IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR UNITED STATES PATENT

SYSTEM AND METHOD FOR CONTROLLING DATA USING CONTAINERS

Inventor(s):

Alan Rodriguez – Dallas, Texas

Attorneys:
Munck Wilson Mandala, L.L.P.
600 Banner Place Tower
12770 Coit Road
Dallas, Texas 75251
(972) 628-3600

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

SYSTEM AND METHOD FOR CONTROLLING DATA USING CONTAINERS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Application No. 63/126,580, filed December 17, 2020, entitled SYSTEM AND METHOD FOR CONTROLLING DATA USING CONTAINERS, the entire contents of which are herein incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates generally to data security methods. More specifically, this disclosure relates to systems and methods for controlling data using containers.

BACKGROUND

[0003] The principles of "notice and choice" have been the key principles of information privacy protection for several decades. These principles of privacy that involve the notion of individual control require sufficient mechanisms for individuals to understand where, when and under what conditions their personal information may be used and transferred and to exercise control over data usage and transference. Therefore, the various sets of fair information practice principles and privacy laws based on these practices include requirements for providing notice about data practices and allowing individuals to exercise control over those practices. Privacy policies, terms of use, and preference center based opt-out mechanisms have become the predominant tools for notice and choice. However, these tools are increasingly insufficient. Serious threats follow from the ease of information storage, transfer, aggregation, analysis and inference. We face the real risk that the technological laws spelled out by Gordon Moore (growth in processing power) and Robert Metcalfe (network effects) will permanently overwhelm existing privacy principles of notice and choice. Privacy policies are long, complicated, inconsistently structured and subject to frequent and unannounced change. Digital services often involve interactions and data exchanges that include third parties unknown to the end user. Each digital service requires specific and tailored advertising preferences selections and can change these choices and associated user selections at any time. In this environment, it is nearly impossible for individuals to control their information usage or related third-party data flows via existing privacy policies and preference center based opt-out mechanism tools for notice and choice.

[0004] The inherently decentralized nature of the internet, being comprised of a multitude of digital services each with its own - advertising preference choices and privacy policies, does not permit acceptable transparency for individuals to understand where, when and under what conditions their personal information may be used and transferred or to exercise control over data usage and transference or to hold digital services and their third party partners accountable for unanticipated and unapproved data usage.

SUMMARY

[0005] This disclosure is directed to systems and methods for controlling data using containers.

[0006] In one aspect, the disclosure is directed to a computing apparatus having at least one microprocessor and memory storing instructions configured to instruct the at least one microprocessor to perform operations. The operations comprise a central user preference center that is configured to store at least one privacy and marketing preference dataset of a user in association with account information identifying an account of the user. The central user preference center is configured to publish at least one privacy and marketing preference dataset of a user to the at least one entity preference center, and the at least one entity preference center is configured to communicate the user's entity preference center privacy and marketing preference dataset to the central preference center.

[0007] In another aspect, the disclosure is also directed to a computer-implemented method. The method comprises storing, in a computing apparatus, data representing a privacy and marketing preferences dataset of a user. It further comprises the step of communicating, by the computing apparatus, the privacy and marketing preferences dataset of the user to an entity in response to an interaction between the user and the computing apparatus or the entity, where the entity stores data about the user and the privacy and marketing preferences dataset controls storage and usage of the data about the user. The method further comprises the step of providing, by the computing apparatus, a communication channel between the user and the entity to customize the privacy and marketing preferences dataset of the user for the data about the user stored by the entity.

[0008] In another aspect, a system for controlling data using containers includes at least one memory, and at least one processor. The system further includes a master data fabric executed by the at least one processor. The master data fabric is configured to manage data container creation and encryption, and store, in the at least one memory, data relating to user data, including data containers, at least one container registry, and data traceability and versioning information. The system further includes a master data controller executed by the at least one processor to manage a master data preference center. The master data controller, using the master data fabric, manages data access requests from container controllers stored on client devices to decrypt and access containers stored in the at least one memory, and sharing of the data containers. The master data controller further determines, using the master data fabric and preferences stored in the data containers, whether to grant or deny access requests based on at least one of requester identity, data or time restrictions, and sharing permissions defining how data in the data container can be shared.

[0009] In another aspect, an electronic device for managing secured data containers includes at least one network interface, at least one memory storing executable instructions, and at least one processor coupled to the at least one network interface and the at least one memory. The at least one processor is configured to and/or execution of the executable instructions by the at least one processor causes the electronic device to receive, via the network interface, a request for data container creation from another electronic device, retrieve data related to the request for data container creation, retrieve one or more parameters constraining use of the data, encrypt the data using a public encryption key, encode the encrypted data into a data storage area of a data container, encode the one or more parameters constraining use of the data into a machine readable parameter storage area of the data container, assign a Universal Unique Identifier (UUID) to the data container, and register the data container in a data container registry based on the UUID of the data container, wherein the data container registry provides for linking and versioning of the data container.

[0010] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to transmit, using the network interface, the data container to a remote device for caching.

[0011] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to receive updated data associated with data stored in a first data container, retrieve at least one parameter constraining use of the updated data, encode the updated data into a second data container, encode the at least one parameter constraining use of the updated data into the second data container, assign a UUID to the second data container, encrypt the second data container, register the second data container in the data container registry based on the UUID of the second data container, and disable a UUID of the first data container in the data container registry, wherein disabling the UUID of the first data container restricts access to the first data container.

[0012] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to transmit a deletion request to the edge node device to delete a cached version of the first data container and store a cached version of the second data container.

[0013] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to receive a deletion request from the other electronic device to delete the data container, delete the data container in response to the request to delete the data container, log the deletion of the data container in an audit log, and disable the UUID of the data container in the data container registry, wherein disabling the UUID of the data container restricts access to the data container by any other devices which still storing the data container.

[0014] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to receive an access request related to data in the data container, determine whether to grant or deny the access request based on the one or more parameters constraining use of the data stored in the data container and based on at least one of a requester identity, temporal parameters, location parameters, functional parameters, proxy parameters, tracking parameters, aggregation parameters, and duration parameters, and log a result of the access request in an audit log.

[0015] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to, when the access request is granted, transmit a communication to allowing decryption of the data container, wherein a private decryption key used for the decryption of the data container is provided by the electronic device, or wherein the private decryption key used for the decryption of the data container is not accessible by the electronic device.

[0016] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to provide, in response to allowing the access request, one or more obfuscated results without providing any of the data from the data container.

[0017] In another embodiment, execution of the executable instructions by the at least one processor further causes the electronic device to create a record associated with the data container in a graph database accessible by the electronic device, wherein the graph database defines relationships between the data container and one or more other data containers and defines access permissions to the data container in accordance with the one or more parameters constraining use of the data.

[0018] In another aspect, a method for managing secured data containers includes receiving a request for data container creation from another electronic device, retrieving data related to the request for data container creation, retrieving one or more parameters constraining use of the data, encrypting the data using a public encryption key, encoding the encrypted data into a data storage area of a data container, encoding the one or more parameters constraining use of the data into a machine readable parameter storage area of the data container, assigning a Universal Unique Identifier (UUID) to the data container, and registering the data container in a data container registry based on the UUID of the data container, wherein the data container registry provides for linking and versioning of the data container.

[0019] In another embodiment, the method further comprises transmitting the data container to a remote device for caching.

[0020] In another embodiment, the method further comprises receiving updated data associated with data stored in a first data container, retrieving at least one parameter constraining use of the updated data, encoding the updated data into a second data container, encoding the at least one parameter constraining use of the updated data into the second data container, assigning a UUID to the second data container, encrypting the second data container, registering the second data container in the data container registry based on the UUID of the second data container, and disabling a UUID of the first data container in the data container registry, wherein disabling the UUID of the first data container restricts access to the first data container.

[0021] In another embodiment, the method further comprises transmitting a deletion request to the edge node device to delete a cached version of the first data container and store a cached version of the second data container.

[0022] In another embodiment, the method further comprises receiving a deletion request from the other electronic device to delete the data container, deleting the data container in response to the request to delete the data container, logging the deletion of the data container in an audit log, and disabling the UUID of the data container in the data container registry, wherein disabling the UUID of the data container restricts access to the data container by any other devices which still storing the data container.

[0023] In another embodiment, the method further comprises receiving an access request related to data in the data container, determining whether to grant or deny the access request based on the one or more parameters constraining use of the data stored in the data container and based on at least one of a requester identity, temporal parameters, location parameters, functional parameters, proxy parameters, tracking parameters, aggregation parameters, and duration parameters, and logging a result of the access request in an audit log.

[0024] In another embodiment, the method further comprises, when the access request is granted, transmitting a communication to allowing decryption of the data container, wherein a private decryption key used for the decryption of the data container is provided by the electronic device, or wherein the private decryption key used for the decryption of the data container is not accessible by the electronic device.

[0025] In another embodiment, the method further comprises providing, in response to allowing the access request, one or more obfuscated results without providing any of the data from the data container.

[0026] In another embodiment, the method further comprises creating a record associated with the data container in a graph database accessible by the electronic device, wherein the graph database defines relationships between the data container and one or more other data containers and defines access permissions to the data container in accordance with the one or more parameters constraining use of the data.

[0027] In another aspect, an electronic device for managing access to secured data containers includes at least one network interface, at least one memory storing executable instructions, and at least one processor coupled to the at least one network interface and the at least one memory, wherein the electronic device is disposed in an edge node at a network edge, and wherein the at least one processor is configured to and/or execution of the executable instructions by the at least one processor causes the electronic device to receive, via the network interface, a request for data container creation from another electronic device, receive, via the at least one network interface, data related to the request for data container creation, generate a command including the request for container creation and the received data, transmit, via the at least one network interface, the command to a master node, receive a transmission from the master node including a data container and a Universal Unique Identifier (UUID) associated with the data container, wherein data in the data container is encrypted, and wherein the data container includes the received data encoded into a data storage area of the data container and one or more parameters constraining use of the data encoded into a machine readable parameter storage area of the data container, cache the data container in association with the UUID in a container cache disposed at the edge node, receive, from a requesting electronic device, an access request related to data in the cached data container, determine whether to grant or deny the access request based on the one or more parameters constraining use of the data stored in the data container and based on at least one of a requester identity, temporal parameters, location parameters, functional parameters, proxy parameters, tracking parameters, aggregation parameters, and duration parameters, log a result of the access request in an audit log, retrieve, based on granting the access request, the data container from the container cache by referencing the UUID of the data container, transmit the data container to the requesting electronic device, receive a deletion request from the other electronic device to delete the data container, delete the data container in response to the request to delete the data container, log the deletion of the data container in an audit log, and transmit, to the master node, a command to disable the UUID of the data container in a data container registry, wherein disabling the UUID of the data container restricts access to the data container by any other devices still storing the data container.

[0028] In one embodiment, the deletion request includes updated data, and wherein execution of the executable instructions by the at least one processor further causes the electronic device to receive the updated data, wherein the updated data is associated with data stored in the data container, retrieve at least one parameter constraining use of the updated data, transmit the updated data and the at least one parameter to the master node, receive, from the master node, a transmission including an updated data container and an associated UUID, wherein the updated data container includes the updated data and the at least one parameter constraining use of the updated data encoded into the second data container, and wherein data in the updated data container is encrypted, and cache the updated data container in the container cache.

[0029] Other technical features may be readily apparent to one skilled in the art from the following figures, descriptions, and claims.

[0030] Before undertaking the DETAILED DESCRIPTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent document. The terms "transmit," "receive," and "communicate," as well as derivatives thereof, encompass both direct and indirect communication. The terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation. The term "or" is inclusive, meaning and/or. The phrase "associated with," as well as derivatives thereof, means to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, have a relationship to or with, or the like.

[0031] Moreover, various functions described below can be implemented or supported by one or more computer programs, each of which is formed from computer readable program code and embodied in a computer readable medium. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures, functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer readable program code. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable memory device.

[0032] As used here, terms and phrases such as "have," "may have," "include," or "may include" a feature (like a number, function, operation, or component such as a part) indicate the existence of the feature and do not exclude the existence of other features. Also, as used here, the phrases “A or B,” “at least one of A and/or B,” or “one or more of A and/or B” may include all possible combinations of A and B. For example, “A or B,” “at least one of A and B,” and “at least one of A or B” may indicate all of (1) including at least one A, (2) including at least one B, or (3) including at least one A and at least one B. Further, as used here, the terms “first” and “second” may modify various components regardless of importance and do not limit the components. These terms are only used to distinguish one component from another. For example, a first user device and a second user device may indicate different user devices from each other, regardless of the order or importance of the devices. A first component may be denoted a second component and vice versa without departing from the scope of this disclosure.

[0033] It will be understood that, when an element (such as a first element) is referred to as being (operatively or communicatively) “coupled with/to” or “connected with/to” another element (such as a second element), it can be coupled or connected with/to the other element directly or via a third element. In contrast, it will be understood that, when an element (such as a first element) is referred to as being “directly coupled with/to” or “directly connected with/to” another element (such as a second element), no other element (such as a third element) intervenes between the element and the other element.

[0034] As used here, the phrase “configured (or set) to” may be interchangeably used with the phrases “suitable for,” “having the capacity to,” “designed to,” “adapted to,” “made to,” or “capable of” depending on the circumstances. The phrase “configured (or set) to” does not essentially mean “specifically designed in hardware to.” Rather, the phrase “configured to” may mean that a device can perform an operation together with another device or parts. For example, the phrase “processor configured (or set) to perform A, B, and C” may mean a generic-purpose processor (such as a CPU or application processor) that may perform the operations by executing one or more software programs stored in a memory device or a dedicated processor (such as an embedded processor) for performing the operations.

[0035] The terms and phrases as used here are provided merely to describe some embodiments of this disclosure but not to limit the scope of other embodiments of this disclosure. It is to be understood that the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise. All terms and phrases, including technical and scientific terms and phrases, used here have the same meanings as commonly understood by one of ordinary skill in the art to which the embodiments of this disclosure belong. It will be further understood that terms and phrases, such as those defined in commonly-used dictionaries, should be interpreted as having a meaning that is consistent with their meaning in the context of the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined here. In some cases, the terms and phrases defined here may be interpreted to exclude embodiments of this disclosure.

[0036] Examples of an “electronic device” according to embodiments of this disclosure may include at least one of a smartphone, a tablet personal computer (PC), a mobile phone, a video phone, an e-book reader, a desktop PC, a laptop computer, a netbook computer, a workstation, a personal digital assistant (PDA), a portable multimedia player (PMP), an MP3 player, a mobile medical device, a camera, or a wearable device (such as smart glasses, a head-mounted device (HMD), electronic clothes, an electronic bracelet, an electronic necklace, an electronic accessory, an electronic tattoo, a smart mirror, or a smart watch). Other examples of an electronic device include a smart home appliance. Examples of the smart home appliance may include at least one of a television, a digital video disc (DVD) player, an audio player, a refrigerator, an air conditioner, a cleaner, an oven, a microwave oven, a washer, a drier, an air cleaner, a set-top box, a home automation control panel, a security control panel, a TV box (such as SAMSUNG HOMESYNC, APPLETV, or GOOGLE TV), a smart speaker or speaker with an integrated digital assistant (such as SAMSUNG GALAXY HOME, APPLE HOMEPOD, or AMAZON ECHO), a gaming console (such as an XBOX, PLAYSTATION, or NINTENDO), an electronic dictionary, an electronic key, a camcorder, or an electronic picture frame. Still other examples of an electronic device include at least one of various medical devices (such as diverse portable medical measuring devices (like a blood sugar measuring device, a heartbeat measuring device, or a body temperature measuring device), a magnetic resource angiography (MRA) device, a magnetic resource imaging (MRI) device, a computed tomography (CT) device, an imaging device, or an ultrasonic device), a navigation device, a global positioning system (GPS) receiver, an event data recorder (EDR), a flight data recorder (FDR), an automotive infotainment device, a sailing electronic device (such as a sailing navigation device or a gyro compass), avionics, security devices, vehicular head units, industrial or home robots, automatic teller machines (ATMs), point of sales (POS) devices, or Internet of Things (IoT) devices (such as a bulb, various sensors, electric or gas meter, sprinkler, fire alarm, thermostat, street light, toaster, fitness equipment, hot water tank, heater, or boiler). Other examples of an electronic device include at least one part of a piece of furniture or building/structure, an electronic board, an electronic signature receiving device, a projector, or various measurement devices (such as devices for measuring water, electricity, gas, or electromagnetic waves). Note that, according to various embodiments of this disclosure, an electronic device may be one or a combination of the above-listed devices. According to some embodiments of this disclosure, the electronic device may be a flexible electronic device. The electronic device disclosed here is not limited to the above-listed devices and may include new electronic devices depending on the development of technology.

[0037] In the following description, electronic devices are described with reference to the accompanying drawings, according to various embodiments of this disclosure. As used here, the term “user” may denote a human or another device (such as an artificial intelligent electronic device) using the electronic device.

[0038] Definitions for other certain words and phrases may be provided throughout this patent document. Those of ordinary skill in the art should understand that in many if not most instances, such definitions apply to prior as well as future uses of such defined words and phrases.

[0039] None of the description in this application should be read as implying that any particular element, step, or function is an essential element that must be included in the claim scope. The scope of patented subject matter is defined only by the claims. Moreover, none of the claims is intended to invoke 35 U.S.C. § 112(f) unless the exact words “means for” are followed by a participle. Use of any other term, including without limitation “mechanism,” “module,” “device,” “unit,” “component,” “element,” “member,” “apparatus,” “machine,” “system,” “processor,” or “controller,” within a claim is understood by the Applicant to refer to structures known to those skilled in the relevant art and is not intended to invoke 35 U.S.C. § 112(f).

BRIEF DESCRIPTION OF THE DRAWINGS

[0040] For a more complete understanding, reference is now made to the following description taken in conjunction with the accompanying Drawings in which:

[0041] FIGURE 1 illustrates a system to communicating privacy preferences in accordance with various embodiments of this disclosure;

[0042] FIGURE 2 illustrates a block diagram of an illustrative electronic device for user management of personal privacy and marketing data in accordance with various embodiments of this disclosure;

[0043] FIGURE 3 illustrates a block diagram of an illustrative but not limiting electronic device for communicating personal privacy and marketing preferences in accordance with various embodiments of this disclosure;

[0044] FIGURE 4 illustrates a method of managing personal privacy and marketing data in accordance with various embodiments of this disclosure;

[0045] FIGURE 5 illustrates a method of managing personal privacy and marketing data in accordance with various embodiments of this disclosure;

[0046] FIGURE 6A illustrates a data control architecture in accordance with various embodiments of this disclosure;

[0047] FIGURE 6B illustrates a diagram of a stack including programmatic data in accordance with various embodiments of this disclosure;

[0048] FIGURE 7 illustrates a container access and control architecture in accordance with various embodiments of this disclosure;

[0049] FIGURES 8A-8C illustrate a data access parameters creation process in accordance with various embodiments of this disclosure;

[0050] FIGURE 9 illustrates an edge computing architecture in accordance with the various embodiments of this disclosure;

[0051] FIGURE 10 illustrates an edge environment container control process in accordance with various embodiments of this disclosure;

[0052] FIGURE 11A illustrates a data container request and caching process in accordance with various embodiments of this disclosure;

[0053] FIGURE 11B illustrates a cached data container request process in accordance with various embodiments of this disclosure;

[0054] FIGURE 12 illustrates a service registration process in accordance with various embodiments of this disclosure;

[0055] FIGURE 13 illustrates an authentication process in accordance with various embodiments of this disclosure;

[0056] FIGURES 14A and 14B illustrate a data access and control process in accordance with various embodiments of this disclosure;

[0057] FIGURE 15 illustrates a data container creation process in accordance with various embodiments of this disclosure;

[0058] FIGURE 16 illustrates a data container update process in accordance with various embodiments of this disclosure;

[0059] FIGURE 17 illustrates a data container deletion process in accordance with various embodiments of this disclosure;

[0060] FIGURE 18 illustrates a data container access request process in accordance with various embodiments of this disclosure;

[0061] FIGURE 19 illustrates a representation of an example graph database configuration in accordance with various embodiments of this disclosure;

[0062] FIGURE 20 illustrates an example container nesting process in accordance with various embodiments of this disclosure;

[0063] FIGURE 21 illustrates an example composable application diagram in accordance with various embodiments of this disclosure;

[0064] FIGURE 22 illustrates an example container access and control architecture incorporating Privacy Enhancing Technologies;

[0065] FIGURE 23 illustrates a container access and control with differential privacy process in accordance with various embodiments of this disclosure;

[0066] FIGURE 24 illustrates a container access and control with federated analysis process in accordance with various embodiments of this disclosure;

[0067] FIGURE 25 illustrates a container access and control with homomorphic encryption process in accordance with various embodiments of this disclosure;

[0068] FIGURE 26 illustrates a container access and control with zero-knowledge proofs process in accordance with various embodiments of this disclosure;

[0069] FIGURE 27 illustrates a container access and control with secure multiparty computation process in accordance with various embodiments of this disclosure;

[0070] FIGURE 28 illustrates a data container access and control blockchain architecture in accordance with various embodiments of this disclosure;

[0071] FIGURE 29 illustrates a data container blockchain and NFT process in accordance with various embodiments of this disclosure; and

[0072] FIGURE 30 illustrates an example electronic device or a system device in accordance with various embodiments of this disclosure.

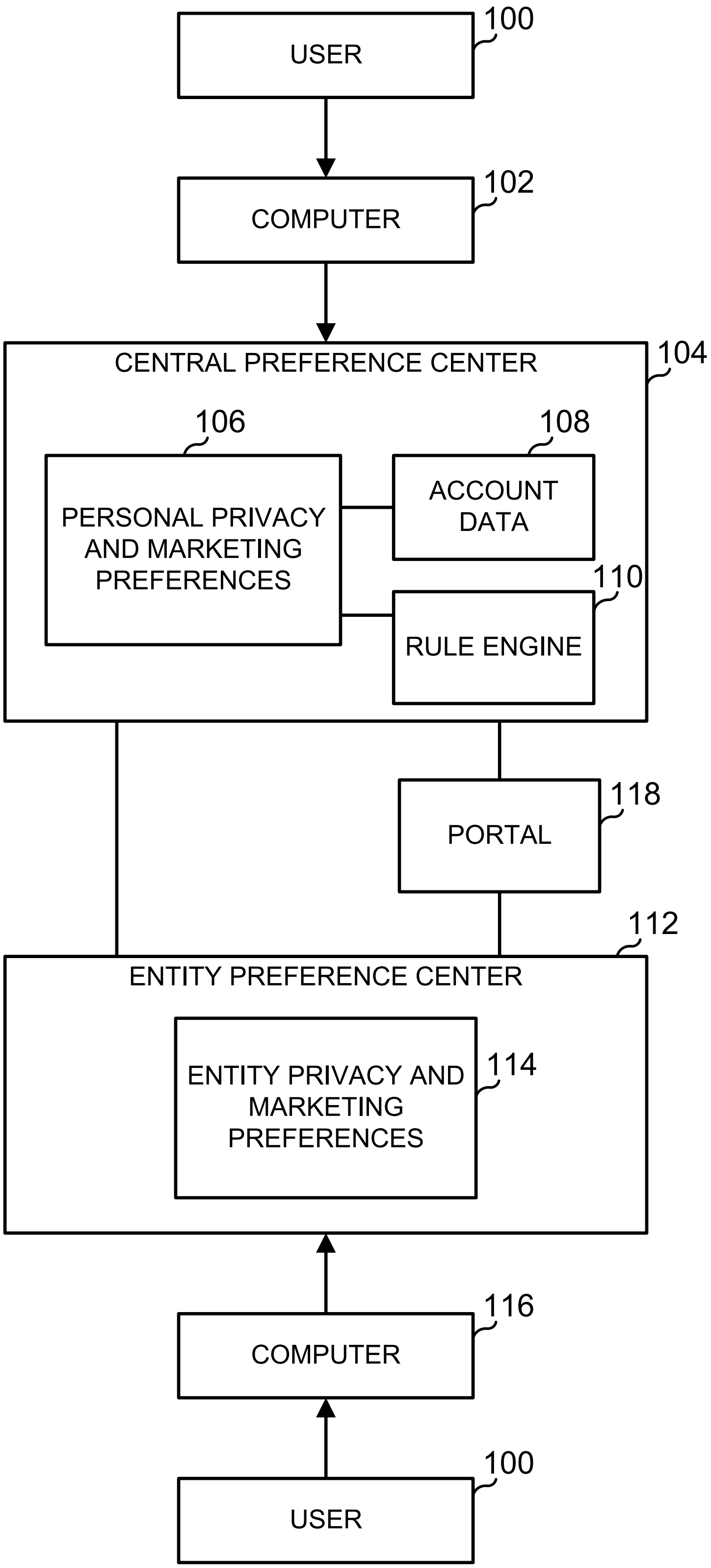
USER
100
COMPUTER
102
CENTRAL PREFERENCE CENTER
104
106
PERSONAL PRIVACY AND MARKETING PREFERENCES
108
ACCOUNT DATA
110
RULE ENGINE
PORTAL
118
112
ENTITY PREFERENCE CENTER
ENTITY PRIVACY AND MARKETING PREFERENCES
114
COMPUTER
116
USER
100

FIG. 1

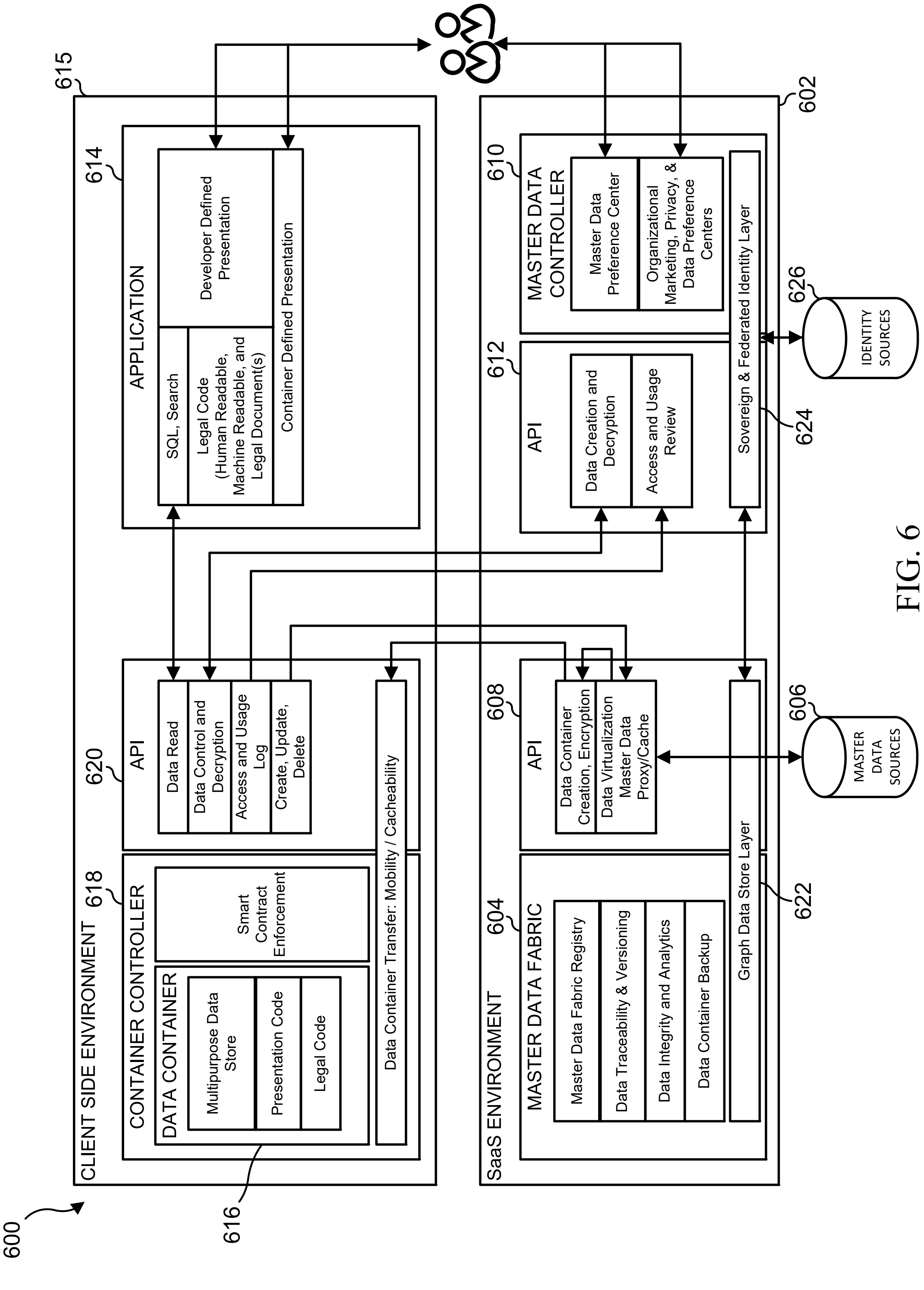
600
615
CLIENT SIDE ENVIRONMENT
614
APPLICATION
SQL, Search
Legal Code (Human Readable, Machine Readable, and Legal Document(s)
Developer Defined Presentation
Container Defined Presentation
620
API
Data Read
Data Control and Decryption
Access and Usage Log
Create, Update, Delete
618
CONTAINER CONTROLLER
Smart Contract Enforcement
DATA CONTAINER
Multipurpose Data Store
Presentation Code
Legal Code
616
Data Container Transfer: Mobility / Cacheability
602
SaaS ENVIRONMENT
610
MASTER DATA CONTROLLER
Master Data Preference Center
Organizational Marketing, Privacy, & Data Preference Centers
612
API
Data Creation and Decryption
Access and Usage Review
Sovereign & Federated Identity Layer
624
626
IDENTITY SOURCES
608
API
Data Container Creation, Encryption
Data Virtualization Master Data Proxy/Cache
604
MASTER DATA FABRIC
Master Data Fabric Registry
Data Traceability & Versioning
Data Integrity and Analytics
Data Container Backup
Graph Data Store Layer
622
606
MASTER DATA SOURCES

FIG. 6

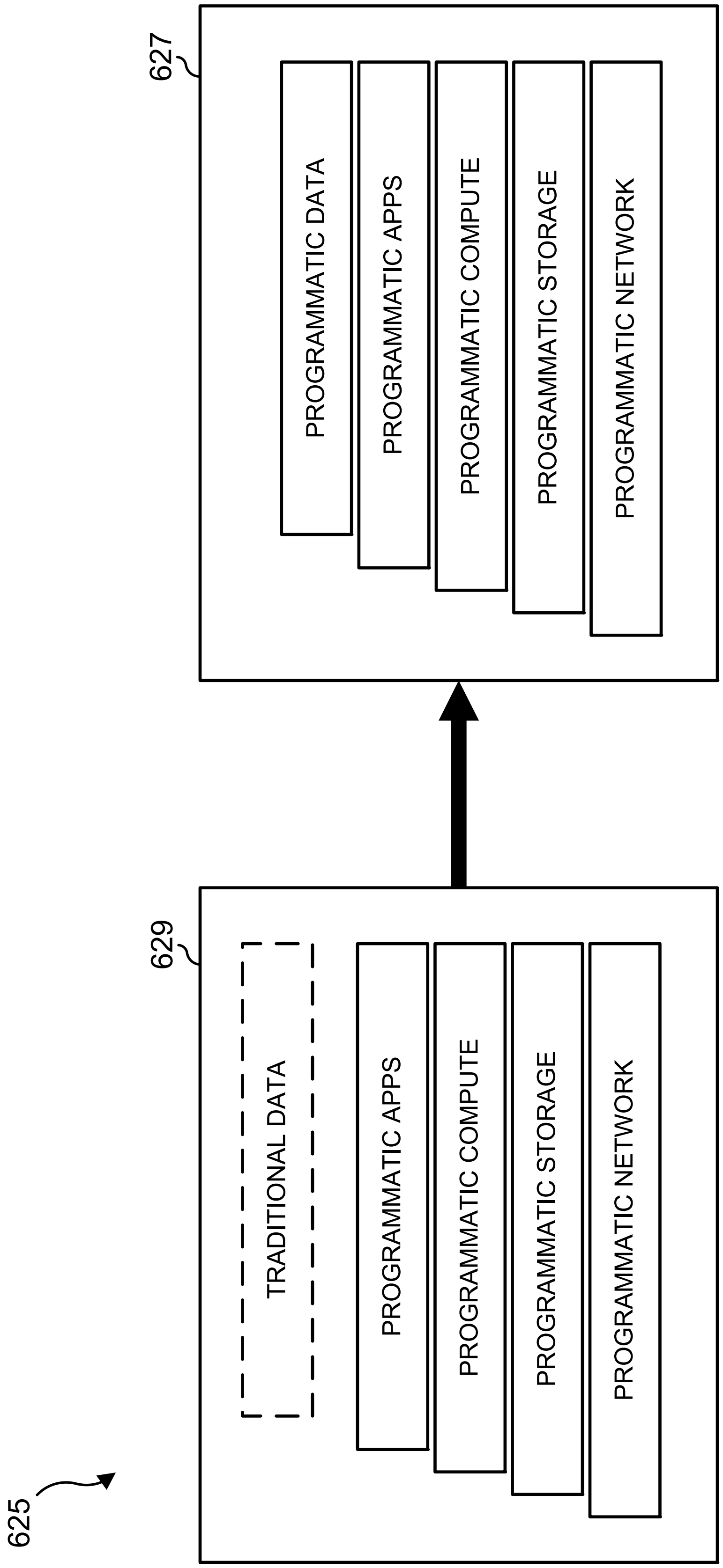
625
629
TRADITIONAL DATA
PROGRAMMATIC APPS
PROGRAMMATIC COMPUTE
PROGRAMMATIC STORAGE
PROGRAMMATIC NETWORK
627
PROGRAMMATIC DATA
PROGRAMMATIC APPS
PROGRAMMATIC COMPUTE
PROGRAMMATIC STORAGE
PROGRAMMATIC NETWORK

FIG. 6B

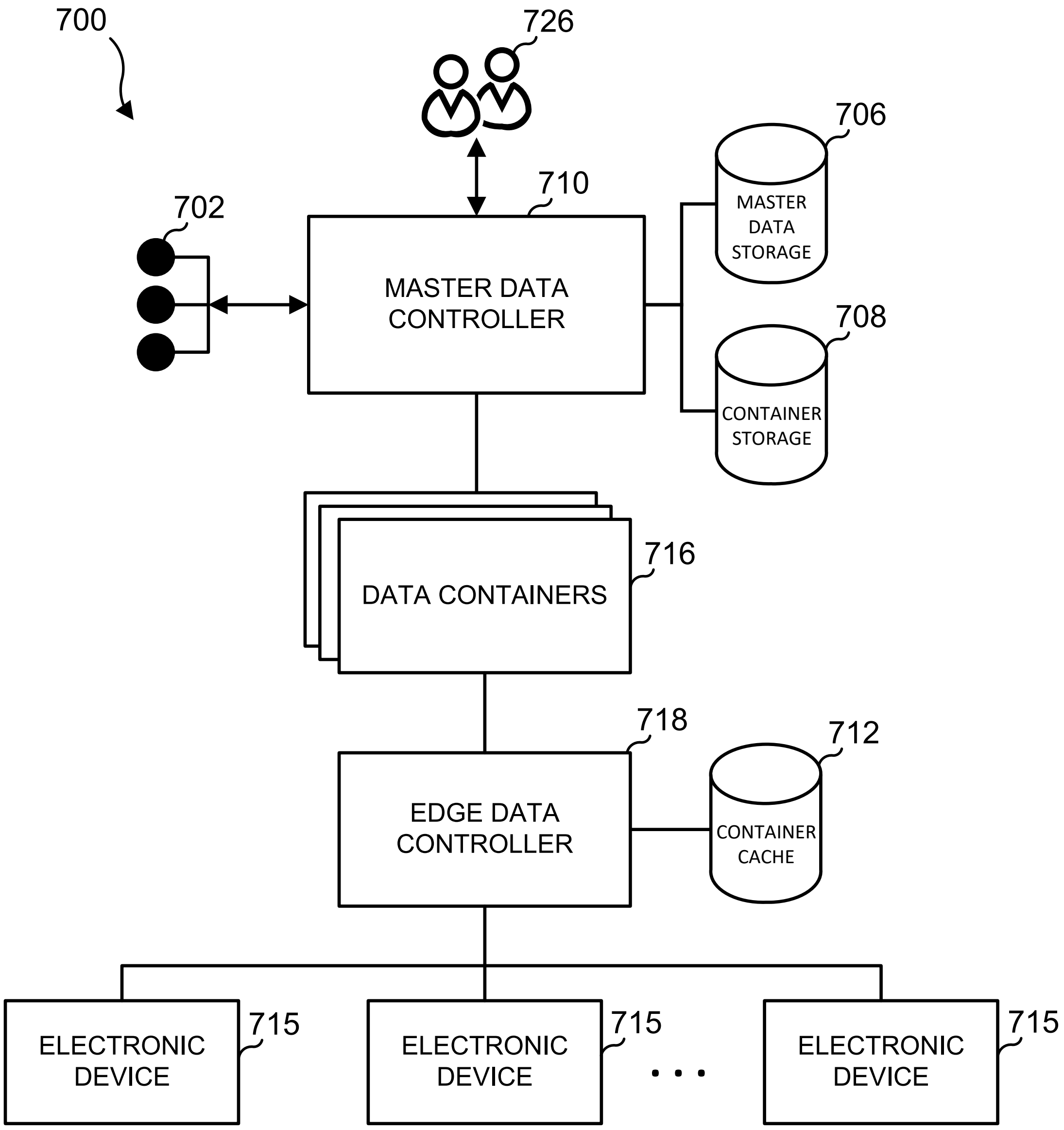
700
726
706
710
702
MASTER DATA STORAGE
MASTER DATA CONTROLLER
708
CONTAINER STORAGE
DATA CONTAINERS
716
718
712
EDGE DATA CONTROLLER
CONTAINER CACHE
ELECTRONIC DEVICE
715
ELECTRONIC DEVICE
715
• • •
ELECTRONIC DEVICE
715

FIG. 7