein the computer-readable medium stores processor-executable instructions, which, on execution, may cause the processor to receive, from an asset, an asset identification (ID) associated with the asset, via a charging station, and authenticate the asset ID based on one or more authentication parameters. The processor-executable instructions may further cause the processor to identify an associated server from a plurality of servers based on the asset ID, and upon authenticating the asset ID and identifying the associated server, request the associated server for an update package associated with the asset. The processor-executable instructions may further cause the processor to establish a secure

communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

**[006]** In another embodiment, a method of updating an asset is disclosed. The method may include receiving an asset identification (ID) associated with an asset from the asset, via a charging station and authenticating the asset ID based on one or more authentication parameters. The method may further include identifying an associated server from a plurality of servers based on the asset ID. The associated server is to provide an update package associated with the asset. The method may further include upon authenticating the asset ID and identifying the associated server, requesting the associated server for an update package associated with the asset, and establishing a secure communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[007]** The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles.

**[008]** **FIG. 1** is a block diagram of a system for updating an asset, in accordance with an embodiment of the present disclosure.

**[009]** **FIG. 2** is a functional block diagram of an updating device, in accordance with an embodiment of the present disclosure.

**[010]** **FIG. 3** is a block diagram of a system for updating an asset, in accordance with an embodiment.

**[011]** **FIG. 4** is a block diagram of a system for updating an asset, in accordance with another embodiment.

**[012]** **FIG. 5** is a flowchart of a method of updating an asset, in accordance with an embodiment of the present disclosure.

## DETAILED DESCRIPTION OF THE DRAWINGS

**[013]** Exemplary embodiments are described with reference to the accompanying drawings. Wherever convenient, the same reference numbers are used throughout the drawings to refer to the same or like parts. While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the spirit

and scope of the disclosed embodiments. It is intended that the following detailed description be considered as exemplary only, with the true scope and spirit being indicated by the following claims. Additional illustrative embodiments are listed.

**[014]** Presently, the auto industry is moving into software-defined architecture, and as such, for software updates for the ECUs of the vehicles, Software-Over-The-Air (SOTA)-based and Firmware-Over-The-Air (FOTA)-based techniques are used. However, the SOTA-based and FOTA-based techniques compromise over security, as these are based on communication over wireless channels.

**[015]** Electric vehicles require regular electric charging to recharge the batteries of the electric vehicles. To this end, electric charging stations are being deployed where electric vehicles can be docked and charged. For example, the electric vehicles may use the compatible charge type ports to charge the vehicles. These charging stations are usually provided by third party entities that may also act as aggregators for different OEMs manufacturing the electric vehicles.

**[016]** The present disclosure provides methods and systems for updating the software associated with the electric vehicles (also referred to as assets in this disclosure), when the electric vehicle is connected to the charging station for charging of the batteries of the electric vehicle. To this end, the charging point of the electric vehicle may be equipped with an on-board diagnostic (OBD) port. The electric vehicle may be typically connected to the charging station over a wired connection. Therefore, information exchange between electric vehicle and the charging station may be carried out via wired lines. Further, the charging station may act as a distributed node and connects to multiple OEM servers over Internet. The charging station may also connect to a user (i.e. an owner of the electric vehicle) via a user device like a smartphone for interacting with the user, for example, for seeking user's permission for updating the ECU of their electric vehicle. Alternately, the charging station may provide a User Interface for allowing the user to interact with the charging station or with the OEM servers. The charging station may connect to a local backend system over a local area network (LAN) system, and the backend system may further connect to OEM servers over Internet. Alternately, the charging station may directly connect to the OEM servers over Internet, with the charging station implementing an Internet connectivity facility.

**[017]** The OEM server may need an identification of the electric vehicle requesting a software update, so that the OEM server can establish a secure channel with the electric vehicle. To establish this secure handshaking, the charging station (e.g. the backend server of the charging station) and the electric vehicle may provide a unique certificate-based identity. The electric vehicle and the charging station may perform an electric exchange and a data exchange (i.e. of vehicle data (asset data), battery

data, and charging related data). In addition to this, the electric vehicle and the charging station may further perform an exchange of the ECU software data (i.e. update package) and instructions.

**[018]** An aggregator server (also referred to as updating device in this disclosure) may be located in a distributed cloud connected via a communication channel. The aggregator server may request an initial aggregator-level authentication to authenticate the electric vehicle (a vehicle identification (VID) associated with the electric vehicle). The aggregator server may onboard the OEM servers to create a database of supported OEMs, vehicle models, software version, etc. As will be understood, this process may be carried out by the third-party entities acting as aggregator service providers. After an initial aggregator-level authentication, the aggregator server may request the OEM server (associated with the electric vehicle) to access the VID. The OEM server may authenticate the validity of the VID as well as the charging station (second-level authentication). After this second-level authentication, the aggregator server may start sending electric vehicle-related information to the OEM server and request latest software over the secure (encrypted) channel.

**[019]** If the aggregator server receives a response from the OEM server about an availability of an upgradable version, the aggregator server may activate a campaign manager to setup the sequence of the upgrade process. The campaign manager may instruct an update manager to send an UI input request to the user via the charging station (i.e. via the User Interface of the charging station or the user device). If the user agrees to upgrade (i.e. grants permission) the ECU software, the update manager may request the OEM server to send valid digitally-signed binary data package. It should be noted that neither the aggregator server nor the charging station saves any data but simply forward the data package to the electric vehicle via the OBD port. Upon completion of the data transmission and upgrade of the ECU, the electric vehicle sends status message to the charging station. The charging station further sends a status back to the OEM server via the aggregator server. The OEM server updates the status of the electric vehicle that has received the update.

**[020]** Referring now to **FIG. 1**, a block diagram of a system 100 for updating an asset is illustrated, in accordance with an embodiment of the present disclosure. By way of an example, the asset (not shown in FIG. 1) may include a vehicle, and in particularly an electric vehicle which is configured to be charged via an electric charging port. The system 100 may include an updating device 102. By way of an example, the updating device 102 may be implemented in an aggregator server (therefore, the terms “updating device 102” and “aggregator server” may have been used interchangeably in the present disclosure). The updating device 102 may be a computing device having data processing capability. Examples of the updating device 102 may include, but are not limited to a desktop, a

laptop, a notebook, a netbook, a tablet, a smartphone, a mobile phone, an application server, a web server, or the like. In particular, the updating device 102 may have capability to update the asset. In particular, the updating device 102 may have the capability to facilitate transmission of an update package from an original equipment manufacturer (OEM) server to the asset so as to update an electronic control unit (ECU) of the asset. As such, the system 100 may further include a plurality of servers 104-1, 104-2, …104-N (hereinafter, collectively referred to as plurality of OEM servers 104, or plurality of servers 104, or individually referred to as server 104).

**[021]** The system 100 may further include a plurality of charging stations 108-1, 108-2, …108-N (hereinafter, collectively, referred to as plurality of charging stations 108, or individually referred to as charging station 108). As will be understood, the plurality of charging stations 108 may be provided at remote locations for allowing the electric vehicles to dock into for charging the batteries of the electric vehicles. As such, each of the plurality of charging stations 108 may have the capability of electrically coupling with the electric vehicles for supplying electric current to the electric vehicles. Each of the plurality of charging stations 108 may be communicatively coupled to the plurality of servers 104.

**[022]** The system may further include a communication network 106. The communication network 106 may be a wired or a wireless network or both, and the examples may include, but are not limited to the Internet, Wireless Local Area Network (WLAN), Wi-Fi, Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), and General Packet Radio Service (GPRS). The plurality of charging stations 108 may be communicatively coupled to the plurality of servers 104 over the communication network 106.

**[023]** The system 100 may interact with one or more external devices 110 over the communication network 106 for sending or receiving various data. Examples of the one or more external devices 110 may include, but are not limited to, a laptop, a tablet, a smartphone, or the like. The updating device 102 may include a processor 112 and a memory 114. The memory 114 may store instructions that, when executed by the processor 112, cause the processor 112 to perform updating, as discussed in greater detail in FIG. 2 to FIG. 5. The memory 114 may be a non-volatile memory or a volatile memory. Examples of non-volatile memory may include, but are not limited to a flash memory, a Read Only Memory (ROM), a Programmable ROM (PROM), Erasable PROM (EPROM), and Electrically EPROM (EEPROM) memory. Examples of volatile memory may include but are not limited to Dynamic Random Access Memory (DRAM), and Static Random-Access memory

(SRAM). The memory 114 may also store various asset data (e.g. asset identification ID) that may be captured, processed, and/or required by the system 100.

**[024]** The updating device 102 (i.e. the aggregator server) may be configured to receive an asset identification (ID) associated with the asset from the asset, via a charging station of the plurality of charging stations 108. The asset may be configured to communicatively couple with the charging station 108, for example, via a wired communication network. The updating device 102 may be further configured to identify an associated server from the plurality of servers 104 based on the asset ID. It should be noted that the associated server may store and therefore provide an update package for updating the ECU of the asset. The updating device 102 may also authenticate (a first level authentication) the asset ID. Upon authentication, the updating device 102 may be request the associated server 104 for the update package associated with the asset. Further, the updating device 102 may be configured to establish a secure communication channel between the associated server 104 and the asset for facilitating a transmission of the update package from the associated server 104 to the asset.

**[025]** In order to perform the above functionalities, the updating device 102 may include a processor 112 and a memory 114. The memory 114 may store instructions that, when executed by the processor 112, cause the processor 112 to update an asset, as discussed in greater detail in FIG. 2 to FIG. 5. The memory 114 may be a non-volatile memory or a volatile memory. Examples of non-volatile memory may include, but are not limited to a flash memory, a Read Only Memory (ROM), a Programmable ROM (PROM), Erasable PROM (EPROM), and Electrically EPROM (EEPROM) memory. Examples of volatile memory may include, but are not limited to Dynamic Random Access Memory (DRAM), and Static Random-Access memory (SRAM). The memory 114 may also store various data (e.g. assed ID, authentication data, etc.) that may be captured, processed, and/or required by the system 100.

**[026]** Referring now to **FIG. 2**, a functional block diagram of the asset updating device 102 is illustrated, in accordance with an embodiment of the present disclosure. In some embodiments, the asset updating device 102 may include an asset identification receiving module 202, an authentication module 204, a server identifying module 206, an asset data transmitting module 208, an update package requesting module 210, an asset access requesting module 212, a secure communication establishing module 214, and a status notifying module 216.

**[027]** The asset identification receiving module 202 may receive the asset ID associated with the asset, from the asset, for example, via the charging station 108. It should be noted that the asset may

be configured to be communicatively coupled with the charging station 108, for example, at the time of charging the asset. In some embodiments, the asset may be communicatively coupled with the charging station 108 over a second network connection. The second network connection may be a wired connection. In particular, the second network connection may be created over the same charging wire which may be used to supply electric charge to the asset for charging the batteries of asset.

**[028]** As will be understood by those skilled in the art, the asset may have an asset ID associated with it. For example, each electric vehicle has a vehicle ID (VID) associated with it. Further, the asset may have an on-board diagnostics (OBD) port (also referred to as communication port in this disclosure) that can additionally act as ECU update gateway. Further, the charging station 108 may include a socket and a communication module for connecting the charging station to the asset and to enable data exchange therebetween. Further, the asset may include an asset identification module which may store the asset ID associated with the asset. The asset identification receiving module 202 may therefore communicate with the asset identification module of the asset via the communication port of the asset and the communication module of the charging station, when the asset is connected to the charging station, to obtain the asset ID.

**[029]** The authentication module 204 may perform a first level authentication of the asset ID based on one or more authentication parameters. The server identifying module 206 may identify an associated server from the plurality of servers 104 based on the asset ID. The associated server is the once that stores and can provide the update package associated with the asset. It should be noted that different OEMs may be associated with their respective OEM servers 104 through which the OEM may seek to update the assets associated with the OEM. The plurality of OEM servers 104 may be registered on the aggregator server 102, i.e. the update device 102. Once the asset ID is received from the asset, the server identifying module 206 may identify a server from the plurality of servers 104 that is associated with the asset connected to the charging station. Once the associated server is identified, the associated server may authenticate the asset ID and the charging station 108.

**[030]** The asset data transmitting module 208 may transmit asset data associated with the asset to the associated server 104. By way of an example, the asset data may include battery data, charging related data, etc. The update package requesting module 210 may query the associated server 104 for presence of the update package corresponding to the asset data. In other words, the update package requesting module 210 may check whether any new update is available from the associated server 104 for updating the ECU of the asset. Upon authenticating the asset ID and identifying the associated

server, the update package requesting module 210 may request the associated server for an update package associated with the asset.

**[031]** The asset access requesting module 212 may request a user associated with the asset for a permission for accessing the asset. In some embodiments, the asset access requesting module 212 may request the user via a User Interface implemented in a display of the charging station 108. In alternate embodiments, the asset access requesting module 212 may request the user via a user device associated with the user and the asset. For example, the user device may be a smartphone with an associated application installed on the smartphone. This associated application may provide an interface to facilitate the user to respond to the request and grant permission to the update device 102 and the associated server 104 to access the asset. To this end, the charging station 108 may be configured to communicatively couple with the user device over a third network connection. For example, the third network connection is a Bluetooth-based connection, or an Internet-based connection. In other words, the user device may communicatively couple with the charging station 108 either via Bluetooth-based connectivity or Internet-based connectivity.

**[032]** Upon authenticating of the asset ID, transmitting the asset data to the associated server 104, and upon determining the presence of the update package, the secure communication establishing module 214 may establish a secure communication channel for facilitating the transmission of the update package from the associated server 104 to the asset via the secure communication channel.

**[033]** Upon completion of the transmission of the update package from the associated server 104 to the asset, the status notifying module 216 may receive a status notification from the asset corresponding to the completion of the transmission of the update package. The status notifying module 216 may further transmit the status notification to the associated server 104.

**[034]** Referring now to **FIG. 3**, a block diagram of a system 300 (corresponding to FIG. 1) for updating an asset is illustrated, in accordance with an embodiment. As shown in FIG. 3, the system 300 may include an updating device 302 which may be implemented in an aggregator server. The system 300 may further include a plurality of OEM servers 304-1, 304-2, …304-N (hereinafter, collectively referred to as plurality of OEM servers 304, or plurality of servers 304, or individually referred to as server 304). The system 300 may further include a charging station 308. The charging station 308 may be communicatively coupled to the updating device 302 over a first network connection. The first network connection may be an Internet-based connection. For example, the charging station 308 may be connected to a local backend system over a local area network (LAN), and the backend system may be further connected to the plurality of OEM servers 304 over Internet.

Alternately, the charging station 308 may directly connect to the plurality of OEM servers 304 over Internet. To this end, the charging station 308 may implement an Internet connectivity facility.

**[035]** The charging station 308 may be provided at remote location for allowing the electric vehicles (assets) to dock into for charging the batteries of the electric vehicles. Therefore, it should be noted that the asset 306 may be configured to be communicatively coupled with the charging station 308, for example, at the time of charging the asset 306. The charging station 308 may have a capability of electrically coupling with an asset 306 for supplying electric current to the asset 306. In other words, the charging station 308 may communicatively couple with the asset 306 over a second network connection. This second network connection may be a wired connection. In particular, the second network connection may be created over the same charging wire which may be used to supply electric charge to the asset for charging the asset.

**[036]** The asset 306 may have an asset ID associated with it. For example, each electric vehicle has a vehicle ID (VID) associated with it. The asset ID may be stored in an asset identification module 318 of the asset 306. The updating device 302 may receive the asset ID associated with the asset from the asset, via the charging station 308. In order to communicate with the asset 306, the charging station 308 may include a socket 310 and communication module 312 for data exchange. The charging station 308 may communicatively couple with the asset 306 over the second network connection (i.e. the wired connection), via the socket 310. For example, a wire from the charging station 308 may include the socket 310 at one end. The socket 310 may be configured to be coupled with a charging port 314 of the asset 306. The communication module 312 may enable data exchange between the charging station 308 and the asset 306.

**[037]** The asset 306 may include a communication port 316 in communication with the charging port 314 of the asset 306. The communication port 314 may provide for data exchange between the communication module 312 of the charging station 308 and the asset. In particular, the communication port 314 may act as gateway to the asset identification module 318 and the ECU of the asset 406. The communication port 314 may therefore provide for data exchange between the communication module 312 of the charging station 308 and the asset identification module 318 as well as the ECU (not shown in FIG. 3) of the asset.

**[038]** The updating device 302 may therefore communicate with the asset identification module 318 of the asset 306 via the communication port 316 of the asset and the communication module 312 of the charging station 308, when the asset 306 is connected to the charging station 308, to obtain the asset ID.

**[039]** The updating device 302 may therefore communicate with the OEM servers 304, and identify an associated server from the plurality of servers 304 based on the asset ID. The OEM servers 304 may be registered on the aggregator server 302, i.e. the updating device 302 at the time of installation of the system 300. Upon receiving the asset ID from the asset 306, the server updating device 302 may identify an associated server 304 from the plurality of servers 304 that is associated with the asset 306 connected to the charging station 308. Once the associated server 304 is identified, the updating device 302 may authenticate (first-level authentication) the asset ID. Later, the associated server 304 may authenticate (second-level authentication) the charging station 308 along with the asset ID associated with the asset 306. Thereafter, the updating device 302 may transmit asset data associated with the asset to the associated server 304. By way of an example, the asset data may include battery data, charging related data, etc.

**[040]** The updating device 302 may then query the associated server 304 for presence of the update package corresponding to the asset data. In other words, update updating device 302 may check whether any new update is available from the associated server 304 for updating the ECU of the asset 306.

**[041]** The updating device 302 may further request a user associated with the asset 306 for a permission for accessing the asset 306, i.e. to carry out updating of the ECU of the asset 306. In some embodiments, the updating device 302 may request the user via a user interface implemented in a display of the charging station 308. In alternate embodiments, the updating device 302 may request the user via a user device 320, for example, a smartphone with a mobile application installed on the smartphone, associated with the user. This mobile application may provide an interface to facilitate the user to respond to the request and grant permission to the updating device 302 and the associated server 304 to access the asset 306. To this end, the charging station 108 may be configured to communicatively couple with the user device 320 over a third network connection. For example, the third network connection is a Bluetooth-based connection, or an Internet-based connection.

**[042]** Upon authenticating of the asset ID and transmitting the asset data to the associated server 304, the updating device 302 may authenticate (second-level authentication) the asset 306 and the charging station 308. It should be noted that alternately the second-level authentication may be performed upon authenticating of the asset ID however before transmitting the asset data to the associated server 340 as well.

**[043]** Upon authenticating of the asset 306 and the charging station 308, transmitting the asset data to the associated server 304, and determining the presence of the update package, the updating device

302 may establish a secure communication channel for facilitating the transmission of the update package from the associated server 304 to the asset 306 via the secure communication channel. As such, the associated server 304 may start sending valid digitally-signed binary data package to the asset 306. As will be appreciated, neither the updating device 302 nor the charging station 308 saves any data but simply forwards the data package to the asset 306.

**[044]** Upon completion of the data transmission and upgrade of the ECU of the asset 306, the asset 306 may send status message to the charging station 308. The charging station 308 may further sends a status to the associated server 304 via the updating device 302. The associated server 304 may update its records for the asset 306 that has received the update.

**[045]** Referring now to **FIG. 4**, a block diagram of a system 400 (corresponding to the system 100 and system 300) for updating an asset is illustrated in accordance with some embodiments. As shown in FIG. 4, the system 400 includes an updating device 402, an OEM server 404, and a charging station 408. The updating device 402 may implement a secure communication channel creation module 412, a first authentication module 414, a campaign management module 416, and an update management module 418. The OEM server 404 may implement a software/firmware database 420 and a second authentication module 422.

**[046]** As mentioned above, when an asset 406 is connected to the charging station 408, the first-level authentication and the second-level authentication may be performed. The updating device 402 may communicate with the asset 406 via the charging station 408, when the asset 406 is connected to the charging station 408, to obtain the asset ID. In some embodiments, the first authentication module 414 of the updating device 402 may authenticate (i.e. perform the first-level authentication) the asset ID, based on one or more authentication parameters. Thereafter, the updating device 402 may transmit asset data associated with the asset to the OEM server 404. The updating device 402 may further query the server 404 for presence of the update package corresponding to the asset data. The software/firmware database 420 of the OEM server 404 may store and provide an update package associated with the asset.

**[047]** When the updating device 402 receives a response from the OEM server 404 about a presence of the update package, the campaign management module 416 may be activated to setup a sequence of the upgrade process. The campaign management module 416 may instruct the update management module 418 to send a User Interface input request to the user via the charging station 408 (i.e. via the User Interface of the charging station 408 or the user device). In other words, the updating device 402 requests the user associated with the asset 406 for a permission for accessing the asset 406, i.e. to

carry out updating of the ECU of the asset 406, as explained above. Once the permission is obtained from the user, the second authentication module 422 of the OEM server 404 may authenticate (i.e. perform the second-level authentication) the asset ID and the charging station 408 based on one or more respective authentication parameters.

**[048]** Once the user agrees (i.e. grants permission) to upgrade the ECU software, the secure communication channel creation module 412 may establish a secure communication channel for facilitating the transmission of the update package from the OEM server 404 to the asset 406 via the secure communication channel.

**[049]** The update management module 418 may further request the OEM server 404 to send valid digitally-signed binary data package to the asset 406. Upon completion of the data package transmission and upgrade of the ECU, the asset 406 may send a status notification corresponding to the completion of the transmission of the update package to the updating device 402. The updating device 402 may transmit the status notification to the OEM server 404. Based on this status notification, the OEM server 404 may update the status of the asset ID associated with the asset 406 that has received the update. In ither words, the OEM server 404 may update its records for the asset 406 that has received the update.

**[050]** Referring now to FIG. 5, a flowchart of a method 500 of updating an asset is disclosed. In some embodiments, the method 500 may be performed by the updating device 102 (or updating device 302 or updating device 402).

**[051]** At step 502, the asset ID associated with an asset may be received from the asset, via the charging station 108. The charging station 108 may be communicatively coupled to the asset updating device over a first network connection. The first network connection may be an Internet-based connection. Further, the charging station 108 communicatively coupled to the asset over a second network connection. The second network connection may be a wired connection.

**[052]** At step 504, the asset ID may be authenticated by the updating device 102 based on one or more authentication parameters. At step 506, an associated server may be identified from a plurality of servers 104 based on the asset ID. The associated server may store and provide an update package associated with the asset. In some embodiments, the associated server may be configured to perform a second-level authentication to authenticate the asset ID associated with the asset and the charging station based on one or more respective authentication parameters.

**[053]** Additionally, in some embodiments, at step 508, asset data associated with the asset may be transmitted to the associated server. Further, at step 510, the associated server may be queried for presence of the update package corresponding to the asset data.

**[054]** At step 512, upon authenticating the asset ID and identifying the associated server, the associated server may be requested for an update package associated with the asset.

**[055]** Additionally, in some embodiments, at step 514, a user associated with the asset may be requested for a permission for accessing the asset. The user may be requested via a user interface implemented in a display of the charging station 108. Alternately, the user may requested via a user device associated with the user and the asset. To this end, the charging station 108 may be configured to communicatively couple with the user device over a third network connection. The third network connection may be one of a Bluetooth-based connection or an Internet-based network connection.

**[056]** At step 516, a secure communication channel may be established between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

**[057]** Additionally, in some embodiments, at step 518, upon completion of the transmission of the update package from the associated server to the asset, a status notification may be received from the asset corresponding to the completion of the transmission of the update package. Further, at step 520, the status notification may be transmitted to the associated server.

**[058]** One or more techniques for updating an asset, for example an electric vehicle are disclosed in the above disclosure. The above techniques overcome the challenges in safety, security, and reliable connectivity faced by various conventional over-the-air (OTA)-based techniques. The above techniques allow for updating of the ECU of the electric vehicles during the time the electric vehicle is charging at a charging station. The charging station is configured to establish a wired connection with the asset over which the data exchange with OEM servers is facilitated. Further, the above techniques provide for a first-level authentication of the asset and a second-level authentication of the asset and the charging station to thereby minimize the possibility of unauthorized device access and online threats.

**[059]** It is intended that the disclosure and examples be considered as exemplary only, with a true scope and spirit of disclosed embodiments being indicated by the following claims.

## CLAIMS

**We Claim:**

**1.** An asset updating device comprising:

a processor; and

a memory communicatively coupled to the processor, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processor to:

receive, from an asset, an asset identification (ID) associated with the asset, via a charging station;

authenticate the asset ID based on one or more authentication parameters;

identify an associated server from a plurality of servers based on the asset ID, wherein the associated server is to provide an update package associated with the asset;

upon authenticating the asset ID and identifying the associated server, request the associated server for an update package associated with the asset; and

establish a secure communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

**2.** The asset updating device as claimed in claim 1,

wherein the charging station is communicatively coupled to the asset updating device over a first network connection,

wherein the first network connection is Internet-based connection; and

wherein the charging station is communicatively coupled to the asset over a second network connection,

wherein the second network connection is a wired connection.

**3.** The asset updating device as claimed in claim 1, wherein the associated server is configured to perform a second-level authentication to authenticate the asset ID associated with the asset and the charging station based on one or more respective authentication parameters.

**4.** The asset updating device as claimed in claim 1, wherein the processor-executable instructions, upon execution, further cause the processor to:

request a user associated with the asset for a permission for accessing the asset, wherein the user is requested via one of:

a user interface implemented in a display of the charging station; or

a user device associated with the user and the asset; and

upon obtaining the permission to access the asset, facilitate transmission of the update package from the server to the asset, via the charging station.

**5.** The asset updating device as claimed in claim 1, wherein the charging station is configured to communicatively couple with the user device over a third network connection,

wherein the third network connection is one of a Bluetooth-based connection or an Internet-based network connection.

**6.** The asset updating device as claimed in claim 1, wherein the processor-executable instructions, upon execution, further cause the processor to:

transmit asset data associated with the asset to the associated server;

query the associated server for presence of the update package corresponding to the asset data; and

upon determining the presence of the update package, establish the secure communication channel for facilitating the transmission of the update package from the associated server to the asset via the secure communication channel.

**7.** The asset updating device as claimed in claim 6, wherein the processor-executable instructions, upon execution, further cause the processor to:

upon completion of the transmission of the update package from the associated server to the asset, receive a status notification from the asset corresponding to the completion of the transmission of the update package; and

transmit the status notification to the associated server.

**8.** A method of updating an asset, the method comprising:

receiving, by an updating device, an asset identification (ID) associated with an asset from the asset, via a charging station;

authenticating, by the updating device, the asset ID based on one or more authentication parameters;

identifying, by the updating device, an associated server from a plurality of servers based on the asset ID, wherein the associated server is to provide an update package associated with the asset;

upon authenticating the asset ID and identifying the associated server, requesting, by the updating device, the associated server for an update package associated with the asset; and

establishing, by the updating device, a secure communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

**9.** The method as claimed in claim 8,

wherein the charging station is communicatively coupled to the asset updating device over a first network connection,

wherein the first network connection is Internet-based connection; and

wherein the charging station is communicatively coupled to the asset over a second network connection,

wherein the second network connection is a wired connection.

**10.** The method as claimed in claim 9, wherein the associated server is configured to perform a second-level authentication to authenticate the asset ID associated with the asset and the charging station based on one or more respective authentication parameters.

**11.** The method as claimed in claim 8 further comprising:

request a user associated with the asset for a permission for accessing the asset, wherein the user is requested via one of:

a user interface implemented in a display of the charging station; or

a user device associated with the user and the asset; and

upon obtaining the permission to access the asset, facilitate transmission of the update package from the server to the asset, via the charging station.

**12.** The method as claimed in claim 8, wherein the charging station is configured to communicatively couple with the user device over a third network connection,

wherein the third network connection is one of a Bluetooth-based connection or an Internet-based network connection.

**13.** The method as claimed in claim 8, further comprising:

transmitting asset data associated with the asset to the associated server;

querying the associated server for presence of the update package corresponding to the asset data; and

upon determining the presence of the update package, establishing the secure communication channel for facilitating the transmission of the update package from the associated server to the asset via the secure communication channel.

**14.** The method as claimed in claim 13 further comprising:

upon completion of the transmission of the update package from the associated server to the asset, receiving a status notification from the asset corresponding to the completion of the transmission of the update package; and

transmitting the status notification to the associated server.

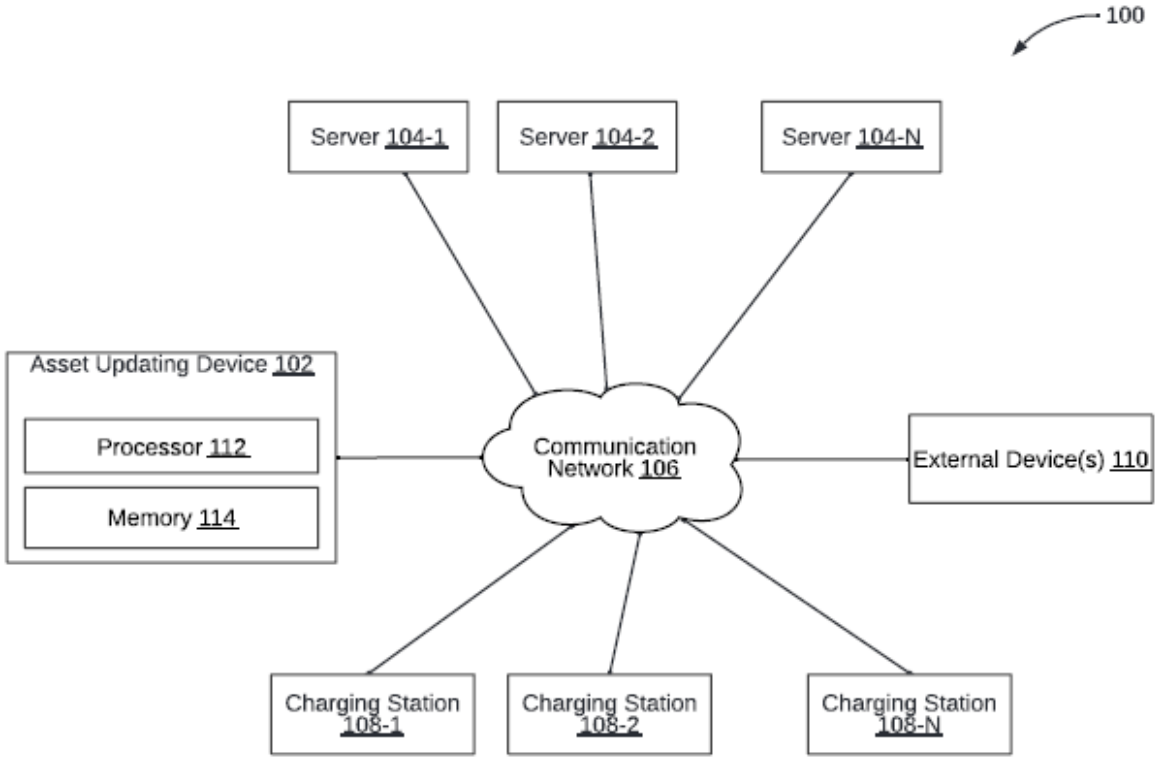
**Dated this 19th Day of March 2022**

**Robin Koshy Varghese (INPA No: 3705)**
**Head, IPR Dept.**
**L&T Technology Services Ltd.**
**DLF 3rd Block, 2nd Floor,**
**Manapakkam, Chennai - 600089.**

**SYSTEM AND METHOD OF UPDATING AN ASSET**


## ABSTRACT

A method and a system for updating an asset is disclosed. The method may include receiving an asset identification (ID) associated with an asset from the asset, via a charging station and authenticating the asset ID based on one or more authentication parameters. The method may further include identifying an associated server from a plurality of servers based on the asset ID. The associated server is to provide an update package associated with the asset. The method may further include upon authenticating the asset ID and identifying the associated server, requesting the associated server for an update package associated with the asset, and establishing a secure communication channel between the associated server and the asset for facilitating a transmission of the update package from the associated server to the asset.

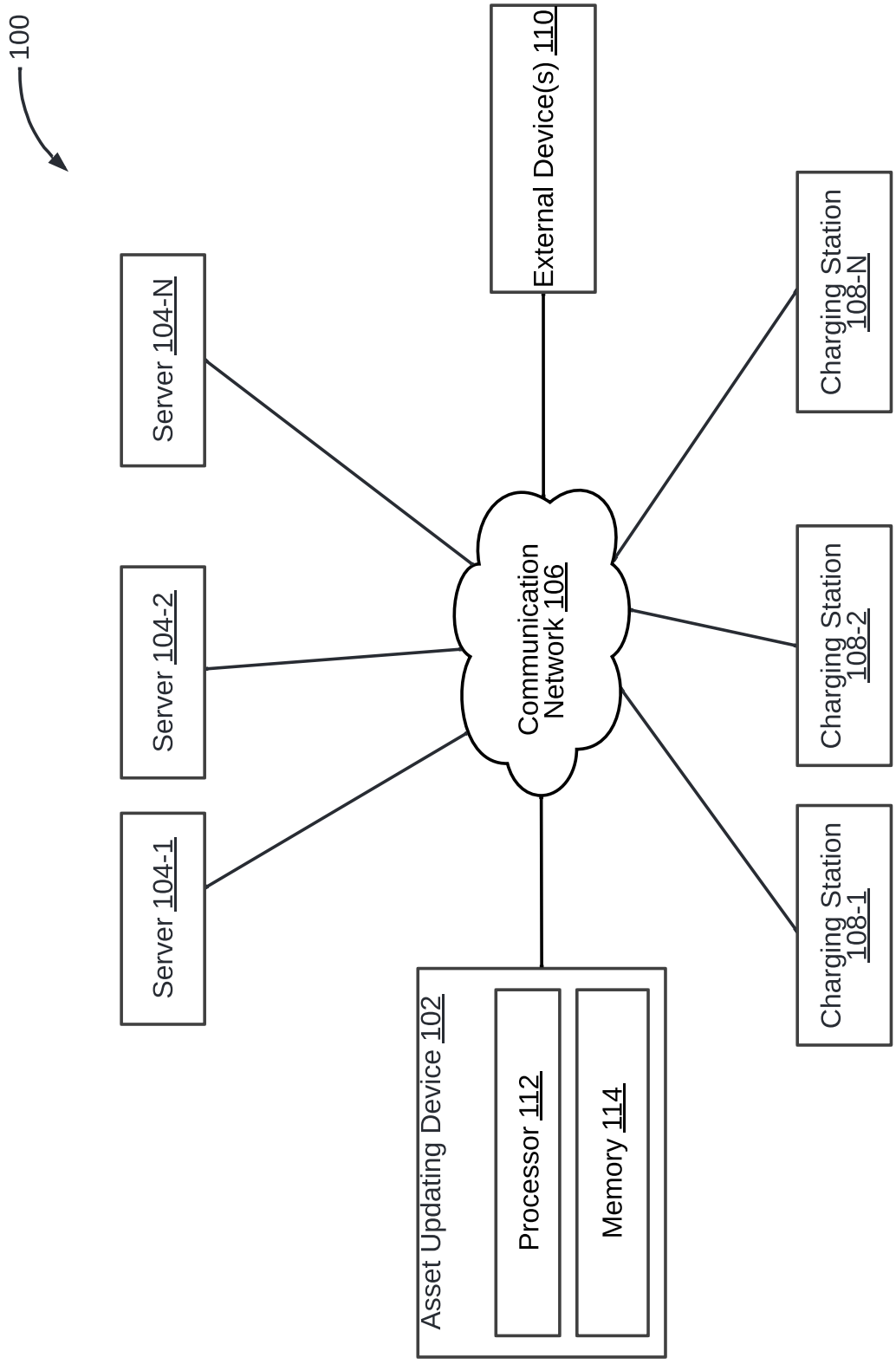



FIG. 1

ROBIN KOSHY VARGHESE (INPA No.: 3705)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600 089.

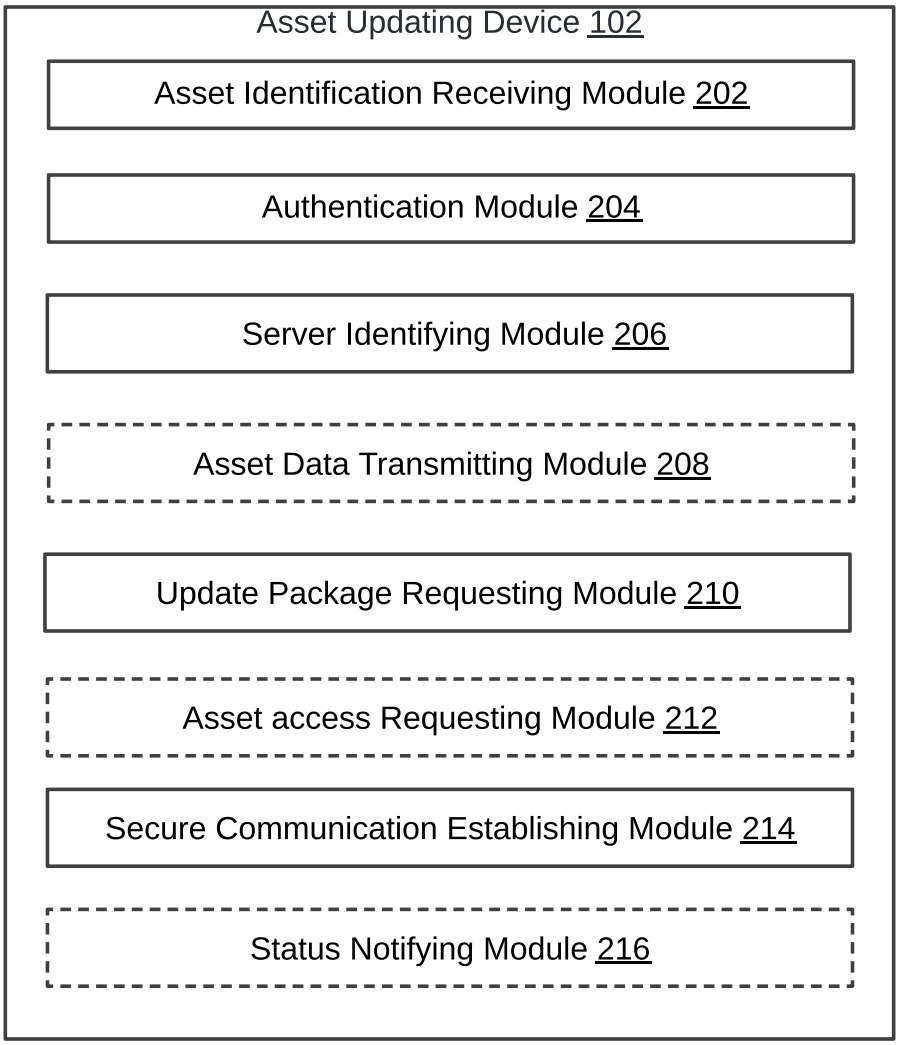



**FIG. 2**

**ROBIN KOSHY VARGHESE (INPA No.: 3705)**
**Head, IPR Dept.,**
**&T Technology Services Limited,**
**DLF 3rd Block, 2nd Floor,**
**Manapakkam, TN, Chennai - 600 089.**

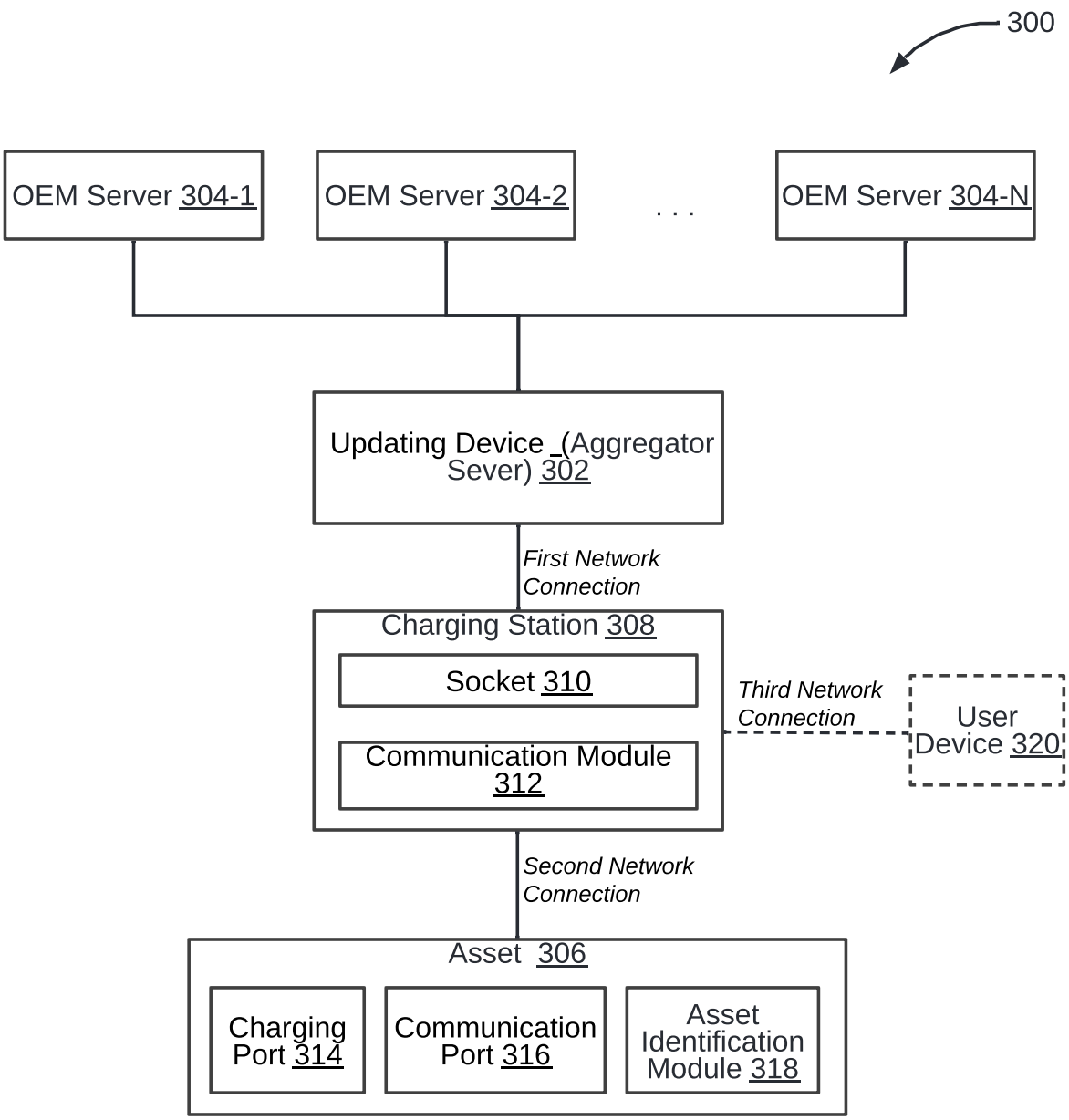



**FIG. 3**

**ROBIN KOSHY VARGHESE (INPA No.: 3705)**
**Head, IPR Dept.,**
**&T Technology Services Limited,**
**DLF 3rd Block, 2nd Floor,**
**Manapakkam, TN, Chennai - 600 089.**

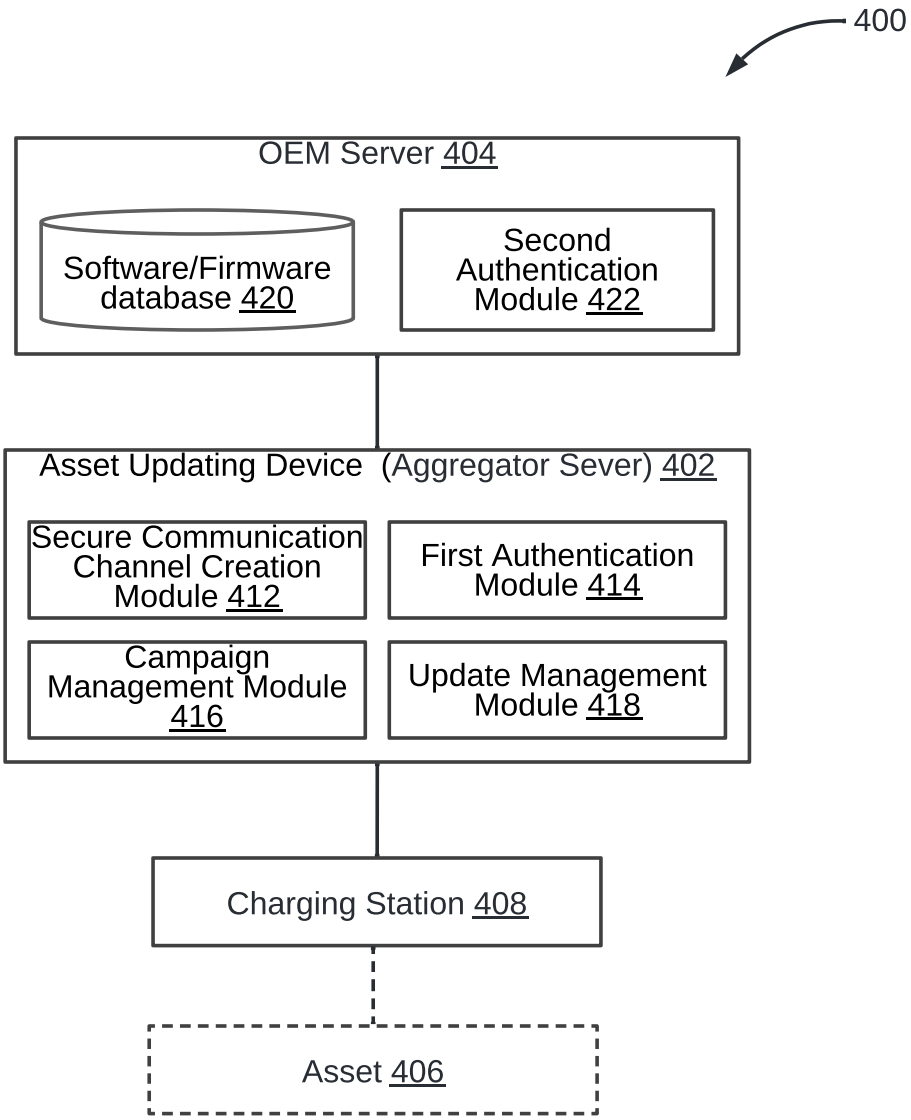



**FIG. 4**

**ROBIN KOSHY VARGHESE (INPA No.: 3705)**
**Head, IPR Dept.,**
**&T Technology Services Limited,**
**DLF 3rd Block, 2nd Floor,**
**Manapakkam, TN, Chennai - 600 089.**

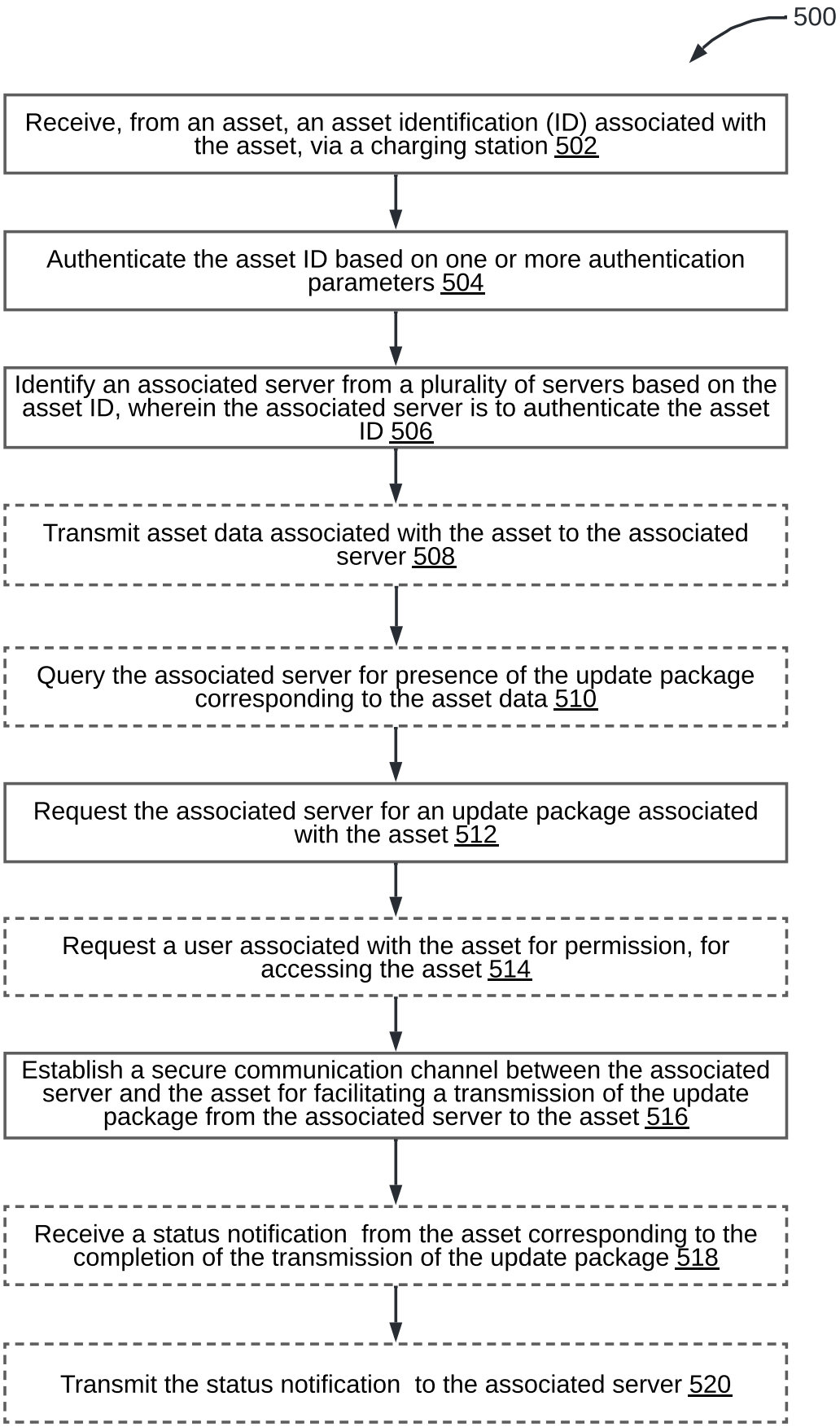



**FIG. 5**

**ROBIN KOSHY VARGHESE (INPA No.: 3705)**
**Head, IPR Dept.,**
**L&T Technology Services Limited,**
**DLF 3rd Block, 2nd Floor,**
**Manapakkam, TN, Chennai - 600 089.**