(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 March 2021 (25.03.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/051259 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/CN2019/106112

(22) International Filing Date:
17 September 2019 (17.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US).

(72) Inventors; and

(71) Applicants *(for US only)*: **BOURDAGES, Simon** [CA/US]; One Microsoft Way, Redmond, Washington 98052 (US). **LOZA, Hani, G.** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US). **YAP, Joe, K.** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US). **ZHANG, Zhigang** [CN/CN]; One Microsoft Way, Redmond, Washington 98052 (US). **ZHU, Hongliang** [CN/CN]; One Microsoft Way, Redmond, Washington 98052 (US). **WANG, Huan** [CN/CN]; One Microsoft Way, Redmond, Washington 98052 (US). **RATNAPARKHI, Yogesh Abhaykumar** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US). **CHAKRAVARTY, Mrinalini** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US). **JANSEN, Dieter** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US).

(74) Agent: **SHANGHAI PATENT & TRADEMARK LAW OFFICE, LLC**; 435 Guiping Road, Shanghai 200233 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

(54) Title: CENTRALIZED REMOTE MIGRATION CLIENT CREDENTIAL MANAGEMENT

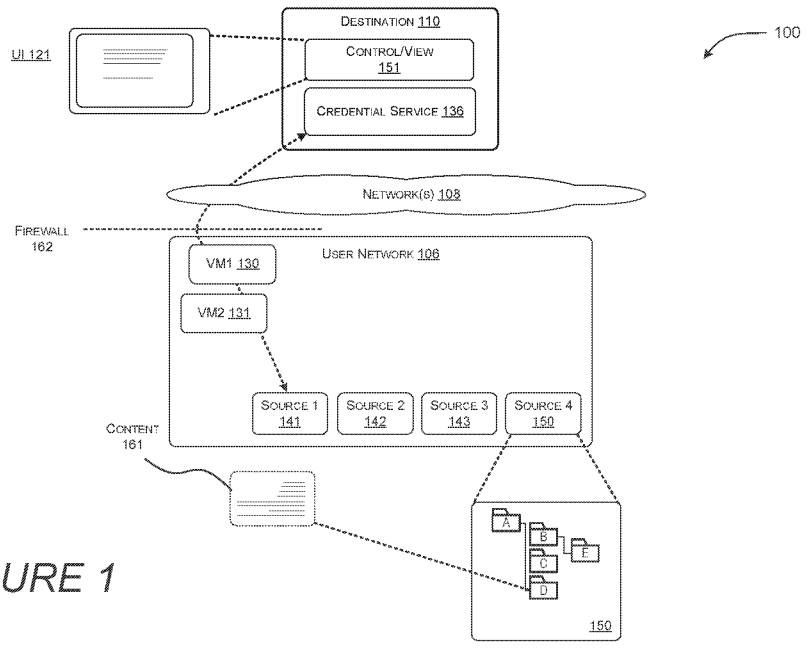

FIGURE 1

(57) Abstract: A cloud-based network receives a public key of a public/private key pair and a credential for accessing secrets associated with a user network. The cloud-based network receives, from a user interface configured to facilitate remote control of the user network, a command to be executed at the user network. The cloud-based network encrypts, using the public key, the credential and the command. The cloud-based network forwards, to one or more client devices, the encrypted credential and command. The client devices are configured to decrypt the encrypted credential and command using a private key of the public/private key pair and execute the command on the user network.

WO 2021/051259 A1

[Continued on next page]

HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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).

Published:

— *with international search report (Art. 21(3))*

CENTRALIZED REMOTE MIGRATION CLIENT CREDENTIAL MANAGEMENT

BACKGROUND

[1] The use of cloud-based computing services has greatly increased in recent years. When enterprises expand their networks to the cloud-based computing services, limitations may be encountered. Ensuring that users can securely access and control their on-premises data can be challenging given the total amount of assets that many users typically have in their networks. Large scale operations such as migration of multiple virtual machines to the cloud may require repetitive tasks to securely access and control the user's machines. Furthermore, security measures such as firewalls typically limit the accessibility of a user's assets from the cloud service provider. This can lead to a number of inefficiencies, as security features must be applied to the user's assets, and yet such security features may hinder the accessibility and control of the user's assets by the cloud service provider. The additional effort and cost may become a barrier for users to migrate their assets to the virtualized environment.

[2] Such limitations can cause a number of inefficiencies and a less than desirable user experience.

SUMMARY

[3] Embodiments of this disclosure are directed to the centralized storage and management of user credentials. It is often desirable to remotely access and control a user's network by a cloud-based service provider. For example, for large scale migration of a user's computing

resources to the cloud involving multiple client machines, the service provider may need to be able to use the correct credentials required for the authorization for movement of content. The disclosed embodiments provide for a centralized location that stores the credentials, receives encrypted commands, and securely pushes down the credentials and commands to enable remote control of the user's assets. This alleviates the need to individually be authorized to access each of the user's machines, while at the same time maintaining security of the user's assets and protecting the integrity of the credentials. Thus the multiple steps to manually access individual machines can be consolidated by allowing for one central location to securely maintain the credentials.

[4] The techniques disclosed herein provide a number of improvements over existing systems. For instance, when the credentials are stored at a centralized service, such as Google Drive, iCloud, or OneDrive, the need to repeatedly access and provide credentials to multiple assets can be avoided, as well as the need to contend with multiple credentials and synchronize credential versions. The techniques disclosed herein further improve user interaction with a computer along with providing improvements with respect to processing resources, network resources, and memory resources.

[5] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter. The term "techniques," for instance, may refer to system(s), method(s), computer-readable instructions, module(s), algorithms, hardware logic, and/or operation(s) as permitted by the context described above and throughout the document.

Brief Description of the Drawings

[6] The Detailed Description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same reference numbers in different figures indicate similar or identical items. References made to individual items of a plurality of items can use a reference number with a letter of a sequence of letters to refer to each individual item. Generic references to the items may use the specific reference number without the sequence of letters.

[7] FIGURE 1 is a block diagram of a system for accessing a user network.

[8] FIGURE 2 is a block diagram showing a system for accessing a user network.

[9] FIGURE 3 is a flow diagram showing aspects of a routine for accessing a user network.

[10] FIGURE 4 is a flow diagram showing aspects of a routine for accessing a user network.

[11] FIGURE 5 is a flow diagram showing aspects of a routine for accessing a user network.

[12] FIGURE 6 is a flow diagram showing aspects of a routine for accessing a user network

[13] FIGURE 7 is a computer architecture diagram illustrating an illustrative computer hardware and software architecture for a computing system capable of implementing aspects of the techniques and technologies presented herein.

[14] FIGURE 8 is a diagram illustrating a distributed computing environment capable of implementing aspects of the techniques and technologies presented herein.

Detailed Description

[15] Various embodiments are described for enabling the centralized storage and management of user credentials. Embodiments provide for a centralized location that stores the credentials, receives encrypted commands, and securely pushes down the credentials and commands to enables remote control of the user's assets.

[16] Referring to FIG. 1, illustrated is an example of a user network 106 that includes a number of user sources 141, 142, 143, and 150. The user network may include one or more virtual machines 130, 131. The sources 141, 142, 143, and 150 may host various data and applications, including, for example, file system 150 that enables access to content 161. The sources 141, 142, 143, and 150 at the user network 106 may be protected via firewall 161. In some cases, the user may wish to remotely access their network and perform operations. For example, the use may wish to migrate some of the user's assets such as virtual machines 130, 131 to a cloud environment 110 via network 108. In user environments with multiple virtual machines and multiple sources, accessing the user's assets by the cloud environment 110 through the firewall may require extensive credential management and complexity. The system 100 can also include one or more networks 108 for enabling the computing devices to communicate. This example is provided for illustrative purposes and is not to be construed as limiting. It can be appreciated that the system 100 can include any number of computers. The cloud service can be in the form of a personal computer, a server farm, a large-scale computer system or any other computing system having components for processing, coordinating, collecting, storing, and/or communicating data between one or more computing devices. Examples of such services include storage services provided by OneDrive, Dropbox, Microsoft, Amazon, Apple, Google, etc.

[17] In an embodiment, a control/view function may be provided that enables an administrator, via UI 121, to remotely initiate actions on the user network 106. A credential service 136 may be provided for centralized control of the user assets. The credential service 136 may provide storage and management of credentials in one location, enabling control of the user assets behind firewall 162.

[18] Referring to FIG. 2, illustrated is a cloud administrator 220 and cloud server 252. The cloud administrator 220 may send tasks and commands to the cloud server 252, and may receive results and reports from cloud server 252. The cloud server 252 may send the tasks and commands to the clients 231 for action and completion. The clients 231 may send results and reports to cloud server 252, which may provide status to the cloud administrator 220, for example via UI 121 of FIG. 1.

[19] In one embodiment, an installer or an agent may be created and installed on each user virtual machine. The installer/agent may, for example, be added to each user virtual machine. In one embodiment, the installer/agent may be unique for each user, for example, with a unique ID or a unique handshake. After the installer/agent is added, a connection may be initiated on each machine. Registration may be unique for each user and destination. In an embodiment, registration may be implemented with credentials via HTTPS and not a virtual private network (VPN). Via the HTTPS connection, commands may be dispatched from the cloud-based platform into a machine inside the user environment in a secure fashion. In one implementation, credentials may be passed to each machine. In some embodiments, access may be focused or limited, for example to access a specific location. For example, each virtual machine may only access what it is authorized for. The disclosed embodiments thus enable a remote service to access on-premise resources via remote and centralized credential management.

[20] The credentials may be of various types, for example username/password, or any form of credential such as multi-factor authentication (MFA), active directory, etc. The commands may include not only migration but any type of command that may be executed at the user network, such as obtaining file system information and deploying file system commands.

[21] FIG. 3 illustrates an example procedure in accordance with the present disclosure. It should be understood that the operations of the methods disclosed herein are not presented in any particular order and that performance of some or all of the operations in an alternative order(s) is possible and is contemplated. The operations have been presented in the demonstrated order for ease of description and illustration. Operations may be added, omitted, and/or performed simultaneously, without departing from the scope of the appended claims.

[22] It also should be understood that the illustrated methods can end at any time and need not be performed in their entireties. Some or all operations of the methods, and/or substantially equivalent operations, can be performed by execution of computer-readable instructions included on a computer-storage media, as defined below. The term "computer-readable instructions," and variants thereof, as used in the description and claims, is used expansively herein to include routines, applications, application modules, program modules, programs, components, data structures, algorithms, and the like. Computer-readable instructions can be implemented on various system configurations, including single-processor or multiprocessor systems, minicomputers, mainframe computers, personal computers, hand-held computing devices, microprocessor-based, programmable consumer electronics, combinations thereof, and the like.

[23] Thus, it should be appreciated that the logical operations described herein are implemented (1) as a sequence of computer implemented acts or program modules running on a computing system and/or (2) as interconnected machine logic circuits or circuit modules within

the computing system. The implementation is a matter of choice dependent on the performance and other requirements of the computing system. Accordingly, the logical operations described herein are referred to variously as states, operations, structural devices, acts, or modules. These operations, structural devices, acts, and modules may be implemented in software, in firmware, in special purpose digital logic, and any combination thereof.

[24] For example, the operations of the routine 400 are described herein as being implemented, at least in part, by modules running the features disclosed herein and can be a dynamically linked library (DLL), a statically linked library, functionality produced by an application programing interface (API), a compiled program, an interpreted program, a script or any other executable set of instructions. Data can be stored in a data structure in one or more memory components. Data can be retrieved from the data structure by addressing links or references to the data structure.

[25] Although the following illustration refers to the components of the figures, it can be appreciated that the operations of the routine 400 may be also implemented in many other ways. For example, the routine 400 may be implemented, at least in part, by a processor of another remote computer or a local circuit. In addition, one or more of the operations of the routine 400 may alternatively or additionally be implemented, at least in part, by a chipset working alone or in conjunction with other software modules. In the example described below, one or more modules of a computing system can receive and/or process the data disclosed herein. Any service, circuit or application suitable for providing the techniques disclosed herein can be used in operations described herein.

[26] In an embodiment, a key pair may be generated including a public key that may be used to encrypt the credentials. The user may retain and store the private key. The cloud provider may

use the public key to encrypt credentials and/or commands. The public key may be saved in a secure store at the cloud provider.

[27] In one embodiment, when a client is registered, the public key may be sent to the cloud service provider, and the key pair may be stored in a secure key store. When a task is created by an administrator, for example at a UI, the task and the encrypted password may be sent to the cloud provider. The cloud provider may send the task to the client (e.g., an entity that will execute the task at the user network) along with the encrypted password. The client may obtain the private key using the credentials.

[28] By using this arrangement, the cloud provider does not need to store user information. The cloud provider encrypts commands and passwords and forwards the encrypted information to the clients for decryption and execution. In an embodiment, the same private key may be used by multiple clients (multiple machines). In one embodiment, a temporary password may be used to protect the private key. The encrypted private key may be forwarded to another machine.

[29] The progress of task completion may be provided to the cloud provider who may render a status of the progress on the UI.

[30] The cloud provider may implement a secure store to store the public key, the encrypted login password (encrypted using the public key), and the encrypted user passwords (encrypted using the public key). The client may use a local key store to store the public key and private key.

[31] When any operation is requested for an asset on the user's network, the described authorization process may be triggered. Once authorized, the accessed machine can treat continue to receive and execute commands from the cloud service provider

[32] By way of example, and not limitation, computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or

technology for storage of information such as computer-readable instructions, data structures, program modules or other data. For example, computer storage media includes, but is not limited to, RAM, ROM, EPROM, EEPROM, flash memory or other solid-state memory technology, CD-ROM, digital versatile disks ("DVD"), HD-DVD, BLU-RAY, or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by the client device 226. For purposes of the claims, the phrase "computer storage medium," "computer-readable storage medium," and variations thereof, does not include waves, signals, and/or other transitory and/or intangible communication media, per se.

[33] Turning now to FIGURE 4, aspects of an example data flow 400 are illustrated, depicting an example implementation of the described techniques. for controlling access to data stored in a cloud-based storage service are shown and described below. In an embodiment, a client 410 may be registered by a cloud service provider 430. A symmetric key may be generated 450 and a public key may be used to encrypt the symmetric key. The cloud service provider 430 may send the encrypted symmetric key to the client 410, who may user a private key to decrypt the encrypted symmetric key.

[34] The client 410 may obtain credentials from secure store 420. The service provider may encrypt a task using the symmetric key and add the encrypted task to queue 440. Client 410 may obtain the encrypted task from queue 440 and decrypt the encrypted task. The client 410 may execute the task.

[35] The client 410 may encrypt a report of the completed task using the symmetric key and add the encrypted report to queue 440. The service provider 430 may obtain the encrypted report from queue 440.

[36] Turning now to FIGURE 5, aspects of an example data flow 400 are illustrated, depicting an example implementation of the described techniques. for controlling access to data stored in a cloud-based storage service are shown and described below.

[37] Turning now to FIGURE 5, aspects of a routine 500 for controlling access to data stored in a cloud-based storage service are shown and described below. With reference to FIGURE 5, the routine 500 begins at operation 501 which illustrates receiving, at a cloud-based network, a public key of a public/private key pair and a credential for accessing secrets associated with a user network.

[38] Next, operation 503 illustrates receiving, at the cloud-based network from a user interface configured to facilitate remote control of the user network, a command to be executed at the user network.

[39] Operation 505 illustrates encrypting, by the cloud-based network using the public key, the credential and the command.

[40] Next, operation 507 illustrates forwarding, by the cloud-based network to one or more client devices, the encrypted credential and command. In an embodiment, the client devices are configured to decrypt the encrypted credential and command using a private key of the public/private key pair and execute the command on the user network.

[41] In an embodiment, the client devices include an agent configured to store the private key and decrypt the encrypted credential and command using the private key.

[42] In an embodiment, the cloud-based network receives, from the client devices, a status indicative of a progress of execution of the command.

[43] In an embodiment, the command is a command to migrate one or more virtual machines from the user network to the cloud-based network.

[44] In an embodiment, the credential is usable to access the user network by a plurality of client devices.

[45] In an embodiment, the encrypted credential and command are sent via an HTTPS connection.

[46] In an embodiment, the user network is protected by a firewall.

[47] In an embodiment, the credential is one or more of a username, password, or MFA credential.

[48] In an embodiment, the cloud-based network does not persistently store the credential in an unencrypted form.

[49] In an embodiment, the user interface is configured to enable a remote user to send a command for execution at the user network.

[50] Turning now to FIGURE 6, aspects of a routine 600 for controlling access to a user network are shown and described below. With reference to FIGURE 6, the routine 600 begins at operation 601 where a cloud-based network receives an encrypted credential and command that is encrypted using a public key of a public/private key pair. In an embodiment, the credential is for accessing secrets associated with a user network and the command is to be executed at the user network.

[51] Next, at operation 603, the encrypted credential and command are decrypted using a private key of the public/private key pair.

[52] Operation 605 illustrates accessing the user network using the decrypted credential.

[53] Operation 607 illustrates executing the decrypted command on the user network.

[54] FIGURE 7 shows additional details of an example computer architecture 700 for a computer, such as the computing device 107 (FIGURE 1), capable of executing the program

components described herein. Thus, the computer architecture 700 illustrated in FIGURE 7 illustrates an architecture for a server computer, a mobile phone, a PDA, a smart phone, a desktop computer, a netbook computer, a tablet computer, and/or a laptop computer. The computer architecture 700 may be utilized to execute any aspects of the software components presented herein.

[55] The computer architecture 700 illustrated in FIGURE 7 includes a central processing unit 702 ("CPU"), a system memory 704, including a random access memory 707 ("RAM") and a read-only memory ("ROM") 708, and a system bus 710 that couples the memory 704 to the CPU 702. A basic input/output system containing the basic routines that help to transfer information between elements within the computer architecture 700, such as during startup, is stored in the ROM 708. The computer architecture 700 further includes a mass storage device 712 for storing an operating system 707, other data, and one or more application programs, such as a productivity application 141 and a synchronization application 142.

[56] The mass storage device 712 is connected to the CPU 702 through a mass storage controller (not shown) connected to the bus 710. The mass storage device 712 and its associated computer-readable media provide non-volatile storage for the computer architecture 700. Although the description of computer-readable media contained herein refers to a mass storage device, such as a solid-state drive, a hard disk or CD-ROM drive, it should be appreciated by those skilled in the art that computer-readable media can be any available computer storage media or communication media that can be accessed by the computer architecture 700.

[57] Communication media includes computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any delivery media. The term "modulated data signal" means

a signal that has one or more of its characteristics changed or set in a manner so as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer-readable media.

[58] By way of example, and not limitation, computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules or other data. For example, computer media includes, but is not limited to, RAM, ROM, EPROM, EEPROM, flash memory or other solid-state memory technology, CD-ROM, digital versatile disks ("DVD"), HD-DVD, BLU-RAY, or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by the computer architecture 700. For purposes of the claims, the phrase "computer storage medium," "computer-readable storage medium" and variations thereof, does not include waves, signals, and/or other transitory and/or intangible communication media, per se.

[59] According to various configurations, the computer architecture 700 may operate in a networked environment using logical connections to remote computers through the network 757 and/or another network (not shown). The computer architecture 700 may connect to the network 757 through a network interface unit 714 connected to the bus 710. It should be appreciated that the network interface unit 714 also may be utilized to connect to other types of networks and remote computer systems. The computer architecture 700 also may include an input/output controller 717 for receiving and processing input from a number of other devices, including a

keyboard, mouse, or electronic stylus (not shown in FIGURE 7). Similarly, the input/output controller 717 may provide output to a display screen, a printer, or other type of output device (also not shown in FIGURE 7).

[60] It should be appreciated that the software components described herein may, when loaded into the CPU 702 and executed, transform the CPU 702 and the overall computer architecture 700 from a general-purpose computing system into a special-purpose computing system customized to facilitate the functionality presented herein. The CPU 702 may be constructed from any number of transistors or other discrete circuit elements, which may individually or collectively assume any number of states. More specifically, the CPU 702 may operate as a finite-state machine, in response to executable instructions contained within the software modules disclosed herein. These computer-executable instructions may transform the CPU 702 by specifying how the CPU 702 transitions between states, thereby transforming the transistors or other discrete hardware elements constituting the CPU 702.

[61] Encoding the software modules presented herein also may transform the physical structure of the computer-readable media presented herein. The specific transformation of physical structure may depend on various factors, in different implementations of this description. Examples of such factors may include, but are not limited to, the technology used to implement the computer-readable media, whether the computer-readable media is characterized as primary or secondary storage, and the like. For example, if the computer-readable media is implemented as semiconductor-based memory, the software disclosed herein may be encoded on the computer-readable media by transforming the physical state of the semiconductor memory. For example, the software may transform the state of transistors, capacitors, or other discrete circuit

elements constituting the semiconductor memory. The software also may transform the physical state of such components in order to store data thereupon.

[62] As another example, the computer-readable media disclosed herein may be implemented using magnetic or optical technology. In such implementations, the software presented herein may transform the physical state of magnetic or optical media, when the software is encoded therein. These transformations may include altering the magnetic characteristics of particular locations within given magnetic media. These transformations also may include altering the physical features or characteristics of particular locations within given optical media, to change the optical characteristics of those locations. Other transformations of physical media are possible without departing from the scope and spirit of the present description, with the foregoing examples provided only to facilitate this discussion.

[63] In light of the above, it should be appreciated that many types of physical transformations take place in the computer architecture 700 in order to store and execute the software components presented herein. It also should be appreciated that the computer architecture 700 may include other types of computing devices, including hand-held computers, embedded computer systems, personal digital assistants, and other types of computing devices known to those skilled in the art. It is also contemplated that the computer architecture 700 may not include all of the components shown in FIGURE 7, may include other components that are not explicitly shown in FIGURE 7, or may utilize an architecture completely different than that shown in FIGURE 7.

[64] FIGURE 8 depicts an illustrative distributed computing environment 800 capable of executing the software components described herein. Thus, the distributed computing environment 800 illustrated in FIGURE 8 can be utilized to execute any aspects of the software

components presented herein. For example, the distributed computing environment 800 can be utilized to execute aspects of the software components described herein.

[65] According to various implementations, the distributed computing environment 800 includes a computing environment 802 operating on, in communication with, or as part of the network 804. The network 804 may be or may include the network 959, described above with reference to FIGURE 9. The network 804 also can include various access networks. One or more client devices 806A-806N (hereinafter referred to collectively and/or generically as "clients 806" and also referred to herein as computing devices 86) can communicate with the computing environment 802 via the network 804 and/or other connections (not illustrated in FIGURE 8). In one illustrated configuration, the clients 806 include a computing device 806A such as a laptop computer, a desktop computer, or other computing device; a slate or tablet computing device ("tablet computing device") 806B; a mobile computing device 806C such as a mobile telephone, a smart phone, or other mobile computing device; a server computer 806D; and/or other devices 806N. It should be understood that any number of clients 806 can communicate with the computing environment 802. Two example computing architectures for the clients 806 are illustrated and described herein with reference to FIGURES 9 and 8. It should be understood that the illustrated clients 806 and computing architectures illustrated and described herein are illustrative, and should not be construed as being limiting in any way.

[66] In the illustrated configuration, the computing environment 802 includes application servers 808, data storage 88, and one or more network interfaces 812. According to various implementations, the functionality of the application servers 808 can be provided by one or more server computers that are executing as part of, or in communication with, the network 804. The application servers 808 can host various services, virtual machines, portals, and/or other

resources. In the illustrated configuration, the application servers 808 host one or more virtual machines 814 for hosting applications or other functionality. According to various implementations, the virtual machines 814 host one or more applications and/or software modules for enabling in-application support for topological changes to files during remote synchronization. It should be understood that this configuration is illustrative, and should not be construed as being limiting in any way. The application servers 808 also host or provide access to one or more portals, link pages, Web sites, and/or other information ("Web portals") 816.

[67] According to various implementations, the application servers 808 also include one or more mailbox services 818 and one or more messaging services 820. The mailbox services 818 can include electronic mail ("email") services. The mailbox services 818 also can include various personal information management ("PIM") and presence services including, but not limited to, calendar services, contact management services, collaboration services, and/or other services. The messaging services 820 can include, but are not limited to, instant messaging services, chat services, forum services, and/or other communication services.

[68] The application servers 808 also may include one or more social networking services 822. The social networking services 822 can include various social networking services including, but not limited to, services for sharing or posting status updates, instant messages, links, photos, videos, and/or other information; services for commenting or displaying interest in articles, products, blogs, or other resources; and/or other services. In some configurations, the social networking services 822 are provided by or include the FACEBOOK social networking service, the LINKEDIN professional networking service, the MYSPACE social networking service, the FOURSQUARE geographic networking service, the YAMMER office colleague networking service, and the like. In other configurations, the social networking services 822 are

provided by other services, sites, and/or providers that may or may not be explicitly known as social networking providers. For example, some web sites allow users to interact with one another via email, chat services, and/or other means during various activities and/or contexts such as reading published articles, commenting on goods or services, publishing, collaboration, gaming, and the like. Examples of such services include, but are not limited to, the WINDOWS LIVE service and the XBOX LIVE service from Microsoft Corporation in Redmond, Washington. Other services are possible and are contemplated.

[69] The social networking services 822 also can include commenting, blogging, and/or micro blogging services. Examples of such services include, but are not limited to, the YELP commenting service, the KUDZU review service, the OFFICETALK enterprise micro blogging service, the TWITTER messaging service, the GOOGLE BUZZ service, and/or other services. It should be appreciated that the above lists of services are not exhaustive and that numerous additional and/or alternative social networking services 822 are not mentioned herein for the sake of brevity. As such, the above configurations are illustrative, and should not be construed as being limited in any way. According to various implementations, the social networking services 822 may host one or more applications and/or software modules for providing the functionality described herein, such as enabling in-application support for topological changes to files during remote synchronization. For instance, any one of the application servers 808 may communicate or facilitate the functionality and features described herein. For instance, a social networking application, mail client, messaging client or a browser running on a phone or any other client 806 may communicate with a networking service 822 and facilitate the functionality, even in part, described above with respect to FIGURE 8. Any device or service depicted herein can be used as a resource for supplemental data, including email servers, storage servers, etc.

[70] As shown in FIGURE 8, the application servers 808 also can host other services, applications, portals, and/or other resources ("other resources") 824. The other resources 824 can include, but are not limited to, document sharing, rendering or any other functionality. It thus can be appreciated that the computing environment 802 can provide integration of the concepts and technologies disclosed herein with various mailbox, messaging, social networking, and/or other services or resources.

[71] As mentioned above, the computing environment 802 can include the data storage 88. According to various implementations, the functionality of the data storage 88 is provided by one or more databases operating on, or in communication with, the network 804. The functionality of the data storage 88 also can be provided by one or more server computers configured to host data for the computing environment 802. The data storage 88 can include, host, or provide one or more real or virtual datastores 826A-826N (hereinafter referred to collectively and/or generically as "datastores 826"). The datastores 826 are configured to host data used or created by the application servers 808 and/or other data. Although not illustrated in FIGURE 8, the datastores 826 also can host or store web page documents, word documents, presentation documents, data structures, algorithms for execution by a recommendation engine, and/or other data utilized by any application program or another module. Aspects of the datastores 826 may be associated with a service for storing files.

[72] The computing environment 802 can communicate with, or be accessed by, the network interfaces 812. The network interfaces 812 can include various types of network hardware and software for supporting communications between two or more computing devices including, but not limited to, the computing devices and the servers. It should be appreciated that the network

interfaces 812 also may be utilized to connect to other types of networks and/or computer systems.

[73] It should be understood that the distributed computing environment 800 described herein can provide any aspects of the software elements described herein with any number of virtual computing resources and/or other distributed computing functionality that can be configured to execute any aspects of the software components disclosed herein. According to various implementations of the concepts and technologies disclosed herein, the distributed computing environment 800 provides the software functionality described herein as a service to the computing devices. It should be understood that the computing devices can include real or virtual machines including, but not limited to, server computers, web servers, personal computers, mobile computing devices, smart phones, and/or other devices. As such, various configurations of the concepts and technologies disclosed herein enable any device configured to access the distributed computing environment 800 to utilize the functionality described herein for providing the techniques disclosed herein, among other aspects. In one specific example, as summarized above, techniques described herein may be implemented, at least in part, by a web browser application, which works in conjunction with the application servers 808 of FIGURE 8.

CLAIMS

What is claimed is:

1. A method for accessing to computing resources, the method comprising:

receiving, at a cloud-based network, a public key of a public/private key pair and a credential for accessing secrets associated with a user network;

receiving, at the cloud-based network from a user interface configured to facilitate remote control of the user network, a command to be executed at the user network;

encrypting, by the cloud-based network using the public key, the credential and the command; and

forwarding, by the cloud-based network to one or more client devices, the encrypted credential and command, wherein the client devices are configured to decrypt the encrypted credential and command using a private key of the public/private key pair and execute the command on the user network.

2. The method of claim 1, wherein the client devices include an agent configured to store the private key and decrypt the encrypted credential and command using the private key.

3. The method of claim 1, further comprising receiving, by the cloud-based network from the client devices, a status indicative of a progress of execution of the command.

4. The method of claim 1, wherein the command is a command to migrate one or more virtual machines from the user network to the cloud-based network.

5. The method of claim 1, wherein the credential is usable to access the user network by a plurality of client devices.

6. The method of claim 1, wherein the encrypted credential and command are sent via an HTTPS connection.

7. The method of claim 1, wherein the user network is protected by a firewall.

8. The method of claim 1, wherein the credential is one or more of a username, password, or MFA credential.

9. The method of claim 1, wherein the cloud-based network does not persistently store the credential.

10. The method of claim 1, wherein the user interface is configured to enable a remote user to send a command for execution at the user network.

11. A system for accessing a user network, the system comprising:

one or more data processing units; and

a computer-readable medium having encoded thereon computer-executable instructions to cause the one or more data processing units to perform operations comprising:

receive, from a cloud-based network, an encrypted credential and command that is encrypted using a public key of a public/private key pair, wherein the credential is for accessing secrets associated with a user network and the command is to be executed at the user network;

decrypt the encrypted credential and command using a private key of the public/private key pair;

access the user network using the decrypted credential; and

execute the decrypted command on the user network.

12. The system of claim 11, wherein the credential and command is entered from a user interface configured to facilitate remote control of the user network.

13. The system of claim 11, further comprising installing an agent configured to store the private key and decrypt the encrypted credential and command using the private key.

14. The system of claim 11, further comprising sending a status indicative of a progress of execution of the command.

15. The system of claim 11, wherein the credential is usable to access the user network by a plurality of client devices.

16. The system of claim 11, wherein the encrypted credential and command are received via an HTTPS connection.

17. The system of claim 11, wherein the credential is one or more of a username, password, or MFA credential.

18. The system of claim 11, wherein the private key is stored in a key store on the system.

19. A computing device comprising:

one or more data processing units; and

a computer-readable medium having encoded thereon computer-executable instructions to cause the one or more data processing units to perform operations comprising:

receiving, at a cloud-based network, a public key of a public/private key pair and a credential for accessing secrets associated with a user network;

receiving, at the cloud-based network from a user interface configured to facilitate remote control of the user network, a command to be executed at the user network;

encrypting, by the cloud-based network using the public key, the credential and the command; and

forwarding, by the cloud-based network to one or more client devices, the encrypted credential and command, wherein the client devices are configured to decrypt the encrypted credential and command using a private key of the public/private key pair and execute the command on the user network.

20. The computing device of claim 19, wherein the client devices include an agent configured to store the private key and decrypt the encrypted credential and command using the private key.

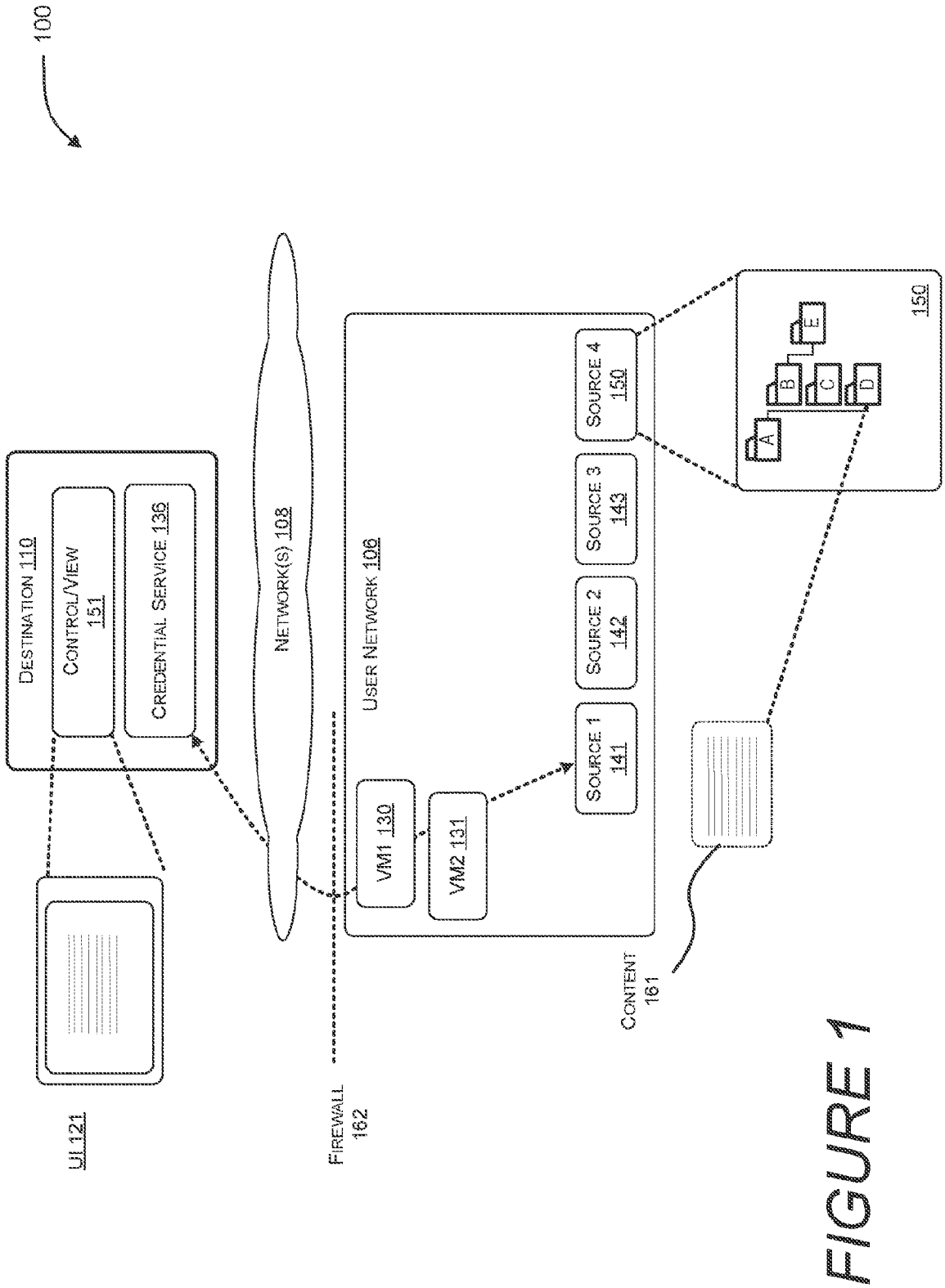
100
DESTINATION 110
CONTROL/VIEW 151
CREDENTIAL SERVICE 136
NETWORK(S) 108
USER NETWORK 106
VM1 130
VM2 131
SOURCE 1 141
SOURCE 2 142
SOURCE 3 143
SOURCE 4 150
150
A
B
C
D
E
CONTENT 161
UI 121
FIREWALL 162

FIGURE 1

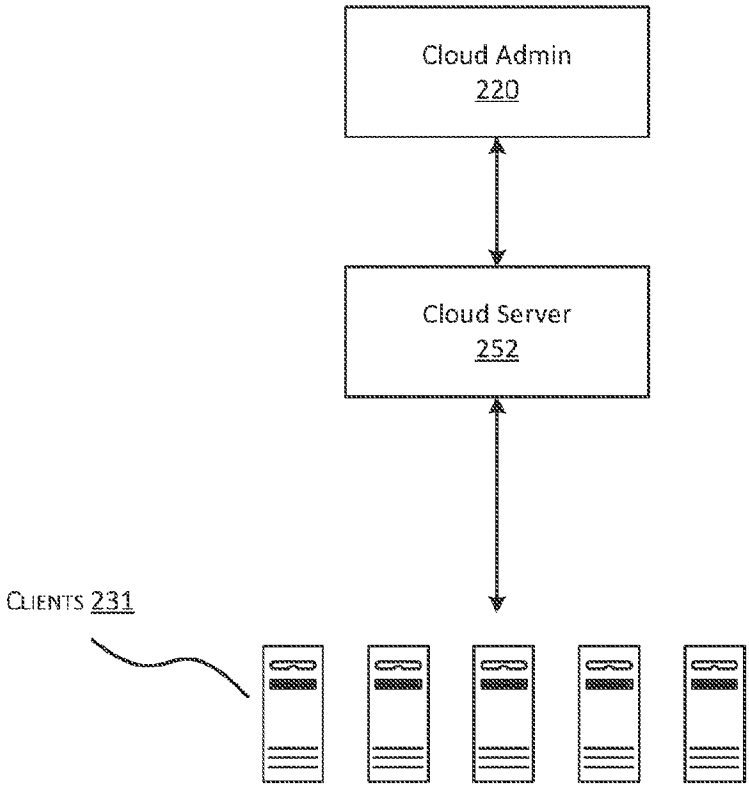

FIG. 2

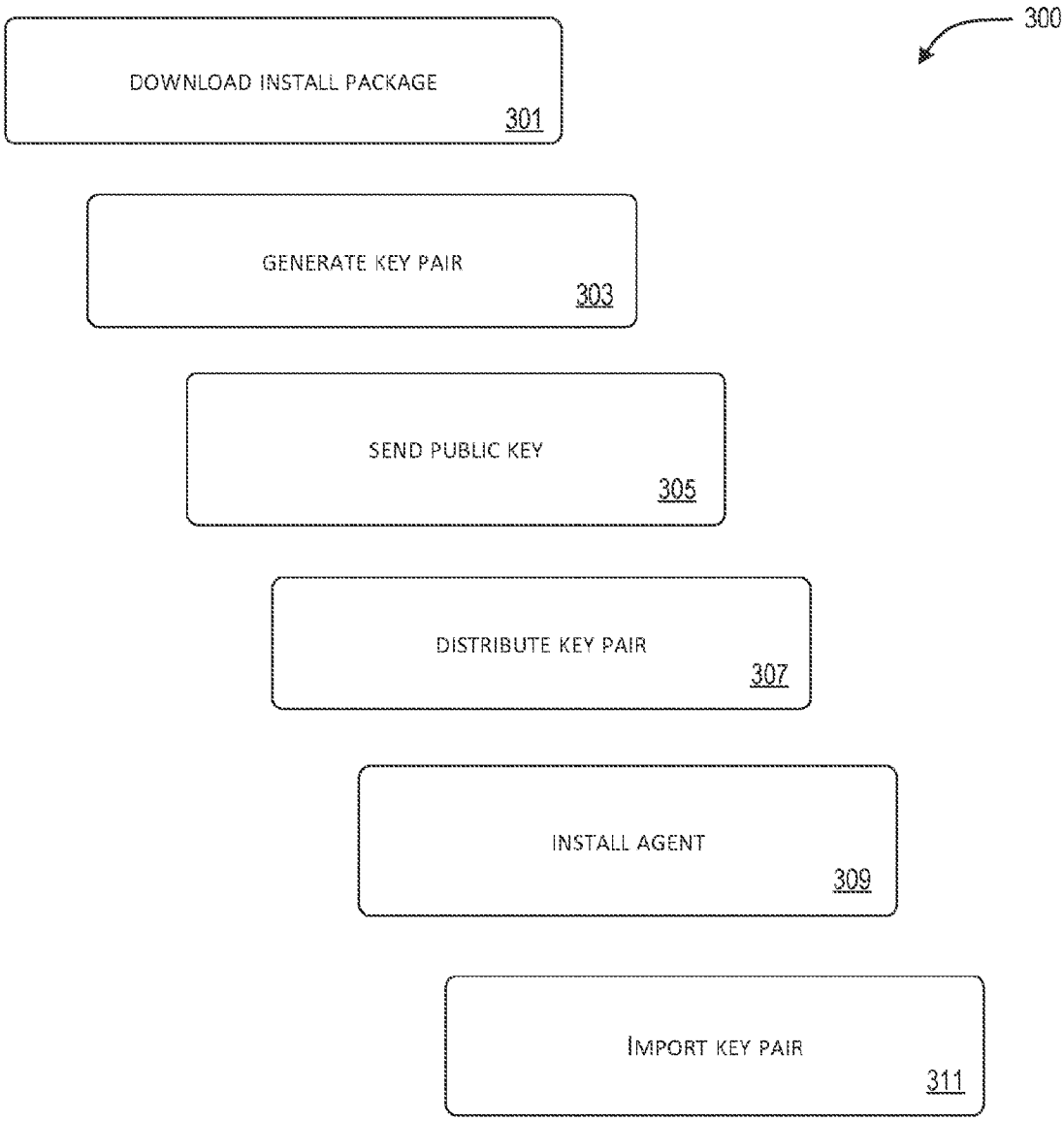
300
DOWNLOAD INSTALL PACKAGE
301
GENERATE KEY PAIR
303
SEND PUBLIC KEY
305
DISTRIBUTE KEY PAIR
307
INSTALL AGENT
309
IMPORT KEY PAIR
311

FIGURE 3

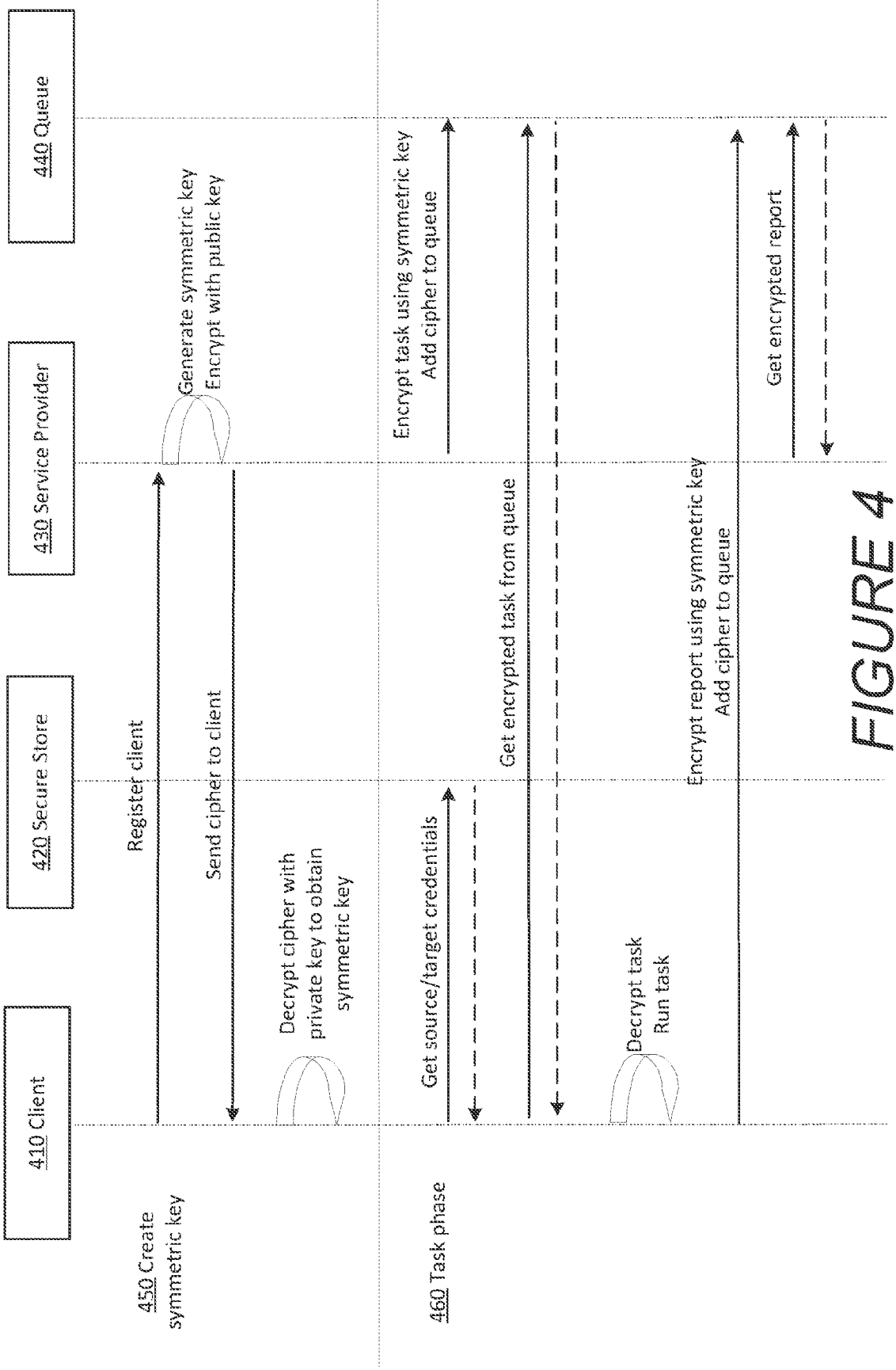
410 Client
420 Secure Store
430 Service Provider
440 Queue
450 Create symmetric key
Register client
Generate symmetric key
Encrypt with public key
Send cipher to client
Decrypt cipher with private key to obtain symmetric key
460 Task phase
Encrypt task using symmetric key
Add cipher to queue
Get source/target credentials
Get encrypted task from queue
Decrypt task
Run task
Encrypt report using symmetric key
Add cipher to queue
Get encrypted report

FIGURE 4

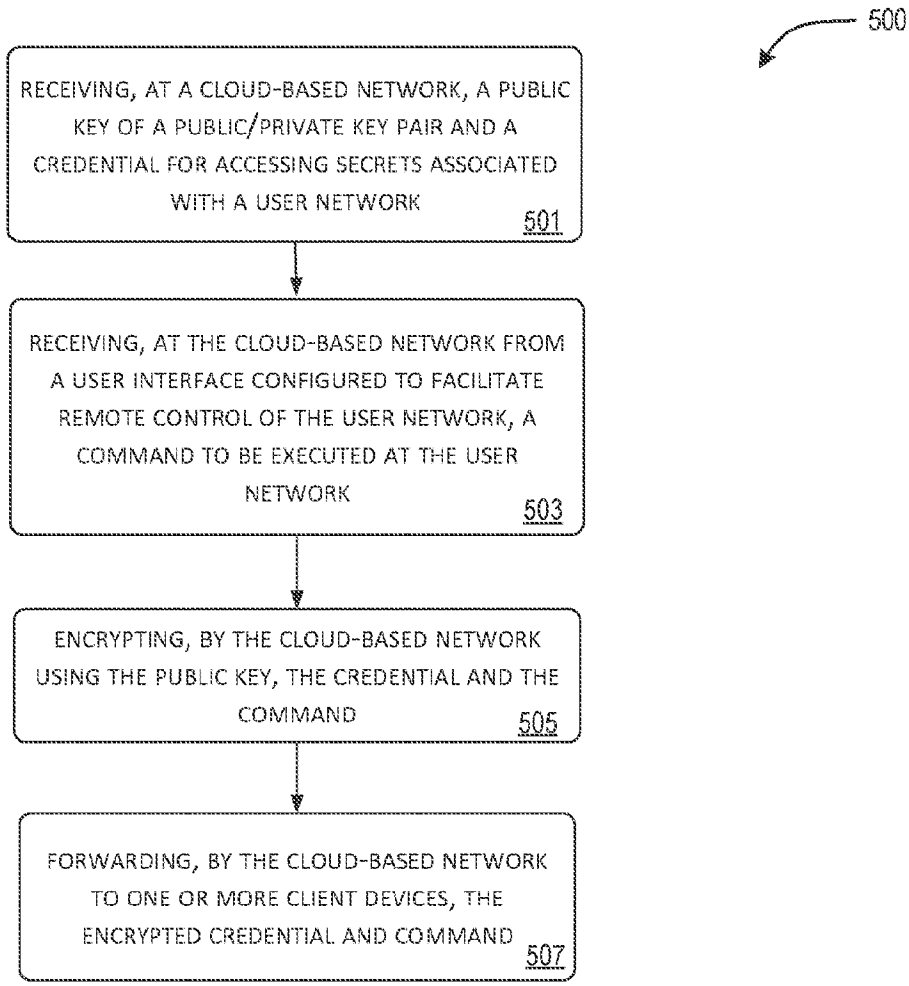
500
RECEIVING, AT A CLOUD-BASED NETWORK, A PUBLIC KEY OF A PUBLIC/PRIVATE KEY PAIR AND A CREDENTIAL FOR ACCESSING SECRETS ASSOCIATED WITH A USER NETWORK
501
RECEIVING, AT THE CLOUD-BASED NETWORK FROM A USER INTERFACE CONFIGURED TO FACILITATE REMOTE CONTROL OF THE USER NETWORK, A COMMAND TO BE EXECUTED AT THE USER NETWORK
503
ENCRYPTING, BY THE CLOUD-BASED NETWORK USING THE PUBLIC KEY, THE CREDENTIAL AND THE COMMAND
505
FORWARDING, BY THE CLOUD-BASED NETWORK TO ONE OR MORE CLIENT DEVICES, THE ENCRYPTED CREDENTIAL AND COMMAND
507

FIGURE 5

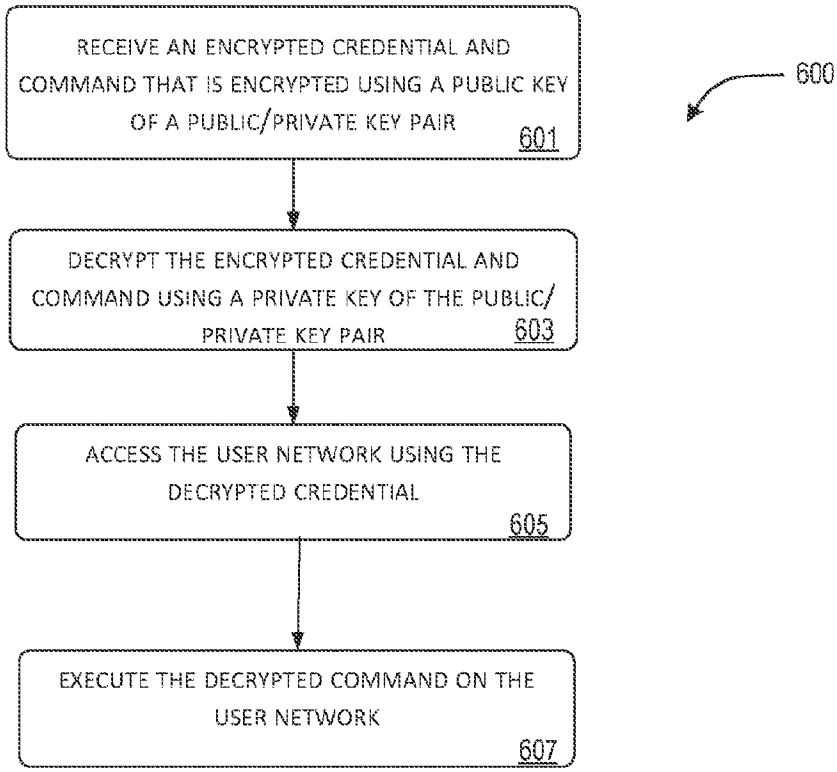
RECEIVE AN ENCRYPTED CREDENTIAL AND COMMAND THAT IS ENCRYPTED USING A PUBLIC KEY OF A PUBLIC/PRIVATE KEY PAIR
601
600
DECRYPT THE ENCRYPTED CREDENTIAL AND COMMAND USING A PRIVATE KEY OF THE PUBLIC/PRIVATE KEY PAIR
603
ACCESS THE USER NETWORK USING THE DECRYPTED CREDENTIAL
605
EXECUTE THE DECRYPTED COMMAND ON THE USER NETWORK
607

FIGURE 6

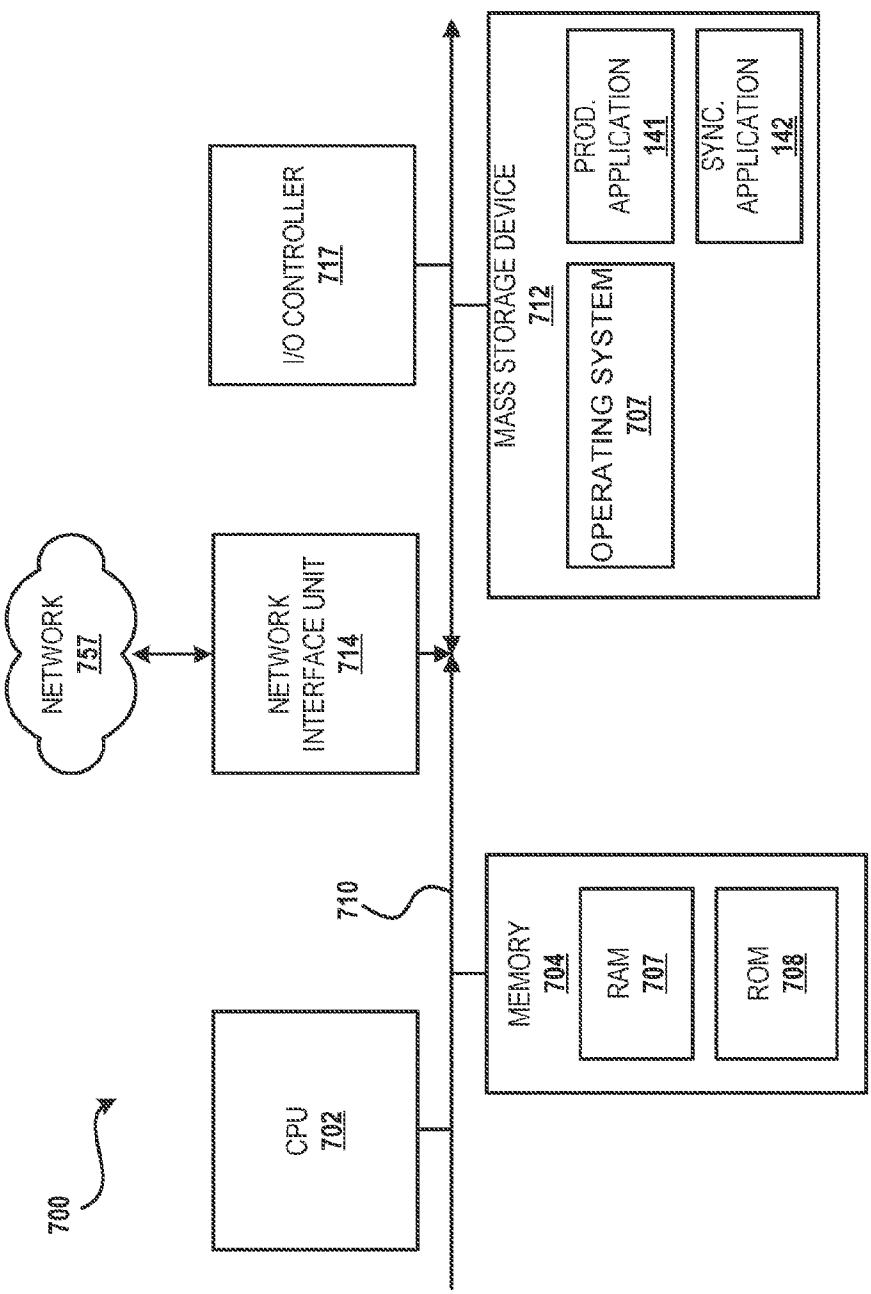
700
CPU
702
710
MEMORY
704
RAM
707
ROM
708
NETWORK
INTERFACE UNIT
714
NETWORK
757
I/O CONTROLLER
717
MASS STORAGE DEVICE
712
OPERATING SYSTEM
707
PROD.
APPLICATION
141
SYNC.
APPLICATION
142

FIGURE 7

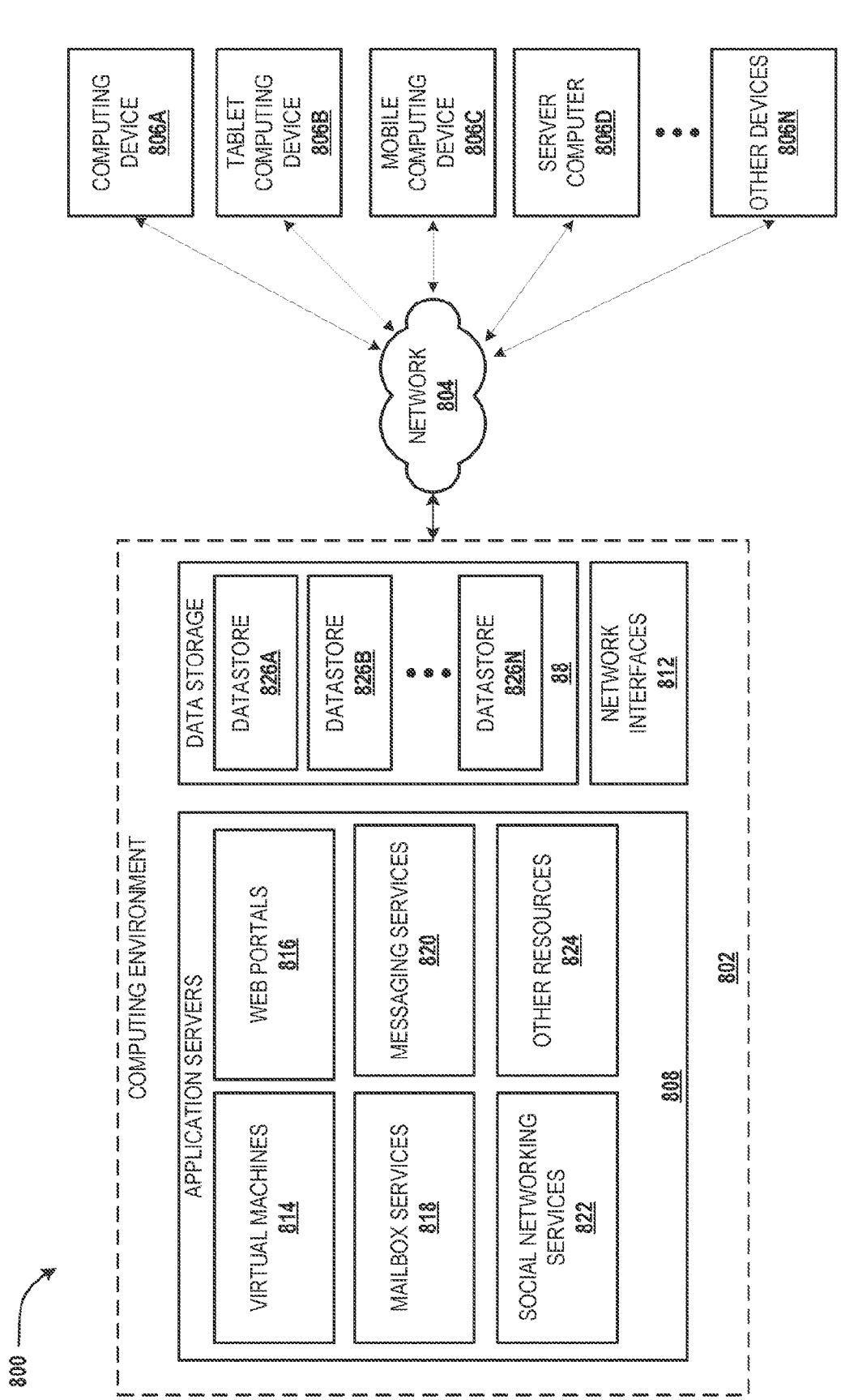
800
COMPUTING ENVIRONMENT
APPLICATION SERVERS
VIRTUAL MACHINES 814
WEB PORTALS 816
MAILBOX SERVICES 818
MESSAGING SERVICES 820
SOCIAL NETWORKING SERVICES 822
OTHER RESOURCES 824
808
DATA STORAGE
DATASTORE 826A
DATASTORE 826B
DATASTORE 826N
88
NETWORK INTERFACES 812
802
NETWORK 804
COMPUTING DEVICE 806A
TABLET COMPUTING DEVICE 806B
MOBILE COMPUTING DEVICE 806C
SERVER COMPUTER 806D
OTHER DEVICES 806N

FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/106112

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)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)

H04L, G06F

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

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

CNPAT,CNKI,WPI,EPODOC,IEEE: cloud, public key, private key, credential, command, execute, encrypt, decrypt, client, migrate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014059541 A1 (INTERNATIONAL BUSINESS MACHINES CORP.) 27 February 2014 (2014-02-27) description, paragraphs [0034]-[0036], [0057]-[0071], and claims 1-10	1-20
A	WO 2018102692 A1 (CARRIER CORP.) 07 June 2018 (2018-06-07) the whole document	1-20
A	CN 107465689 A (DATANG GAOHONG XIN'AN ZHEJIANG INFORMATION TECHNOLOGY CO., LTD.) 12 December 2017 (2017-12-12) the whole document	1-20
A	CN 102986190 A (INTERNATIONAL BUSINESS MACHINES CORP.) 20 March 2013 (2013-03-20) the whole document	1-20

☐ 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	Date of mailing of the international search report
02 June 2020	**16 June 2020**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China**	Authorized officer **SUN,Guohui**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(10)-53961538**

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/106112

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2014059541	A1	27 February 2014	CN	103631638	A	12 March 2014
WO	2018102692	A1	07 June 2018	CN	110036385	A	19 July 2019
CN	107465689	A	12 December 2017		None		
CN	102986190	A	20 March 2013	DE	112011101729	T5	02 May 2013
				WO	2012004185	A1	12 January 2012
				GB	2494834	A	20 March 2013
				US	2012011578	A1	12 January 2012