(12)Indian Patent Application

---

(21) Application Number: 6010/CHE/2014

(22) Filing Date: 01/12/2014 (43) Publication Date: 26/08/2016

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

(72) Inventor(s): SANZGIRI, MAHESH
PATTNAIK, GYANA BARDHAN
RAMKUMAR, V
ATTILI, APARNNA
SMITHA, K. (4 more...)

(51) International Classifications: H04N

(54) Title: Domain Cloud and Device Agnostic Systems and Method Thereof

(57) Abstract: According to an embodiment of the invention, a system and method for providing machine-to-machine (M2M) cloud mobility is disclosed. The disclosed system includes a cloud agnostic component, a domain agnostic component and one or more display component(s). The domain agnostic component is configured to receive data from one or more devices independent of protocols followed by the device. The received data is converted to one or more domain specific standards pertaining to the data and communicated to the cloud agnostic component. One or more display components provide an interface to access the domain agnostic component and the cloud agnostic component.

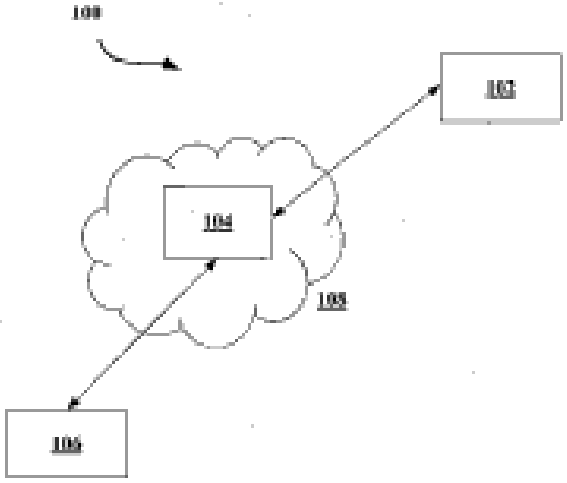

Figure 1

ABSTRACT

According to an embodiment of the invention, a system and method for providing machine-to-machine (M2M) cloud mobility is disclosed. The disclosed system includes a cloud agnostic component, a domain agnostic component and one or more display component(s). The domain agnostic component is configured to receive data from one or more devices independent of protocols followed by the device. The received data is converted to one or more domain specific standards pertaining to the data and communicated to the cloud agnostic component. One or more display components provide an interface to access the domain agnostic component and the cloud agnostic component.

We claim :
~~Claims:~~

1. A system for providing machine-to-machine(M2M) cloud mobility, the system comprising:

a cloud agnostic component;

a domain agnostic component is configured to:

receive data from one or more devices independent of protocols followed by the device;

convert the received data to one or more domain specific standards pertaining to the data; and

communicate the received data to the cloud agnostic component; and

one or more display components for providing an interface to access the domain agnostic component and the cloud agnostic component.

2. The system of claim 1 wherein the domain agnostic component communicates with the cloud agnostic component using any wired or wireless internet connection.

3. The system of claim 1 wherein the domain agnostic component comprises at least one cloud connectivity sub component, at least one data controller sub component, at least one security sub component, at least one out transit queue, at least one intelligent information, at least one data acquisition, at least one communication protocol container and at least one physical communication container.

4. The system of claim 1 wherein the domain agnostic component communicates the received data to the cloud agnostic component based on data accumulation or user preferences.

5. The system of claim 1 wherein the domain agnostic component receives data from the one or more devices according to a preconfigured time interval.

6. The system of claim 1 wherein the domain agnostic component is further configured to establish communication with the cloud agnostic component by sending a request or on subscription to a notification mechanism.

7. The system of claim 1 wherein the cloud agnostic component comprises at least one security boundary sub component, at least one service engine sub component, at least one domain specific standards sub component, at least one service information sub component, at least one secure connectivity sub component, at least one admin configuration sub component and at least one log manager sub component.

8. The system of claim 1 further comprising an authentication module to validate communication between the domain agnostic component and the cloud agnostic component.

9. The system of claim 1 further comprising a web application dashboard for provisioning and de-provisioning of applications, gateways and devices with auto device detection feature.

Dated this 30th day of November 2015

Mohammed Faisal (INPA No: 1941)
Head, IPR
L&T Technology Services Ltd.

FIELD OF INVENTION

The invention generally relates to systems and methods for providing cloud based services and more particularly to systems and methods for providing domain and cloud agnostic cloud based services.

BACKGROUND

Cloud computing provides computation, capacity, networking, and storage on demand. Typically, computing resources such as computing machines, storage devices, and/or network devices are simulated by one or more virtual machines. Several virtual machines may be hosted from a single physical hardware infrastructure resource (e.g., a server). Multiple virtual machines may be associated within a cloud infrastructure to form combinations of resources known as computing environments. Individual users of cloud computing services may lease the processing and storage services of one or more virtual machines, distributed among one or more physical infrastructure resources in a cloud data centre. Typical cloud computing allows a virtually unlimited amount of computing resources to be dynamically requisitioned, on demand, from a pool of shared computing resources offered by a cloud computing provider. Thus, cloud computing users can elastically provision infrastructure resources from the provider's pool only when needed.

Although cloud computing allows users quicker access to the computing resources relative to traditional technology models, cloud computing also presents significant and distinct challenges. Typically, the cloud computing systems entertain specific platform depend application. So the users have limited application options.

The present invention is directed to overcoming one or more of the problems as set forth above.

SUMMARY OF THE INVENTION

According to an embodiment of the invention, a system and method for providing machine-to-machine (M2M) cloud mobility is disclosed. The disclosed system includes a cloud agnostic component, a domain agnostic component and one or more display component(s). The domain agnostic component is configured to receive data from one or more devices independent of protocols followed by the device. The received data is converted to one or more domain specific standards pertaining to the data and communicated to the cloud agnostic component. One or more display components provide an interface to access the domain agnostic component and the cloud agnostic component.

BRIEF DESCRIPTION OF DRAWINGS

Other objects, features, and advantages of the invention will be apparent from the following description when read with reference to the accompanying drawings. In the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

Figure 1 illustrates a block diagram of exemplary domain and cloud agnostic system;

Figure 2 illustrates a block diagram of a domain agnostic component according to an exemplary embodiment of the invention; and

Figure 3 illustrates a block diagram of a cloud agnostic component according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF DRAWINGS

According to an embodiment of the invention, domain and cloud agnostic system and method is disclosed. Figure 1 illustrates a block diagram of exemplary domain and cloud agnostic system 100. The disclosed system 100 may have a domain agnostic component 102, a cloud agnostic component 104 and one or more display component(s) 106. The domain agnostic component may be configured to receive data from one or more devices independent of protocols followed by the device. According to an embodiment, the domain agnostic component may include a processor to convert the data to one or more domain specific standards. According to another embodiment, the domain agnostic component 102 may include a domain agnostic framework that may communicate with cloud agnostic component 104 using any wired or wireless communication network 108 such as, but not limited to, 2G, 3G, Wi-Fi, data card, wired internet connection etc. According to yet another embodiment, the domain agnostic component 102 may provide end-to-end solution by interfacing between devices from various domains and user applications available on different devices. The domain agnostic component 102 may further safeguard industry standards, security and encrypted data transfer to cloud agnostic component 104. According to further embodiment, the display component 106 may provide an interface for accessing the domain agnostic component 102 and the cloud agnostic component 104.

The domain agnostic component 102 may enable device data transfer to Cloud to achieve M2M Cloud mobility enterprise solution by facilitating communication with devices from

different industries following different protocols. The domain agnostic component 102 may enable deployment of the disclosed system 100 for identified device types such as auto, medical, energy meters etc. According to embodiments of the invention, the domain agnostic component 102 may automate the communication with one or more devices as per a time interval configured by user. The configuration of time interval may depend upon the capability of hardware and network speed. According to yet another embodiment, the domain agnostic component 102 may transfer the device data to cloud agnostic component based on the data accumulation or time as per user preference.

According a further embodiment, the system 100 may have a component which provides a feature of Cloud agnostic to public or private clouds for different business models and to address data security and confidentiality. The system 100 may provide a plug-in architecture for plugging in different Security algorithms for data at rest. The system may also supports standard security algorithms for security of data in transit. The system 100 may support the component which has the feature of build once and deploy on any (iOS, Andriod, Windows) smart phone device.

According to yet another embodiment, the system 100 may also provide Web based application dashboard which is an admin console for provisioning and de-provisioning of applications, gateways and devices of different communication modes and associated parameters with auto device detection feature. This component may provide a Web based application dashboard reports of the transactions happening within the framework for monitoring and control. This component may also act as a portal for management, provisioning and reporting of applications, gateways and devices (sensors, instruments, equipment).

Figure 2 illustrates a block diagram of the domain agnostic component 102 according to an exemplary embodiment of the invention. As illustrated, the domain agnostic component 102 may have various sub components such as, but not limited to, a cloud connectivity 202, a data controller 204, a security 206, an out-transit queue 208, an intelligent information system 210, a domain specific standards 212, a data acquisition 214, a communication protocol container 216, a physical communication container 218 etc.

The cloud connectivity sub component 202 may provide different connectivity options for the devices to connect to the cloud agnostic component 104. The connectivity may be through a wired communication network such as but not limited to, LAN, DSL etc. or through a wireless communication network such as, but not limited to, 2G, 3G, Wi-Fi, etc.

The data controller sub component 204 may manage interaction between the cloud agnostic component 104 and the domain agnostic component 102. According to an embodiment, push may be used to send data from the domain agnostic component 102 to the cloud agnostic component 104. According to another embodiment, pull may be used as receiver for the data sent by the cloud agnostic component 104. According to yet another embodiment, MQTT Client may be used to publish data to the cloud agnostic component 104 or subscribe the data from the cloud agnostic component 104.

The security sub component 206 may provide functionalities including encryption/decryption, authentication, authorization and CRC check.

The out-transit queue sub component 208 may store data received from the devices until said data is synchronized with the cloud agnostic component 102. According to an embodiment, the data may be deleted on synchronization with the cloud agnostic component 102. According to another embodiment, frequency of data synchronization may be configurable.

According to an embodiment, the Intelligent Information system sub component 210 may initiate the data collection using one or more devices. The intelligent information system sub component 210 may include modules such as but not limited to a scheduler module 210a, a health check module 210b, a reporting module 210c and a notification module 210d.

The scheduler module 210a may initiate data collection from the devices connected to the system 100 based on configuration of the scheduler module 210a. According to an embodiment, the scheduler module 210a may initiate data collection weekly, monthly or/and annually.

The health check module 210b may check the status of one or more devices connected to the system 100. According to an embodiment, the health check module 210b may check the alive status of the devices at regular intervals. The reporting module 210c may report functionality failures and device status to user. According to an embodiment, the reporting module 210c may report functionality failures such as, but not limited to, connection failure from the device, connection failure to the cloud agnostic component 102 etc. According to another embodiment, the reporting module 210c may report information to user about the status of the connected device. According to yet another embodiment, an interface may be provided to report information about the status of the connected device. The notification module 210d may generate notifications on connectivity problems that may require

immediate actions, using one or more communication mode such as, but not limited to, SMS, e-mail, etc.

The domain specific standards sub component 212 may include standards pertaining to one more products. According to an exemplary embodiment, the domain specific standards sub component 212 may include standers such as, but not limited to, HL7, DLMS etc. The HL7 is international healthcare informatics interoperability standards. According to an embodiment, the HL7 may provide a framework (and related standards) for exchange, integration, sharing and retrieval of electronic health information. The DLMS are set of standards for electricity metering by International Electro technical Commission. According to an embodiment, the DLMS may provide a framework for data exchange for meter reading, tariff and load control.

The data acquisition sub component 214 may collect data from the devices based on the request from the scheduler module of intelligent information system 210.

The communication protocol container sub component 216 may hold different protocols that may communicate with the devices. According to an embodiment, the protocols supported by the communication protocol container sub component 216 may be Modbus, DNP3, DLMS etc.

The physical communication/connection container 218 may be a collection of communication modes that may support the device connection type. According to an embodiment, the physical connection container 218 may provide a channel of communication based on the configuration for the current request. According to an exemplary embodiment, the physical

connection container may support connections such as, but not limited to, Bluetooth, RS232, USB, Zigbee, Ethernet, Wi-Fi etc.

Once the communication is established, the data acquisition may start. The listener may wait for the requested data to arrive and the polling engine may process the request and receive the data. The In-Transient queue may further manage multiple requests and the received data for further processing. The received data may be converted to one or more domain specific standards (if required) and the converted data may move to the data queue to dispatch from the domain agnostic component 102. The system may optionally perform security check measures such as, but not limited to, encryption and credential verification. The secured data along with the domain agnostic component 102 identity may be transferred to a cloud through the cloud connectivity interface.

According to an embodiment, the domain agnostic component 102 may establish communication with the cloud agnostic component 104 by sending a request. On verification, the cloud agnostic component 104 may acknowledge the request with one or more security measure such as one time password. On validation, the domain agnostic component 102 may receive the configuration file from the cloud agnostic component 104. The configuration file, received by the domain agnostic component 102 may be used in the parameter settings of different layers of the domain agnostic component 102.

According to another embodiment, the domain agnostic component 102 may establish communication with the cloud agnostic component 104 on subscription to a notification mechanism. The notification may be in the form of message or e-mail.

Figure 3 illustrates a block diagram of the cloud agnostic component 104 according to an exemplary embodiment of the invention. As illustrated, the cloud agnostic component 104 may have various sub components such as, but not limited to, a Secure Connectivity 302, a Service Information 304, a Domain Specific Standards 306, a Service Engine 308 and a Security Boundary 310. The cloud agnostic component 104 may include other components such as, but not limited to, Admin Configuration etc.

The secure connectivity sub component 302 may provide data security, cloud security, security testing of the cloud application, identity and access management. The secure connectivity sub component 302 may provide functions such as, but not limited to, encryption/decryption, authentication, authorization, CRC check etc.

The service information sub component 304 may provide notification, monitoring and reporting services. According to an embodiment, the notification service may include e-mail or sms notification for issuing notification such as, but not limited to, failure on database update, connectivity lost etc. According to another embodiment, the monitoring service may include data traffic monitoring between the cloud agnostic component and the domain agnostic component. According to yet another embodiment, the reporting service may generate report for operational, management and controlled details based on configuration by user. According to an embodiment, the reporting service may generate report daily, weekly, monthly and/or annually.

The domain specific standards sub component 306 may select the data depending upon the domain to which the data belongs to and may set the standards accordingly. According to an exemplary embodiment, the domain specific standards sub component 306 may set standard

HL7 for the data belonging to medical domain and DLMS for the data belonging to Electric meter devices.

The service engine subcomponent 308 may receive the data or command through a push or pull service for the data update or query response.

The security boundary sub component 310 may provide functions such as, but not limited to, encryption/decryption, authentication, authorization, CRC check. According to embodiment of the invention, before initiating data communication, an authentication process may be used to validate data transfer between the domain agnostic component 102 and the cloud agnostic component 104.

The admin configuration sub component may allow an administrator to define basic settings of the cloud agnostic component 104. According to an embodiment, the basic settings may include settings such as, but not limited to, role based access control, device management, scheduler settings, connectivity settings, protocol settings, notification settings etc.

In the drawings and specification there has been set forth preferred embodiments of the invention, and although specific terms are employed, these are used in a generic and descriptive sense only and not for purposes of limitation. Changes in the form and the proportion of parts, as well as in the substitution of equivalents, are contemplated as circumstances may suggest or render expedient without departing from the spirit or scope of the invention.

L&T Technology Services Limited

6010/CHE/2014

Total number of Sheets: 3
Sheet No. 1 of 3

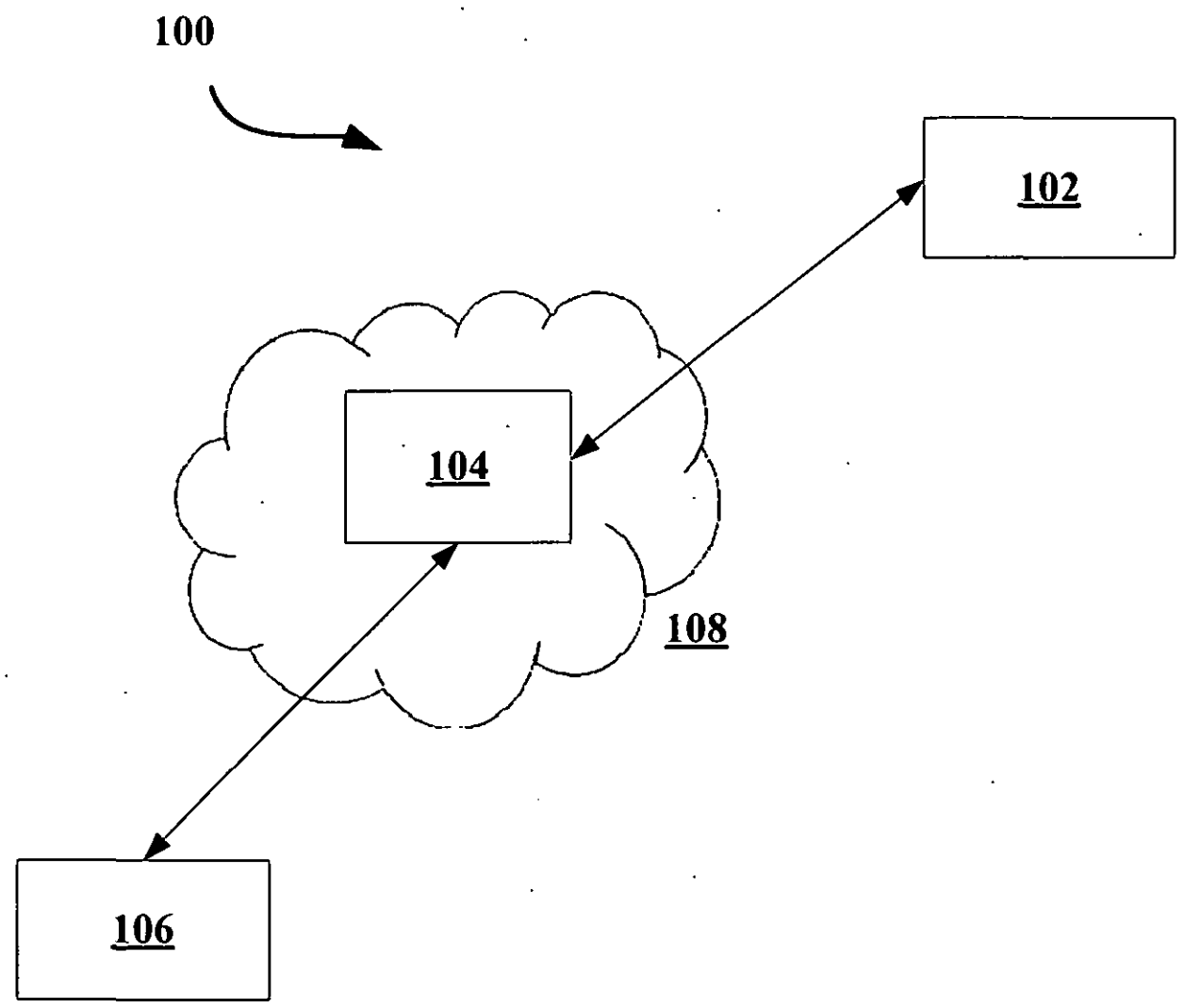

Figure 1

Mohammed Faisal (INPA No: 1941)
Head, IPR
L&T Technology Services Limited

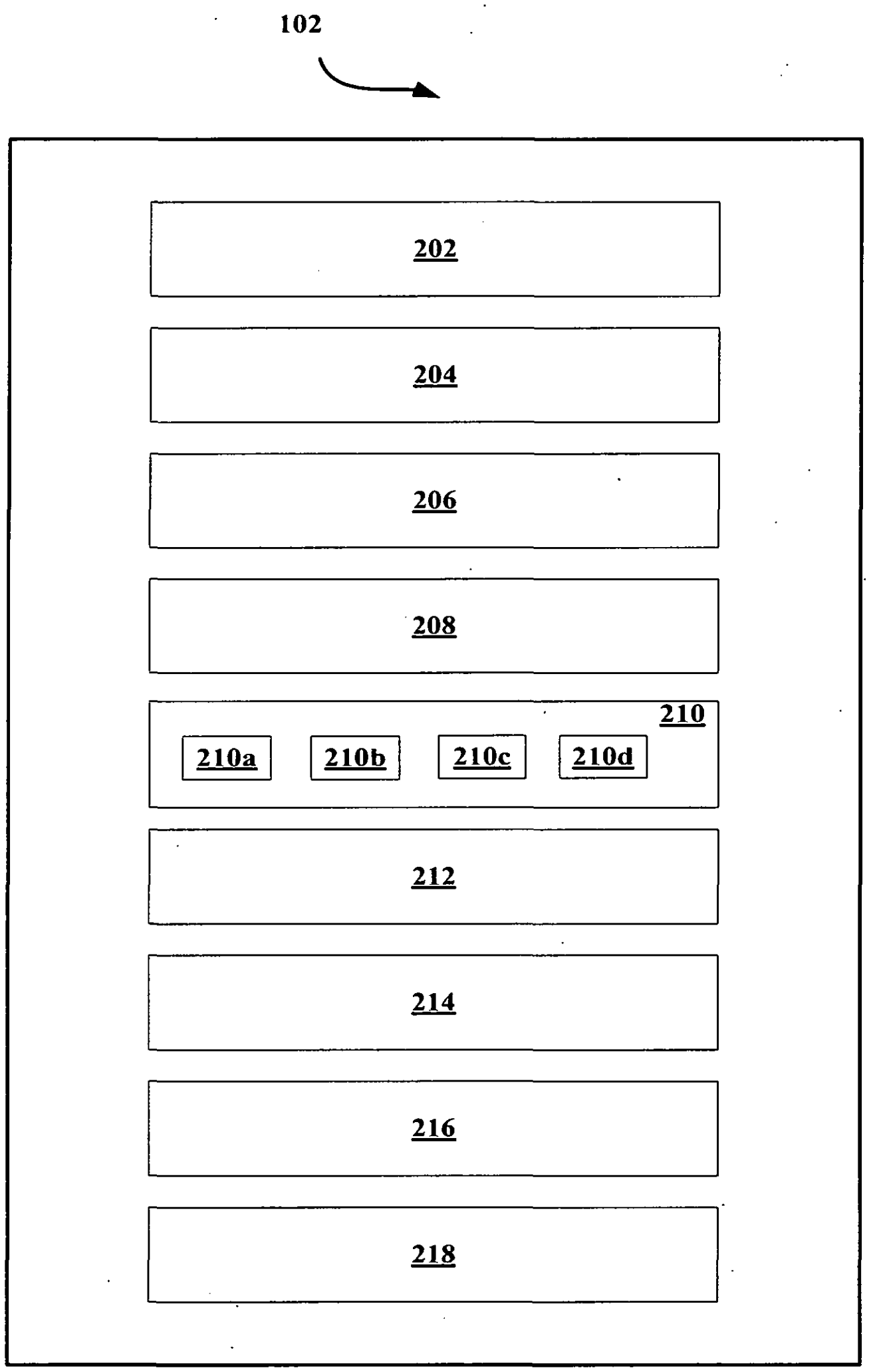

Figure 2

Mohammed Faisal (INPA No: 1941)
Head, IPR
L&T Technology Services Limited

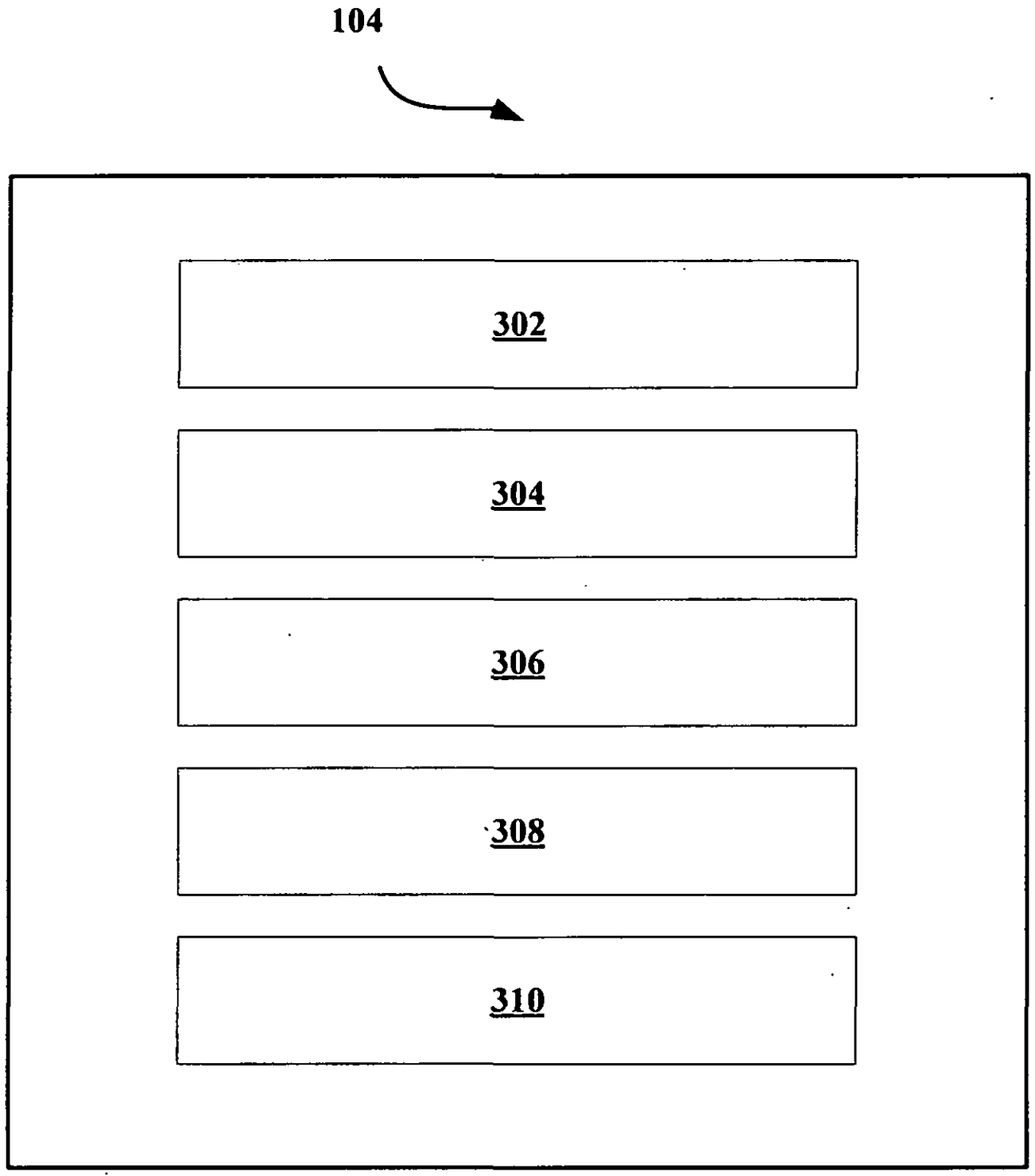

Figure 3

Mohammed Faisal (INPA No: 1941)
Head, IPR
L&T Technology Services Limited