



US 20240022609A1

(19) **United States**

(12) **Patent Application Publication**
Smith et al.

(10) **Pub. No.: US 2024/0022609 A1**

(43) **Pub. Date: Jan. 18, 2024**

(54) **SECURITY AND RESILIENCY FOR CLOUD
TO EDGE DEPLOYMENTS**

Publication Classification

(71) Applicants: **Ned M. Smith**, Beaverton, OR (US);
Kshitij Arun Doshi, Tempe, AZ (US);
Sunil Cheruvu, Tempe, AZ (US);
Malini Bhandaru, San Jose, CA (US);
Anahit Tarkhanyan, Cupertino, CA
(US); **Mats Gustav Agerstam**,
Portland, OR (US); **Bruno Vavala**,
Hillsboro, OR (US); **Vidya**
Ranganathan, Bangalore (IN)

(51) **Int. Cl.**
H04L 9/40 (2006.01)
G06F 9/50 (2006.01)
(52) **U.S. Cl.**
CPC **H04L 63/20** (2013.01); **G06F 9/5088**
(2013.01)

(72) Inventors: **Ned M. Smith**, Beaverton, OR (US);
Kshitij Arun Doshi, Tempe, AZ (US);
Sunil Cheruvu, Tempe, AZ (US);
Malini Bhandaru, San Jose, CA (US);
Anahit Tarkhanyan, Cupertino, CA
(US); **Mats Gustav Agerstam**,
Portland, OR (US); **Bruno Vavala**,
Hillsboro, OR (US); **Vidya**
Ranganathan, Bangalore (IN)

(57) **ABSTRACT**

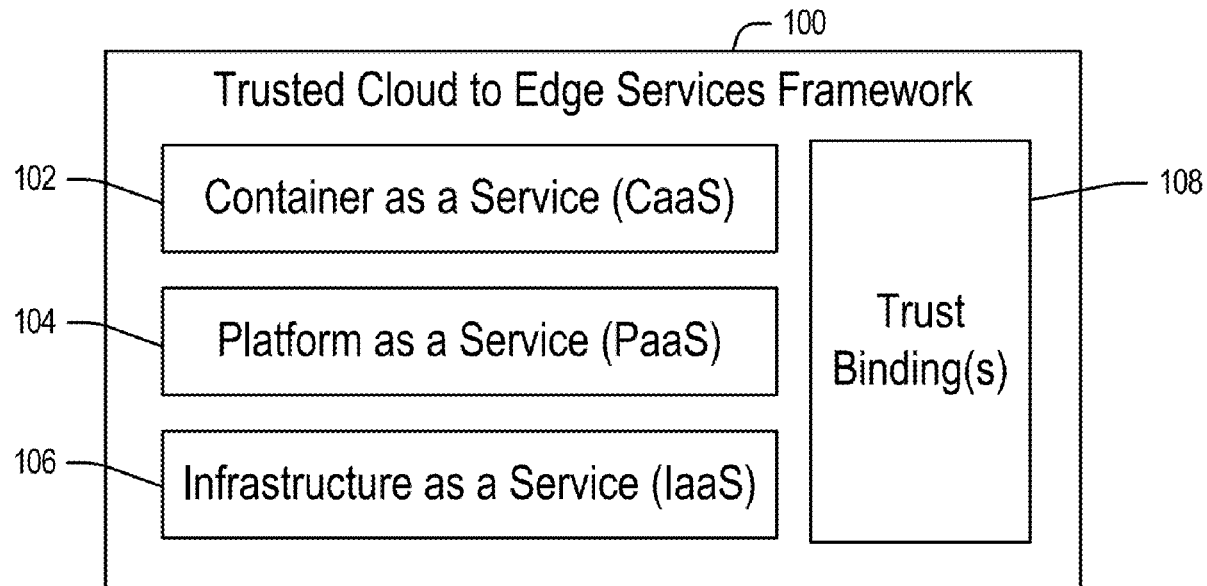
Various systems and methods are described for implement-
ing cloud-to-edge (C2E) security are disclosed, including
systems and methods for the execution of various workloads
that are distributed among multiple edge computing nodes.
An example technique for managing distributed workloads
includes: identifying characteristics of a distributed work-
load from an execution of the distributed workload, for a
distributed workload that is partitioned among multiple
computing nodes; evaluating a trust status of the distributed
workload in response to a change in the execution of the
distributed workload, including verifying resources to
execute the distributed workload and verifying security
policies associated with the resources; and controlling the
execution of the distributed workload among the multiple
computing nodes, based on the characteristics and the evalu-
ated trust status.

(21) Appl. No.: **18/373,059**

(22) Filed: **Sep. 26, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/456,310, filed on Mar.
31, 2023.



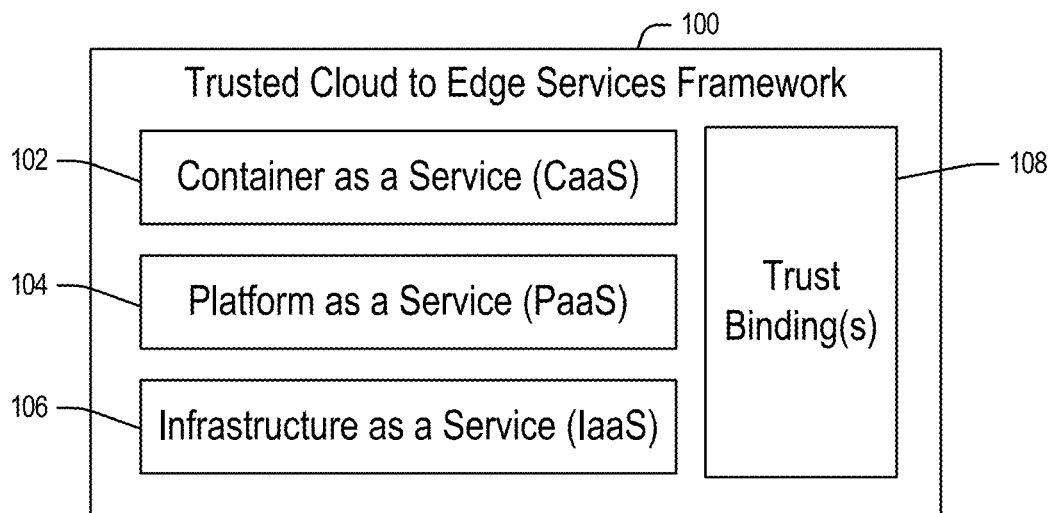


FIG. 1

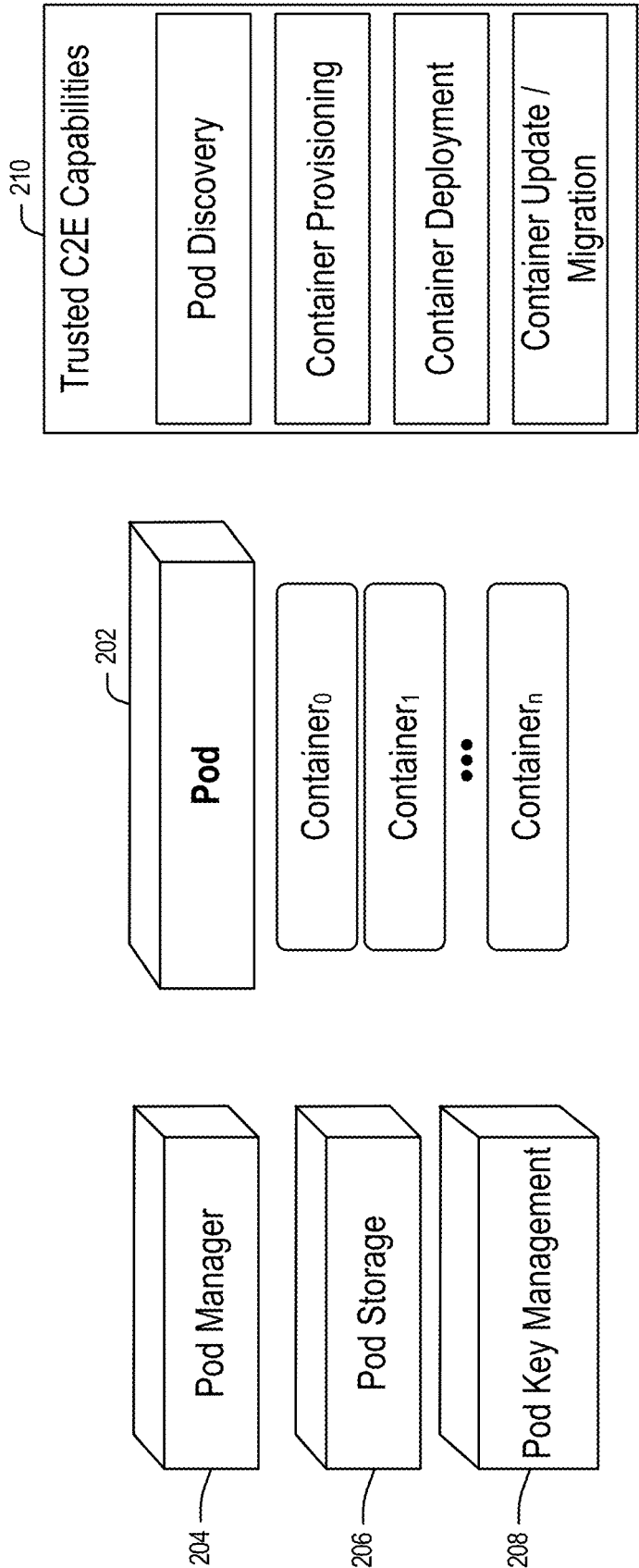


FIG. 2

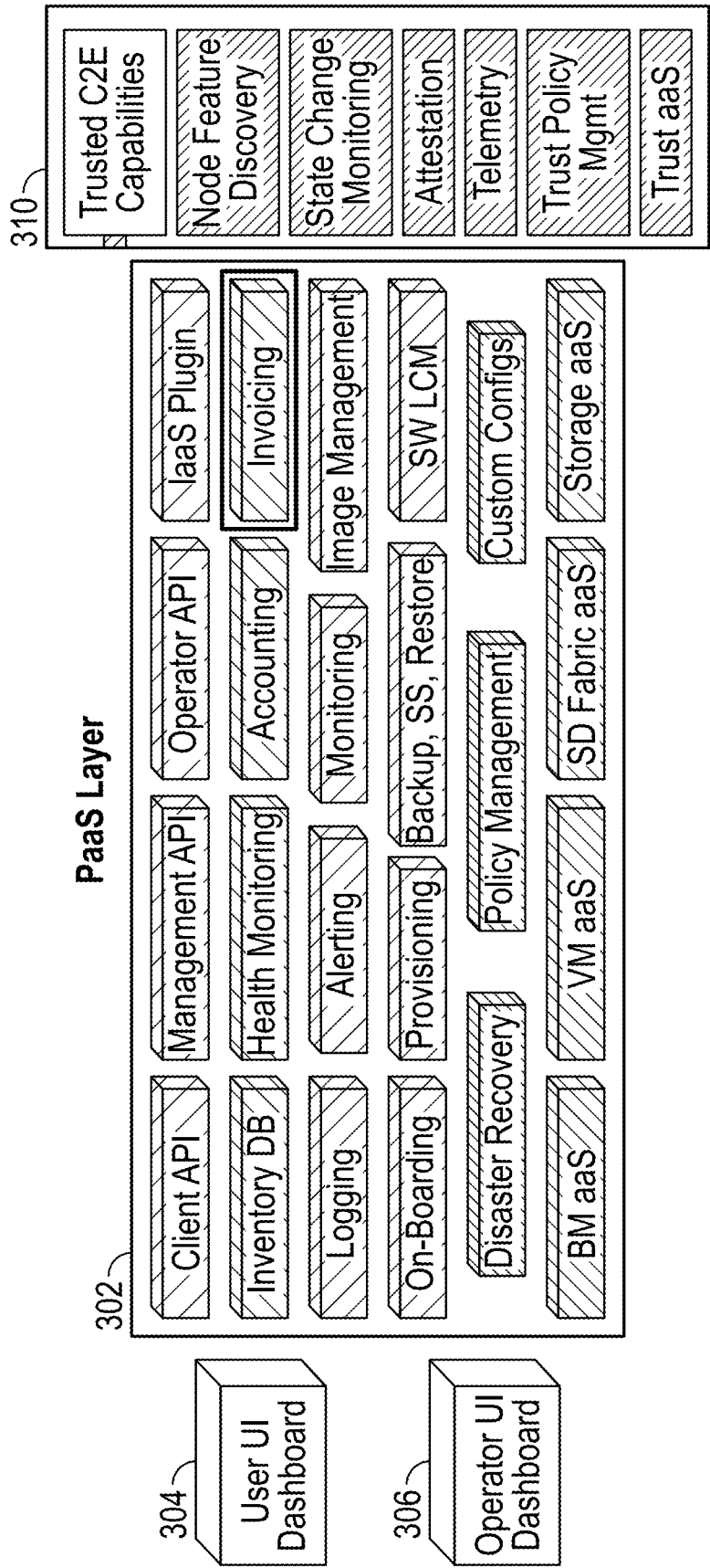


FIG. 3

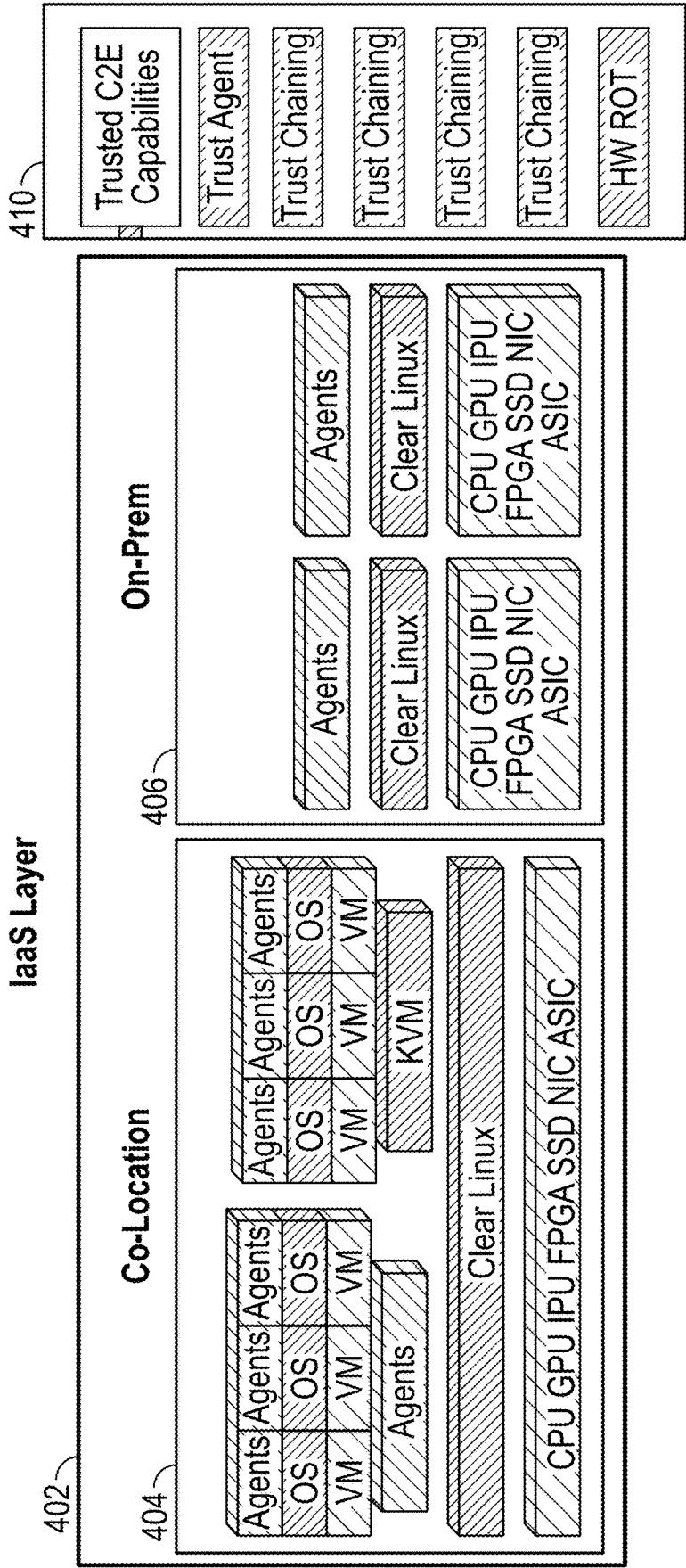


FIG. 4

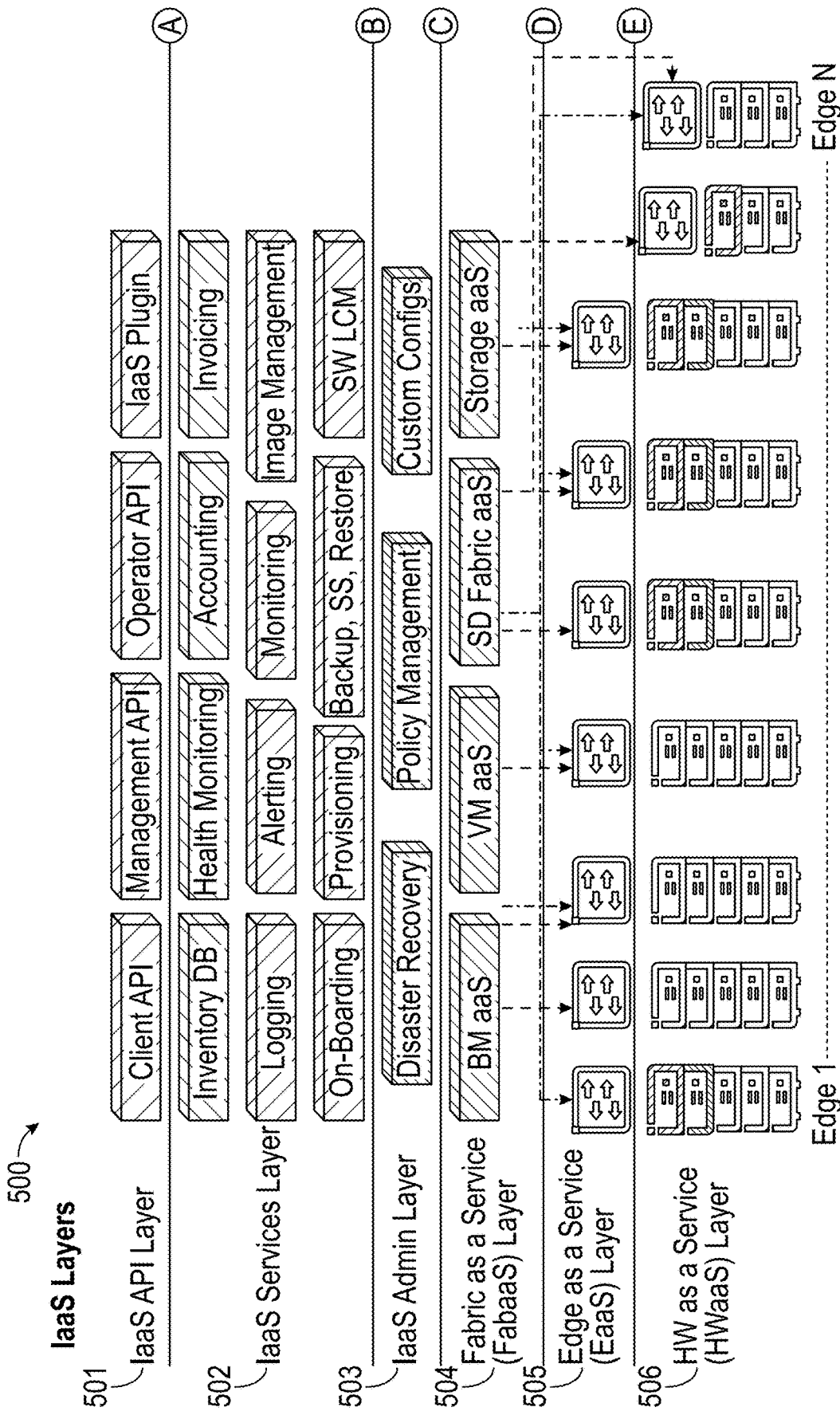


FIG. 5

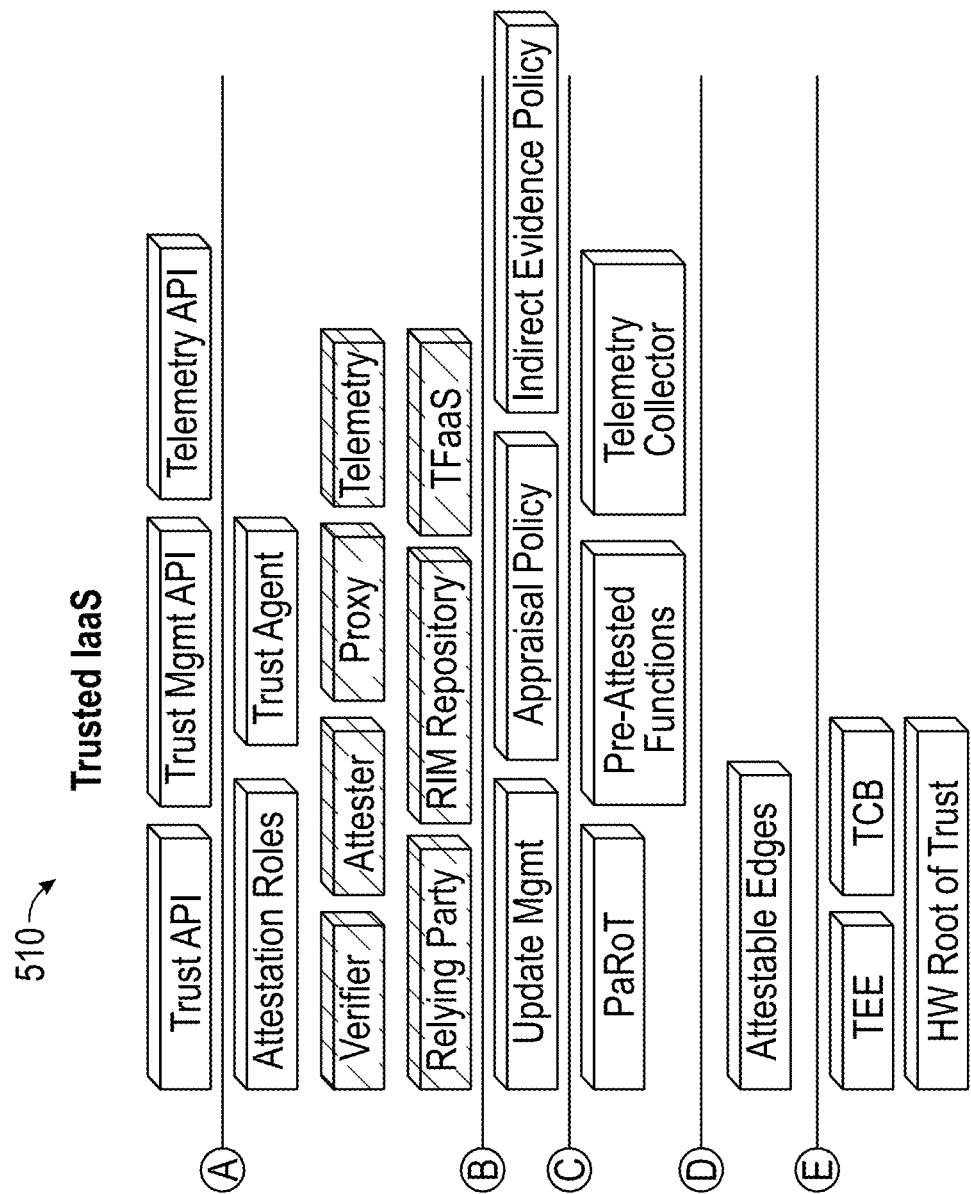


FIG. 5 (Continued)

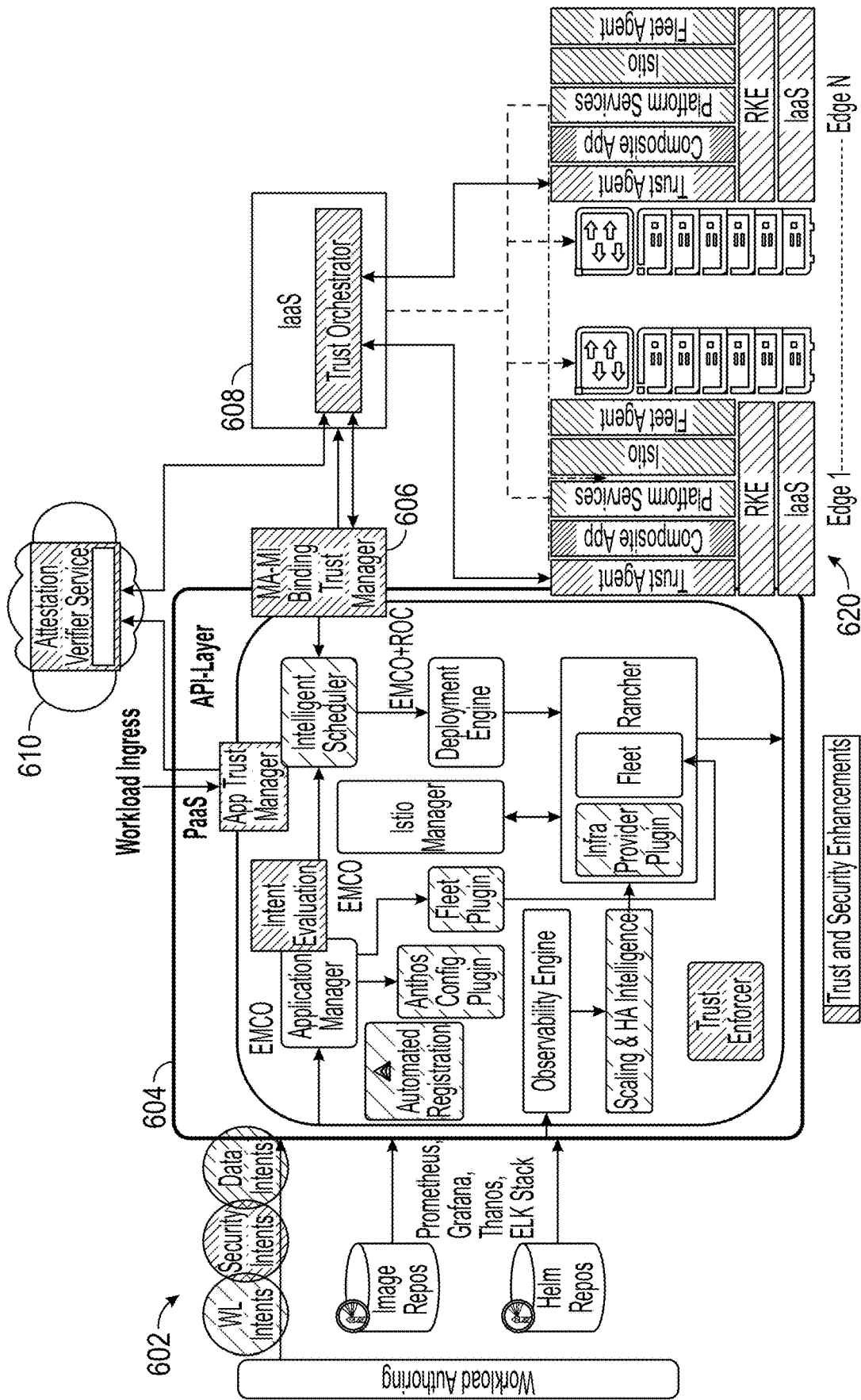


FIG. 6

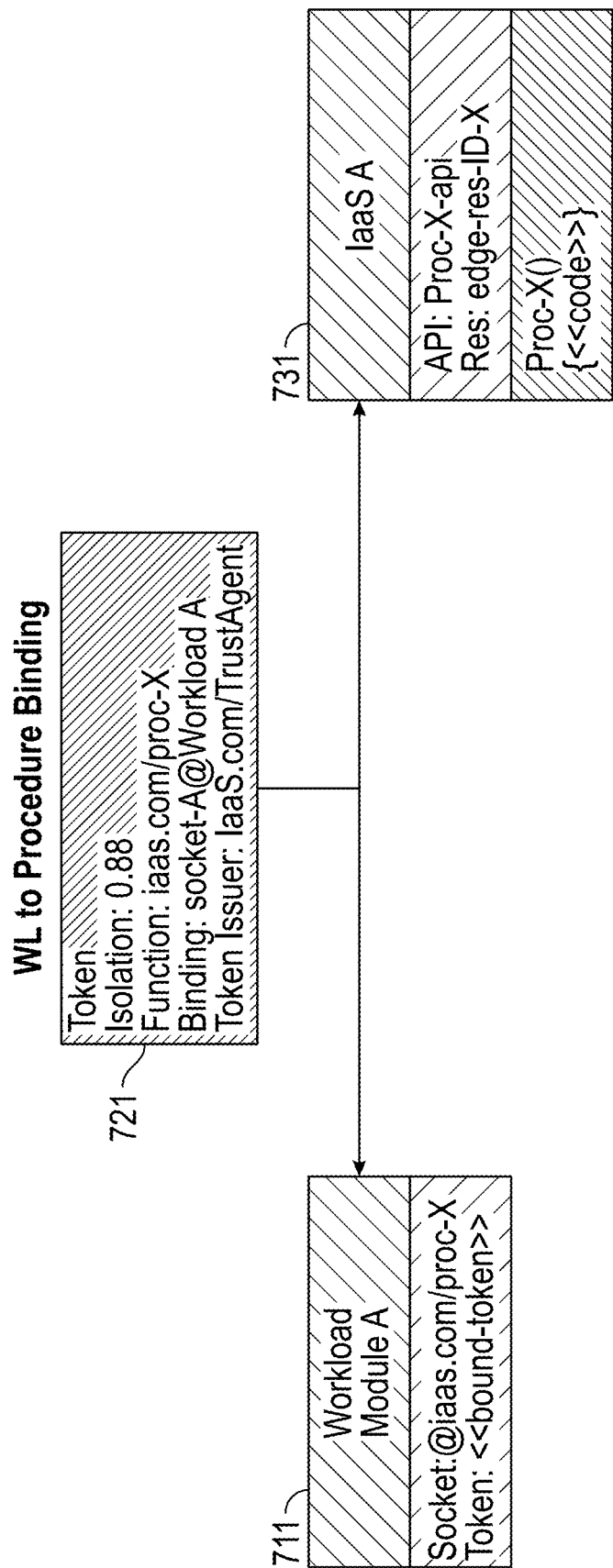


FIG. 7

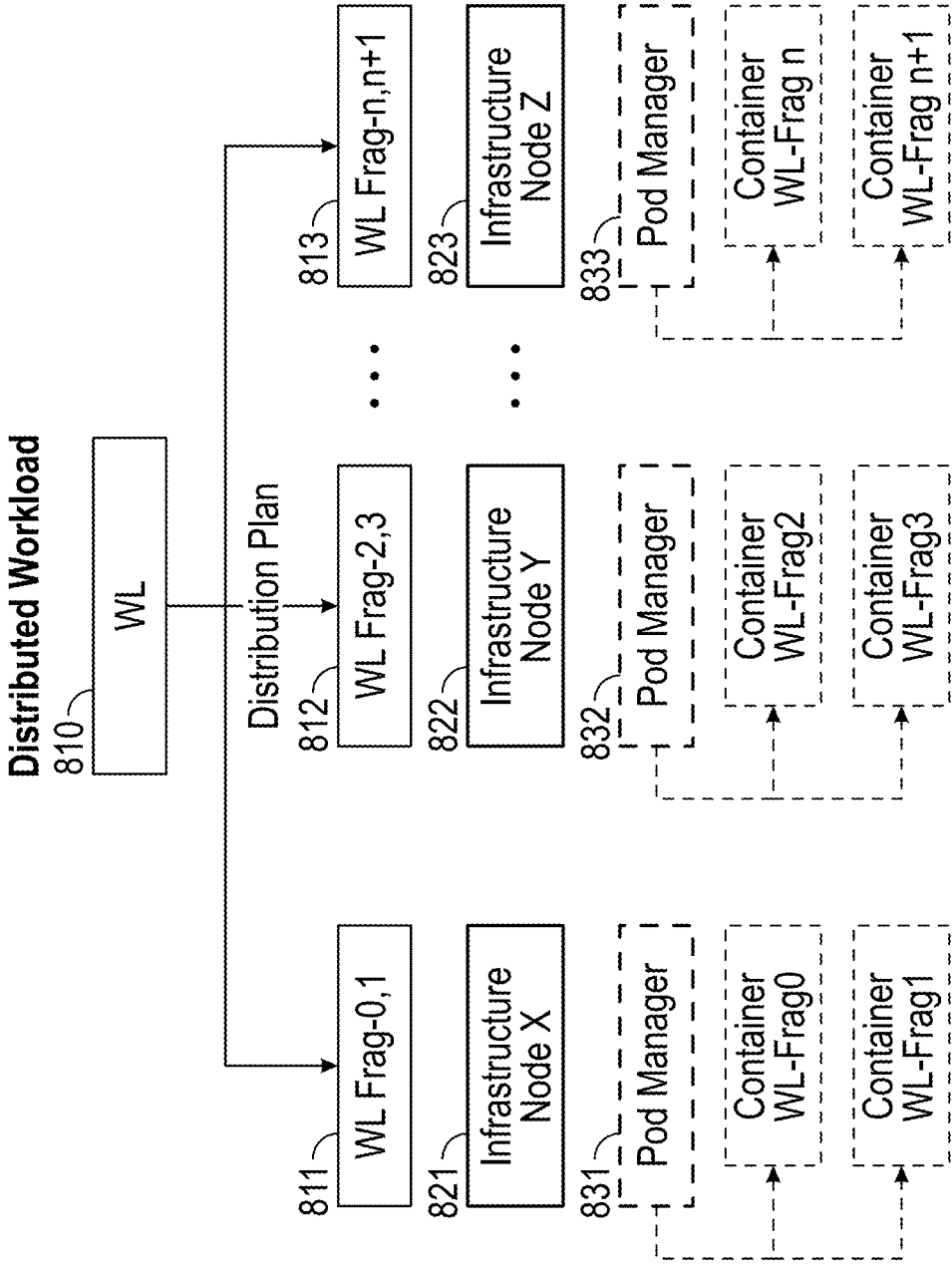


FIG. 8

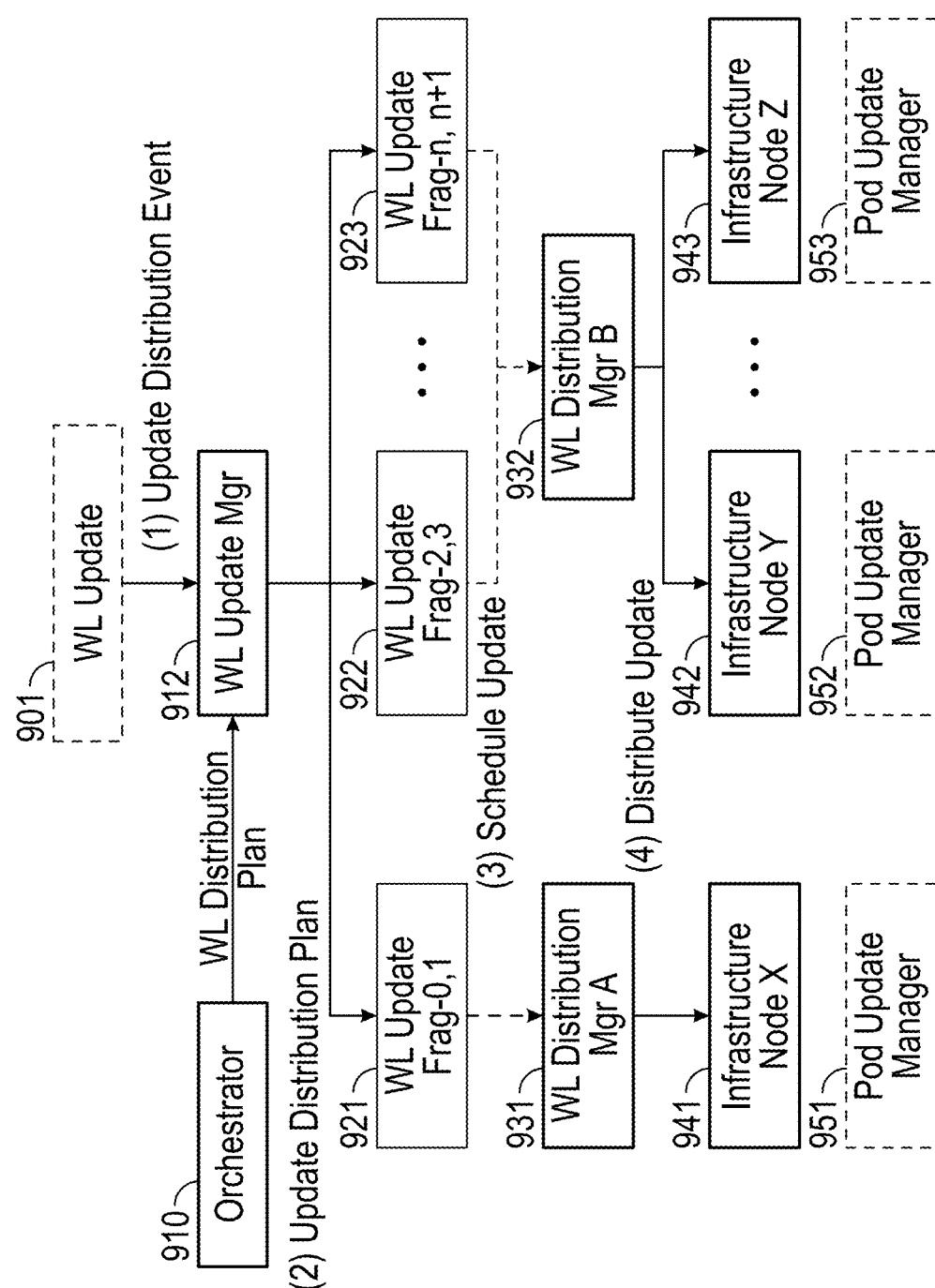


FIG. 9

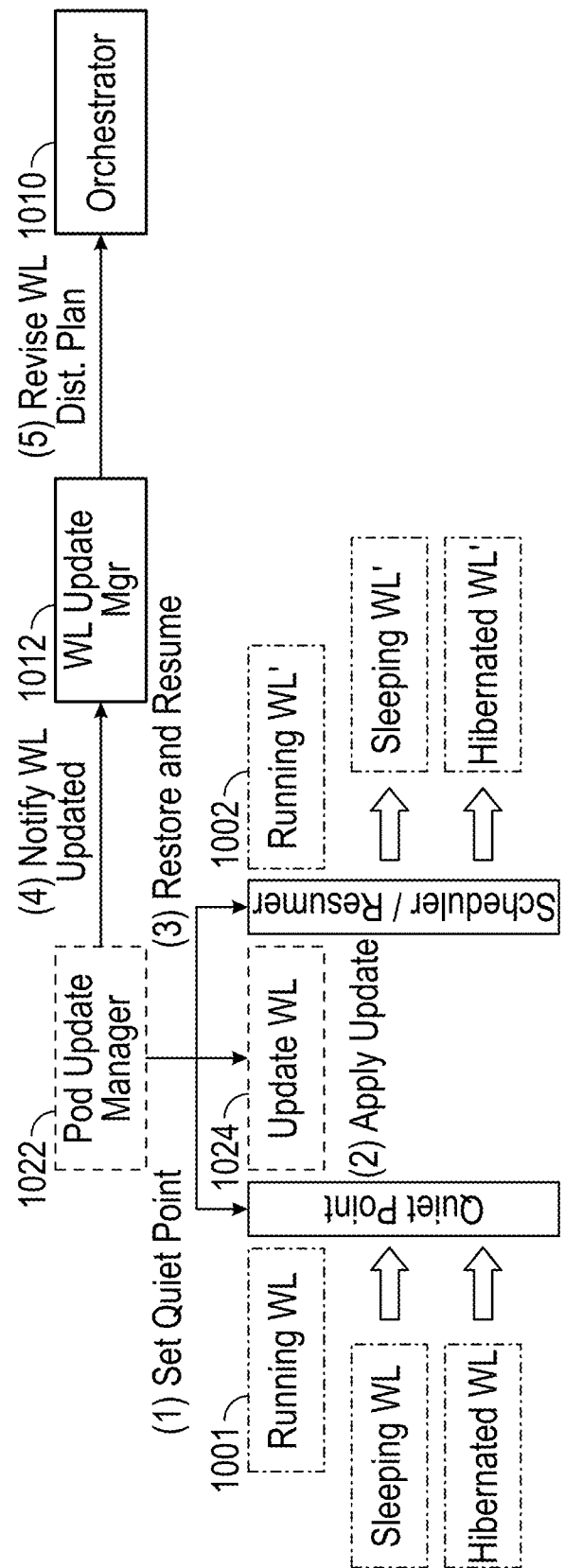


FIG. 10

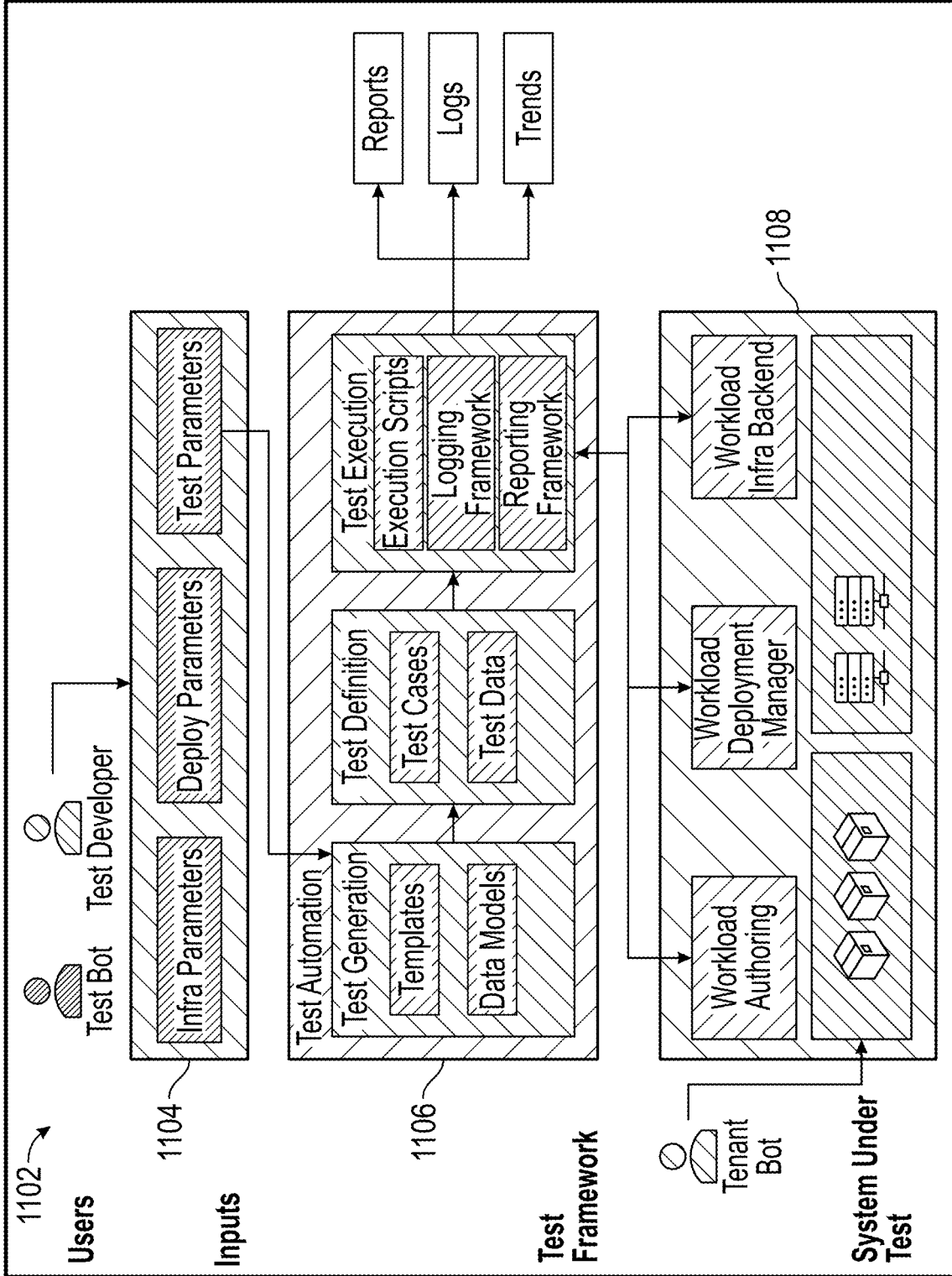


FIG. 11

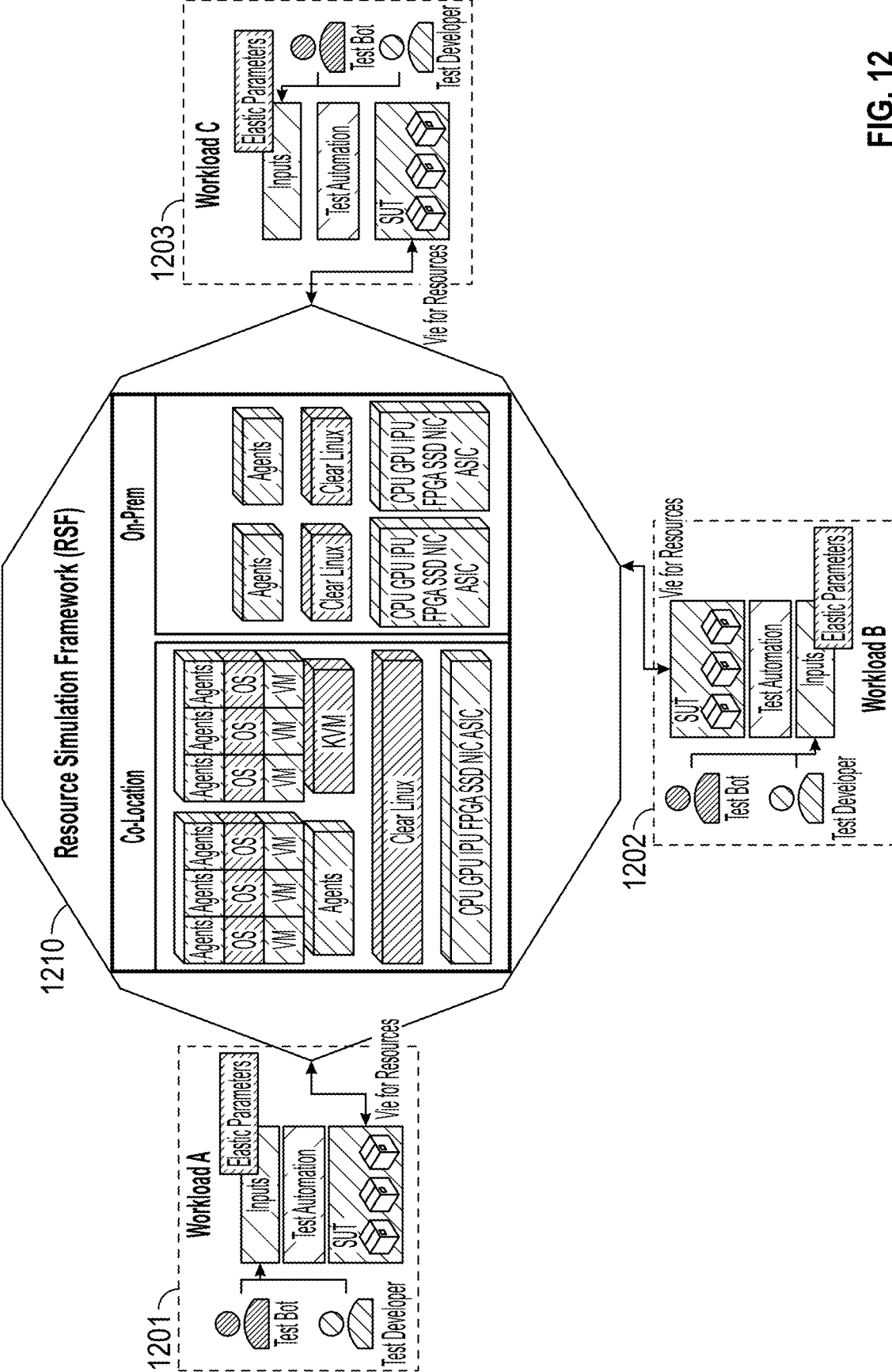


FIG. 12

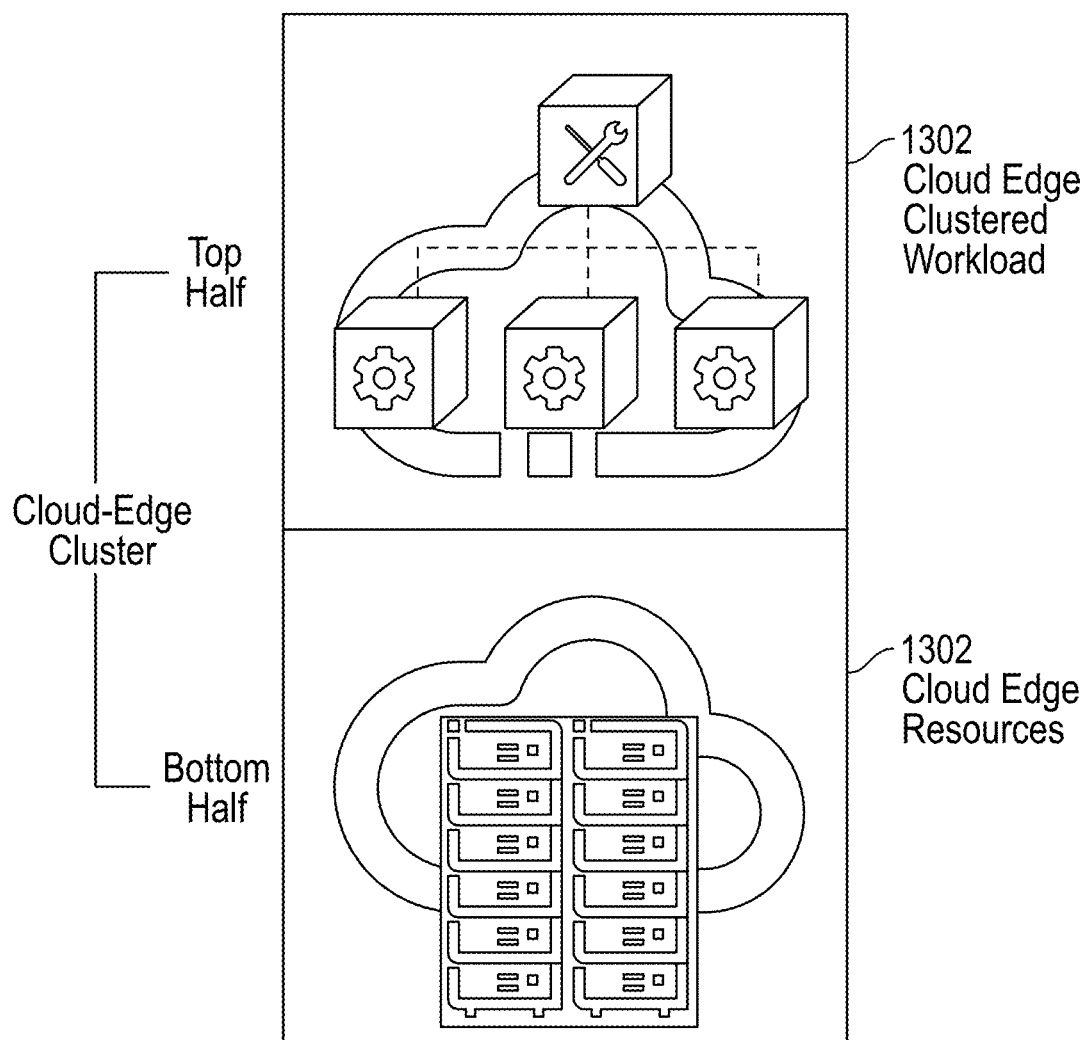


FIG. 13

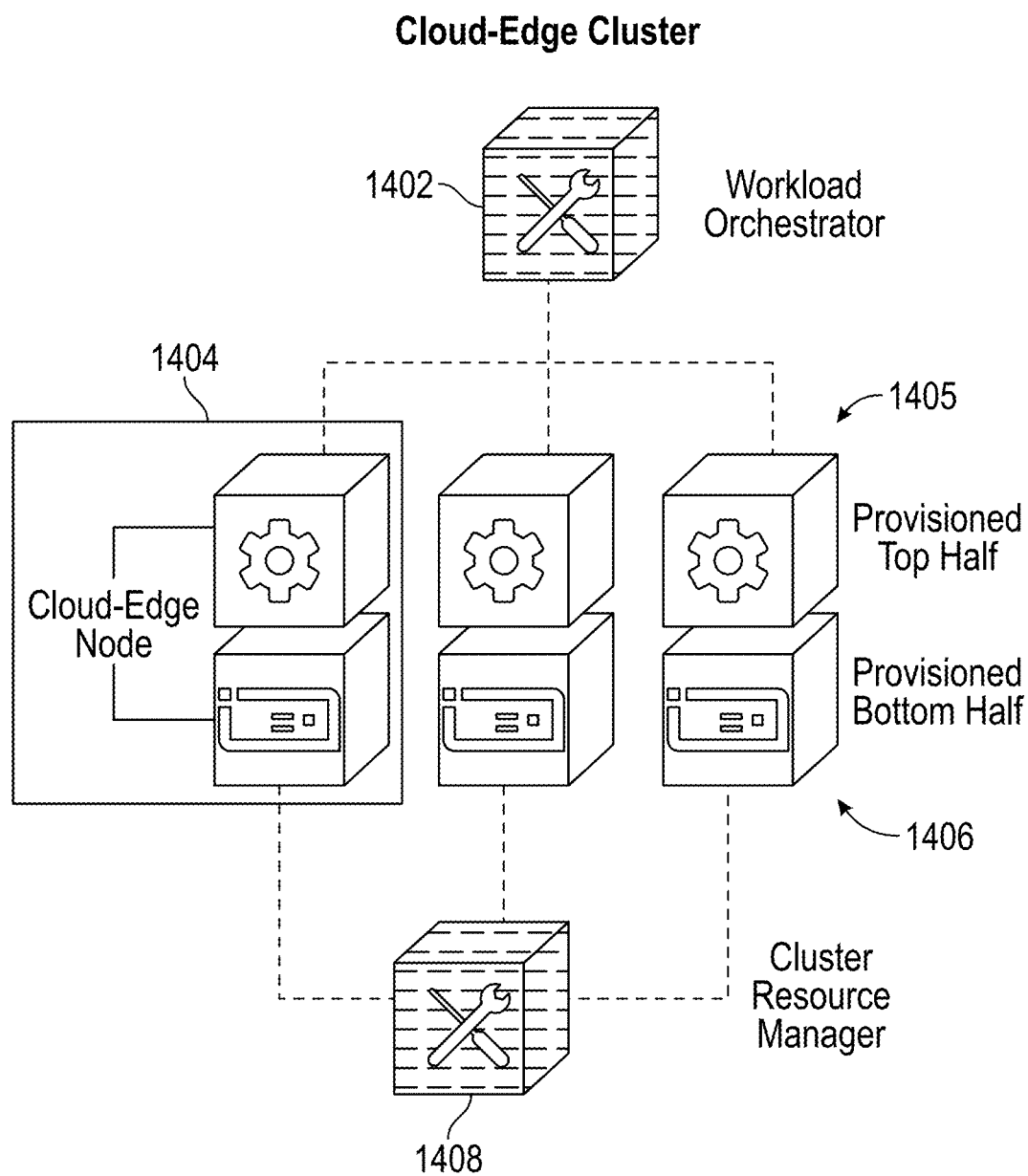


FIG. 14

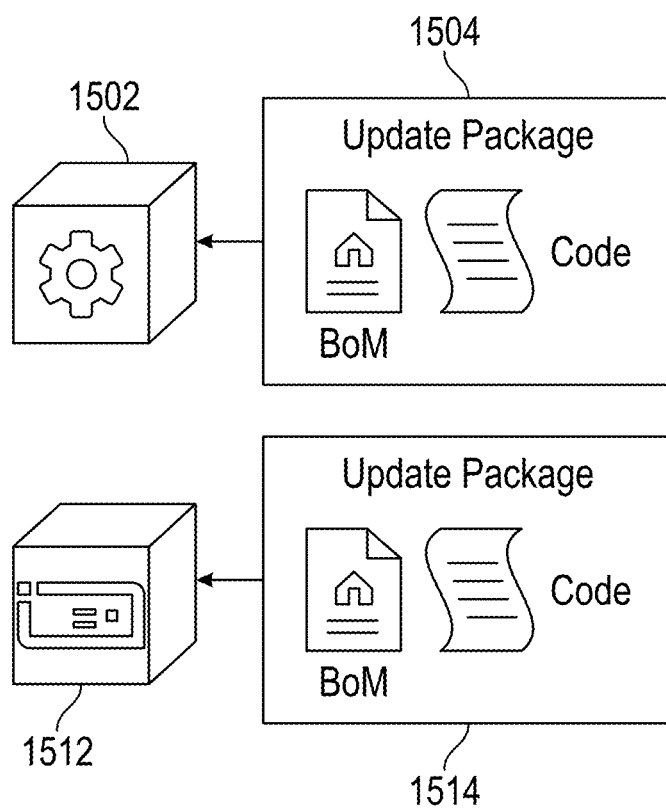


FIG. 15

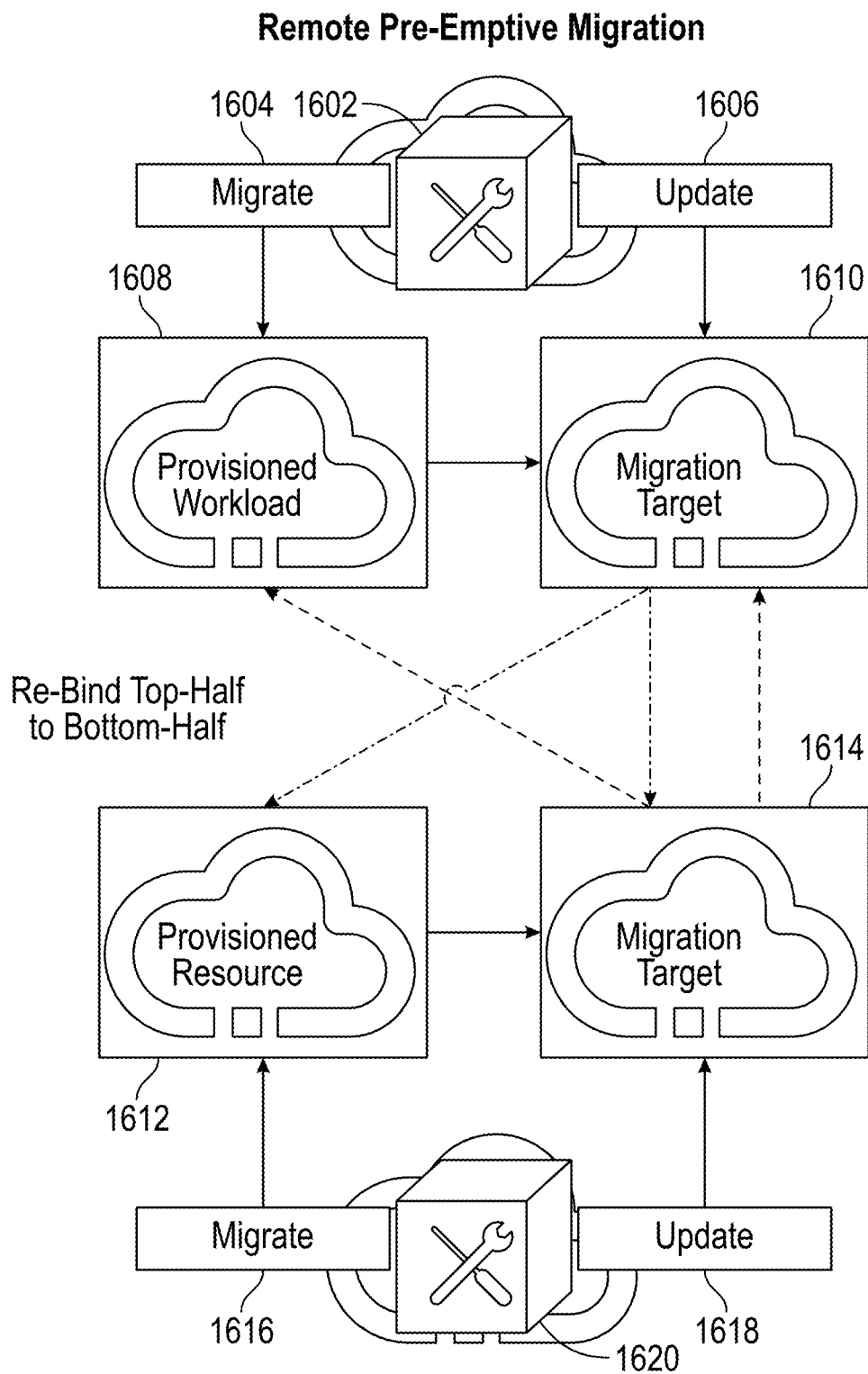


FIG. 16

Local Pre-Emptive Migration

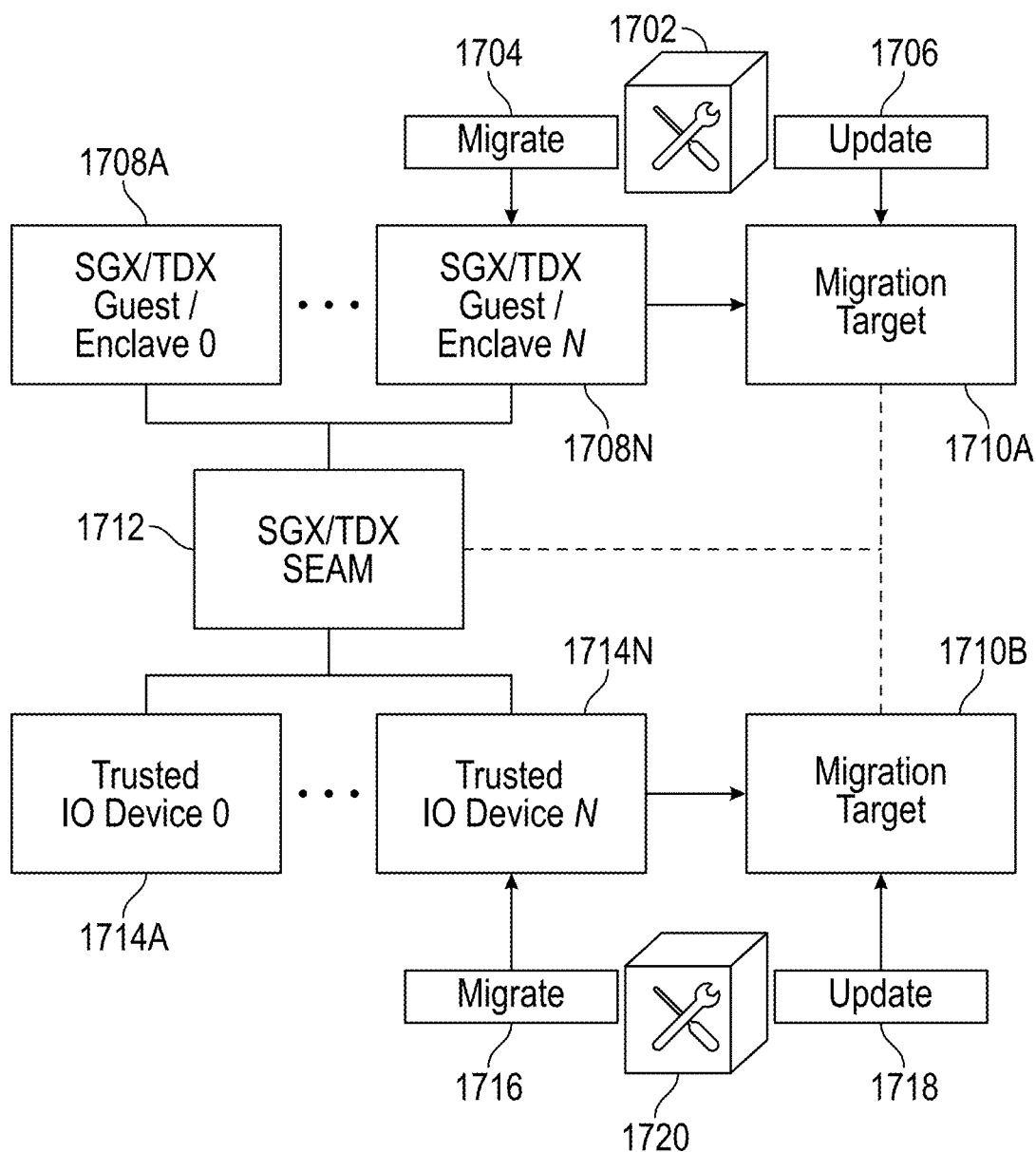


FIG. 17

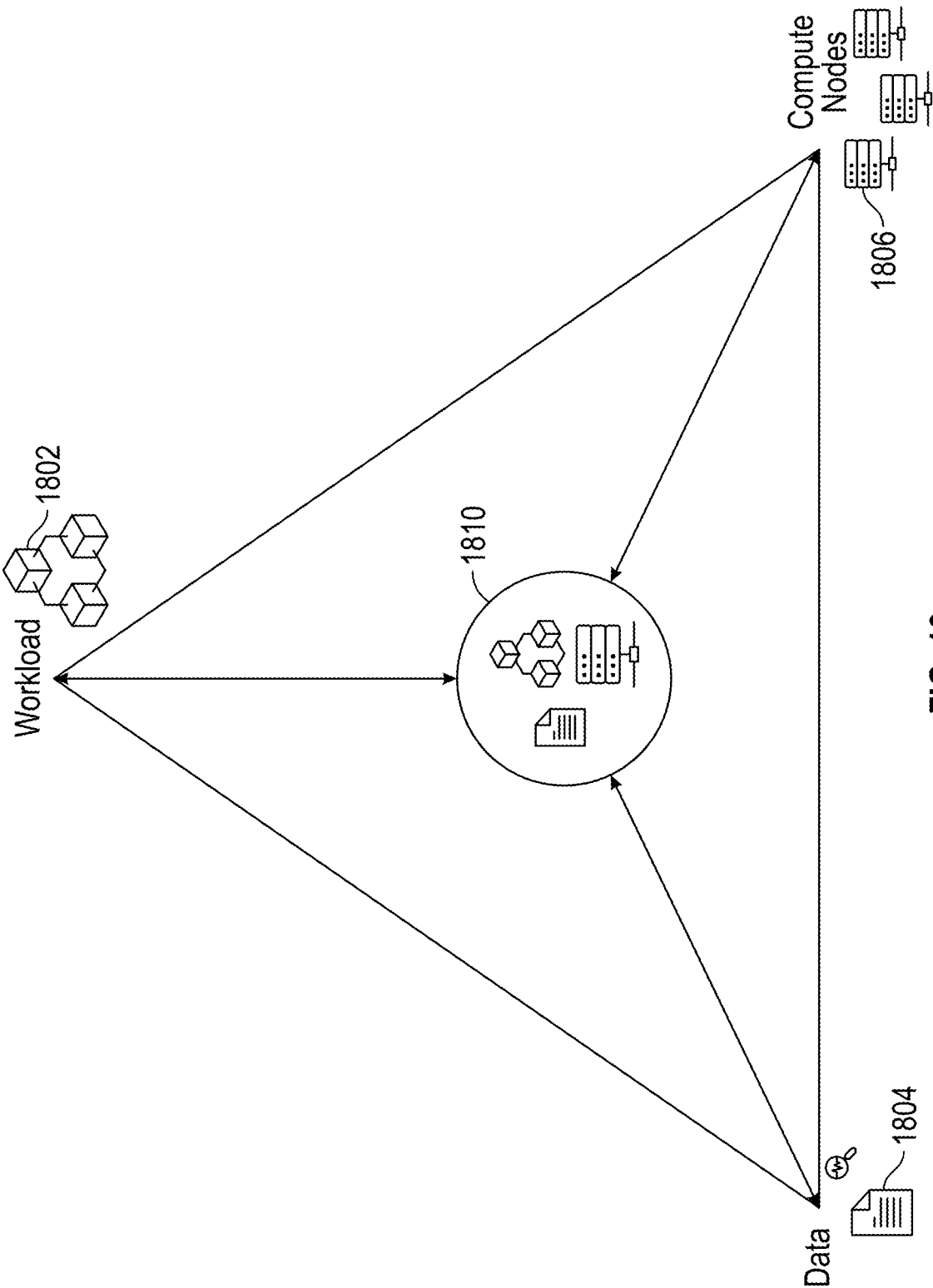


FIG. 18

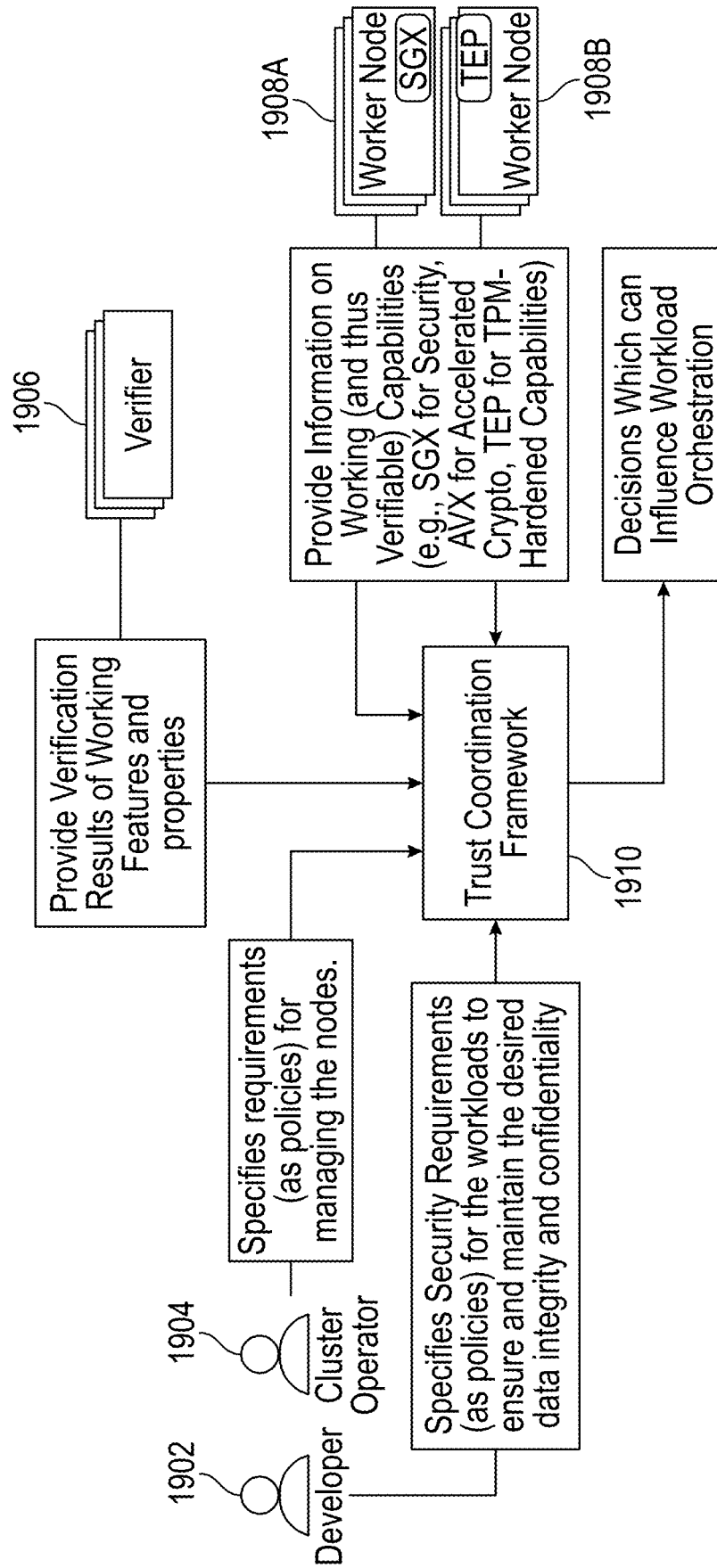


FIG. 19

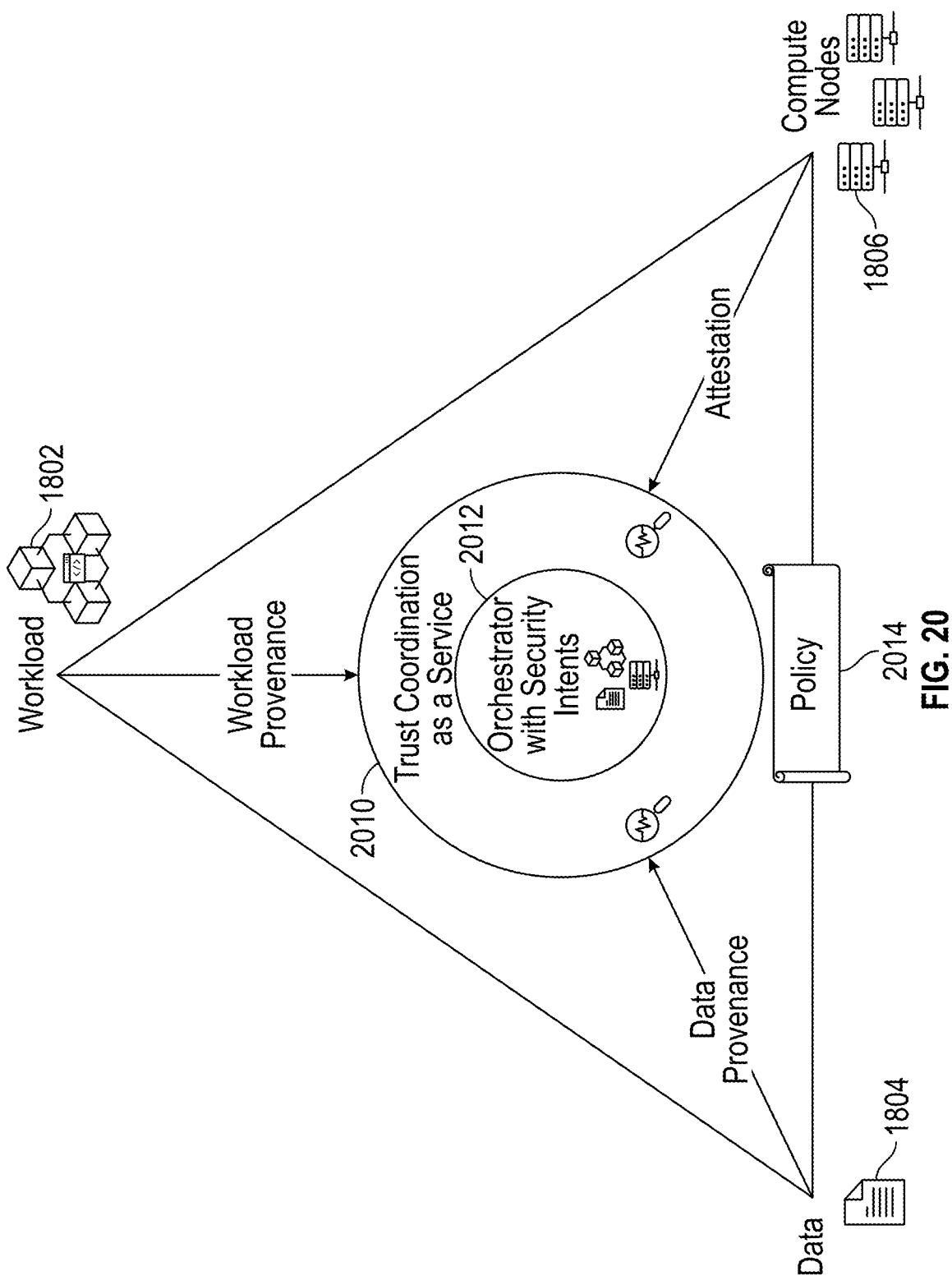


FIG. 20

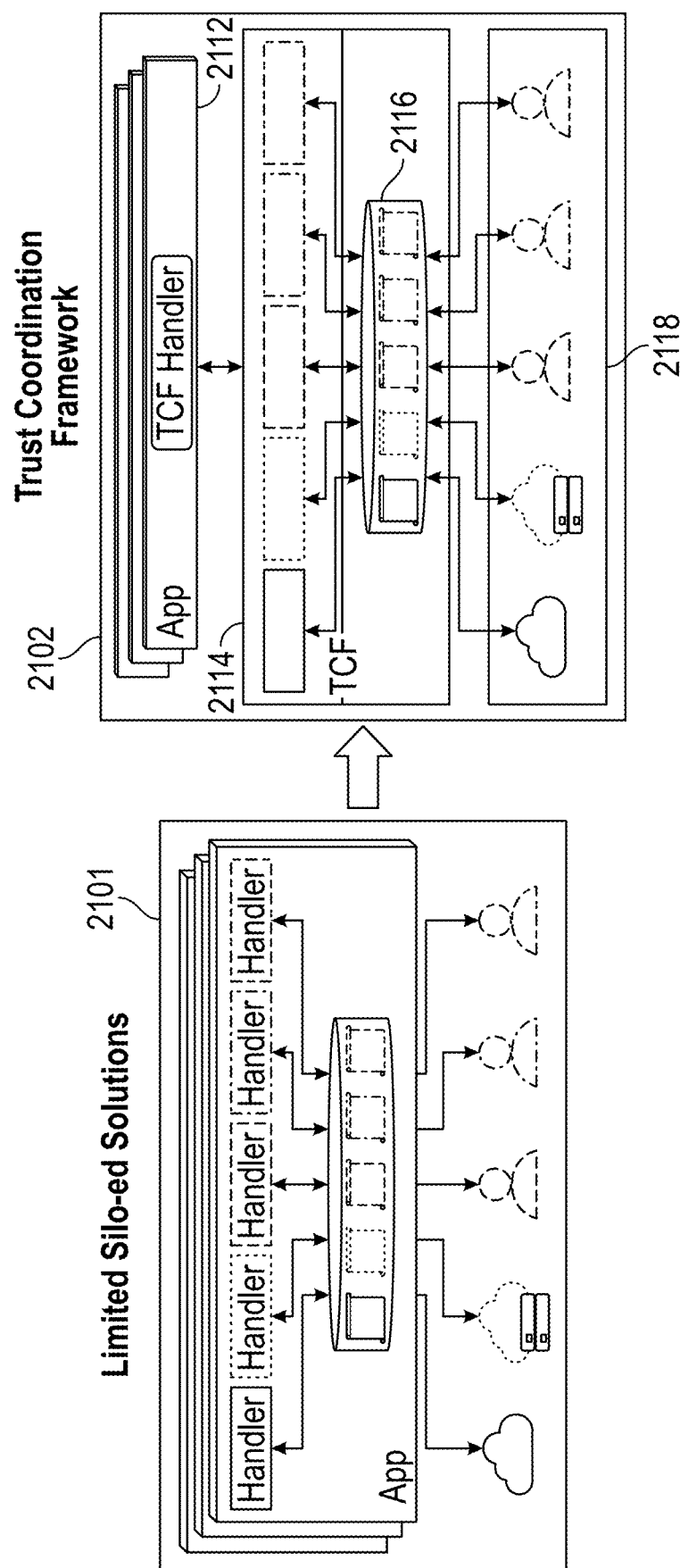


FIG. 21

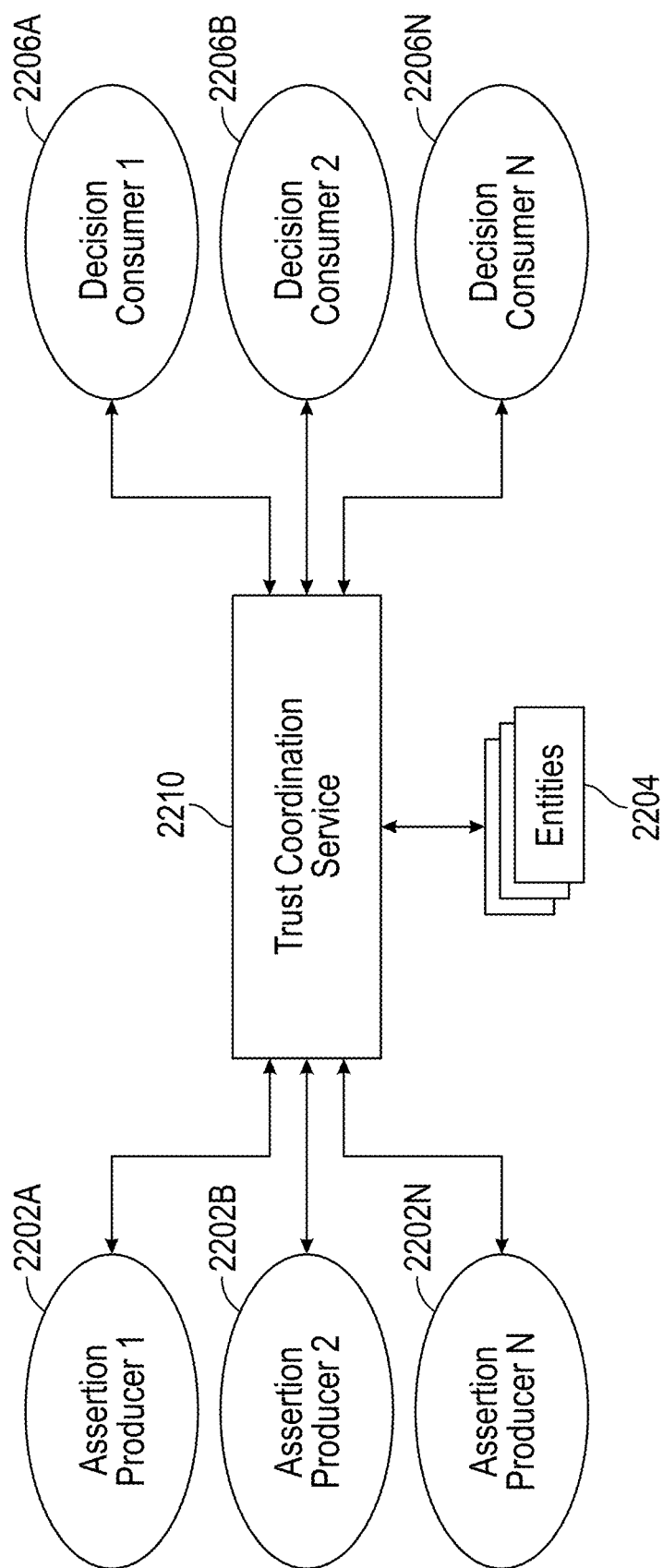


FIG. 22

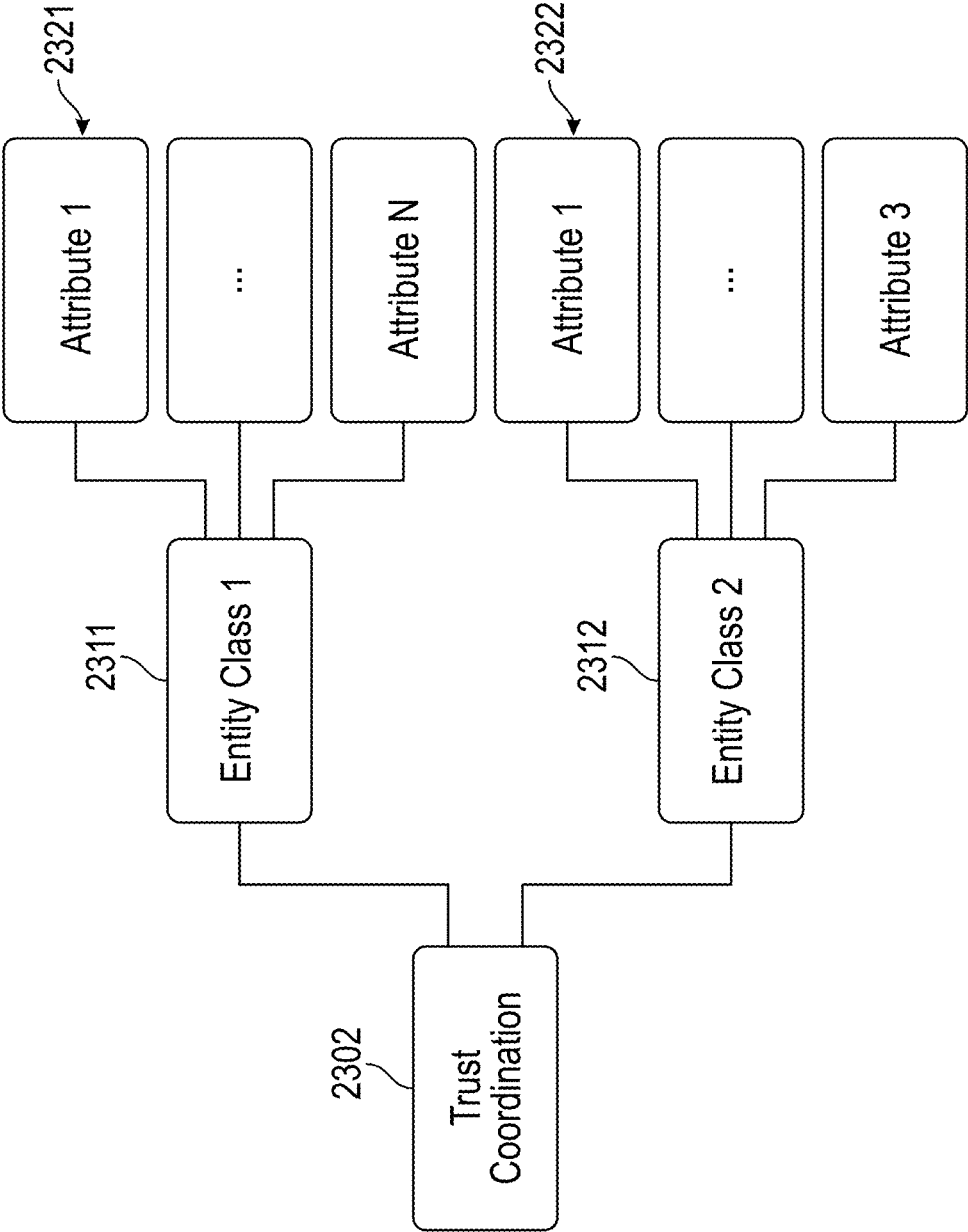


FIG. 23

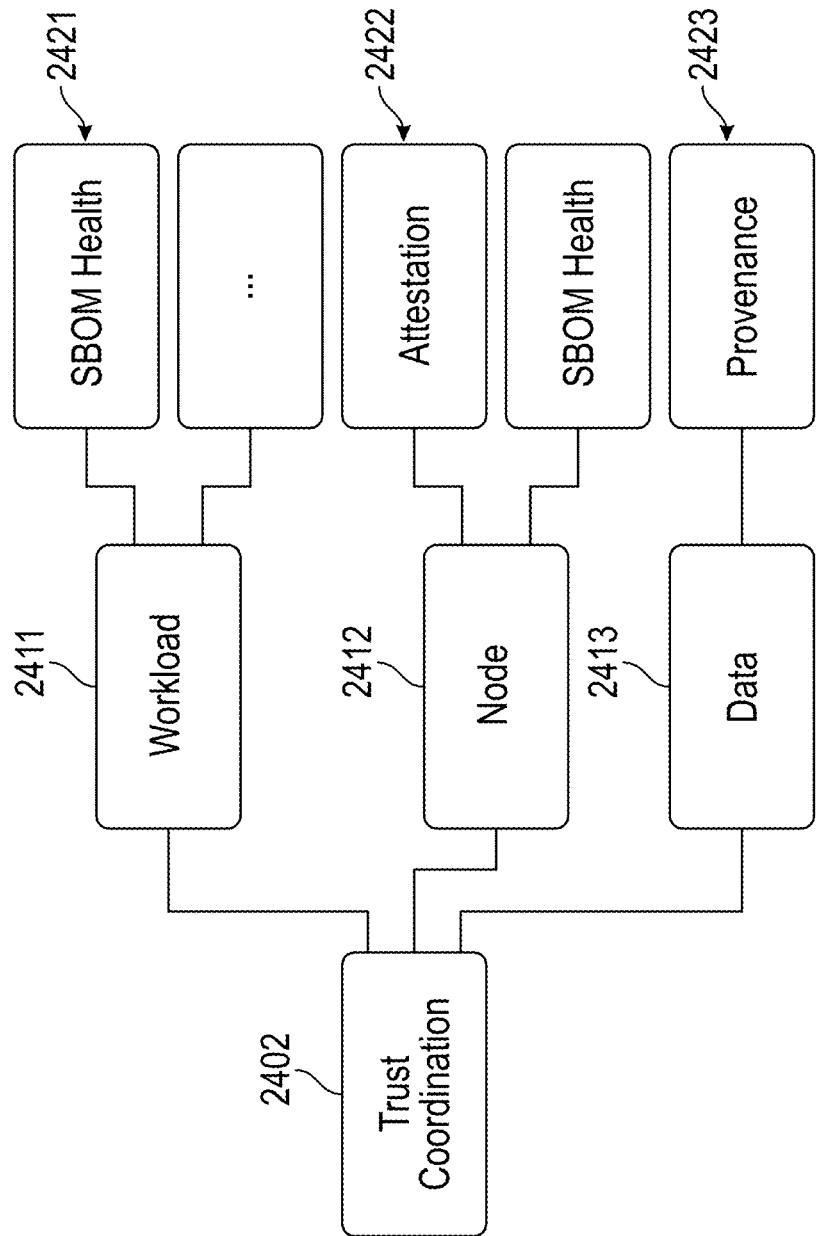


FIG. 24

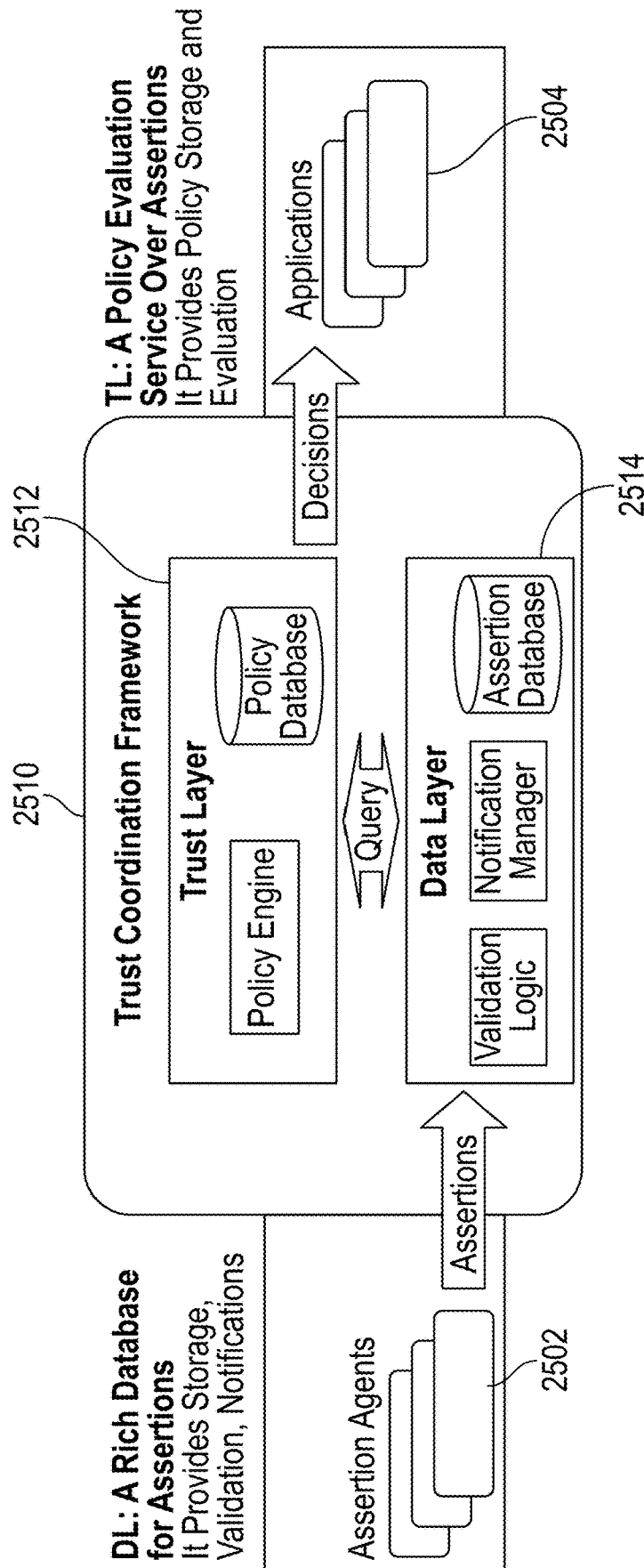


FIG. 25

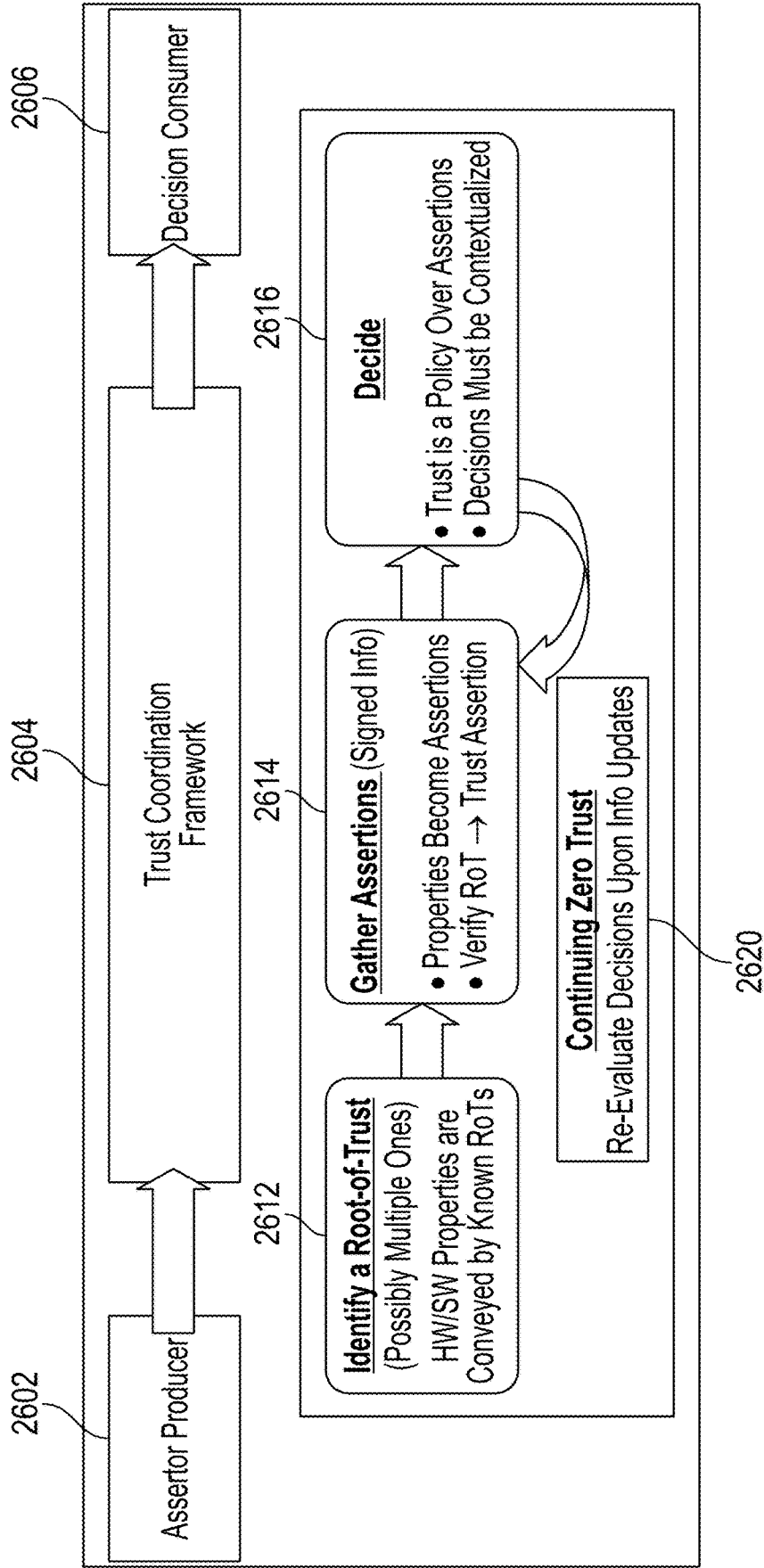


FIG. 26

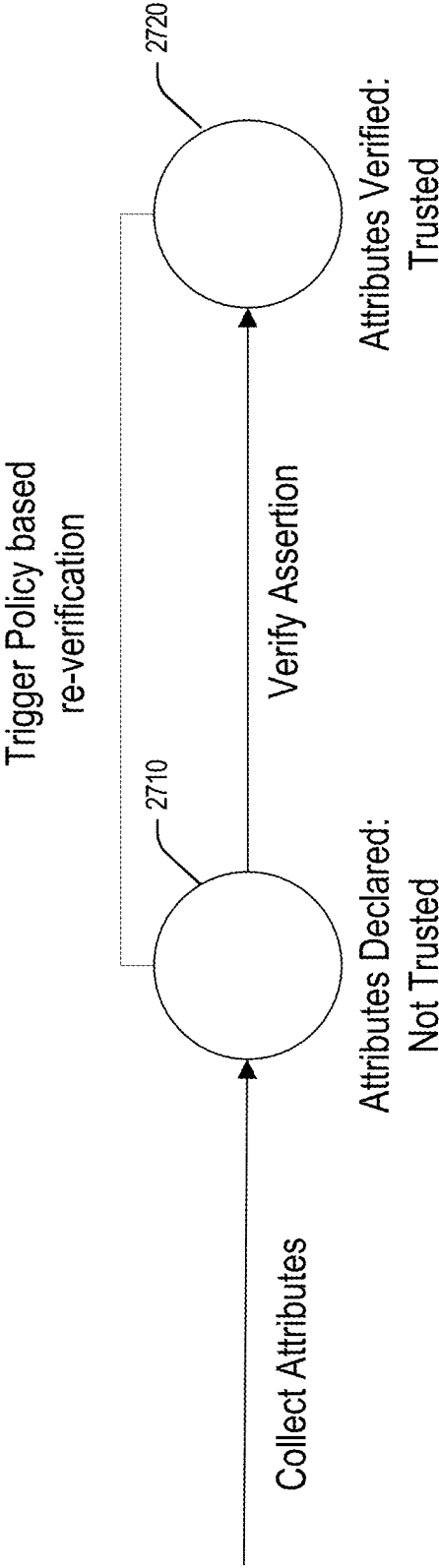


FIG. 27

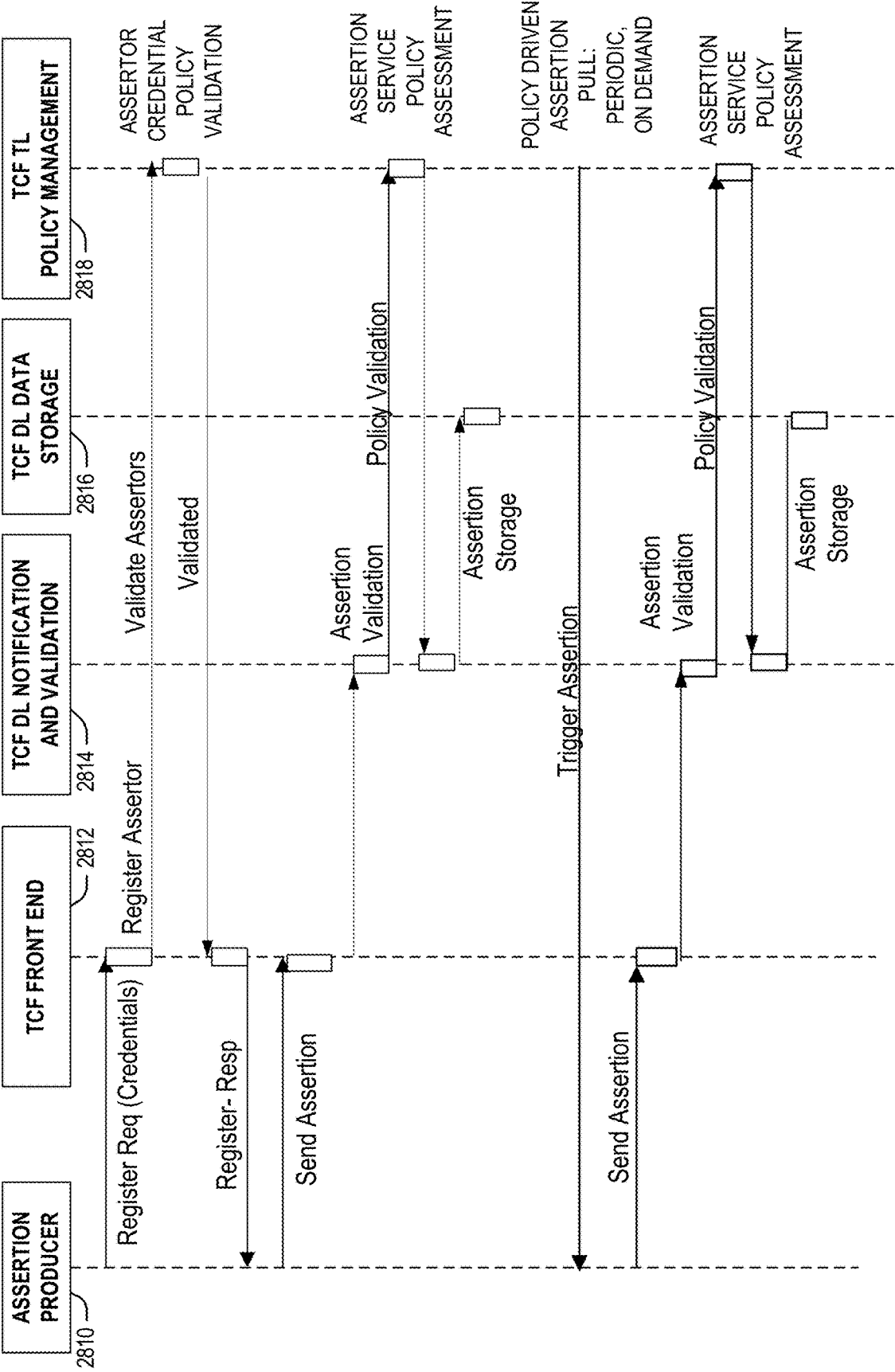


FIG. 28

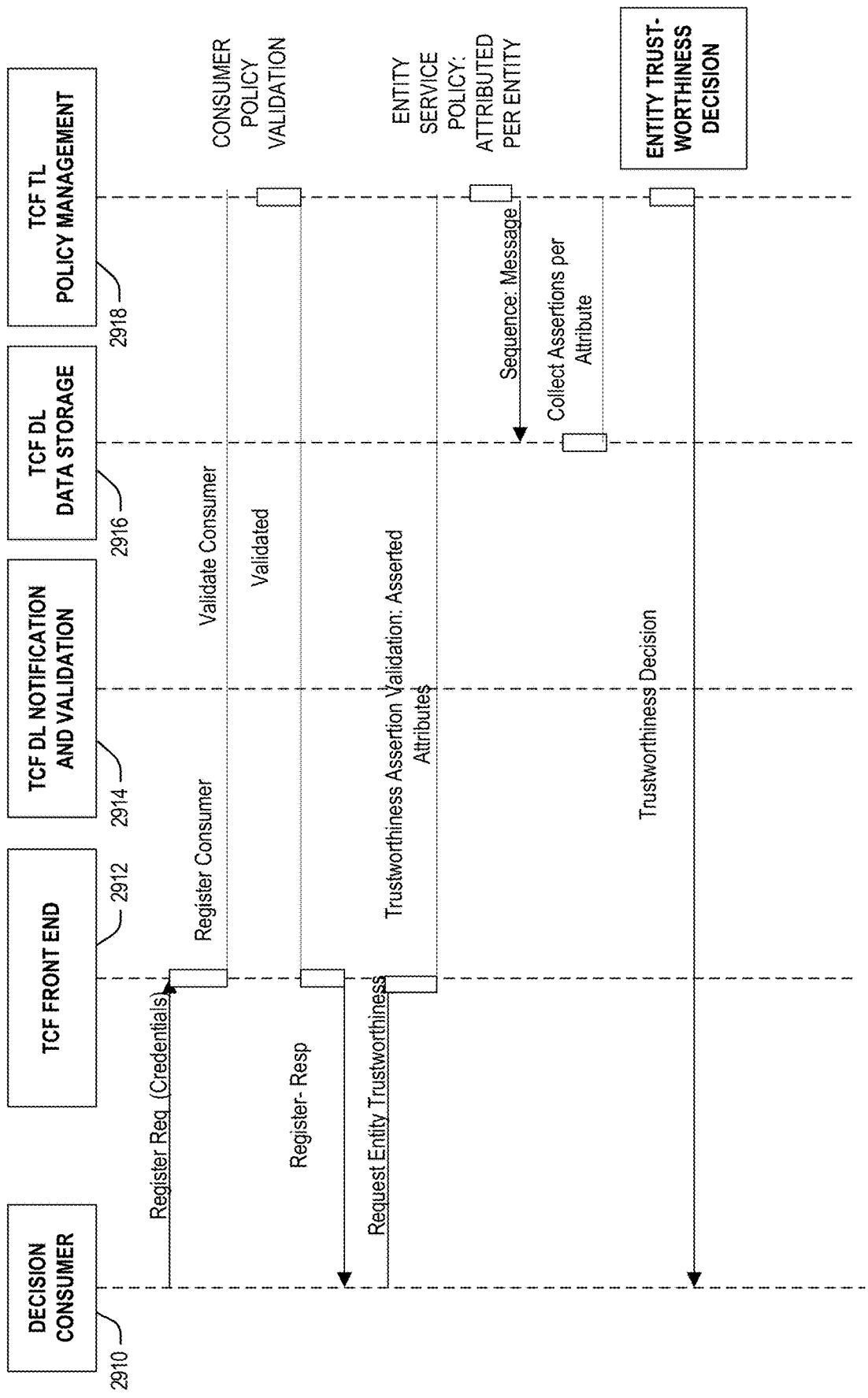


FIG. 29

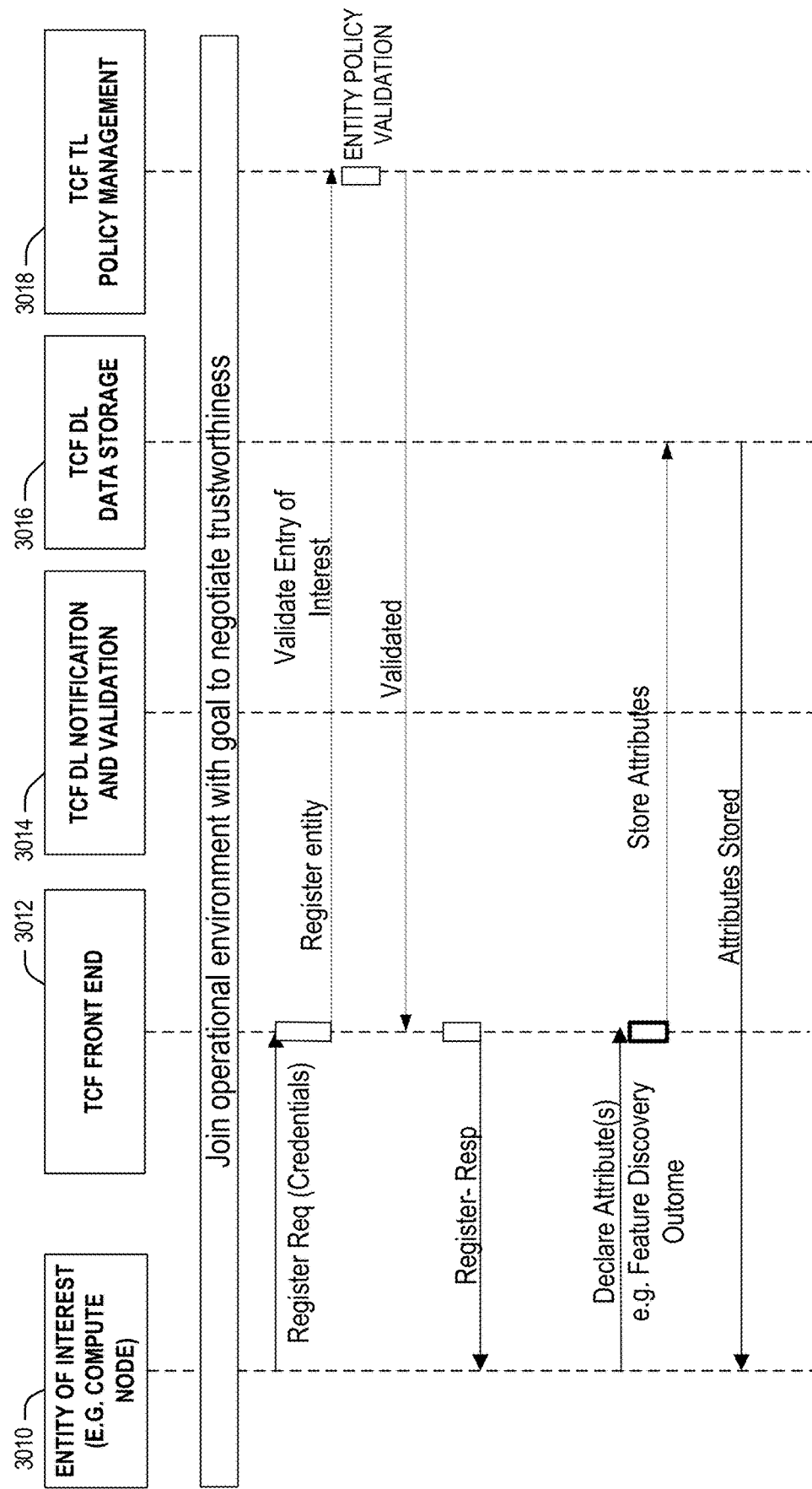


FIG. 30

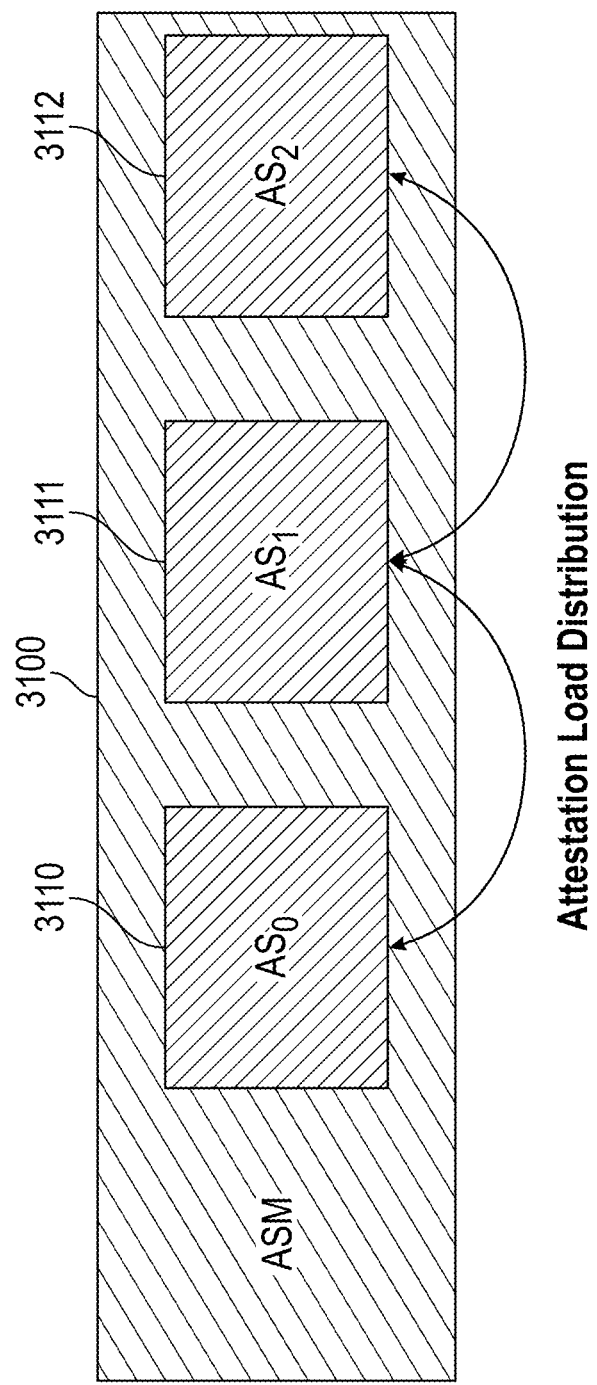
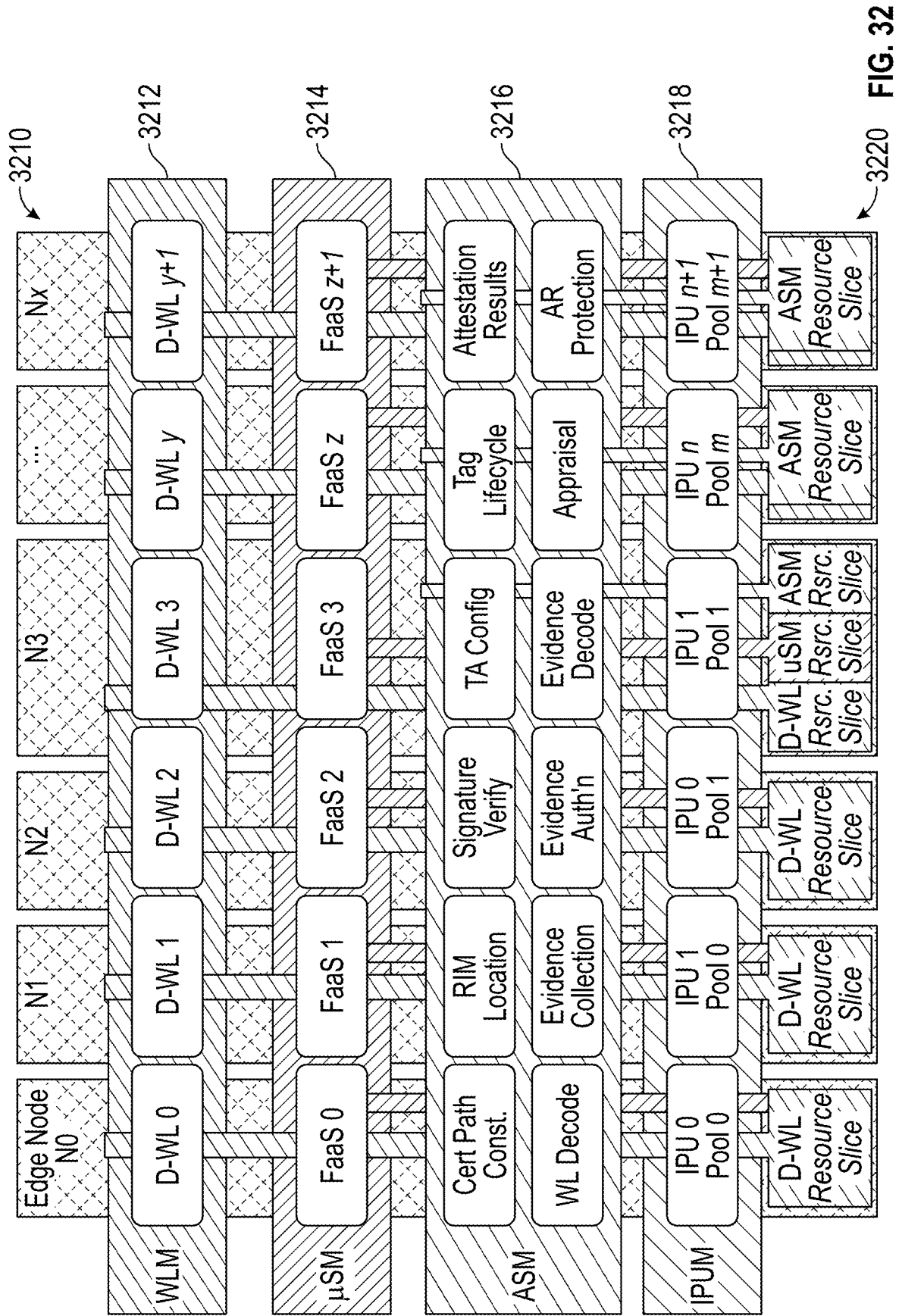


FIG. 31



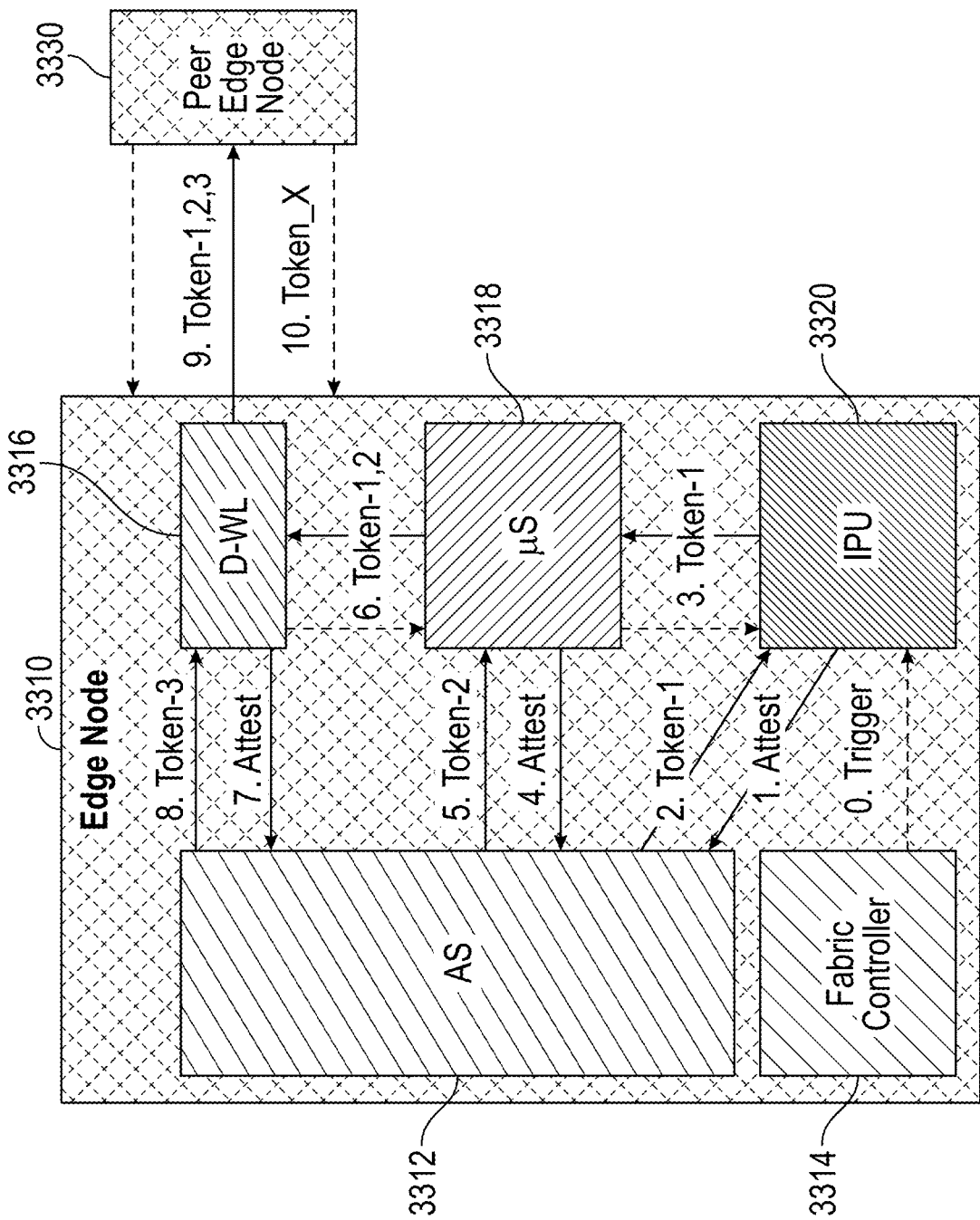


FIG. 33

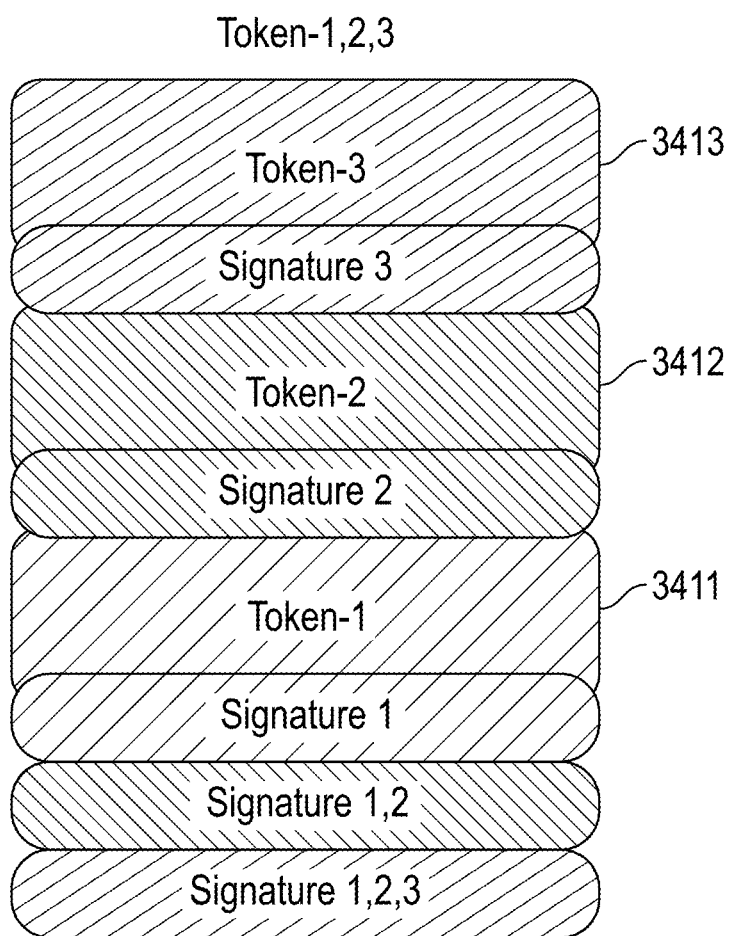


FIG. 34

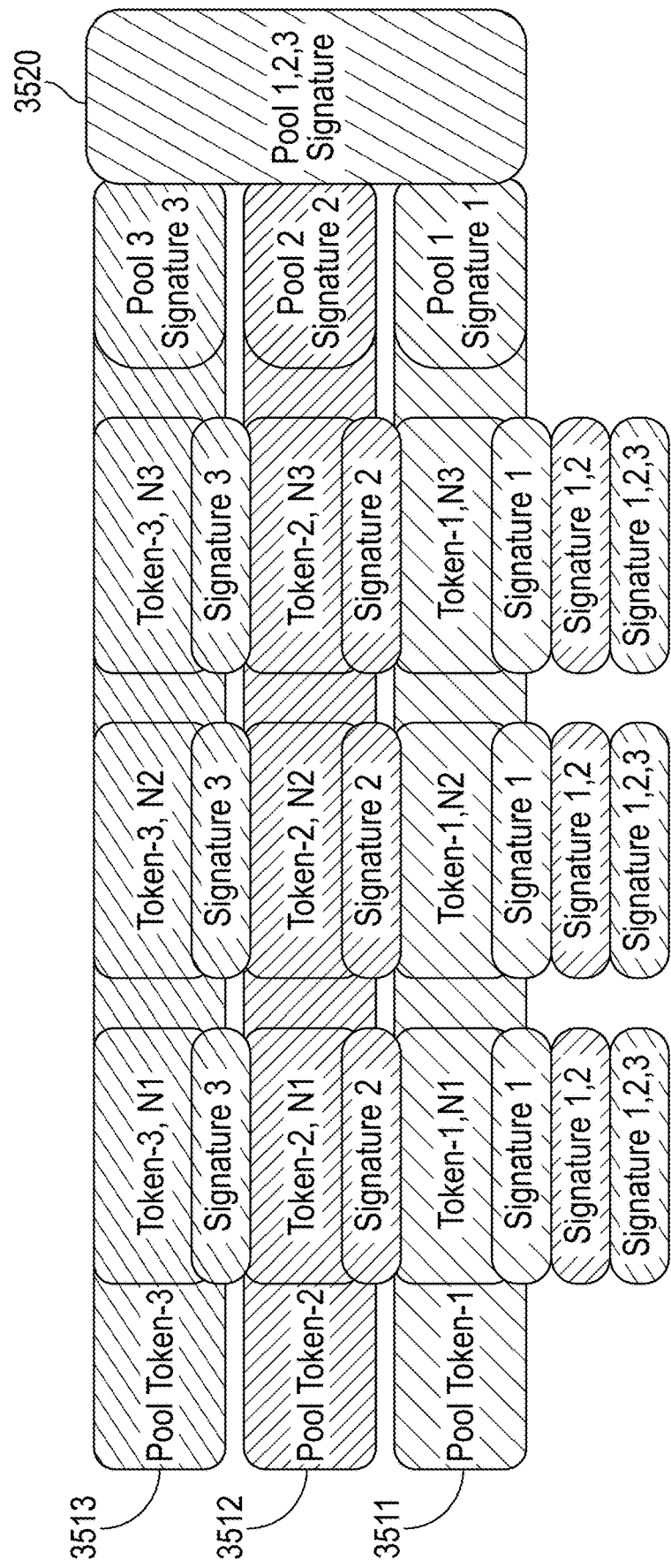


FIG. 35

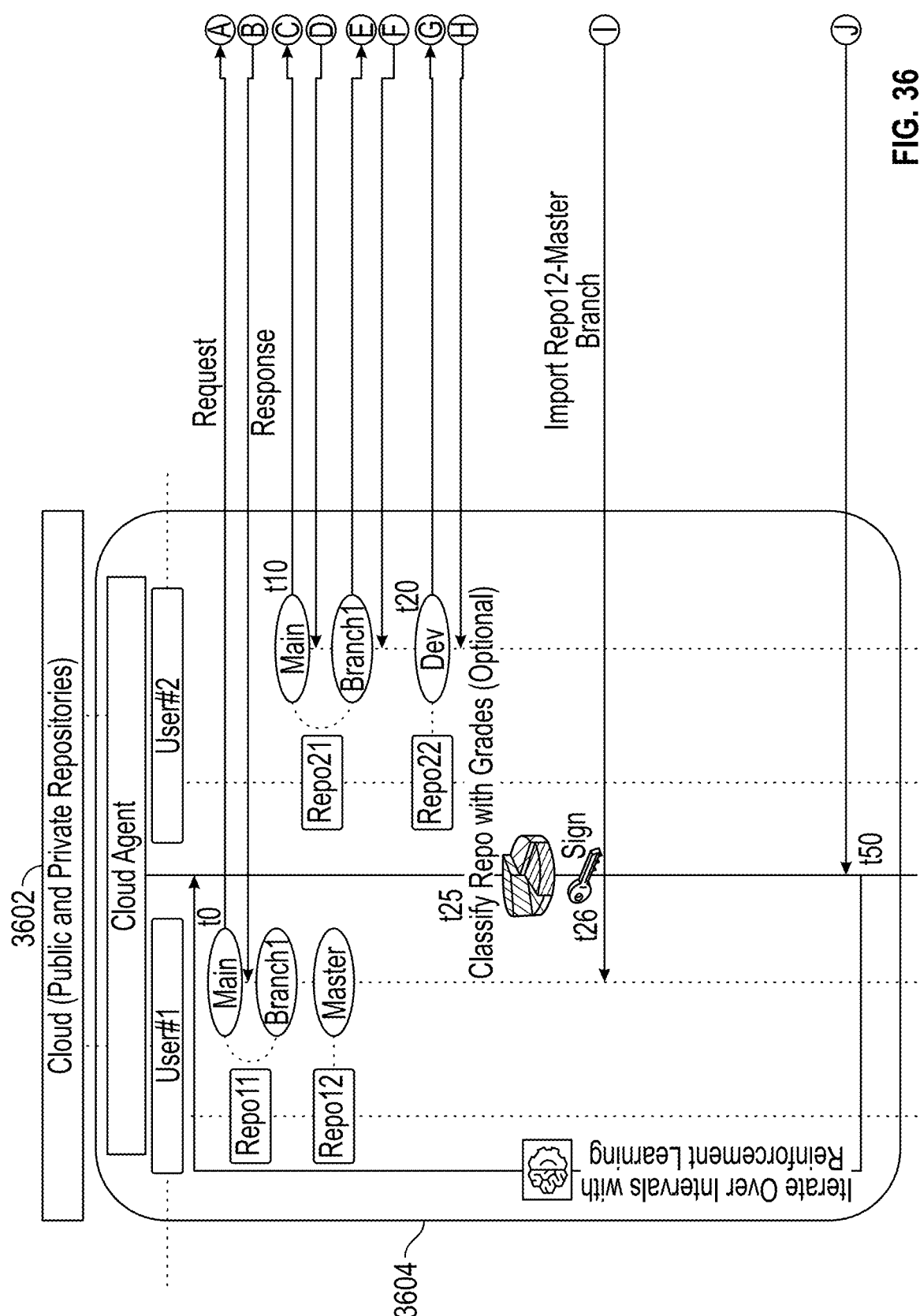


FIG. 36

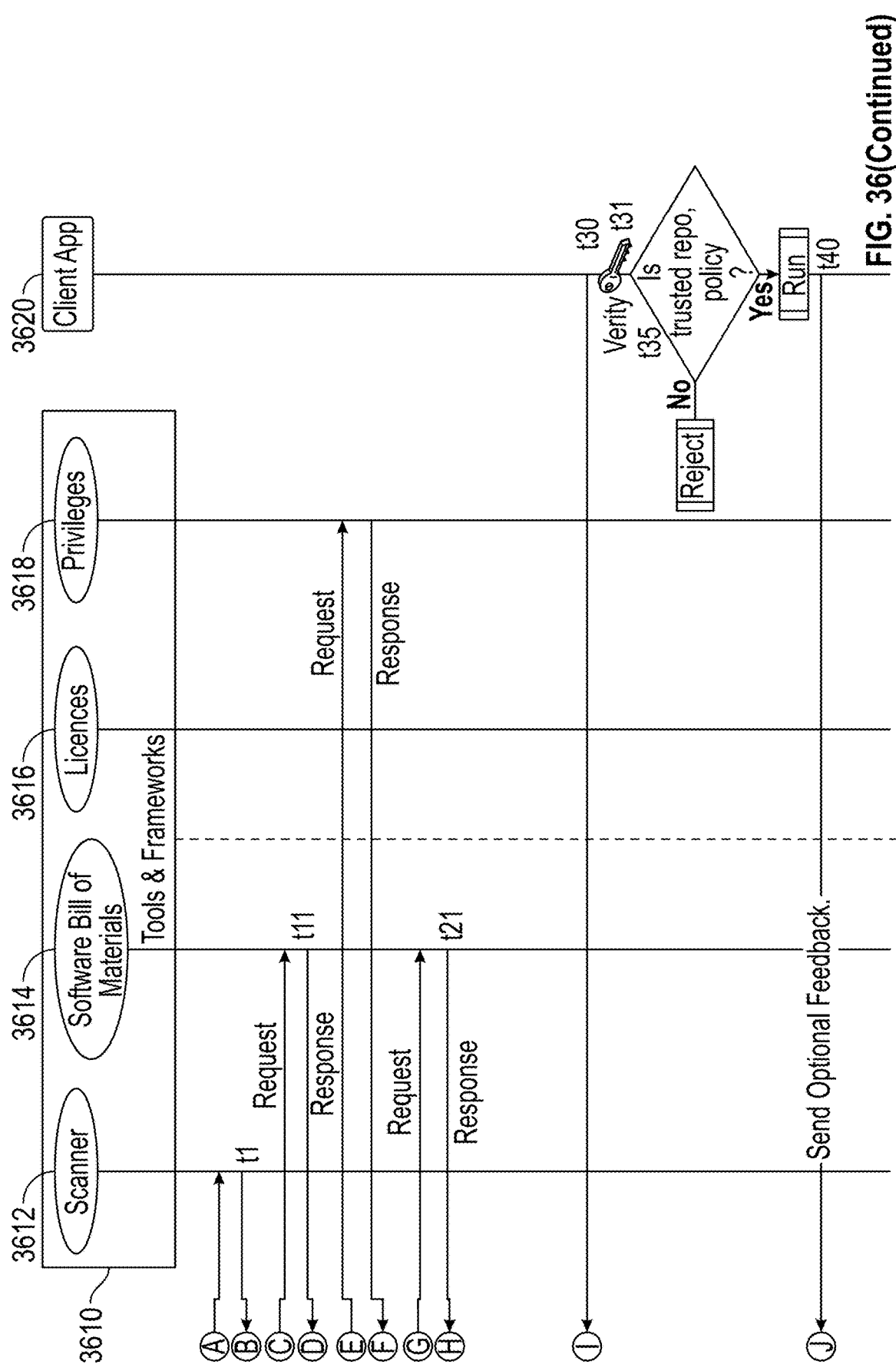


FIG. 36(Continued)

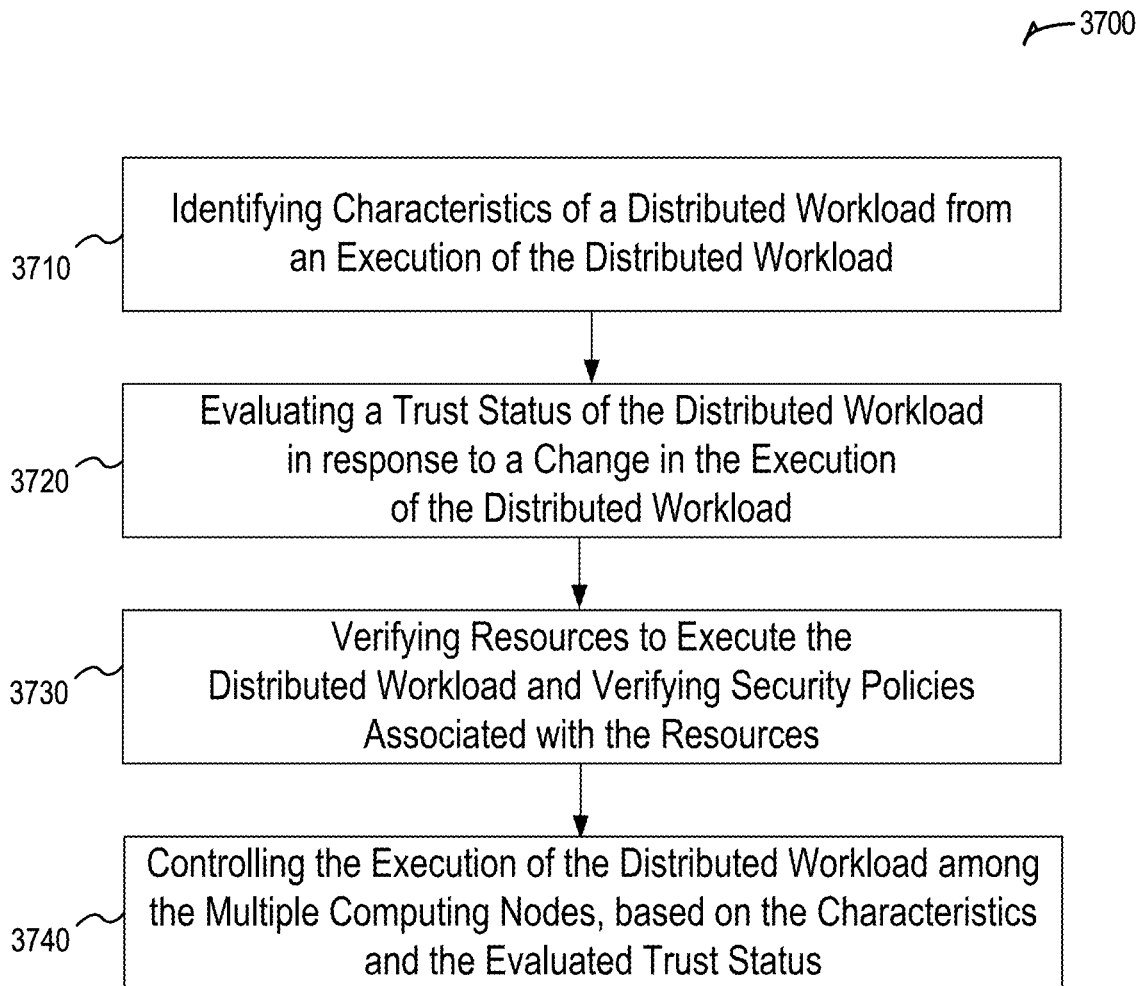


FIG. 37

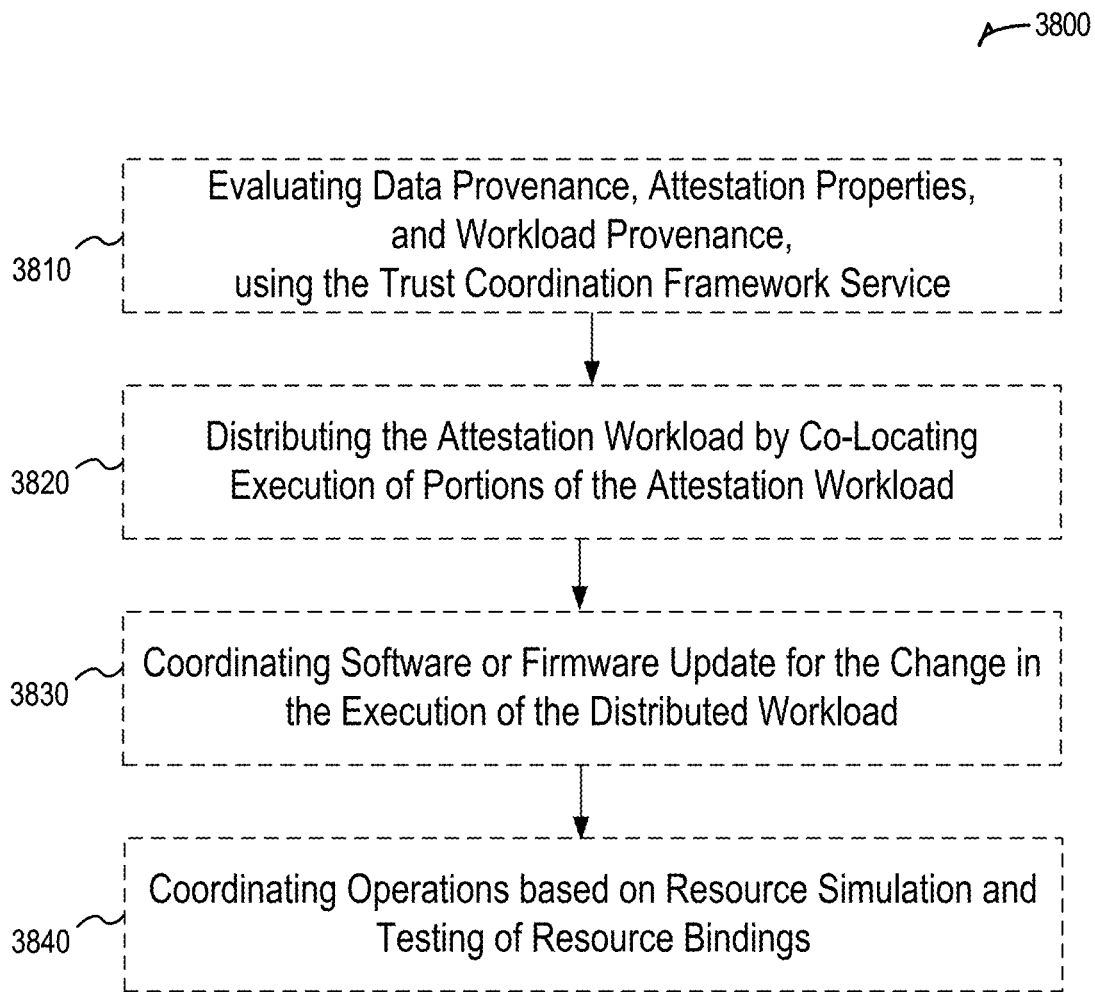


FIG. 38

3900

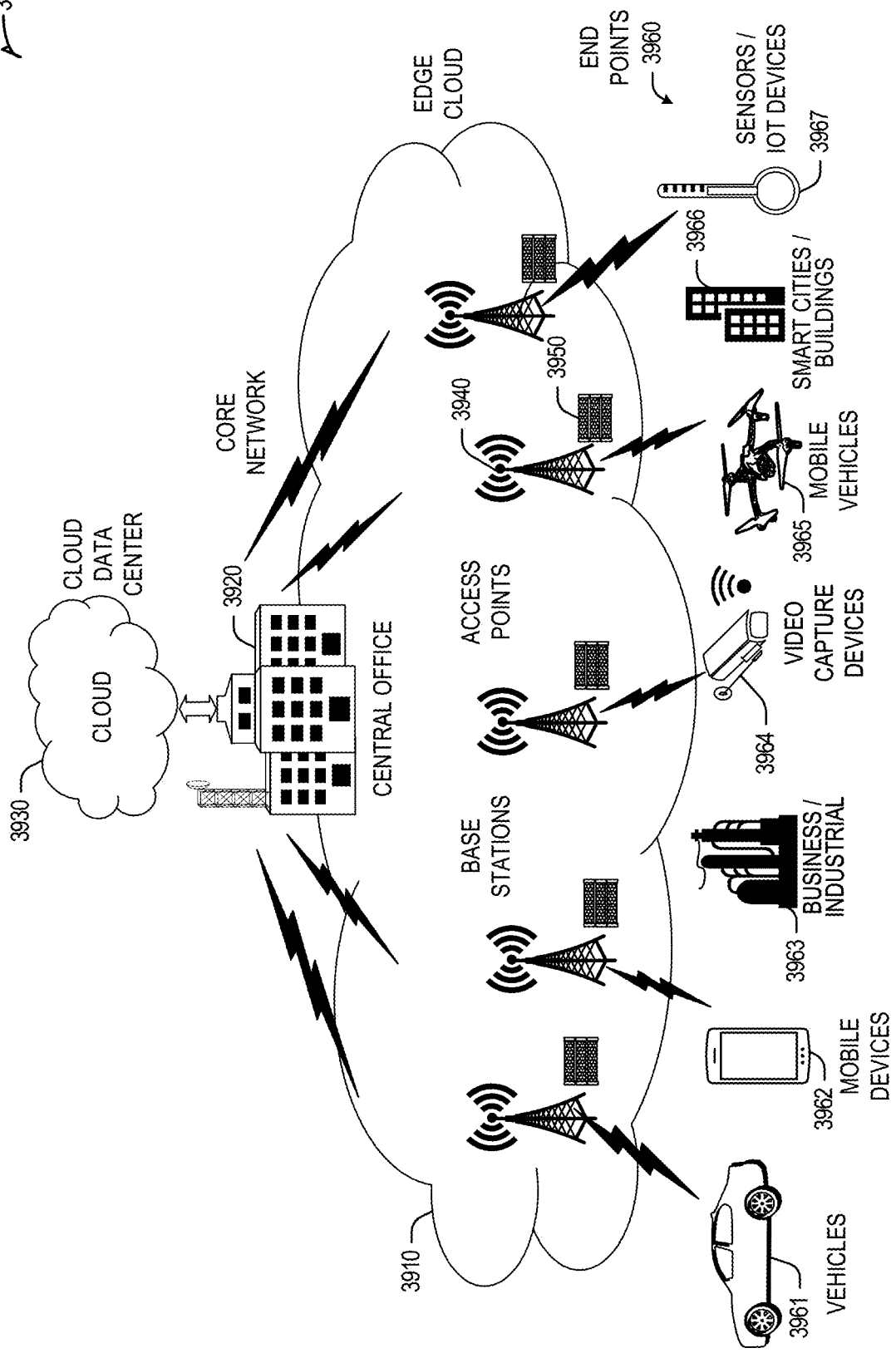


FIG. 39

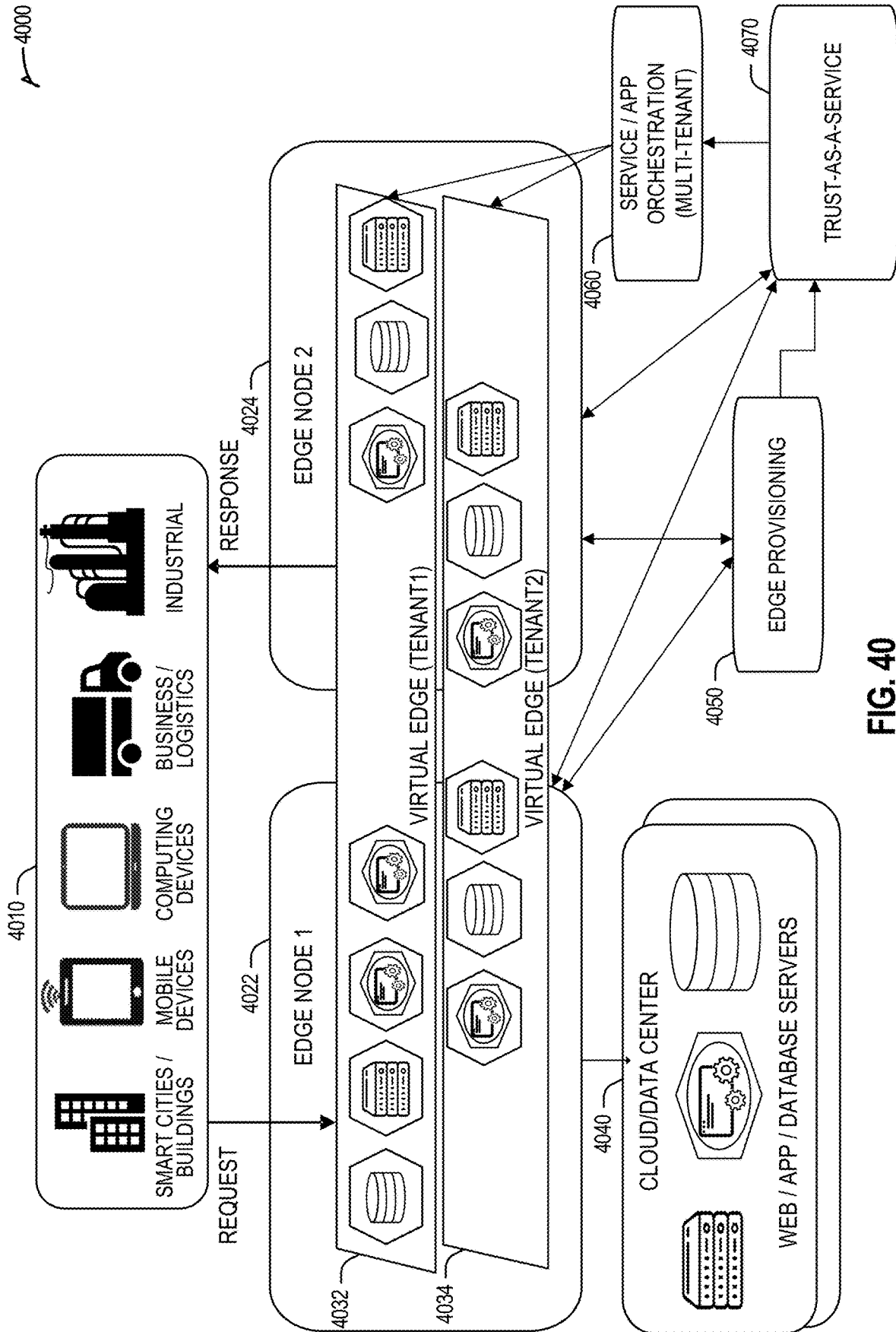


FIG. 40

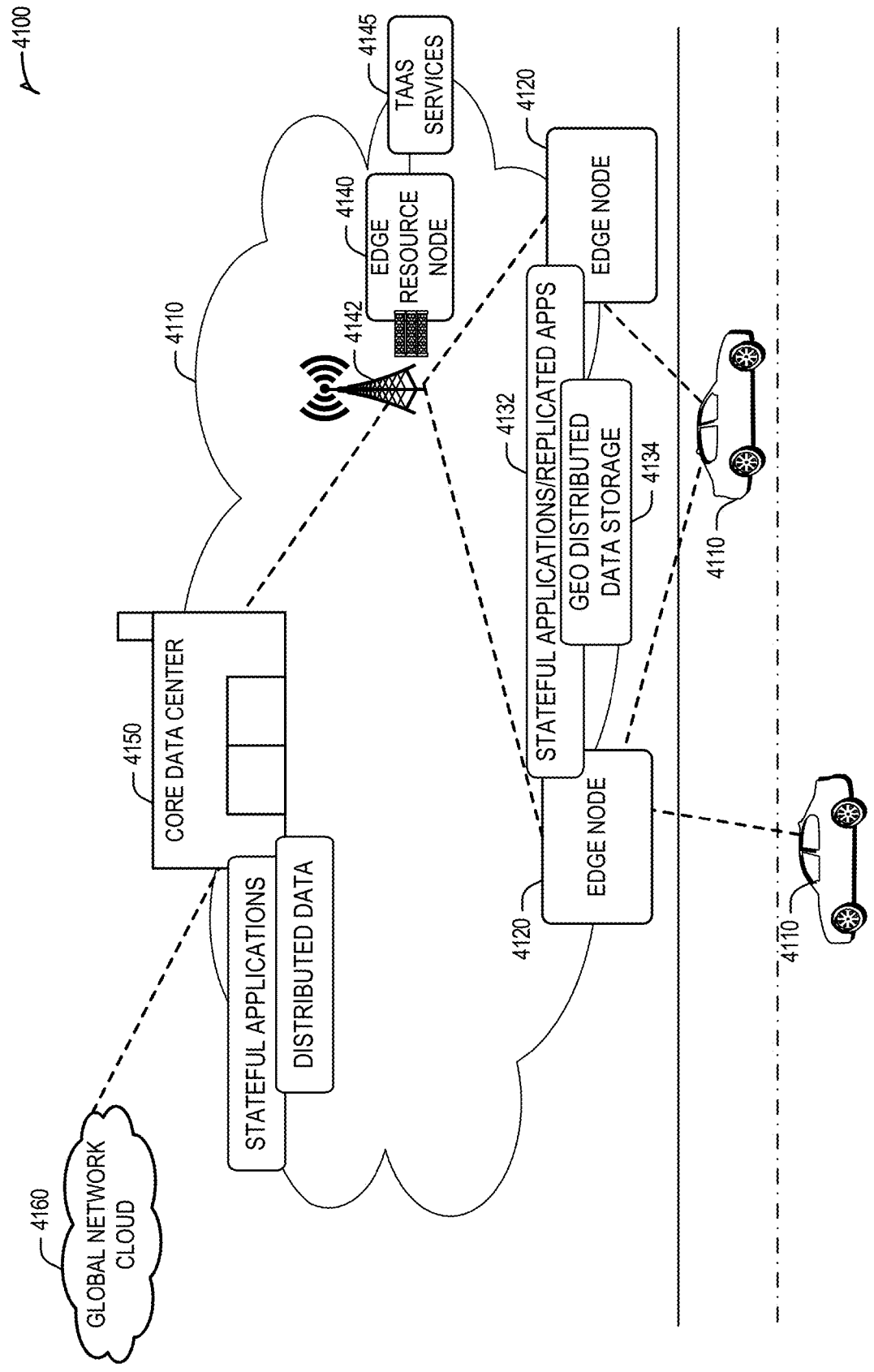


FIG. 41

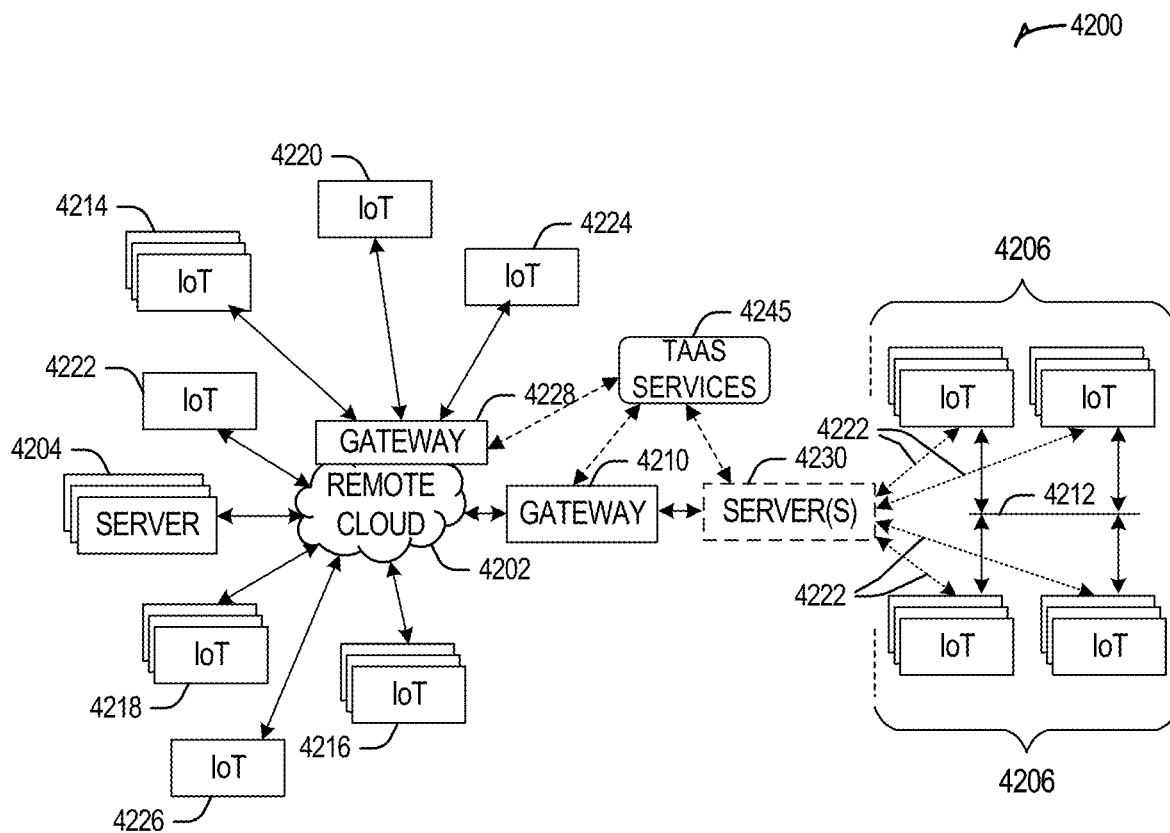


FIG. 42

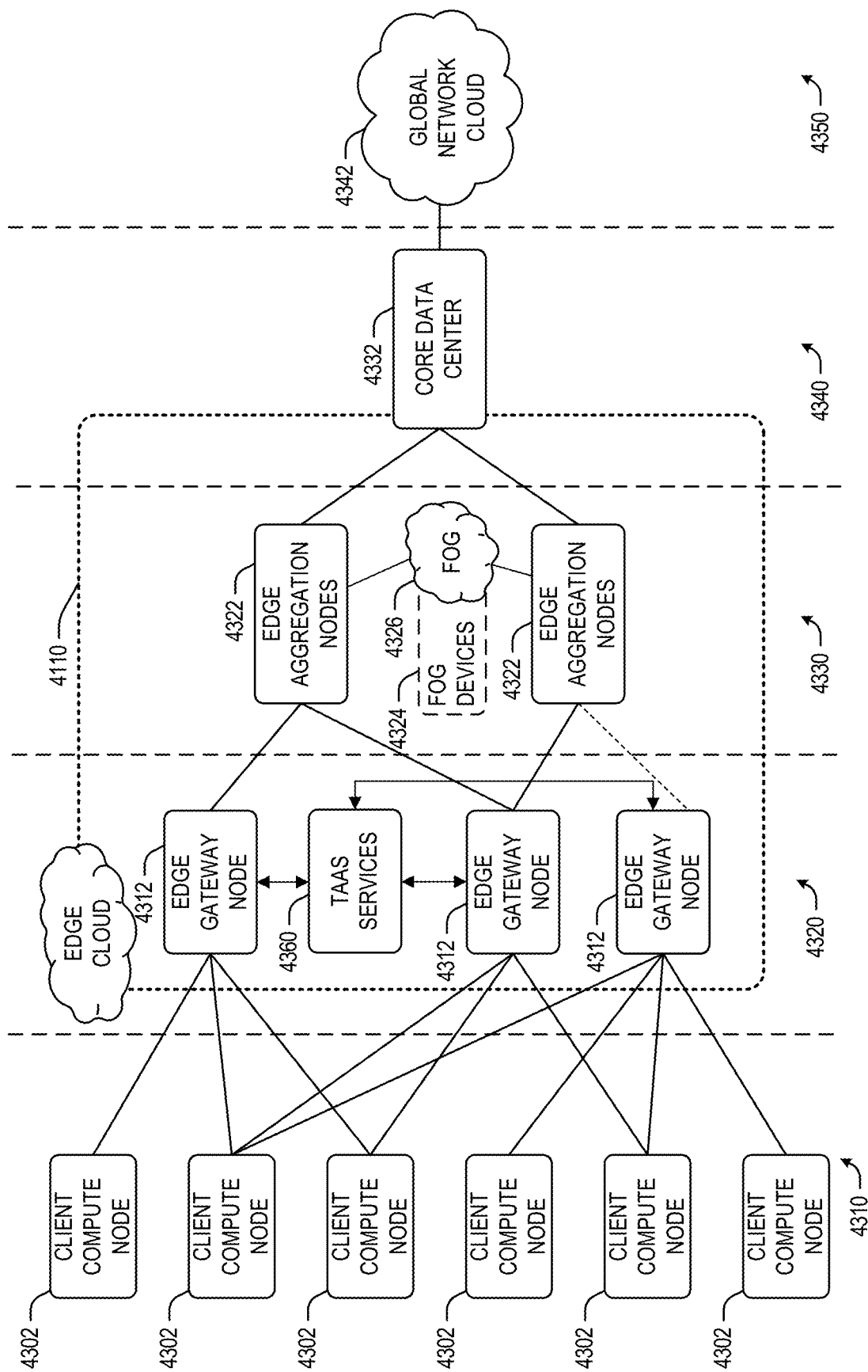


FIG. 43

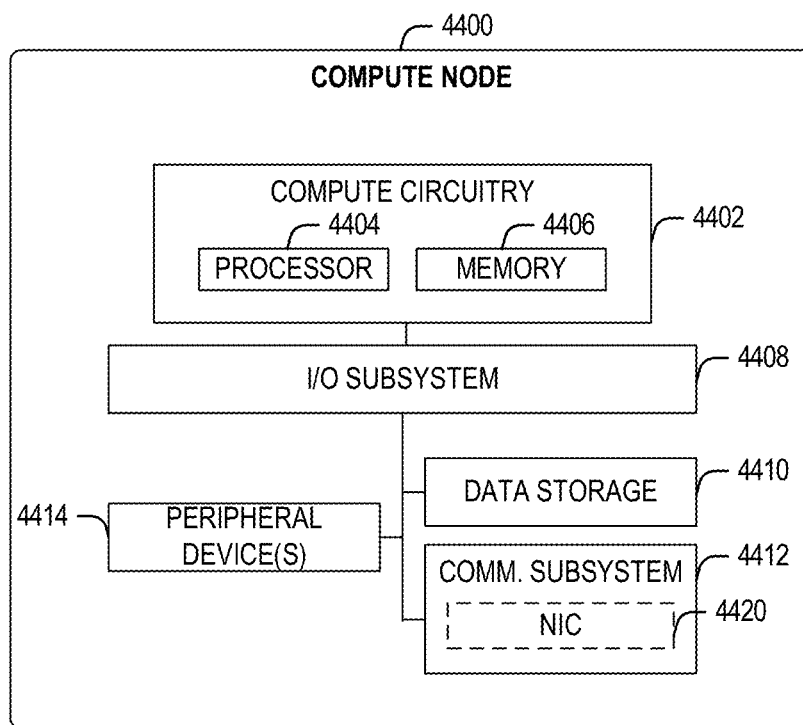


FIG. 44

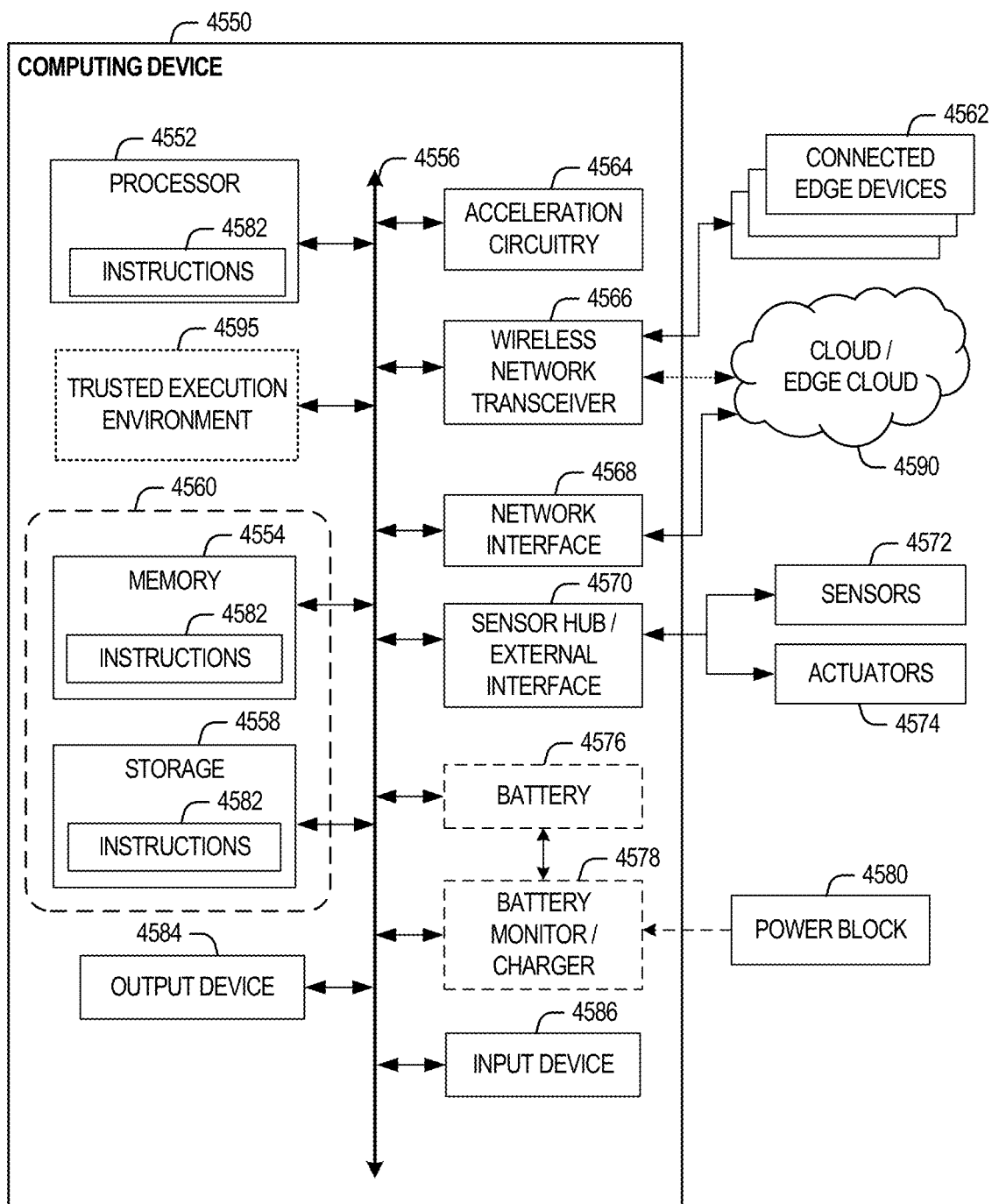


FIG. 45

4600

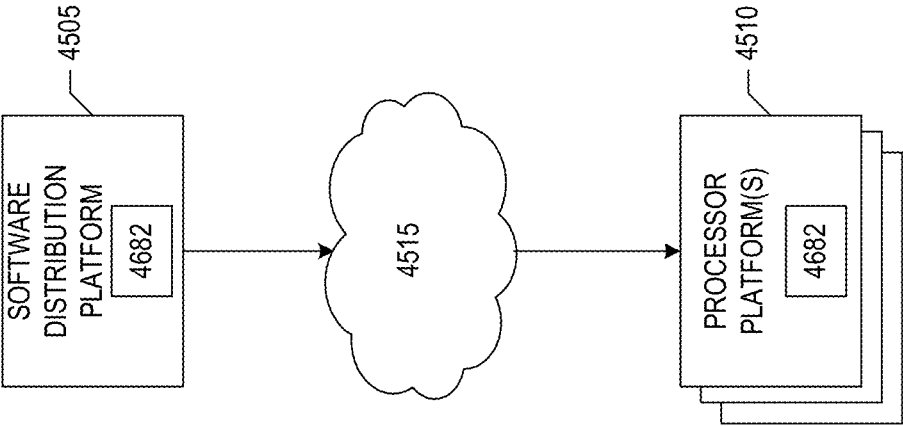


FIG. 46

SECURITY AND RESILIENCY FOR CLOUD TO EDGE DEPLOYMENTS

PRIORITY CLAIM

[0001] This application claims the benefit of priority to U.S. Provisional Patent Application No. 63/456,310, filed Mar. 31, 2023, and titled “CLOUD TO EDGE SECURITY”, which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] Edge computing, at a general level, refers to the transition of compute and storage resources closer to end-point devices (e.g., consumer computing devices, user equipment, etc.), in order to optimize total cost of ownership, reduce application latency, improve service capabilities, and improve compliance with compute security or data privacy requirements. Edge computing may, in some scenarios, provide a cloud-like distributed service that offers orchestration and management for applications among many types of storage and compute resources.

[0003] Some implementations of edge computing have been referred to as the “edge cloud” or the “fog,” as powerful computing resources previously available only in large remote data centers are moved closer to endpoints and made available for use by consumers at the “edge” of the network. The use of edge computing, and the many flavors of distributed or centralized cloud computing, have led to a variety of technical issues involving security, reliability, and resource usage.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] In the drawings, which are not necessarily drawn to scale, like numerals may describe similar components in different views. Like numerals having different letter suffixes may represent different instances of similar components. Some embodiments are illustrated by way of example, and not limitation, in the figures of the accompanying drawings in which:

[0005] FIG. 1 is a block diagram illustrating a trusted cloud-to-edge services framework, according to an example;

[0006] FIG. 2 is a block diagram illustrating the components of a Container-as-a-Service layer, according to an example;

[0007] FIG. 3 is a block diagram illustrating the components of a Platform-as-a-Service layer, according to an example;

[0008] FIG. 4 is a block diagram illustrating the components of an Infrastructure-as-a-Service layer, according to an example;

[0009] FIG. 5 is a block diagram illustrating various Infrastructure-as-a-Service layers and trust management capabilities, according to an example;

[0010] FIG. 6 is a block diagram illustrating a workflow of a workload, according to an example;

[0011] FIG. 7 is a block diagram illustrating a method of binding a workload to a procedure, according to an example;

[0012] FIG. 8 is a block diagram illustrating an elastic workload distribution plan involving a workload distribution manager interacting with pod managers, according to an example;

[0013] FIG. 9 is a block diagram illustrating an elastic workload update manager, according to an example;

[0014] FIG. 10 is a block diagram that illustrates a save-restore workflow, according to an example;

[0015] FIG. 11 is a block diagram illustrating a classical workload testing infrastructure, according to an example;

[0016] FIG. 12 is a block diagram illustrating an elastic workload testing and resource simulation framework, according to an example;

[0017] FIG. 13 is a block diagram illustrating a cloud-edge cluster, according to an example;

[0018] FIG. 14 is a block diagram illustrating a cloud-edge cluster after provisioning a distributed workload, according to an example;

[0019] FIG. 15 is a block diagram illustrating updated packages for top and bottom half components in a distributed edge cluster, according to an example;

[0020] FIG. 16 is a block diagram illustrating remote cloud-to-edge node migration, according to an example;

[0021] FIG. 17 is a block diagram illustrating local preemptive migration, according to an example;

[0022] FIG. 18 is a diagram illustrating the elements of a hyperconnected compute continuum, according to an example;

[0023] FIG. 19 is a diagram illustrating trust coordination, according to an example;

[0024] FIG. 20 illustrates the use of a trust coordination as a service, according to an example;

[0025] FIG. 21 illustrates existing approaches and the advancement to a trust coordination framework, according to an example;

[0026] FIG. 22 is a diagram illustrating interoperability of the trust coordination service, according to an example;

[0027] FIG. 23 is a block diagram illustrating a general hierarchy of classes and attributes, according to an example;

[0028] FIG. 24 is a block diagram illustrating a specific hierarchy of classes and attributes, according to an example;

[0029] FIG. 25 is a block diagram illustrating a trust coordination framework architecture, according to an example;

[0030] FIG. 26 is a block diagram illustrating high-level operations in a trust coordination framework architecture, according to an example;

[0031] FIG. 27 is a block diagram illustrating state transitions of trustworthiness attributes, according to an example;

[0032] FIGS. 28-30 are swim lane diagrams illustrating interactions between components of a trust coordination framework architecture, according to various examples;

[0033] FIG. 31 is a block diagram illustrating attestation load distribution, according to an example;

[0034] FIG. 32 is a block diagram illustrating an elastic workload mesh architecture, according to an example;

[0035] FIG. 33 is a block diagram illustrating attestation of a distributed workload using an attestation mesh, according to an example;

[0036] FIG. 34 is a block diagram illustrating an attestation mesh token structure, according to an example;

[0037] FIG. 35 is a block diagram illustrating a fully articulate attestation mesh token, according to an example;

[0038] FIG. 36 is a swim lane diagram illustrating interactions between entities to build a trusted repository, according to an example;

[0039] FIG. 37 is a flowchart illustrating operations for managing distributed workloads in an edge computing environment, according to an example;

[0040] FIG. 38 is a flowchart illustrating operations for adapting execution of distributed workloads in an edge computing environment, according to an example;

[0041] FIG. 39 illustrates an overview of an edge cloud configuration for edge computing, according to an example;

[0042] FIG. 40 illustrates deployment and orchestration for virtual edge configurations across an edge-computing system operated among multiple edge nodes and multiple tenants, according to an example;

[0043] FIG. 41 illustrates a vehicle compute and communication use case involving mobile access to applications in an edge-computing system, according to an example;

[0044] FIG. 42 illustrates a block diagram depicting deployment and communications among several Internet of Things (IoT) devices, according to an example;

[0045] FIG. 43 illustrates an overview of layers of distributed compute deployed among an edge computing system, according to an example;

[0046] FIG. 44 illustrates an overview of example components deployed at a compute node system, according to an example;

[0047] FIG. 45 illustrates a further overview of example components within a computing device, according to an example; and

[0048] FIG. 46 illustrates a software distribution platform to distribute software instructions and derivatives, according to an example.

DETAILED DESCRIPTION

[0049] In the following description, methods, configurations, and related apparatuses are disclosed for implementation in a cloud-to-edge (C2E) framework. As used herein, “cloud-to-edge” generally refers to functionality to move workloads and capabilities that were traditionally located in a cloud computing setting towards distributed edge computing locations. Such functionality is particularly applicable to the deployment and execution of elastic workloads (WLs), which involve workloads that are distributed across multiple nodes, migrated, and dynamically coalesced again—independent of a workload orchestrator.

[0050] Edge computing has introduced scenarios involving elastic workloads where a traditional monolithic workload, which may run on a single Edge node, may be decomposed into two or more sub-workloads that are distributed across multiple Edge nodes. The distributed workload may be partially or fully consolidated or decomposed even further to accommodate the changing resource dynamics of edge-cloud deployments for both stationary and mobile users and user equipment, or stationary and mobile edge nodes. These dynamics creates an environment for elastic edge computing capabilities that include dynamic binding of workloads, resources, and compute.

[0051] Trusted Cloud-to-Edge Framework

[0052] The use of elastic WLs is designed to provide flexibility to accommodate distribution and dynamism inherent in edge computing. A dynamic C2E framework is needed to ensure that trust within a complex elastic WL infrastructure is preserved throughout the many types of WL configurations and use cases.

[0053] Existing container-as-a-service (CaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) capabilities expect that trust is established statically at an initial deployment of a WL, and such capabilities generally will not re-evaluate trust during WL execution. The dynam-

ics of an elastic WL in an C2E deployment, however, change the WL from being a monolithic WL to a distributed WL having dynamic properties that distribute the WL processing across multiple nodes. This is further complicated because nodes may dynamically migrate to other hosting environments at lower framework layers, resulting in broken trust semantics.

[0054] The systems and methods described herein implement an elastic WL framework with security and trust capabilities at operational layers involving workload execution environments (e.g., containers, virtual machines, etc.), platforms, and infrastructure, and these layers’ associated services (Container-as-a-Service (CaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)). The following systems and methods introduce a Trust Binding Manager to actively monitor and apply trust bindings between the artifacts at respective layers that require consistent trust properties, while responding to dynamic conditions that otherwise will break trust properties. This enables elastic WL frameworks to establish and preserve intended trust properties of a WL throughout the WL execution and lifecycle despite the occurrence of dynamic changes in resources, location, and data sources/sinks.

[0055] A trusted C2E services framework for elastic workloads is adapted as follows to ensure various “anything-as-a-service” (X-aaS) capabilities in a services framework. This is used to establish and maintain trust within the respective framework layers, e.g., CaaS, PaaS, and IaaS, and between C2E framework layering, e.g., CaaS to PaaS, and PaaS to IaaS. The Trust Binding Manager component is used to establish and maintain trust properties for an elastic WL that is implemented using a trusted C2E framework. The C2E framework integrates a Trust Binding Manager component that enables creation, simulation, deployment, and maintenance of trusted elastic WLs following a WL lifecycle.

[0056] FIG. 1 is a block diagram illustrating an example of a trusted cloud-to-edge (C2E) services framework 100, according to an example. The trusted C2E services framework 100 includes a Container-as-a-Service (CaaS) layer 102, a Platform-as-a-Service (PaaS) layer 104, and an Infrastructure-as-a-Service (IaaS) layer 106, which are managed by using trust bindings 108.

[0057] The CaaS layer 102 creates a uniform abstraction for describing a workload that is independent of a particular platform. A distributed WL may partition the WL into logical sub-workloads that are related by a workflow model where the partial results from one sub-workload may be input to another sub-workload. The workflow may divide WL computations into execution operations that are in a particular sequence or in a particular concurrence. An individual sub-workload should have the same trust semantics as the monolithic WL. Monolithic WL trust may be established as part of an SLA (service level agreement) between the WL tenant and a WL service provider. Elastic WL execution may result in a distributed WL having multiple sub-workloads hosted by many nodes. The WL partitioning and execution workflow may introduce challenges to trust where the expected trust agreed to initially as part of an SLA agreement may disappear due to differences in platform and infrastructure options introduced by PaaS and IaaS framework layers.

[0058] FIG. 2 is a block diagram illustrating the components of an example CaaS layer (e.g., corresponding to layer

102), according to an example. Here, a pod 202 is used to deploy multiple containers (labeled as container 0 to container n). Functionality used in the CaaS layer includes a pod manager 204, pod storage 206, and pod key management 208. The features discussed herein introduce the use of trusted C2E capabilities 210 for the CaaS layer, which include but are not limited to: pod discovery; container provisioning; container deployment; and container update or migration.

[0059] Returning to FIG. 1, the PaaS layer 104 creates a uniform platform abstraction that facilitates workload deployment where the sub-workload fragments of a distributed workload execute within one or more virtual and physical platform environments. The PaaS layer 104 abstraction hides hardware, system software, and cloud platform specific artifacts so that the workload designer does not need to adapt the workload to differences found at lower layers. The PaaS layer 104 abstraction also hides trust properties inherent to lower layers resulting in workloads that ignore the risks associated with untrusted hosting environments. In general, PaaS may depend on additional infrastructure layers that may themselves have layer abstractions and packaged as services (e.g., IaaS, hardware-as-a-service (HWaaS), etc.). Workload designers may not be aware of the various deployment options available at infrastructure layers. The services ecosystem may outsource some or all of workload deployment to a services abstraction. Consequently, workload security policies may need to be adapted, translated, and negotiated to the specific security postures at respective infrastructure layers and with respective service providers.

[0060] FIG. 3 is a block diagram illustrating the components of a PaaS layer (e.g., corresponding to layer 104), according to an example. Here, a PaaS layer 302 includes a variety of APIs, functions, and services to host and operate the platform. The PaaS layer 302 is operably coupled with a user (e.g., services user) dashboard UI 304 and an operator (e.g., administrator) dashboard UI 306 to invoke use of these APIs, functions, and services. The features discussed herein introduce the use of trusted C2E capabilities 310 for the PaaS layer, which include but are not limited to: node feature discovery; state change monitoring; attestation; telemetry; trust policy management; and trust services (e.g., in a “trust-as-a-service” or “TaaS” implementation).

[0061] Returning to FIG. 1, the IaaS layer 106 creates a uniform interface for allocating WL resources, e.g., compute, memory, storage, and communication that satisfy expected performance and availability requirements as specified by an SLA. The infrastructure has physical security properties such as a hardware root of trust (RoT), secure storage for keys, trusted software, and protection of secret data. Mechanisms for discovering and attesting the trustworthiness properties of the IaaS resources need to be built into the IaaS infrastructure or trust in the upper C2E framework layers cannot be guaranteed.

[0062] FIG. 4 is a block diagram illustrating the components of an IaaS layer (e.g., corresponding to layer 106), according to an example. The IaaS layer 402 of FIG. 4 depicts the use of co-located computing resources 404, and on-premise computing resources 406. A variety of types of computing scenarios involving virtual machines, operating systems, and hardware is also depicted. The features discussed herein introduce the use of trusted C2E capabilities 410 for the IaaS layer, which include but are not limited to:

a trust agent; trust chaining (including multiple instances of such trust chaining); and a hardware root of trust.

[0063] The systems and methods described herein provide CaaS, PaaS, and IaaS layers with trusted computing capabilities that ensures the security and trust properties of the workload are represented and enforced at appropriate CaaS, PaaS, and IaaS layers. With use of the aforementioned trusted C2E capabilities, security and trust can be provided even if every infrastructure layer has an X-aaS abstraction.

[0064] FIG. 5 is a block diagram illustrating additional aspects of IaaS layers and trust management capabilities, according to an example. The IaaS layers 500 depicted in FIG. 5 may include aspects such as: an API layer 501; a services layer 502; an admin layer 503; a Fabric-as-a-Service layer 504; an Edge-as-a-Service layer 505; and a Hardware-as-a-Service layer 506.

[0065] The IaaS layers 500 are adapted to provide trusted computing capabilities, using features of a trusted IaaS environment 510 that are supplied by trusted hardware. The relevant trusted computing capabilities include but are not limited to: HW roots of trust, trusted execution environments, edge attestation, attestation evidence collector/lead attester (e.g., “PaRoT”), pre-attested functions, trusted telemetry collection, update management, appraisal policies, evidence policies, attestation ecosystem roles, and interfaces for the underlying trust, management, and telemetry capabilities.

[0066] FIG. 6 is a block diagram illustrating a workflow of a workload, according to an example. The C2E framework provides trust capabilities that are also integrated in a PaaS layer 604, with the use of a trust binding manager 606. The trust binding manager 606 links trusted resources with trusted containers such that the binding between a container, platform, and resource is verifiable by another entity such as an attestation verifier service 610. This enables an IaaS layer 608 to successfully distribute the workloads to resources at one or more edge computing locations 620.

[0067] Trust in the container begins as part of workload authoring where the WL author supplies security intents and other intents metadata 602 that describes the parameters of trust such as expected attestation values and results. Workload authoring may also include elastic WL properties that aid in decomposing a monolithic WL into distributable parts using metadata in the form of WL intents, security intents, and data intents. This metadata may describe expected or allowed WL, module, and data composition/decomposition points as well as data ingress/egress behavior for WL nodes that optimize for remote data hosting with data flow ingress/egress. Additionally, data sensitivities are described by metadata that include policies that describe safe HW and SW environments where sensitive data may be safely and confidentially manipulated such as Intel® SGX/TDX, ARM® TrustZone, AMD® SEV, etc.

[0068] FIG. 7 is a block diagram illustrating a method of binding a workload to a procedure, according to an example. The workload binding capability is performed by the trust binding manager 606 (e.g., depicted in FIG. 6) and may be facilitated by the security intents metadata 602. The example in FIG. 7 shows a security intents token 721 that describes expected trust properties that should exist between a workload container 711, e.g., ‘Module A’ and infrastructure resources supplied by IaaS ‘A’ 731. The example describes a container socket that may be satisfied by a resource exposing a resource interface that supplies the resource,

(e.g., edge-res-ID-X) and procedure (e.g., ‘Proc-X()’) that exists inside a trusted execution environment (e.g., Intel® TDX trust domain or IPU).

[0069] The trust binding manager **606** ensures that the binding occurs following an expected binding procedure, e.g., `website-for-the-iaas-platform.com/proc-X`, using an expected container socket, e.g., `socket-A@Workload-A`, with an expected isolation factor, e.g., ‘0.88’. The binding operation may produce a token that is given to WL A and presented to an IaaS resource hosting a processing unit (e.g., a networked infrastructure processing unit or “IPU”) where it is evaluated upon resource access to verify that the binding operation has taken place. The token may expire to ensure the binding operation is periodically reestablished or the token is dynamically regenerated if either the resource environment or the container environment changes in a way that affects trust.

[0070] Agile Pod Creation Following Automated Updates

[0071] Elastic WL updates are more sophisticated than traditional cloud or edge WL updates because elastic WLs may be partitioned and distributed dynamically after the orchestrator commissions the WL for execution. Elastic WLs possess metadata that describes the various ways that a WL may be partitioned and distributed such that the global execution objective remains the same after elastic partitioning and distributed hosting. Nevertheless, elastic WLs are subject to updates and patches that correct bugs, close security holes, or provide efficiency, reliability, resiliency, and availability improvements. Updates will comprehend the dynamically applied partitioning and distribution functions that have been applied or updates will likely fail. Otherwise, the partitioning and distribution optimizations may need to be backed out, and then the update can be applied before reapplying the partitioning and distribution operations, which incurs significant deployment cost.

[0072] The systems and methods described herein address gaps in workload software and firmware updates, particularly through the application of attestation and stronger platform integrity management. The broader industry is demanding these capabilities (e.g., attested workloads) as part of a “Zero-Trust Architecture”, see SP 800-207, Zero Trust Architecture, published by the NIST Computer Security Resource Center (CSRC) which defines a set of requirements and principles for trustworthy enterprise, edge and cloud deployments. In particular, the systems and methods described herein solve the problem of uncoordinated and disruptive updates for elastic WLs by leveraging elastic WL metadata that describes the ways in which a WL may be partitioned and distributed. The metadata is used to design WL update images that align with current deployments. The most appropriate update image is delivered to the currently deployed WL fragment for application/installation. The approaches include elastic WL metadata that is used to construct, distribute, and apply WL updates. The approaches include use of an elastic WL Distribution Manager (WDM), Workload Update Manager (WUM), Pod Update Manager (PUM), and other infrastructure.

[0073] If a WL—or pod of containers that implements the WL—is part of an elastic deployment (e.g., replica set), the systems and methods described herein use an API to temporarily disable the workload deployment following the approach: “do not try to adjust number of active copies.” If the instance on the machine that needs an upgrade is paused, the deployment operator would require new resources to

recreate the pod elsewhere. After the WL/Pod is upgraded, the WL/Pod in that machine is restarted. This approach saves time, overhead and cost, whereas downloading the pod image elsewhere, allocating resources, setting up IP connectivity, etc. is significant. A respective infrastructure node has a local PUM, and this local PUM interacts with a WUM that coordinates application of updates across the cluster of elastic WL containers and nodes.

[0074] FIG. 8 is a block diagram illustrating an elastic WL distribution plan involving a WDM interacting with Pod Managers **831**, **832**, **833**, according to an example. A WL distribution plan may describe the ways in which an elastic workload may be divided into WL fragments **811**, **812**, **813** such that the overall execution of the monolithic WL **810** is isomorphic to the fragmented WL. The WL fragments **811**, **812**, **813** may be distributed across edge network resources, such as Infrastructure Nodes X, Y, Z **821**, **822**, **823**. An edge hosting infrastructure may be used to host one or more of the WL fragments **811**, **812**, **813**.

[0075] A respective K8S Pod Manager may be used to manage and track multiple WL fragments hosted by a common IaaS partition. For example, an IaaS Node X **821** may host fragments (0, 1) of a WL while Node Y **822** hosts fragments (2, 3) and Node Z **823** hosts fragments (n, n+1) and so forth.

[0076] It is understood that the Elastic Infrastructure Node (EIN) may support multi-tenancy where different tenants operate their own pod of containers. Examples described herein also depict a single-tenant scenario.

[0077] FIG. 9 is a block diagram illustrating an elastic workload update manager, according to an example. The elastic WUM depicted in FIG. 9 includes a WUM **912** that receives a WL distribution plan from a WL orchestrator **910** and a WL update distribution event **901** (Operation 1), which is used to identify the distributed elastic WL nodes to target for update with the fragments **921**, **922**, **923**. An update distribution plan is created and distributed (Operation 2) to affected WL Distribution Managers (WDM **931**, **932**) that schedule affected nodes for update (Operation 3). The WDMs distribute and otherwise apply the update to affected infrastructure nodes (Node X **941**, Node Y **942**, . . . , Node Z **943**) (Operation 4), where a local pod update manager (PUM **951**, PUM **952**, PUM **953**) completes the update.

[0078] Distributed workloads in an elastic WL are images that are in various stages of a deployment lifecycle involving creation, distribution, resource binding, execution, update, coalescence, and retirement. Elastic WLs have elasticity parameters that are described by metadata (e.g., where WL node replicas can exist and where several nodes serve as redundant nodes that may perform parallel execution of a node). Additionally, pipelined execution can exist where the input of one node in an elastic WL cluster is satisfied by the output of another cluster node forming a chain of operations that execute in sequence. Elastic WL data objects may be assigned to one or more WL nodes for shared or exclusive access. A hierarchical lock structure may be used to guarantee sequential and parallel executions can occur simultaneously while still maintaining overall integrity of the elastic workload.

[0079] A WL node may have multiple execution states, (e.g., ready to run, running, blocked on hosting resource, blocked on input, blocked on output, blocked on partitioning, frozen, zombie, etc.). The WL node’s image therefore

can be copied, replicated, stored, encrypted, etc. to comply with node lifecycle, security, resiliency, and durability requirements.

[0080] An elastic WL has various lifecycle and execution states that can be represented as one or more file images. A “pod” filesystem therefore can be used that allows WL images to be manipulated by a distributed files system interface (e.g., IPFS, GFS, HDFS, Ceph) where a distributed filesystem hierarchy contains WL images are serialized Pods, Containers, Workloads, Distributed Workloads, etc. that map to objects in an Elastic Workload Filesystem (EWFS). As used herein, an EWFS refers to any cloud- or edge-distributed filesystem containing serialized WL images. The EWFS configuration may be described by metadata such as SWID or CoSWID that models a filesystem abstraction, where a distributed filesystem is also described by a filesystem abstraction. Here, different nodes in an elastic cluster can a namespace in a filesystem hierarchy and the various elastic workload lifecycle states may be represented as files or sub-directories of the EWFS filesystem namespace. The EWFS metadata may be used to specify an expected deployment configuration, deployment status context, deployment lifecycle archive, and elastic workload data distribution model.

[0081] The elastic WL configuration enables performance improvements while being cyber-resilient. Elastic WL telemetry and AI/ML algorithms may add greater context for leveraging WL archives that quantify WL lifecycle overhead (e.g., pause/restart vs. decommission/recommission). For example, the elastic WL equivalent of a suspend-resume state “S3” in an operating system process suspend/resume may record resource utilization, latency, network bandwidth and so forth. Thus, the overhead that is associated with WL lifecycle transitions can be analyzed, when these measurements are available for analysis and optimization of WL microservices.

[0082] FIG. 10 is a block diagram that illustrates a save-restore workflow, according to an example. Here, WL security islands combined with failsafe protocols create safe enclaves in edge deployments that may facilitate secure and reliable infrastructure upgrades. Further, a WL’s self-management capability can be used to implement ‘save-restore’ or ‘save-restore-reinit-resume’ workflows.

[0083] As depicted in FIG. 10, a running WL **1001** receives a request to update a distributed WL node with a new WL image triggering the setting of a quiet point (Operation 1). The quiet point applies to WL images in other operational states such as sleep or hibernate. Workloads that are blocked on a quiet point move to a safe operational state such as pending transactions, cached writes, and inner loop execution context. The WL update **1024** may be applied by the Pod Update Manager (PUM **1022**) (Operation 2). Subsequently, the updated WL resumes processing the WL (as running WL’ **1002**) and the saved state is restored to resume processing (Operation 3). In the case of sleeping or hibernated WL states, these states can be returned to with use of a sleeping or hibernated WL’ image. After successful application of the update (or error state), the PUM **1022** notifies the Workload Update Manager (WUM **1012**) regarding the update status (Operation 4). The WUM **1012** may further notify an Orchestrator **1010** where notifications from across the elastic edge may be assessed (Operation 5). Distributing WL update operations improves scalability of elastic (distributed) WLs because the distributed WL does not need to

be coalesced to a central node to apply an update then re-distribute the WL. The Orchestrator nevertheless maintains a central and consistent view of update application using notifications and the WL metadata.

[0084] Using Simulated Test Flows for Workload Binding

[0085] Traditional workload simulation environments create a test framework that employs test automation controls. These test automation controls are designed to exercise a workload given a synthetic data set and prescribed test case functions and deployment parameters. Workload execution may be instrumented and logged to validate expected intermediate results. Workloads operate with an expectation of ready access to resources.

[0086] This existing approach is insufficient for testing elastic workloads in simulation due to elastic resource requirements and competition for resources as workloads fragment, proliferate, and compete for limited resources. Elastic workloads are comprised of both executable flow and data sources or data sinks where workflow logic targets data repositories for sourcing or syncing persistent data. The systems and methods described herein provide a simulation environment that addresses these challenges.

[0087] As stated, existing workload simulation solutions do not exercise the functionality and resource management limitations anticipated when deploying elastic workloads. The problem with deploying elastic workloads into production networks that do not simulate and test resource starvation, oversubscription, and availability given workload elasticity dynamics means that the production network is at risk of workload failure, slow down, security, or resiliency events. Such risks are particularly possible as new or updated elastic workloads are introduced to Edge and Cloud-connected Edge networks, resulting in increased operational costs, failure to meet service level agreements, damage to resources, and even physical harm.

[0088] The implementation described herein leverages existing workload simulation building blocks with a simulated infrastructure resource supply and elastic intents. These intents can be used to enable multiple systems under test to compete for a simulated finite set of resources as elastic intents are used to direct workloads to fragment and distribute across the simulated resource infrastructure. Multiple distribution and coalescence scenarios can be exercised while also manipulating resource availability profiles that fully exploit the effects of elasticity for a given set of elastic workloads. This also enables testing of elastic workload behaviors in simulation before subjecting them to production deployments where risks of misbehavior are multiplied.

[0089] FIG. 11 is a block diagram illustrating a classic workload testing infrastructure, according to an example. Existing WL testing infrastructure automates a singleton WL for pre-determined test case operation according to a prescribed test scenario. In this test scenario, users **1102** establish inputs **1104**, to automate a test with a test framework **1106**. The test framework **1106** is then used to generate respective scripts for a system under test **1108**. The test scenario is repeatable, as WL execution follows a predetermined flow that uses resources according to the same prescribed pattern and according to a testing iteration. In this setting, regression profiles can identify anomalies in performance, resource utilization, and functional capabilities. Security testing can be performed by running pre-deployment scans on software and configuration settings. However, test scenarios may not simulate real-world use cases for

elastic workloads that must handle resource starvation, adversarial competition, and disaster recovery in simulation.

[0090] Simulation of elastic workload operations prior to real-world deployment is important to ensure robust continuous operation. Such simulation requires a representation of all resources for the target system under test (SUT) environments such that they may bind to the elastic workload nodes that may further be distributed and fragmented as part of workload elasticity. The resource simulation framework specifies resource allocation profiles and WL node assignment and how resources are bound to WL nodes. Binding may further require attestation that ensures WL security sensitivity requirements can be met by a resource allocation and assignment.

[0091] Simulation is also important for critical infrastructure deployments to ensure that use of new or modified WLs do not introduce failures. A key component to the improved implementation is the use of metadata that describes the simulation environment, the simulated workload, and the resource profile. The simulation environment orchestrates the orchestrator, resource managers and other control surfaces in the elastic workload environment. The simulation environment also leverages the workload metadata that specifies security, resiliency, and distribution intent (called ‘intents’) that is used for normal operation of an elastic workload.

[0092] FIG. 12 is a block diagram illustrating an elastic workload testing and a resource simulation framework (RSF 1210), according to an example. The elastic WL testing configuration and RSF 1210 builds on existing WL testing infrastructures but also handles multiple workloads (WLs 1201, 1202, 1203) vying for the same set of (simulated) resources.

[0093] The WLs 1201, 1202, 1203 may be unrelated in terms of their collaboration objectives, or they may be in competition for assets (e.g., goods and services—not just resources). For example, WL A 1201 in a supplier network might estimate a supply of 100 cameras is needed, while WL B 1202 may require 200 cameras. If WL C 1203, a camera supplier, can produce 250 cameras, there is a net deficit of 50 cameras. If the test objective is to determine whether WL A 1201 behavior can dynamically adapt to a new change in available resources, WL goods and services, etc., then the simulation environment will accommodate multiple simultaneous workloads.

[0094] Simulation itself is a workload that may iteratively model the most basic and important resource bindings, followed by resource fragmentation and re-binding as elastic WLs fragments are distributed. This modeling is followed by resource starvation, sharing, over subscription, failover, and so forth. Although Kubernetes (K8S) testing frameworks consider CPU, memory, and disk as important resources to track and manage, existing K8S testing frameworks do not fully support advanced distributed resource contention scenarios or scenarios.

[0095] The resource simulation framework is highly scalable to use common resource behavior profiles that model and simulate starvation, distribution, fragmentation, over-subscription, failover etc., including with models that can cover a spectrum of use cases and deployments. Additionally, resource profiles may be used in the following framework to model multiple trusted resources as a way to exercise the full flexibility of elastic intents (especially where WL fragmentation and distribution might not stop at

a single pod/cluster). Such WL fragmentation and distribution may result in multiple clusters that organically form around data lakes, availability of acceleration farms, or mobile trajectories common to Multi-access Edge Computing (MEC).

[0096] In further examples, the resource simulation framework may monitor resource utilization across various WL clusters to eliminate clusters that do not meet KPIs or latency requirements (e.g., such as due to data lake access latency, set to a high bar policy). Additionally, the WL KPI test metrics (e.g., CPU utilization) may be combined with cybersecurity attributes (e.g., redundancy), including to incorporate a toolbox for cyber-resilience testing (e.g., Mitre’s ‘Att&ck’ toolbox) and produce an audit report containing a cybersecurity gap analysis. Toolbox extensibility may include Digital Twin (DT) support where platform implementations that support DT features may instantiate mirror copies of a WL node resulting in additional pressure on overall resources.

[0097] In still further examples, the resource simulation framework may define a simulation pod “SimPods” abstraction where an elastic WL is fragmented and distributed to form a ‘pod’—similar in concept to a K8S pod—where pod behavior is the focus of simulation. The simulation objective then can be performed to optimize resource allocation and assignment according to the SimPod.

[0098] System Firmware and Software Update and Relaunch Processes

[0099] Elastic C2E workloads may be continuously integrated and deployed (e.g., with continuous integration and continuous delivery/continuous deployment (CI/CD) software practices). Security vulnerability events (e.g., Common Vulnerabilities and Exposures (CVEs)) may be reported that render portions of attested elastic workloads insecure despite having contradictory attestation results. CVE detection, correction, and redeployment of elastic workloads is challenging due to the dynamic nature of elastic workloads because the elastic workload can be distributed across multiple nodes, migrated, and coalesced again dynamically independent of workload orchestrator knowledge. The following implementation uses a cloud-edge cluster manager and late binding of workloads and workload data to execution resources to implement workload elasticity properties. This implementation enables CVE notifications and re-attestations to be applied as part of a dynamic ‘top-half and ‘bottom-half’ binding operation.

[0100] Existing solutions rely on CVE notifications to software supply chain developers and operators who then review software inventories to determine if any deployed products are affected by a CVE. This approach requires careful records and diligence on behalf of the software vendors to determine if a released binary actually is affected by a CVE. This approach does not scale because elastic workloads are dynamically partitioned according to metadata that is embedded in the workload, making it nearly impossible for an operator to predict which deployed nodes are affected by a CVE at any given time.

[0101] The implementation described herein integrates attestation with elastic workload deployments using orchestrators for top-half workload deployments, and cluster resource managers that provide bottom-half resource management. In the bottom-half resource management, the binding of resources to a workload (or elastic workload fragment) is subject to attestation and CVE assessment. The

elastic workload is designed using a metadata scheme that identifies the possible ways that the workload might be dissected during deployment to optimize available resources. The metadata may be used to assess a CVE and determine which workload fragment in deployment is affected.

[0102] Workload migration and update mechanisms are repurposed to seamlessly apply CVE-driven countermeasures that patch/update workload fragments in replica or digital twins that may undergo a loss of operational integrity as a result of applying the countermeasure. The replica workload fragment may be used to migrate a functioning workload fragment from a vulnerable node to a non-vulnerable node seamlessly and without requiring the distributed workload to be coalesced. This enables elastic workloads that have been partitioned and optimized for maximum resource efficiency to remain operational in their optimized form, while still being able to detect and apply CVE resolutions.

[0103] FIG. 13 is a block diagram illustrating a cloud-edge cluster, according to an example. The cloud-edge cluster shows a typical C2E deployment having a top half 1302 with one or more C2E Workloads and a bottom half 1304 with one or more resources (e.g., CPU, storage, memory, sensing, etc.) that are bound to the top-half workload. A workload can be monolithic or divided into distributed workload parts (e.g., with respective parts performing a portion of the monolithic workload). The workload data may be merged or integrated with the workload execution or may be accessed remotely upon demand or may be cached to minimize network latency overhead. Cached data may be updated as needed and write-through caching may be used to ensure data consistency.

[0104] The top half 1302 is bound to bottom half 1304 resources as part of a C2E Cluster deployment. Initial deployment may allocate a set of top half nodes that are scheduled to run using bottom half resource nodes. Binding activity may involve attestation of the resources by the top half 1302 prior to binding to a bottom half 1304 or attestation (e.g., WL/data provenance evaluation) of the top-half workload and data by a bottom-half node prior to binding. Binding may be facilitated by orchestration or resource manager nodes.

[0105] After binding, the resultant cloud-edge node may begin processing the workload. Distributed workloads may produce output that is consumed by a peer cloud-edge node originating from the same monolithic workload. Peer cloud-edge nodes that act as consumers or producers of other peers may attest the peer prior to consuming WL inputs from a peer or prior to sending WL outputs to a peer. Mutual attestation ensures the peers are indeed peers and that they are bound to resources that satisfy an overarching and consistently secure workload policy.

[0106] FIG. 14 is a block diagram illustrating a cloud-edge cluster after provisioning a distributed workload, according to an example. After provisioning all peer nodes in a distributed workload, the operational cluster is depicted in FIG. 14 and includes one or more cloud-edge nodes (e.g., node 1404) where a top-half workload 1405 (or partitioned workload) is bound to a bottom-half resource 1406 (or set of resources). The top-half workload 1405 may be orchestrated by an orchestration agent 1402 (e.g., Helm, Rancher) that may interface with a top-half workload 1405 (e.g., K8S pod manager). Additionally, the provisioned bottom-half

resource 1406 may have a cluster resource manager 1408 that oversees operation resource utilization and optimization. The cluster resource manager 1408 may assign/deassign resources (e.g., CPU, memory, storage, XPU, etc.) as needed to meet workload QoS requirements and to optimize power or performance.

[0107] FIG. 15 is a block diagram illustrating updated packages for top and bottom half components (e.g., a top-half migration target 1502 and a bottom-half migration target 1512) in a distributed edge cluster, according to an example. The top-half update package 1504 may include a Bill of Materials (BoM) describing software, firmware, drivers, or hardware components. The BoM may include attestation reference values for matching attestation evidence, endorsed values that represent attributes and properties of the component known to the component vendor, supplier, or deployment agent. The bottom-half update package 1514 may contain updated firmware, software, settings, configuration parameters, calibration parameters, policies or other information related to applying the update. It may also contain attestation verification policies and resource descriptions that identify resources that are equivalent or similar that may substitute for other resources that may differ in terms of vendor, model, version, etc.

[0108] The top-half update package 1504 also may contain updated workload code, settings, configuration parameters, quality-of-service policies, key performance indicators, metrics, data source, data sink parameters, etc. It may contain attestation information in the form of reference values, endorsed values, device identity certificates and other information used to attest the workload and to verify peer workloads.

[0109] An orchestration agent or cluster resource manager may be used to perform migration operations to update a deployed C2E cluster node. For example, a deployed workload may be modified to add, remove, or change workload behavior. Similarly, deployed resources may be updated to install or replace hardware modules, device drivers, system software, framework software.

[0110] When updates are applied, they may invalidate current attestation and trust contexts. Hence, application of an update can affect the risk management posture of the workload or operational resources even if there is no change to behavior or data. Some or all of the operational prerequisites (such as attestation) may need to be redone after applying an update. If the workload has availability requirements that disallows halting the workload to apply the update and re-initialize the trust context, but retains the requirement to maintain robust trust context, the C2E cluster node may employ an update migration method designed to minimize workload disruption. Prior to the update package being installed, a new cluster node is provisioned, and the update package applied to the new node. In the case where a top-half workload node is to be updated, a new workload node may be provisioned and updated. Similarly, a bottom-half resource node may be provisioned, and update applied. The newly provisioned node may be attested and verified according to normal attestation procedures.

[0111] The update process involves migrating the currently executing workload (or resource) node to the newly provisioned node. There are two forms of migration, remote and local. Remote migration involves C2E nodes that are

hosted on different physical platforms, while local migration is applied to logical or virtual contexts on the same physical platform.

[0112] FIG. 16 is a block diagram illustrating remote cloud-to-edge node preemptive migration, according to an example. Specifically, this diagram shows remote proactive migration in response to an available update. When an update to a top-half component 1602 is available, a new workload node can be allocated where the affected workload container is replicated and the replicant is updated with update operations 1606. The replicated container becomes a migration target 1610 to which the existing provisioned workload 1608 is migrated, based on migration operations 1604. Migration operations 1604 may include copying workload context, settings, connections, data, and memory state to the migration target 1610. After which, the migration target 1610 may be attested to account for the updated software, settings, and configuration.

[0113] Similarly, an update to the bottom-half component 1620 may proactively allocate a migration target 1614 that is a clone of the provisioned resource 1612 to which the update is applied (with update operations 1618). After the update operations 1618, the bottom-half target may be attested to account for measurement changes resulting from applying the update. The top-half migration target 1610 and the bottom-half migration target 1614 are re-bound to re-establish an attested trust relationship between the two halves (depicted by diagonal lines in FIG. 16). For example, the bottom-half target may contain an attesting environment that can measure the top-half migration target 1610. Alternatively, an orchestration agent or attestation service provider may invoke attestation agents in top/bottom half targets to perform a similar attestation function, resulting in attestation evidence linking the top and bottom half (trust dependency) targets. Alternatively, the update is applied to either the top-half or the bottom-half target resulting in migration of only the top (or bottom) half target. Nevertheless, trust dependency is re-established with the non-migrated component (depicted by diagonal lines in FIG. 16).

[0114] After re-attestation occurs, the connection state may need to be reestablished between top and bottom half entities. Information consumed by the top-half from the bottom-half is contingent on the trust dependency context. If the trust context is disrupted, the data and control planes are also disrupted. Reestablishment of a control/data plane context may include reestablishment of connection state. For example, if a Transport Layer Security (TLS) or Security Protocol and Data Model (SPDM) connection existed before, the session keys may be renegotiated. The protocol key exchange may call for inclusion of Attestation state in session key generation or may log session handshake messages showing the attestation state, or session state (such as a session MACing key) may include attestation state. Session reestablishment refreshes the session state to reflect the trust impact from having applied the updates.

[0115] FIG. 17 is a block diagram illustrating local preemptive migration, according to an example. In this scenario, a top-half guest or secure enclave 1708A to 1708N (e.g., provided by an Intel® SGX/TDX environment) communicates to bottom half IO devices 1714A to 1714N through a Secure-Arbitration Mode (SEAM) component or another similar security-services module 1712.

[0116] When updates 1720 are applied at a bottom-half resource to update an IO device, a new IO device driver

context (virtual IO device) is created that has an update 1718 applied, such as an updated driver. The previous driver or IO device remains operational during this process started with a migration 1716. The new (updated, virtual) device 1710B establishes a new connection to the security-services module 1712 which may include attestation of the new device 1710B. The security-services module 1712 advertises availability of the new device to the guests. The guests that depend on the IO device may, at their convenience, open a connection to the new device 1710B and close the connection to the previous device. The data on the device remains available and consistent across both virtual devices as a property of virtualization abstraction.

[0117] Updates 1702 that are applied to the top-half guest or secure enclave 1708A to 1708N may impact trust dependency on lower layer IO devices. A proactive migration 1704 may apply to top-half nodes as well. A new migration target 1710A (guest or secure enclave) is created with a clone of the guest/enclave to be migrated, and then the update 1706 is applied. The migration target 1710A creates a new connection to the security-services module 1712 which multiplexes with the IO devices. The old enclave/guest migrates workload and data to the migration target 1710A and begins using the target's attested connection to the security-services module 1712. Migration of the workload and data may be further facilitated by virtualizing the workload and data into memory that is shared across old and new target. The updated and attested part of the workload are held separately.

[0118] When the node completes migration, the attested state of the new node reflects the update. When the node interacts with a peer node that requires knowledge of the node's attestation state, the new node may re-attest to an orchestrator, attestation service or the peer node directly to obtain an attestation token representing the updated state. Previously minted tokens are discarded in favor of the most recently issued token. Tokens may expire requiring periodic reissuance.

[0119] This implementation uses intent-based declarative operations that describe the various ways an elastic workload can be partitioned and distributed. Thus, the precise resource requirements for a WL partition are readily available to orchestrators or cluster resource managers for dynamic distribution or coalescence operations.

[0120] In further examples, the elastic workload infrastructure may be diverse in terms of hardware and software BoM that are used. The CVEs may be prioritized based on rank (e.g., ranking of an impact if compromised for a given vulnerability) and this rank may assist in the upgrade strategy that is applied across the orchestration and deployment infrastructure. This may leverage residual compute resources to minimize operational runtime impact on the upgrade process by providing recommendation to the back-end services. A small amount of partitioned capacity may be reserved in respective nodes so that the workload can be migrated to its optimized partitioned capacity first (without having to drain the workload or migrate it long distance), and then restored to full capacity after a CVE fix is applied and rebooted.

[0121] Manifest standards contain BoM lifecycle intents where updates and patches are tracked by a BoM. A challenge is the older images do not know about newer images that superseded them. However, newer images may contain references to older images (in the BoM) such that a cluster

resource manager can trace the lineage and determine if a CVE applies to an older revision of a workload fragment. An update service may be needed that maintains a database of update dependencies such that older images that are not aware of newer images can be searched efficiently. A publish/subscribe system could be used to multi-cast lifecycle notifications so that workload fragments are aware of the most current images and which lifecycle states apply for current configurations. Other secure environments (such as Intel® TDX) may be used as a more secure hosting environment for elastic workloads that uses an IO resource. The IO resource driver or firmware may be updated by its device vendor or an administrative service provider that is not controlled by the workload orchestrator or cluster manager. The update may change the attested and assessed trust context resulting in a stale attestation result. Secure execution applications may want to prevent updates so they can optimize on a particular KPI vector while retaining a known attestation result. However, elastic cloud-to-edge may not have a central orchestrator that maintains attestation and update consistency. Elastic workload intents may describe the artifacts of the workload that should be negotiated in terms of how to effectively trade-off attestation integrity with operational availability.

[0122] A CVE may differentiate between an exterior and interior impact. By applying a patch to a component outside the workload (BoM of Platform) may be effective way to mitigate the threat (e.g., by applying a software firewall) Or patching may be applied within the workload (BoM of WL) to correct a vulnerability (e.g., by closing a buffer overflow).

[0123] If there is an increasing CVE backlog, a backlog threshold (e.g., a min rate of burning backlog is greater than rate of new CVEs including weighted severity) may define a grace period with policy-based rules where the update can be safely applied. Cyber Resiliency is affected in that a Cyber-Resilient Triad exists where the workload, data, and host node encounter independent CI/CD processes, but the triad is reconciled by metadata intents that allow the CVE impact to be traced to a specific workload fragment and resource that contains the vulnerability.

[0124] Trust Coordination Across Computing Elements in an Edge to Cloud Continuum

[0125] Distributed compute and networking have evolved into a hyper-connected compute continuum with the introduction of various C2E approaches. C2E approaches are expected to be adopted by many industry participants, including cloud service providers (CSPs), communications service providers (CoSPs), and enterprise providers. C2E approaches enable the transition from vertically integrated, industry-specific solutions to horizontal platforms where all compute nodes can execute workloads, produce, and consume data.

[0126] FIG. 18 is a diagram illustrating the elements of a hyperconnected compute continuum, according to an example. Three elements primarily participate in the hyper-connected compute continuum: workloads **1802**, data **1804**, and compute nodes **1806**. Security is a key contributing factor for compute elasticity in C2E deployments **1810** that use these elements, to ensure the capability to move workloads across the different end points of execution.

[0127] Industry participants may have the view that unreliable security hinders C2E operations. Security requirements cannot be addressed without establishing trust between the elements of the compute continuum. Protecting

edge components with intrinsic security of applications, data and infrastructure is also a concern. This complex technical problem, driven by multi-party supply chains and customer interactions, also needs to be scalable.

[0128] Existing attempts for trust establishment have been based on siloed, vertical attestation for a compute node or workload (e.g., Intel® SGX attestation, Secure Boot using Trusted Platform Module (TPM), DICE, or SPIRE). Accordingly, there are not suitable Data Provenance attestation solutions available, and existing approaches are limited to per-app or per-microservice implementations. For example, consider the use of OPA (Open Policy Agent), which is an open source, general-purpose policy engine that unifies policy enforcement across a software stack. It provides a high-level declarative language to specify policy as code and APIs to offload policy decision-making. However, OPA lacks the aggregation of the assertions and ability to reassess the assertions (metadata) runtime.

[0129] There are other deficiencies with existing approaches for trust establishment. For instance, implementations follow needs, which may create lag in deployments. Further, there is fragmentation and redundancy among many approaches, resulting in failure-prone implementations. There are also implementation inefficiencies, such as hard-coded policies, which are difficult to maintain. Thus, existing implementations often have a lack of consistency, use an ad hoc format, are standard-adverse, are difficult to scale (being embedded in other code/product), and are difficult to secure (and if they are embedded, they may need additional technical solutions).

[0130] The following addresses aspects of multi-party trust coordination, to provide trustworthiness from the exchange of metadata, evaluation of metadata per policies, and decision making. This trust coordination is applicable to complex C2E compute environments that enable multiple parties to provide heterogeneous metadata and associated policies and entity capabilities. Further, the following also provides approaches to collect, analyze, make decision, and reassess the trustworthiness assertion based on policies and entity capabilities.

[0131] FIG. 19 is a diagram illustrating trust coordination, according to an example. As observed by reviewing FIG. 19, there are many problems and challenges in solving trust coordination. A developer **1902** may specify security requirements (in policies) for workloads, whereas a cluster operator **1904** may specify requirements (in policies) for managing nodes which operate the workload. Multiple policies contribute metadata relating to security (e.g., relating to the policies, requirements, working capabilities, and software properties). However, this metadata is often heterogeneous (e.g., is not bound to a particular software or hardware technology). Additionally, a verifier **1906** may be invoked to obtain verification results of working features and properties. Additionally, a worker node **1908A** or **1908B** may use different technologies and provide information on working (and thus verifiable) capabilities.

[0132] Systems and methods described herein provide for trust coordination across heterogeneous elements in an C2E setting, with use of a trust coordination framework **1910**. This framework **1910** provides a mechanism for processing of heterogeneous multi-party metadata that includes collection, analysis (reasoning) and dynamic reassessment of policies over metadata. The framework **1910** simplifies evaluation of relevant metadata and policy management, and

makes or assists decisions that influence workload orchestration. The framework **1910** relieves reliant services (e.g., dependent services) from the complexity of handling meta-data and policies (in terms of quantity, size, and heterogeneity), such as by SGX attestations, TPM attestations (like in Keylime), software supply chain assertions, data provenance assertions, etc. The framework **1910** also consolidates metadata and policy handling in a single instance for multiple relying services. The framework **1910** also minimizes code maintenance of relying services to update metadata formats and policies.

[0133] Compared to a singular attestation approach, the following trust coordination implementation will enable specific requirements of entities such as devices, workloads, or data instances to support assertion policies. For example, the trust coordination implementation can introduce new methods, protocols and interfaces for registration, and the exchange and query of assertions and for registration and evaluation of policies (e.g., APIs available to the edge and cloud customers to specify or select an attestation policy when they want to run a sensitive workload in the cloud that requires protection from software and hardware exploits).

[0134] FIG. 20 illustrates the use of a trust coordination as a service, according to an example. This implementation demonstrates trust coordination across heterogeneous elements of computing in an C2E framework. Trust Coordination Framework (TCF) can be an implementation that can be presented as a Trust Coordination as a Service (TCaaS) engine **2010** integrated into Cloud-to-Edge Orchestration Solutions. Here, the workload **1802** can be associated with workload provenance characteristics; the data **1804** can be associated with data provenance characteristics; the compute nodes **1806** can be associated with attestation values. The TCaaS engine **2010** may be operated or used by an orchestrator **2012**, to consider security intents and other aspects of the policy **2014**.

[0135] FIG. 21 illustrates existing siloed approaches as contrasted with an advancement to a trust coordination framework (TCF), according to an example. Current deployments **2101** use metadata collection and analysis on a per-app (per-microservice) basis, and are typically not scalable while being difficult to build and maintain. In contrast, a TCF **2102** acts as an active intermediary to establish trustworthiness based on verifiable information across compute nodes, workloads, and data. The TCF **2102** separates metadata collection, handling, and policy management from apps/microservices **2112**. The TCF **2102** provides a single framework for multiple deployment scenarios **2114**. The TCF **2102** allows reuse of metadata, handlers, and policies **2116** and enables policy decisions over heterogeneous metadata/technologies and users **2118**.

[0136] The TCF **2102** simplifies metadata and policy management by relieving “relying” services (e.g., dependent services) from the complexity of handling metadata and policies—in terms of quantity, size, and heterogeneity. For instance, the relying services may include Intel® SGX, Intel® TDX, DICE or TPM attestations (or attestations from a similar secure environment), software supply chain assertions, data provenance assertions, etc. Use of the TCF **2102** also consolidates metadata and policy handling in a single instance for multiple relying services and avoids code maintenance of relying services to update metadata formats and policies.

[0137] FIG. 22 is a diagram illustrating interoperability of a trust coordination service, according to an example. Trust coordination in this scenario includes the following Actors: assertion producers **2202A**, **2202B**, . . . **2202N**, which produces assertion related to the entity capabilities, platform properties, and/or verification results (e.g., related to hardware-based attestations, SW properties, etc.); decision consumers **2206A**, **2206B**, . . . **2206N**, which consumes a policy trustworthiness decision per requested entity; Entities **2204**, which are the subject for trustworthiness that present attributes of trustworthiness; and a trust coordination service **2210**, which aggregates the metadata and makes decisions based on provided policies.

[0138] FIG. 23 is a block diagram illustrating a general hierarchy of classes and attributes, according to an example. A respective component of the compute continuum can associate trust coordination **2302** with several entity classes (e.g., **2311**, **2312**). A respective entity class may have associated trustworthiness attributes (e.g., **2321**, **2322**), such as attestation, provenance, a Software Bill of Material (SBOM) assertion, safety, resiliency, etc.

[0139] FIG. 24 is a block diagram illustrating a specific hierarchy of classes and attributes, according to an example. Here, there are three classes that are illustrated for trust coordination **2402**: workload **2411**, associated with attributes **2421** for native workload or containers; node **2412**, associated with attributes **2422** for compute resources; and data **2413**, associated with attributes **2423** for structured or unstructured data that is generated or consumed.

[0140] FIG. 25 is a block diagram illustrating a trust coordination framework architecture, according to an example. An embodiment of a trust coordination framework **2510** illustrated in FIG. 25 includes two layers. A data layer **2512** is responsible for the assertion validation, collection, storage, and notification. A trust layer **2514** contains a policy engine and provides policy storage and evaluation services. Assertion agents **2502** feed assertions to the data layer. Such assertions are signed for accountability and integrity. The trust layer finally provides policy decisions (evaluated over the assertions in the data layer) to applications **2504** (or relying parties).

[0141] FIG. 26 is a block diagram illustrating high-level operations in a trust coordination framework architecture, according to an example. These operations are coordinated among an assessor producer **2602**, providing information to a trust coordination framework **2604** for evaluation, which then provides decision information to a decision consumer **2606**.

[0142] The high-level operations are used to assess the trustworthiness of platforms, software, or workloads. First, the necessary Root-of-Trusts (RoTs) are defined at operation **2612**. The RoTs will convey (or will certify other parties who will convey) software and/or hardware features and properties. Second, assertions are collected at operation **2614**. Finally, a policy is evaluated at operation **2616** to determine a decision. As the context changes (e.g., new assertions are collected, or previous assertions are updated), policies are (or can be) re-evaluated at operation **2620** to confirm previous decisions, or to trigger contingency actions. In further examples, open-source solutions such as Open Policy Agent (OPA) or another policy engine can be used for policy specification and evaluation.

[0143] FIG. 27 is a block diagram illustrating state transitions of trustworthiness attributes, according to an

example. Attributes transition from a non-trusted state **2710** to a trusted state **2720**, based on verifying a declared attribute assertion. Subsequent re-verification may be used which triggers a policy. (In practice, the attributes may be continually in a trusted state, but the relying party that is modeling attribute trust may maintain a distinct or separate attribute state machine that models the attribute state transition as a way to achieve trust consistency over a distributed set of nodes).

[0144] FIGS. **28-30** are swim lane diagrams illustrating interactions between respective components of a trust coordination framework architecture, according to various examples.

[0145] In FIG. **28**, an assertion producer **2810** provides a request to a trust coordination framework front end **2812**. The trust coordination framework data layer (DL) provides notification and validation functions **2814** and data storage functions **2816**, whereas the trust coordination framework trust layer (TL) provides policy management functions **2818**.

[0146] In FIG. **29**, a decision consumer **2910** provides a request to a trust coordination framework front end **2912**. The trust coordination framework data layer (DL) provides notification and validation functions **2914** and data storage functions **2916**, whereas the trust coordination framework trust layer (TL) provides policy management functions **2918**.

[0147] In FIG. **30**, an entity of interest **3010** (such as a compute node) communicates with a trust coordination framework front end **3012** to join the operational environment. The trust coordination framework data layer (DL) provides notification and validation functions **3014** and data storage functions **3016**, whereas the trust coordination framework trust layer (TL) provides policy management functions **3018**.

[0148] Attestation Microservices and Service Mesh for Elastic Workloads

[0149] Many attestation services are based on a centralized deployment model where workload nodes request attestation following a passport model. The passport is presented to WL orchestrators who vet the node and schedule the WL as appropriate. In elastic compute scenarios, however, WL nodes are not static. Portions of a WL may be dynamically partitioned where WL partitions are also dynamically provisioned to a microservices hosting node. For instance, consider a scenario where a respective microservice (also referred to as a “μService”) obtains a passport (token) from an attestation verification service, which results in $O(n \log n)$ to $O(n^2)$ latency overhead; here, n is the number of microservice partitions as a microservice cross-checks the other n microservices. This does not scale well for C2E infrastructures.

[0150] Other approaches rely on a cloud service abstraction that centralizes attestation processing as a service abstraction. The cloud services provider may scale the service by adding resources to the server backplane. This approach does not address edge network environments that typically have compute dispersed at different locations with differing compute, connectivity, resource, and latency properties. As noted above, centralized attestation services, e.g., hosted in a cloud, also introduce latency in an edge network.

[0151] The following system and methods integrate an attestation mesh into an edge mesh that optimizes edge WLs. In an example, this optimization is provided by co-locating

FaaS functions on hardware such as IPUs that are also hosting a distributed WL. The attestation WL is then decomposed into FaaS functions for easy co-location with the other WL/FaaS mesh execution locations. The various stages of attestation processing may rely on attestation inputs, e.g., evidence, reference values, endorsed values, policies, which are supplied by support services but may be cached locally by the hardware (e.g., IPUs) of a mesh node.

[0152] This approach allows attestation appraisals to occur within the latency envelope that is appropriate for the edge workload node. More frequent or timely attestation appraisals can be performed because the mesh node with attestation support can cache the various appraisal inputs and manage the cache along with the other mesh-aware WL caching policy.

[0153] FIG. **31** is a block diagram illustrating attestation load distribution, according to an example. An attestation service mesh (ASM) **3100** is a cluster of attestation service nodes that cooperate to distribute attestation workloads in a distributed or decentralized elastic WL. A respective Attestation Service (AS) (shown with AS instances **3110**, **3111**, **3112**) may be provided by a microservice that specializes in attestation verification processing. A respective AS may be further divided into FaaS functions that specialize in implementation of an aspect of attestation verification processing (e.g., certificate path construction, RIM location/collection, document signature verification, trust anchor repository access (per tenant), document format decoding, evidence collection, evidence integrity verification, evidence format decoding, tag lifecycle management, appraisal, attestation results creation, attestation results integrity protection, or attestation results creation/passport/token issuance and delivery). As an attestation microservice, these functions can be elastically hosted on/near elastic WL nodes.

[0154] The ASM **3100** may be hosted on the same infrastructure nodes used to host (e.g., execute) decentralized elastic WLs. The elastic and ASM WLs are treated as different tenants utilizing hardware and software isolation techniques including OS process isolation, containers, micro-kernels, virtual memory, processor operational modes, virtualization, or physical and virtual segmentation, such as with use of technologies such as Intel® SGX, Intel® TDX, AMD® Secure Encrypted Virtualization (SEV), ARM® TrustZone and so forth. The ASM microservices (AS0, AS1, . . . , ASn, shown with instances **3110**, **3111**, **3112**) are provisioned with cryptographic identities, credentials, and policies that establish them as a trusted group within the ASM **3100**. The microservices maintain cross-connections that may be utilized to quickly offload attestation processing functions and to share (cache) various attestation related data including endorsement manifests, reference value manifests, device certificates, device sessions (e.g., SPD, RA-TLS, Attested TLS, or HTTP-Attest), device decentralized identifiers (DID), tokens (e.g., OAuth2, OpenID-Connect, IETF EAT, IETF JWT, or IETF CWT), D-WL policies such as SLAs, SLOs, trust anchors, security policy, security settings, intermediate attestation results, final attestation results (AR), audit information, telemetry information and any other data that may be generated as a result of operating a robust ASM.

[0155] FIG. **32** is a block diagram illustrating an elastic workload mesh architecture, according to an example. The elastic workload may be distributed across multiple nodes **3210** forming a workload mesh **3212** (WLM) that functions

as a cohesive WL but is distributed or decentralized in terms of the logical, virtual, or physical processing nodes. The WLM may rely on a set of WL metadata that describes the WL functions, data, partitioning semantics and may have specified quality, performance, trust, security, resiliency, privacy, and availability requirements. The WLM may support multiple WL per infrastructure node using tenant isolation techniques as described herein.

[0156] The WLM may interface with a microservice mesh **3214** (μ SM) that implements and deploys popular FaaS functions commonly used across multiple WLs. The μ SM may be implemented on the same infrastructure nodes as other mesh capabilities including WLM, ASM, and so forth. The μ SM FaaS functions are isolated using tenant isolation technology as described elsewhere in this document.

[0157] The μ SM may interface with an attestation service mesh **3216**, which may perform a variety of functions for attestation services, as discussed above.

[0158] Infrastructure nodes may be hosted by an infrastructure processor mesh **3218** (IPUM) that maintains pools for compute resources configured to host mesh-based workloads (as described above) that are optimized for efficient edge operation. For example, a pool of IPU may be integrated on a common backplane, rack, cluster, geo-location network, etc., having memory, storage, acceleration, and network connectivity resources readily available for pool IPU consumption. IPU pools may be connected for efficient resource sharing, load balancing, and resiliency, including for respective resource slices **3220**.

[0159] FIG. 33 is a block diagram illustrating attestation of a distributed workload using an attestation mesh, according to an example. A respective cross-section of an edge node **3310** and mesh layer (as illustrated in FIG. 32) may be required to attest the resource to an AS microservice **3312** in the ASM as a condition of participation in the mesh and as a condition of participation in a D-WL vertical stack (as illustrated in FIG. 33). An IPU **3320** (or similar edge processing unit) may utilize a Fabric Controller **3314** (FC) that is responsible for triggering attestation of an IPU resource upon appropriate events such as power reset, system reset, fault or interrupt handling, microcode update, firmware update, failure event, and so forth. The FC trigger results in at least the IPU **3320** requesting attestation by an Attestation Service (AS) (shown in operation 1), such as an AS microservice **3312** that is assigned to the IPU **3320**, that results in a verification on the IPU **3320**.

[0160] An attestation result in the form of an attestation token (shown in operation 2) may utilize industry standard token structures such as CBOR Web Token, JSON Web Token, Concise Evidence, W3C DID/VC, X.509 certificates, Trusted Platform Module etc. or proprietary formats such as Intel® SGX attestation block, etc. The attestation token may be returned to the IPU **3320** upon successful verification and appraisal (e.g., as outlined in an IETF RATS Architecture (RFC9334), which provides an example approach of attestation appraisal). The token may be presented to another mesh layer node such as a WL FaaS μ Service **3318** in response to a request to obtain IPU resources or in response to other events that bind WL hosting resources. The token (e.g., token-1, shown in operation 3) may contain the AS issue attestation result, a token validity period, policies for proper use, and additional security related attributes including authentication credentials, authorization policies, an audit policy, access control rules and so forth. The token

may be evaluated by the μ Service **3318** to facilitate binding the μ Service layer resources to the IPU layer resources. It may also be supplied with an attestation payload to an AS microservice **3312** (FIG. 33, operation 4) to request an attestation token describing the μ Service node. The token-2 (FIG. 33, operation 5) may contain token-1 to form a composite token, Token-1,2 (FIG. 33, operation 6). The composite token may be issued by an AS microservice **3312** by verifying attestation evidence supplied by the μ Service **3318** and may include evaluation of the lower layer token (e.g., token-1). Verification of token-1 may suffice for establishing attestation properties as a performance optimization that avoids unnecessarily re-attesting the IPU resource. The D-WL **3316** may trigger a FaaS μ Service attestation as part of a request to perform the μ Function. The μ Service **3318** may return an attestation token (FIG. 33, operation 6) that contains attestation results for the μ Service **3318** and IPU layered resources to the D-WL **3316** (FIG. 33, operation 7). The D-WL **3316** may be expected to coordinate with a peer D-WL node and where coordination/interaction is contingent on obtaining an attestation token. The D-WL **3316** may obtain an attestation token-3 (FIG. 33, operation 8). The attestation request may include lower layer attestation tokens (token-1,2) in addition to D-WL collected evidence. The AS microservice **3312** may evaluate D-WL evidence and verify the lower layer tokens' attestation results rather than re-attesting lower layers. Although, such re-attestation may be performed if there is reason to questioning the validity of the token such as if the token expiration has been exceeded. The D-WL **3316** may receive a token-1,2,3 (FIG. 33, operation 9) that is supplied to a peer Edge node **3330** in response to a request to receive such token or as a parameter to an edge API (such as a RESTful web interface) as a condition of interaction with the peer node. The peer node may be required by the D-WL **3316** (or indirectly by the AS microservice **3312** supporting the D-WL **3316**) to attest the peer node (FIG. 32, operation 10). In this manner, bilateral attestation may be accomplished by D-WL nodes.

[0161] A WLM may elastically increase/decrease the number of nodes in the distributed workload resulting in inaccurate attestation tokens. However, fully (exhaustively) re-attesting every D-WL and all the layers to the IPU/root-of-trust may not be required. Only the configurations affected by D-WL manipulation need to be re-issued.

[0162] FIG. 34 is a block diagram illustrating an attestation mesh token structure, according to an example. The token structure contains separate sections **3411**, **3412**, **3413** for attestation results relating to disparate attestation verification requests where a respective verification is recorded and digitally signed separately. Hence, these results can be dismantled and reconstructed accordingly to represent the current composition (or re-composition) of the WL/D-WL.

[0163] For instance, in FIG. 34, first IPU resource attestation results are shown as token-1 **3411** with an associated token signature, Signature 1. A second attestation token is shown as token-2 **3412** with attestation results for a μ Service module, and an associated signature, Signature 2. Additionally, a Signature 1,2 is added that establishes the binding between μ Service and IPU layers. Similarly, for the D-WL layer a token-1,2,3 is represented showing a third layer token as token-3 **3413**, having a Signature 3, plus a Signature 1,2,3 indicating the binding across the three layers. Signature 1,2 and Signature 1,2,3 may counter-sign signatures 1, 2, or 3 respectively as a way to assert the discrete

tokens were verified and processed according to a workflow such as is described by FIG. 33.

[0164] FIG. 35 is a block diagram illustrating a fully articulate attestation mesh token, according to an example. The WLM, USM, and IPUM mesh layers can function as a pool of resources that may be used in various ways to achieve greater operational efficiency, availability, and resiliency. The attestation token structure supports such scenarios by grouping pools of mesh layer resources having pre-computed attestation results for a respective pool member. For example, an IPU mesh consisting of a first IPU node may have attestation results represented by (token-1,N1). A second IPU node may have attestation results represented by (token-1,N2) and so forth. The pool of attestation results may be authenticated by a pool signature, Pool 1, Signature 1. Similarly, other mesh pools may have pooled tokens following a similar convention. A token may represent fully an attested mesh of a deployed workload as depicted by a token consisting of a Pool 1,2,3 token signed by a signature across the pools **3511**, **3512**, **3513** (horizontally) and across the layers (vertically) that may be used to efficiently verify a single token signature **3520**.

[0165] If the mesh deployments are static (do not contain changes that trigger reissuance of any sub-token) then the 'Pool Token 1,2,3' may be reused by any node in the pool/mesh to satisfy attestation checking requirements by checking a single signature and singleton token properties.

[0166] The pool-token for attestation (and other token forms) described herein may contain additional attributes for Authentication, Authorization, Audit, or Access control (in addition to Attestation). The token may be referred as an AAAA or "A4" token or "A5" token respectively. As such, the A4/A5 token may be supplied with a variety of network interfaces in Edge, Cloud, DApp deployments having minimal impact to API/interface design. The token may be passed directly over the interface or a reference to the token given where the receiver may obtain the token out-of-band. The token may be realized using existing standard token structures including W3C DID, CWT, JWT, XML-DSIG, CMS, and others.

[0167] Building Trusted Public or Private Repository Hosting Services

[0168] Edge customers are looking for actionable insights anywhere across the C2E spectrum with data flowing across IoT devices, IoT Edge, Network Edge, Core Network, and Data Center. This digital transformation is increasing demand for container workloads that depend on securing both public and private repositories.

[0169] With existing approaches, container workloads and sources on public and private repositories are often picked up by frameworks and solutions into their products in an "as-is" format. This legacy architecture fundamentally lets consumer WLMs become imported or migrated into cloud or edge hosting environments. This leads to security gaps and concerns, when repository artifacts get carried along by default. As a result, the security issues are on the forefront of concern as data owners expect vulnerability and integrity checks will be applied as precautionary measure (at data ingress), and at its termination point (at data egress) before being consumed by WL processors.

[0170] In existing systems, source code and container-based artifacts located in public and private cloud repositories lack attestation of repository contents. Workload contents and ingredients are often opaque such that when

workload data arrives at a destination, it is subject to integrity and trust verification, which leads to repetitive consumption of compute, resulting in lower overall compute capacity. Data integrity checking can also lead to additional expense and compute latency. However, the overall C2E ecosystem requires these Zero-Trust mechanisms. One objective introduced herein is to provide improvements to these mechanisms at a lower cost.

[0171] The following framework described herein aims to address Zero-Trust requirements relating to data privacy laws in a way that will accelerate C2E security. This framework includes a trust on-demand capability that is easily consumed by elastic workload frameworks. The systems and methods support building of trusted containers or source repositories, to also facilitate secure workload migration and orchestration.

[0172] The present systems and methods automate building of trusted repositories at the locations where WLMs are hosted. These may be cloud and edge public and private repositories containing sensitive trusted identities.

[0173] FIG. 36 is a swim lane diagram illustrating interactions between entities to build a trusted repository, according to an example. The architecture for building a trusted repository includes a cloud repository infrastructure **3602** hosting a group of tools and frameworks **3610** such as a scanner **3612**, a software bill of materials generator **3614**, a license detector **3616**, and privileges detector **3618**, in addition to a trusted repository cloud agent **3604**.

[0174] In more detail, the scanner **3612** (e.g., provided by Synk, Sysdig scanners) are tools and frameworks detect vulnerabilities in container images and packages. The software bill of material (SBOM) generator **3614** (e.g., provided by Docker Sbom, Tern, etc.) are used to produce SBOMs, which provide a formal record containing the details of the supply chain relationships of various components used in building software. SBOM components, including libraries and modules, can be open source or proprietary. Thus, tracking and recording dependencies will impact WL execution trust. The license detector **3616** (e.g., provided by Black Duck Binary Analysis, Docker tools) is a tool to detect license risks in software binaries (e.g., using tools like BDBA). The privileges detector **3618** (e.g., provided by S-trace, Linux operating system kernel, etc.) is used to evaluate the software binary executables' privileges. These privileges are capabilities that are integral to execution and enforced by system calls into the kernel. The greater the privilege needed, the greater the security risk as OS kernels operate with ring-0 (e.g., superuser) privilege, which should be minimized given the potential for malicious binaries.

[0175] The end-to-end workflow illustrated in FIG. 36 illustrates a dynamic building of trusted repositories where a cloud hosting environment hosts public and private repositories, and where a client application interacts with live repositories. The cloud hosting environment uses the cloud agent **3604** to ensure the security and integrity of the repositories while being hosted. Multiple workload contexts are represented as "users" (e.g., User1, User2), where a user context may interact with a particular workload (e.g., Client App). User activity could result in corruption or compromise of the repository. To address such concerns, the cloud agent **3604** ensures repositories are security and integrity checked based on built-in repository tooling (e.g., AV scan, integrity scan, SBOM checking, license use and checks, access privilege management and enforcement, etc.). The cloud agent

3604 may apply one or more checks as a prerequisite to a repository lifecycle status change, such as branching content for modification by a user, or merging a branch, or protecting an original (also referred to as a “master”) image.

[0176] Repositories may be shared across multiple users and workloads using an access control mechanism that labels or categorizes the content according to an access policy. For instance, a repository may be labeled as ‘critical’ for use in critical infrastructure deployments, while another repository may be labeled as ‘personal’ for content that contains Personally Identifiable Information (PII).

[0177] Remote access by a workload may use cryptographic keys that attest repository trust properties to a client app. Repository attestation may include attestation of the cloud agent(s), users, and repo lifecycle status change histories. Client apps may likewise authenticate and attest to the cloud agent as a condition of accessing a repository.

[0178] The cloud repository may support staged deployment of workloads by partitioning repository resources according to a staging policy that identifies resources that are in (a) full, (b) preliminary, (c) simulated, (d) pre-onboarded, and (e) quarantined deployment stages. Staged deployments enable various forms of deployment risk to be mitigated. Storage resource partitioning may be applied using IO virtualization (e.g., using Intel® TDX-Connect), process virtualization (e.g., using Intel® VT-x, VT-d, TDX, SGX technologies), and containers (e.g., K8S, Kata). A deployment staging policy may be applied by the Cloud Agent on behalf of Users and Client App subscribers.

[0179] Turning to FIG. 36, the transactions are as follows. Consider a cloud repository host that includes users (user1 and user2 as a simple illustration) with a respective user holding multiple repositories and branches. At time t_0 , operations begin with the trust agent in the cloud repository host initiating a request for evaluating metrics on vulnerabilities for user1->repo11->main. The response is received at t_1 , with set of detected vulnerabilities categorized as high, medium, and low. Additionally, other metrics including a software bill of materials, privileges, and license details are obtained for user1->repo11->main branch over upcoming requests and cycles to arrive at a consolidated evaluation of security vectors for the cloud repository host.

[0180] At time t_{10} , the request is sent for user2->repo-branch1 seeking the SBOM on the binaries in the repository, followed by a response received at time t_{11} . This exercise of a request and response can be repeated for all the repositories and branches, over various vectors of security across relevant tools, to obtain appropriate grading by the system and trust cloud agent.

[0181] At time t_{25} , once all the vectors have been evaluated for the repository, the vectors are subjected to classification with grading (e.g., as red, white, yellow, green, blue, black). A grading scale may be used where the better the grading, the better is the repository with respect to security integrity.

[0182] At time t_{26} , the metadata obtained by the trusted cloud agent is signed using a hashing algorithm (e.g., SHA256).

[0183] If the content of the repository is considered for consumption by the client application by way of import at time t_{30} , the content can be subject to verification at t_{31} . This is followed by a verification from the application’s security policy engine to determine if the import is from a trusted repository or not. This can be allowed based on the

policy set by the application; otherwise the execution or deployment of the workload can be rejected.

[0184] Optionally, at time t_{40} the client application sends feedback to the host repository, which includes observations with respect to the grading it has received from the repo host during import. The feedback received from the client application can also be considered for further fine tuning the grading on the repository as well.

[0185] At time t_{50} , the trust cloud agent iterates an evaluation of the repositories against security vectors at certain intervals or cadence. The feedback obtained from execution of frameworks/tools and client application can be fed back for further reinforcement or improvement purposes (e.g., using reinforcement learning in a machine learning inference model).

[0186] The consumer may optionally consume the metadata offered by the cloud repository or generate metadata their own. However, many the trusted repositories are trusted by default and ready to be consumed by the user.

[0187] Another benefit the trusted repositories is to enable workload definitions and specifications (e.g., in YAML format) to represent a resource entry as a trusted repository. This can enable a policy engine at a client side to accept or reject deployments across the orchestration accordingly. A typical implementation of such an approach can be adopted by an orchestration layer.

[0188] Another aspect of building trust may include running workloads with various input touch points to gain an incremental generation of trust, and to present information related to the trust on a user interface or dashboard. Statistical graph/metrics on behavior of a workload can be obtained based on variations of data with respective iterations of execution. The incremental executions can be achieved by running the workloads inside a container runtime (e.g., kata containers).

[0189] In further examples, the cloud agent **3604** may be hardened using a trusted execution environment technology (e.g., Intel® SGX/TDX, ARM® TrustZone, AMD® SEV, etc.). Root-of-trust technology (e.g., DICE, SGX, TPM, TXT, Boot Guard, etc.) may be used for attestable identities and attestation evidence creation. Industry standards (e.g., DMTF SPDM, IETF CoRIM, TCG DICE, C2PA, OpenSSF SBOM and others) provide standardized building blocks for attesting hardware, software, containers, and data. Accordingly, these functionalities can be integrated as part of a web/edge/cloud services solution, including the cloud-to-edge deployments discussed herein.

[0190] A variety of use cases may be provided with the use of trusted repositories. Additional functional specifications and features of the system are referenced in the following use cases.

[0191] A use case may enable a continuous run of scans on the WLS hosted in the repositories. Here, a respective WL can be subjected to run at a regular cadence with up-to-date attestations.

[0192] Another use case may include having respective repositories obtain a class of grading (e.g., using colors corresponding to grades represented by red, white, yellow, orange, green, blue, brown, and black; or by weighted values as described by IETF AR4SI—Attestation Results for Secure Interactions), based on the validity of attestation as approved by the consumer and the quality of WLS sitting in the repository.

[0193] Another use case includes repositories that mark the metadata obtained from tools and frameworks into respective classifications (e.g., based on classifications such as in red, yellow, orange, and green, corresponding to high, low, medium, and good statuses). In other examples, the classification of metadata into grades for repositories is optional. In other examples, repositories are gauged alone by the metadata generated. For instance, the metadata generated by the repositories can be marked as private or public by the repository owners regardless of the public and private status of the repository by itself. In other examples, the quality of the WL can be evaluated by an age of vulnerability that is embedded into the WL.

[0194] Another use case includes a validation of trust generated by the repository compared with consumer approval, based on the attestation and risk of WL acceptance with respect to access control. For instance, the rating on the trust for repository can be marked based on a verification of attestation by the consumer (and the feedback given by the consumer). In further examples, more than “N” consumers perform verifications of the attestations granted by the trusted repository, to obtain a particular grading class.

[0195] In further examples, the orchestration layer can indicate a repository as trusted, requiring no further security checks from the consumer. For example, repositories may be marked as trusted based on SBOMs, vulnerabilities, licenses and privileges generated.

[0196] Another use case includes providing workload definitions in the form of YAMLS or packages, to carry a “trusted repository” resource entry with location of details on the security vectors across the repository. A policy engine may allow or reject execution of deployment based on the trusted repository resource entry that was received on import from the cloud repository.

[0197] Another use case includes obtaining feedback by iterations of execution by the trust cloud agent. Such iterations may be subjected to reinforcement learning for pattern-based inferences. In further examples, workloads are subjected to iterative runs with various input touchpoints. Also in further examples, workloads that are subjected to iterative runs can be represented in a user interface dashboard with the observations and newer ratings.

Implementation Examples

[0198] FIG. 37 is a flowchart illustrating operations for managing distributed workloads in an edge computing environment, according to an example.

[0199] Operation 3710 includes identifying characteristics of a distributed workload from an ongoing execution of the distributed workload. As discussed in the examples above, a distributed workload may include a workload that is partitioned among multiple computing nodes for processing and/or execution. In a specific example, the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, and the operations of the computing system are coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload, such that the IaaS configuration provides a uniform interface for allocating trusted resources to the distributed workload. In another specific example, the multiple computing nodes are provided by a cloud repository infrastructure, and the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

[0200] Operation 3720 includes evaluating a trust status of the distributed workload, using the identified characteristics, in response to a change in the execution of the distributed workload. In a specific example, operations for evaluating the trust status may be performed by a trust coordination framework service. Also in a specific example, the characteristics of the distributed workload include expected trust properties to exist between a workload execution environment and respective infrastructure resources. These expected trust properties are used to enable control of the execution of the distributed workload based on use of a token that includes security intents metadata to describe the expected trust properties.

[0201] Operation 3730 includes verifying resources to execute the distributed workload and verifying security policies associated with the resources. Additional operations for evaluating the trust status and verifying the resources may be performed as discussed in the various examples above.

[0202] Operation 3740 includes controlling the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status. This may include the various workload execution and management operations discussed above.

[0203] FIG. 38 is a flowchart illustrating operations for adapting execution of distributed workloads in an edge computing environment, according to an example. In some examples, these operations may be optionally performed, performed in another order, or repeated based on the examples provided above.

[0204] Operation 3810 includes evaluating data provenance, attestation properties, and workload provenance, using a trust coordination framework service. The trust coordination framework service may provide evaluation results based on these properties, which are used to control of the execution of the distributed workload among the multiple computing nodes.

[0205] Operation 3820 includes distributing an attestation workload (associated with the distributed workload) by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload. This attestation workload processing may occur based on the attestation workload management techniques discussed above. Here, portions of the attestation workload may be used to determine attestation of the multiple computing nodes, to provide information that is useful to evaluate the trust status of the distributed workload or of resources to execute the distributed workload.

[0206] Operation 3830 includes coordinating a software or firmware update for the change in the execution of the distributed workload. In this setting, a change in the execution of the distributed workload may be provided from a software or firmware update to at least one of the multiple computing nodes. In a further example, the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource. In another example, the software or firmware update is coordinated by a workload update manager, and the workload update manager operates to coordinate distribution of the software or firmware update among respective workload execution environments and resources of the multiple computing nodes.

[0207] Operation 3840 includes coordinating operations based on resource simulation and testing of resource bind-

ings. As an example, the determined characteristics of the distributed workload may be based on results from a resource simulation performed on the distributed workload. Additionally, the resource simulation may include testing of resource bindings to be used by the distributed workload among simulated distributed resources.

[0208] Additional examples of the presently described method, system, and device embodiments include the following, non-limiting implementations. Each of the following non-limiting examples may stand on its own or may be combined in any permutation or combination with any one or more of the other examples provided below or throughout the present disclosure.

[0209] Example 1 is a computing system configured to manage distributed workloads, comprising: processing circuitry; and a memory device including instructions embodied thereon, wherein the instructions, which when executed by the processing circuitry, configure the processing circuitry to cause operations that: identify characteristics of a distributed workload from an ongoing execution of the distributed workload, the distributed workload being partitioned among multiple computing nodes; evaluate a trust status of the distributed workload in response to a change in the execution of the distributed workload, including verifying resources to execute the distributed workload and verifying security policies associated with the resources; and control the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status.

[0210] In Example 2, the subject matter of Example 1 optionally includes subject matter where the characteristics of the distributed workload include expected trust properties to exist between a workload execution environment and respective infrastructure resources, and wherein the control of the execution of the distributed workload is based on use of a token that includes security intents metadata to describe the expected trust properties.

[0211] In Example 3, the subject matter of any one or more of Examples 1-2 optionally include subject matter where the operations to evaluate the trust status are performed by a trust coordination framework service, and wherein the instructions further configure the processing circuitry to cause operations that: evaluate data provenance of data associated with the distributed workload, attestation properties of the resources to execute the distributed workload, and workload provenance of respective portions of the distributed workload, using the trust coordination framework service; wherein the control of the execution of the distributed workload among the multiple computing nodes is further based on evaluation results from the trust coordination framework service.

[0212] In Example 4, the subject matter of any one or more of Examples 1-3 optionally include subject matter where the distributed workload is associated with an attestation workload, and wherein the instructions further configure the processing circuitry to cause operations that: distribute the attestation workload by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload; wherein the portions of the attestation workload are used to determine attestation

of the multiple computing nodes, to provide information to evaluate the trust status of the distributed workload.

[0213] In Example 5, the subject matter of any one or more of Examples 1-4 optionally include subject matter where the change in the execution of the distributed workload is provided from a software or firmware update to at least one of the multiple computing nodes.

[0214] In Example 6, the subject matter of Example 5 optionally includes subject matter where the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource.

[0215] In Example 7, the subject matter of any one or more of Examples 5-6 optionally include subject matter where the software or firmware update is coordinated by a workload update manager, and wherein the workload update manager is to coordinate distribution of the software or firmware update among respective workload execution environments and resources of the multiple computing nodes.

[0216] In Example 8, the subject matter of any one or more of Examples 1-7 optionally include subject matter where the multiple computing nodes are provided by a cloud repository infrastructure, and wherein the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

[0217] In Example 9, the subject matter of any one or more of Examples 1-8 optionally include subject matter where the characteristics of the distributed workload are based on results from a resource simulation performed on the distributed workload, and wherein the resource simulation includes testing of resource bindings to be used by the distributed workload among simulated distributed resources.

[0218] In Example 10, the subject matter of any one or more of Examples 1-9 optionally include subject matter where the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, wherein the operations of the computing system are coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload, and wherein the IaaS configuration provides a uniform interface for allocating trusted resources to the distributed workload.

[0219] Example 11 is at least one non-transitory machine-readable storage medium comprising instructions stored thereupon, which when executed by processing circuitry of a computing machine, cause the processing circuitry to: identify characteristics of a distributed workload from an ongoing execution of the distributed workload, the distributed workload being partitioned among multiple computing nodes; evaluate a trust status of the distributed workload in response to a change in the execution of the distributed workload, including verifying resources to execute the distributed workload and verifying security policies associated with the resources; and control the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status.

[0220] In Example 12, the subject matter of Example 11 optionally includes subject matter where the characteristics of the distributed workload include expected trust

properties to exist between a workload execution environment and respective infrastructure resources, and wherein the control of the execution of the distributed workload is based on use of a token that includes security intents metadata to describe the expected trust properties.

[0221] In Example 13, the subject matter of any one or more of Examples 11-12 optionally include subject matter where operations to evaluate the trust status are performed by a trust coordination framework service, and wherein the instructions cause the processing circuitry to: evaluate data provenance of data associated with the distributed workload, attestation properties of the resources to execute the distributed workload, and workload provenance of respective portions of the distributed workload, using the trust coordination framework service; wherein the control of the execution of the distributed workload among the multiple computing nodes is further based on evaluation results from the trust coordination framework service.

[0222] In Example 14, the subject matter of any one or more of Examples 11-13 optionally include subject matter where the distributed workload is associated with an attestation workload, and wherein the instructions further cause the processing circuitry to: distribute the attestation workload by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload; wherein the portions of the attestation workload are used to determine attestation of the multiple computing nodes, to provide information to evaluate the trust status of the distributed workload.

[0223] In Example 15, the subject matter of any one or more of Examples 11-14 optionally include subject matter where the change in the execution of the distributed workload is provided from a software or firmware update to at least one of the multiple computing nodes.

[0224] In Example 16, the subject matter of Example 15 optionally includes subject matter where the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource.

[0225] In Example 17, the subject matter of any one or more of Examples 15-16 optionally include subject matter where the software or firmware update is coordinated by a workload update manager, and wherein the workload update manager is to coordinate distribution of the software or firmware update among respective workload execution environments and resources of the multiple computing nodes.

[0226] In Example 18, the subject matter of any one or more of Examples 11-17 optionally include subject matter where the multiple computing nodes are provided by a cloud repository infrastructure, and wherein the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

[0227] In Example 19, the subject matter of any one or more of Examples 11-18 optionally include subject matter where the characteristics of the distributed workload are based on results from a resource simulation performed on the distributed workload, and wherein the resource simulation includes testing of

resource bindings to be used by the distributed workload among simulated distributed resources.

[0228] In Example 20, the subject matter of any one or more of Examples 11-19 optionally include subject matter where the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, wherein operations of the computing machine are coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload, and wherein the IaaS configuration provides a uniform interface for allocating trusted resources to the distributed workload.

[0229] Example 21 is a method of managing distributed workloads, comprising: identifying characteristics of a distributed workload from an ongoing execution of the distributed workload, the distributed workload being partitioned among multiple computing nodes; evaluating a trust status of the distributed workload in response to a change in the execution of the distributed workload, including verifying resources to execute the distributed workload and verifying security policies associated with the resources; and controlling the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status.

[0230] In Example 22, the subject matter of Example 21 optionally includes subject matter where the characteristics of the distributed workload include expected trust properties to exist between a workload execution environment and respective infrastructure resources, and wherein the control of the execution of the distributed workload is based on use of a token that includes security intents metadata to describe the expected trust properties.

[0231] In Example 23, the subject matter of any one or more of Examples 21-22 optionally include subject matter where the evaluating the trust status is performed by a trust coordination framework service, and wherein the method further comprises: evaluating data provenance of data associated with the distributed workload, attestation properties of the resources to execute the distributed workload, and workload provenance of respective portions of the distributed workload, using the trust coordination framework service; wherein the control of the execution of the distributed workload among the multiple computing nodes is further based on evaluation results from the trust coordination framework service.

[0232] In Example 24, the subject matter of any one or more of Examples 21-23 optionally include subject matter where the distributed workload is associated with an attestation workload, and wherein the method further comprises: distributing the attestation workload by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload; wherein the portions of the attestation workload are used to determine attestation of the multiple computing nodes, to provide information to evaluate the trust status of the distributed workload.

[0233] In Example 25, the subject matter of any one or more of Examples 21-24 optionally include subject matter where the change in the execution of the dis-

tributed workload is provided from a software or firmware update to at least one of the multiple computing nodes.

[0234] In Example 26, the subject matter of Example 25 optionally includes subject matter where the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource.

[0235] In Example 27, the subject matter of any one or more of Examples 25-26 optionally include subject matter where the software or firmware update is coordinated by a workload update manager, and wherein the workload update manager is to coordinate distribution of the software or firmware update among respective workload execution environments and resources of the multiple computing nodes.

[0236] In Example 28, the subject matter of any one or more of Examples 21-27 optionally include subject matter where the multiple computing nodes are provided by a cloud repository infrastructure, and wherein the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

[0237] In Example 29, the subject matter of any one or more of Examples 21-28 optionally include subject matter where the characteristics of the distributed workload are based on results from a resource simulation performed on the distributed workload, and wherein the resource simulation includes testing of resource bindings to be used by the distributed workload among simulated distributed resources.

[0238] In Example 30, the subject matter of any one or more of Examples 21-29 optionally include subject matter where the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, wherein the method is coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload, and wherein the IaaS configuration provides a uniform interface for allocating trusted resources to the distributed workload.

[0239] Overview of Edge Computing Environments

[0240] FIG. 39 is a block diagram 3900 showing an overview of a configuration for edge computing, which includes a layer of processing referenced in many of the current examples as an “edge cloud.” As shown, the edge cloud 3910 is co-located at an edge location, such as an access point or base station 3940, a local processing hub 3950, or a central office 3920, and thus may include multiple entities, devices, and equipment instances. The edge cloud 3910 is located much closer to the endpoint (consumer and producer) data sources 3960 (e.g., autonomous vehicles 3961, user equipment 3962, business and industrial equipment 3963, video capture devices 3964, mobile vehicles (e.g., drones) 3965, smart cities and building devices 3966, sensors and IoT devices 3967, etc.) than the cloud data center 3930. Compute, memory, and storage resources which are offered at the edges in the edge cloud 3910 are critical to providing ultra-low latency response times for services and functions used by the endpoint data sources 3960 as well as reduce network backhaul traffic from the edge cloud 3910 toward cloud data center 3930 thus improving energy consumption and overall network usages among other benefits.

[0241] Compute, memory, and storage are scarce resources, and generally, decrease depending on the edge location (e.g., fewer processing resources being available at consumer end point devices than at a base station or at a central office). However, the closer that the edge location is to the endpoint (e.g., UEs), the more that space and power are constrained. Thus, edge computing, as a general design principle, attempts to minimize the resources needed for network services, through the distribution of more resources which are located closer both geographically and in-network access time. In this manner, edge computing attempts to bring the compute resources to the workload data where appropriate, or bring the workload data to the compute resources.

[0242] The following describes aspects of an edge cloud architecture that covers multiple potential deployments and addresses restrictions that some network operators or service providers may have in their own infrastructures. These include, variation of configurations based on the edge location (because edges at a base station level, for instance, may have more constrained performance and capabilities in a multi-tenant scenario); configurations based on the type of compute, memory, storage, fabric, acceleration, or like resources available to edge locations, tiers of locations, or groups of locations; the service, security, and management and orchestration capabilities; and related objectives to achieve usability and performance of end services. These deployments may accomplish processing in network layers that may be considered as “near edge,” “close edge,” “local edge,” “middle edge,” or “far edge” layers, depending on latency, distance, and timing characteristics.

[0243] Edge computing is a developing paradigm where computing is performed at or closer to the “edge” of a network, typically through the use of a compute platform (e.g., x86, AMD or ARM hardware architectures) implemented at base stations, gateways, network routers, or other devices which are much closer to end point devices producing and consuming the data. For example, edge gateway servers may be equipped with pools of memory and storage resources to perform computation in real-time for low latency use-cases (e.g., autonomous driving or video surveillance) for connected client devices. Or as an example, base stations may be augmented with compute and acceleration resources to directly process service workloads for connected user equipment, without further communicating data via backhaul networks. Or as another example, central office network management hardware may be replaced with compute hardware that performs virtualized network functions and offers compute resources for the execution of services and consumer functions for connected devices. Within edge computing networks, there may be scenarios in services in which the compute resource will be “moved” to the data, as well as scenarios in which the data will be “moved” to the compute resource. Or as an example, base station compute, acceleration and network resources can provide services to scale to workload demands on an as-needed basis by activating dormant capacity (subscription, capacity-on-demand) to manage corner cases, emergencies or to provide longevity for deployed resources over a significantly longer implemented lifecycle.

[0244] In contrast to the network architecture of FIG. 39, traditional endpoint (e.g., UE, vehicle-to-vehicle (V2V), vehicle-to-everything (V2X), etc.) applications are reliant on local device or remote cloud data storage and processing

to exchange and coordinate information. A cloud data arrangement allows for long-term data collection and storage but is not optimal for highly time-varying data, such as a collision, traffic light change, etc. and may fail in attempting to meet latency challenges.

[0245] Depending on the real-time requirements in a communications context, a hierarchical structure of data processing and storage nodes may be defined in an edge computing deployment. For example, such a deployment may include local ultra-low-latency processing, regional storage, and processing as well as remote cloud data center-based storage and processing. Key performance indicators (KPIs) may be used to identify where sensor data is appropriately transferred and where it is processed or stored. This typically depends on the ISO layer dependency of the data. For example, lower layer (PHY, MAC, routing, etc.) data typically changes quickly and is better handled locally to meet latency requirements. Higher layer data such as Application-Layer data is typically less time-critical and may be stored and processed in a remote cloud data center.

[0246] FIG. 40 illustrates deployment and orchestration for virtual edge configurations across an edge computing system operated among multiple edge nodes and multiple tenants. Specifically, FIG. 40 depicts coordination of a first edge node 4022 and a second edge node 4024 in an edge computing system 4000, to fulfill requests and responses for various client endpoints 4010 (e.g., smart cities/building systems, mobile devices, computing devices, business/logistics systems, industrial systems, etc.), which access various virtual edge instances. The virtual edge instances 4032, 4034 (or virtual edges) provide edge compute capabilities and processing in an edge cloud, with access to a cloud/data center 4040 for higher-latency requests for websites, applications, database servers, etc. Thus, the edge cloud enables coordination of processing among multiple edge nodes for multiple tenants or entities.

[0247] In the example of FIG. 40, these virtual edge instances include a first virtual edge 4032, offered to a first tenant (Tenant 1), which offers a first combination of edge storage, computing, and services; and a second virtual edge 4034, offering a second combination of edge storage, computing, and services, to a second tenant (Tenant 2). The virtual edge instances 4032, 4034 are distributed among the edge nodes 4022, 4024, and may include scenarios in which a request and response are fulfilled from the same or different edge nodes. The configuration of the individual edge nodes 4022, 4024 to operate in a distributed yet coordinated fashion occurs based on edge provisioning functions 4050. The functionality of the edge nodes 4022, 4024 to provide coordinated operation for applications and services, among multiple tenants, occurs based on orchestration functions 4060.

[0248] It should be understood that some of the devices in 4010 are multi-tenant devices where Tenant1 may function within a Tenant1 ‘slice’ while a Tenant2 may function within a Tenant2 ‘slice’ (and, in further examples, additional or sub-tenants may exist; and a respective tenant may be specifically entitled and transactionally tied to a specific set of features all the way to specific hardware features). A trusted multi-tenant device may further contain a tenant-specific cryptographic key such that the combination of a key and a slice may be considered a “root of trust” (RoT) or tenant-specific RoT. A RoT may further be computed dynamically composed using a compute security architec-

ture, such as a DICE (Device Identity Composition Engine) architecture where a DICE hardware building block is used to construct layered trusted computing base contexts for secured and authenticated layering of device capabilities (such as with use of a Field Programmable Gate Array (FPGA)). The RoT also may be used for a trusted computing context to support respective tenant operations, etc. Use of this RoT and the compute security architecture may be enhanced by the attestation operations further discussed herein.

[0249] Edge computing nodes may partition resources (memory, central processing unit (CPU), graphics processing unit (GPU), interrupt controller, input/output (I/O) controller, memory controller, bus controller, etc.) where respective partitionings may contain a RoT capability and where fan-out and layering according to a DICE model may further be applied to Edge Nodes. Cloud computing nodes consisting of containers, FaaS (function as a service) engines, servlets, servers, or other computation abstraction may be partitioned according to a DICE layering and fan-out structure to support a RoT context for each. Accordingly, the respective RoTs spanning devices in 4010, 4022, and 4040 may coordinate the establishment of a distributed trusted computing base (DTCB) such that a tenant-specific virtual trusted secure channel linking all elements end-to-end can be established.

[0250] Further, it will be understood that a container may have data or workload-specific keys protecting its content from a previous edge node. As part of the migration of a container, a pod controller at a source edge node may obtain a migration key from a target edge node pod controller where the migration key is used to wrap the container-specific keys. When the container/pod is migrated to the target edge node, the unwrapping key is exposed to the pod controller that then decrypts the wrapped keys. The keys may now be used to perform operations on container specific data. The migration functions may be gated by properly attested edge nodes and pod managers (as described above).

[0251] As an example, the edge computing system may be extended to provide orchestration of multiple applications through the use of containers (a contained, deployable unit of software that provides code and needed dependencies), in a multi-owner, multi-tenant environment. A multi-tenant orchestrator may be used to perform key management, trust anchor management, and other compute security functions related to the provisioning and lifecycle of the trusted ‘slice’ concept in FIG. 40. An orchestrator may use a DICE layering and fan-out construction to create a root of trust context that is tenant specific. Thus, orchestration functions, provided by an orchestrator, may participate as a tenant-specific orchestration provider.

[0252] Accordingly, an edge-computing system may be configured to fulfill requests and responses for various client endpoints from multiple virtual edge instances (and, from a cloud or remote data center, not shown). The use of these virtual edge instances supports multiple tenants and multiple applications (e.g., augmented reality (AR)/virtual reality (VR), enterprise applications, content delivery, gaming, compute offload) simultaneously. Further, there may be multiple types of applications within the virtual edge instances (e.g., normal applications, latency-sensitive applications, latency-critical applications, user plane applications, networking applications, etc.). The virtual edge instances may also be spanned across systems of multiple

owners at different geographic locations (or, respective computing systems and resources which are co-owned or co-managed by multiple owners).

[0253] For instance, a respective edge node **4022**, **4024** may implement the use of containers, such as with the use of a container “pod” **4026**, **4028** providing a group of one or more containers. In a setting that uses one or more container pods, a pod controller or orchestrator is responsible for local control and orchestration of the containers in the pod. Various edge node resources (e.g., storage, compute, services, depicted with hexagons) provided for the respective edge slices of virtual edges **4032**, **4034** are partitioned according to the needs of a respective container.

[0254] With the use of container pods, a pod controller oversees the partitioning and allocation of containers and resources. The pod controller receives instructions from an orchestrator (e.g., performing orchestration functions **4060**) that instructs the controller on how to appropriately partition physical resources and for what duration, such as by receiving key performance indicator (KPI) targets based on SLA contracts. The pod controller determines which container uses which resources and for how long to complete the workload and satisfy the SLA. The pod controller also manages container lifecycle operations such as: creating the container, provisioning it with resources and applications, coordinating intermediate results between multiple containers working on a distributed application together, dismantling containers when workload completes, and the like. Additionally, a pod controller may serve a compute security role that prevents the assignment of resources until the right tenant authenticates or prevents provisioning of data or a workload to a container until an attestation result is satisfied.

[0255] Also, with the use of container pods, tenant boundaries can still exist but in the context of a respective pod of containers. If a respective tenant-specific pod has a tenant-specific pod controller, there may be a shared pod controller that consolidates resource allocation requests to avoid typical resource starvation situations. Further controls may be provided to ensure the attestation and trustworthiness of the pod and pod controller. For instance, the orchestrator **4060** may provision an attestation verification policy to local pod controllers that perform attestation verification. If an attestation satisfies a policy for a first tenant pod controller but not a second tenant pod controller, then the second pod may be migrated to a different edge node that does satisfy it. Alternatively, the first pod may be allowed to execute and a different shared pod controller is installed and invoked before the second pod executing.

[0256] In further examples, edge computing systems may deploy containers in an edge computing system. As a simplified example, a container manager is adapted to launch containerized pods, functions, and functions-as-a-service instances through execution via compute nodes, or to separately execute containerized virtualized network functions through execution via compute nodes. This arrangement may be adapted for use by multiple tenants in system arrangement, where containerized pods, functions, and functions-as-a-service instances are launched within virtual machines specific to an individual tenant (aside from the execution of virtualized network functions).

[0257] Within the edge cloud, a first edge node **4022** (e.g., operated by a first owner) and a second edge node **4024** (e.g., operated by a second owner) may operate or respond to a container orchestrator to coordinate the execution of various

applications within the virtual edge instances offered for respective tenants. For instance, the edge nodes **4022**, **4024** may be coordinated based on edge provisioning functions **4050**, while the operation of the various applications is coordinated with orchestration functions **4060**.

[0258] Various system arrangements may provide an architecture that treats VMs, Containers, and Functions equally in terms of application composition (and resulting applications are combinations of these three ingredients). A respective ingredient may involve the use of one or more accelerator (e.g., FPGA, ASIC, cryptographic execution) components as a local backend. In this manner, applications can be split across multiple edge owners, coordinated by an orchestrator.

[0259] It should be appreciated that the edge computing systems and arrangements discussed herein may be applicable in various solutions, services, and/or use cases. As an example, FIG. **41** shows a simplified vehicle compute and communication use case involving mobile access to applications in an edge computing system **4100** that implements an edge cloud **3910** connected to Trust-as-a-Service (TaaS) instances **4145**. In this use case, a client compute node **4110** may be embodied as in-vehicle compute systems (e.g., in-vehicle navigation and/or infotainment systems) located in corresponding vehicles that communicate with the edge gateway nodes **4120** during traversal of a roadway. For instance, edge gateway nodes **4120** may be located in roadside cabinets, which may be placed along the roadway, at intersections of the roadway, or other locations near the roadway. As a vehicle traverses along the roadway, the connection between its client compute node **4110** and a particular edge gateway node **4120** may propagate to maintain a consistent connection and context for the client compute node **4110**. The respective nodes of the edge gateway nodes **4120** includes some processing and storage capabilities and, as such, some processing and/or storage of data for the client compute nodes **4110** may be performed on one or more of the edge gateway nodes **4120**.

[0260] A respective node of the edge gateway nodes **4120** may communicate with one or more edge resource nodes **4140**, which are illustratively embodied as compute servers, appliances or components located at or in a communication base station **4142** (e.g., a base station of a cellular network). As discussed above, a respective edge resource node **4140** includes some processing and storage capabilities, and, as such, some processing and/or storage of data for the client compute nodes **4110** may be performed on the edge resource node **4140**. For example, the processing of data that is less urgent or important may be performed by the edge resource node **4140**, while the processing of data that is of a higher urgency or importance may be performed by edge gateway devices or the client nodes themselves (depending on, for example, the capabilities of a respective component). Further, various wired or wireless communication links (e.g., fiber optic wired backhaul, 5G wireless links) may exist among the edge nodes **4120**, edge resource node(s) **4140**, core data center **4150**, and network cloud **4160**.

[0261] The edge resource node(s) **4140** also communicate with the core data center **4150**, which may include compute servers, appliances, and/or other components located in a central location (e.g., a central office of a cellular communication network). The core data center **4150** may provide a gateway to the global network cloud **4160** (e.g., the Internet) for the edge cloud **3910** operations formed by the edge

resource node(s) **4140** and the edge gateway nodes **4120**. Additionally, in some examples, the core data center **4150** may include an amount of processing and storage capabilities and, as such, some processing and/or storage of data for the client compute devices may be performed on the core data center **4150** (e.g., processing of low urgency or importance, or high complexity). The edge gateway nodes **4120** or the edge resource nodes **4140** may offer the use of stateful applications **4132** and a geographically distributed data storage **4134** (e.g., database, data store, etc.).

[0262] In further examples, FIG. **41** may utilize various types of mobile edge nodes, such as an edge node hosted in a vehicle (e.g., car, truck, tram, train, etc.) or other mobile units, as the edge node will move to other geographic locations along the platform hosting it. With vehicle-to-vehicle communications, individual vehicles may even act as network edge nodes for other cars, (e.g., to perform caching, reporting, data aggregation, etc.). Thus, it will be understood that the application components provided in various edge nodes may be distributed in a variety of settings, including coordination between some functions or operations at individual endpoint devices or the edge gateway nodes **4120**, some others at the edge resource node **4140**, and others in the core data center **4150** or the global network cloud **4160**.

[0263] In further configurations, the edge computing system may implement FaaS computing capabilities through the use of respective executable applications and functions. In an example, a developer writes function code (e.g., “computer code” herein) representing one or more computer functions, and the function code is uploaded to a FaaS platform provided by, for example, an edge node or data center. A trigger such as, for example, a service use case or an edge processing event, initiates the execution of the function code with the FaaS platform.

[0264] In an example of FaaS, a container is used to provide an environment in which function code is executed. The container may be any isolated-execution entity (a workload execution environment) such as a process, a Docker or Kubernetes container, a virtual machine, etc. Within the edge computing system, various data center, edge, and endpoint (including mobile) devices are used to “spin up” functions (e.g., activate and/or allocate function actions) that are scaled on demand. The function code gets executed on the physical infrastructure (e.g., edge computing node) device and underlying virtualized containers. Finally, the container is “spun down” (e.g., deactivated and/or deallocated) on the infrastructure in response to the execution being completed.

[0265] Further aspects of FaaS may enable deployment of edge functions in a service fashion, including support of respective functions that support edge computing as a service. Additional features of FaaS may include: a granular billing component that enables customers (e.g., computer code developers) to pay only when their code gets executed; common data storage to store data for reuse by one or more functions; orchestration and management among individual functions; function execution management, parallelism, and consolidation; management of container and function memory spaces; coordination of acceleration resources available for functions; and distribution of functions between containers (including “warm” containers, already deployed or operating, versus “cold” which require deployment or configuration).

[0266] Example Internet of Things Architectures

[0267] As a more detailed illustration of an Internet of Things (IoT) network, FIG. **42** illustrates a drawing of a cloud or edge computing network **4200**, in communication with several IoT devices and a TaaS instance **4245**. The IoT is a concept in which a large number of computing devices are interconnected with one other and to the Internet to provide functionality and data acquisition at very low levels. Thus, as used herein, an IoT device may include a semiautonomous device performing a function, such as sensing or control, among others, in communication with other IoT devices and a wider network, such as the Internet.

[0268] Often, IoT devices are limited in memory, size, or functionality, allowing larger numbers to be deployed for a similar (or lower) cost compared to the cost of smaller numbers of larger devices. However, an IoT device may be a smartphone, laptop, tablet, or PC, or other larger device. Further, an IoT device may be a virtual device, such as an application on a smartphone or other computing device. IoT devices may include IoT gateways, used to couple IoT devices to other IoT devices and to cloud applications, for data storage, process control, and the like.

[0269] Networks of IoT devices may include commercial and home automation devices, such as water distribution systems, electric power distribution systems, pipeline control systems, plant control systems, light switches, thermostats, locks, cameras, alarms, motion sensors, and the like. The IoT devices may be accessible through remote computers, servers, and other systems, for example, to control systems or access data.

[0270] Returning to FIG. **42**, the network **4200** may represent portions of the Internet or may include portions of a local area network (LAN), or a wide area network (WAN), such as a proprietary network for a company. The IoT devices may include any number of different types of devices, grouped in various combinations. For example, a traffic control group **4206** may include IoT devices along streets in a city. These IoT devices may include stoplights, traffic flow monitors, cameras, weather sensors, and the like. The traffic control group **4206**, or other subgroups, may be in communication within the network **4200** through wired or wireless links **4208**, such as LPWA links, optical links, and the like. Further, a wired or wireless sub-network **4212** may allow the IoT devices to communicate with one another, such as through a local area network, a wireless local area network, and the like. The IoT devices may use another device, such as a gateway **4210** or **4228** to communicate with remote locations such as remote cloud **4202**; the IoT devices may also use one or more servers **4230** to facilitate communication within the network **4200** or with the gateway **4210**. For example, the one or more servers **4230** may operate as an intermediate network node to support a local edge cloud or fog implementation among a local area network. Further, the gateway **4228** that is depicted may operate in a cloud-to-gateway-to-many edge devices configuration, such as with the various IoT devices **4214**, **4220**, **4224** being constrained or dynamic to an assignment and use of resources in the network **4200**.

[0271] In an example embodiment, the network **4200** can further include or be communicatively coupled to a Trust-a-a-Service instance or deployment configured to perform trust attestation operations within the network **4200**, such as that discussed above.

[0272] Other example groups of IoT devices may include remote weather stations 4214, local information terminals 4216, alarm systems 4218, automated teller machines 4220, alarm panels 4222, or moving vehicles, such as emergency vehicles 4224 or other vehicles 4226, among many others. These IoT devices may be in communication with other IoT devices, with servers 4204, with another IoT device or system, another edge computing or “fog” computing system, or a combination therein. The groups of IoT devices may be deployed in various residential, commercial, and industrial settings (including in both private or public environments).

[0273] As may be seen from FIG. 42, a large number of IoT devices may be communicating through the network 4200. This may allow different IoT devices to request or provide information to other devices autonomously. For example, a group of IoT devices (e.g., the traffic control group 4206) may request a current weather forecast from a group of remote weather stations 4214, which may provide the forecast without human intervention. Further, an emergency vehicle 4224 may be alerted by an automated teller machine 4220 that a burglary is in progress. As the emergency vehicle 4224 proceeds towards the automated teller machine 4220, it may access the traffic control group 4206 to request clearance to the location, for example, by lights turning red to block cross traffic at an intersection in sufficient time for the emergency vehicle 4224 to have unimpeded access to the intersection.

[0274] Clusters of IoT devices may be equipped to communicate with other IoT devices as well as with a cloud network. This may allow the IoT devices to form an ad-hoc network between the devices, allowing them to function as a single device, which may be termed a fog device or system. Clusters of IoT devices, such as may be provided by the remote weather stations 4214 or the traffic control group 4206, may be equipped to communicate with other IoT devices as well as with the network 4200. This may allow the IoT devices to form an ad-hoc network between the devices, allowing them to function as a single device, which also may be termed a fog device or system.

[0275] In further examples, a variety of topologies may be used for IoT networks comprising IoT devices, with the IoT networks coupled through backbone links to respective gateways. For example, a number of IoT devices may communicate with a gateway, and with each other through the gateway. The backbone links may include any number of wired or wireless technologies, including optical networks, and may be part of a local area network (LAN), a wide area network (WAN), or the Internet. Additionally, such communication links facilitate optical signal paths among both IoT devices and gateways, including the use of MUXing/demuxing components that facilitate the interconnection of the various devices.

[0276] The network topology may include any number of types of IoT networks, such as a mesh network provided with the network using Bluetooth low energy (BLE) links. Other types of IoT networks that may be present include a wireless local area network (WLAN) network used to communicate with IoT devices through IEEE 802.11 (Wi-Fi®) links, a cellular network used to communicate with IoT devices through an LTE/LTE-A (4G) or 5G cellular network, and a low-power wide-area (LPWA) network, for example, a LPWA network compatible with the LoRaWan specification promulgated by the LoRa alliance, or an IPv6 over Low

Power Wide-Area Networks (LPWAN) network compatible with a specification promulgated by the Internet Engineering Task Force (IETF).

[0277] Further, the respective IoT networks may communicate with an outside network provider (e.g., a tier 2 or tier 3 provider) using any number of communications links, such as an LTE cellular link, a LPWA link, or a link based on the IEEE 802.15.4 standard, such as Zigbee®. The respective IoT networks may also operate with the use of a variety of network and internet application protocols such as the Constrained Application Protocol (CoAP). The respective IoT networks may also be integrated with coordinator devices that provide a chain of links that forms a cluster tree of linked devices and networks.

[0278] IoT networks may be further enhanced by the integration of sensing technologies, such as sound, light, electronic traffic, facial and pattern recognition, smell, vibration, into the autonomous organizations among the IoT devices. The integration of sensory systems may allow systematic and autonomous communication and coordination of service delivery against contractual service objectives, orchestration, and quality of service (QoS) based swarming and coordination/combinations of resources.

[0279] An IoT network, arranged as a mesh network, for instance, may be enhanced by systems that perform inline data-to-information transforms. For example, self-forming chains of processing resources comprising a multi-link network may distribute the transformation of raw data to information in an efficient manner, and the ability to differentiate between assets and resources and the associated management of the assets and resources. Furthermore, the proper components of infrastructure and resource-based trust and service indices may be inserted to improve the data integrity, quality, assurance, and deliver a metric of data confidence.

[0280] Example Computing Devices

[0281] At a more generic level, an edge computing system may be described to encompass any number of deployments operating in the edge cloud 3910, which provide coordination from client and distributed computing devices. FIG. 43 provides a further abstracted overview of layers of distributed compute deployed among an edge computing environment for purposes of illustration.

[0282] FIG. 43 generically depicts an edge computing system for providing edge services and applications to multi-stakeholder entities, as distributed among one or more client compute nodes 4302, one or more edge gateway nodes 4312, one or more edge aggregation nodes 4322, one or more core data centers 4332, and a global network cloud 4342, as distributed across layers of the network. The implementation of the edge computing system may be provided at or on behalf of a telecommunication service provider (“telco” or “TSP”), internet-of-things service provider, a cloud service provider (CSP), enterprise entity, or any other number of entities. Various forms of wired or wireless connections may be configured to establish connectivity among the nodes 4302, 4312, 4322, 4332, including interconnections among such nodes (e.g., connections among edge gateway nodes 4312, and connections among edge aggregation nodes 4322). Such connectivity and federation of these nodes may be assisted with the use of TaaS services 4360 and service instances, as discussed herein.

[0283] A respective node or device of the edge computing system is located at a particular layer corresponding to

layers **4310**, **4320**, **4330**, **4340**, and **4350**. For example, the client compute nodes **4302** are located at an endpoint layer **4310**, while the edge gateway nodes **4312** are located at an edge devices layer **4320** (local level) of the edge computing system. Additionally, the edge aggregation nodes **4322** (and/or fog devices **4324**, if arranged or operated with or among a fog networking configuration **4326**) is located at a network access layer **4330** (an intermediate level). Fog computing (or “fogging”) generally refers to extensions of cloud computing to the edge of an enterprise’s network, typically in a coordinated distributed or multi-node network. Some forms of fog computing provide the deployment of compute, storage, and networking services between end devices and cloud computing data centers, on behalf of the cloud computing locations. Such forms of fog computing provide operations that are consistent with edge computing as discussed herein; many of the edge computing aspects discussed herein apply to fog networks, fogging, and fog configurations. Further, aspects of the edge computing systems discussed herein may be configured as a fog, or aspects of a fog may be integrated into an edge computing architecture.

[0284] The core data center **4332** is located at a core network layer **4340** (e.g., a regional or geographically-central level), while the global network cloud **4342** is located at a cloud data center layer **4350** (e.g., a national or global layer). The use of “core” is provided as a term for a centralized network location—deeper in the network—which is accessible by multiple edge nodes or components; however, a “core” does not necessarily designate the “center” or the deepest location of the network. Accordingly, the core data center **4332** may be located within, at, or near the edge cloud **3910**.

[0285] Although an illustrative number of client compute nodes **4302**, edge gateway nodes **4312**, edge aggregation nodes **4322**, core data centers **4332**, and global network clouds **4342** are shown in FIG. 43, it should be appreciated that the edge computing system may include more or fewer devices or systems at respective layers. Additionally, as shown in FIG. 43, the number of components of respective layers **4310**, **4320**, **4330**, **4340**, and **4350** generally increases at lower levels (e.g., when moving closer to endpoints). As such, one edge gateway node **4312** may service multiple client compute nodes **4302**, and one edge aggregation node **4322** may service multiple edge gateway nodes **4312**.

[0286] Consistent with the examples provided herein, a client compute node **4302** may be embodied as any type of end point component, device, appliance, or “thing” capable of communicating as a producer or consumer of data. Further, the label “node” or “device” as used in the edge computing system **4300** does not necessarily mean that such node or device operates in a client or minion/follower/agent role; rather, any of the nodes or devices in the edge computing system **4300** refer to individual entities, nodes, or subsystems which include discrete or connected hardware or software configurations to facilitate or use the edge cloud **3910**.

[0287] As such, the edge cloud **3910** is formed from network components and functional features operated by and within the edge gateway nodes **4312** and the edge aggregation nodes **4322** of layers **4320**, **4330**, respectively. The edge cloud **3910** may be embodied as any type of network that provides edge computing and/or storage resources which are proximately located to radio access

network (RAN) capable endpoint devices (e.g., mobile computing devices, IoT devices, smart devices, etc.), which are shown in FIG. 43 as the client compute nodes **4302**. In other words, the edge cloud **3910** may be envisioned as an “edge” which connects the endpoint devices and traditional mobile network access points that serves as an ingress point into service provider core networks, including carrier networks (e.g., Global System for Mobile Communications (GSM) networks, Long-Term Evolution (LTE) networks, 5G networks, etc.), while also providing storage and/or compute capabilities. Other types and forms of network access (e.g., Wi-Fi, long-range wireless networks) may also be utilized in place of or in combination with such 3GPP carrier networks.

[0288] In some examples, the edge cloud **3910** may form a portion of or otherwise provide an ingress point into or across a fog networking configuration **4326** (e.g., a network of fog devices **4324**, not shown in detail), which may be embodied as a system-level horizontal and distributed architecture that distributes resources and services to perform a specific function. For instance, a coordinated and distributed network of fog devices **4324** may perform computing, storage, control, or networking aspects in the context of an IoT system arrangement. Other networked, aggregated, and distributed functions may exist in the edge cloud **3910** between the cloud data center layer **4350** and the client endpoints (e.g., client compute nodes **4302**). Some of these are discussed in the following sections in the context of network functions or service virtualization, including the use of virtual edges and virtual services which are orchestrated for multiple stakeholders.

[0289] The edge gateway nodes **4312** and the edge aggregation nodes **4322** cooperate to provide various edge services and compute security features to the client compute nodes **4302**. Furthermore, because an individual client compute node **4302** may be stationary or mobile, a respective edge gateway node **4312** may cooperate with other edge gateway devices to propagate presently provided edge services and compute security features as the corresponding client compute node **4302** moves about a region. To do so, respective nodes of the edge gateway nodes **4312** and/or edge aggregation nodes **4322** may support multiple tenants and multiple stakeholder configurations, in which services from (or hosted for) multiple service providers and multiple consumers may be supported and coordinated across a single or multiple compute devices.

[0290] In further examples, any of the compute nodes or devices discussed with reference to the present edge computing systems and environment may be fulfilled based on the components depicted in FIGS. 44 and 45. An edge compute node may be embodied as a type of device, appliance, computer, or other “thing” capable of communicating with other edge, networking, or endpoint components. For example, an edge compute device may be embodied as a personal computer, a server, smartphone, a mobile compute device, a smart appliance, an in-vehicle compute system (e.g., a navigation system), a self-contained device having an outer case, shell, etc., or other devices or systems capable of performing the described functions.

[0291] In the simplified example depicted in FIG. 44, an edge compute node **4400** includes a compute engine (also referred to herein as “compute circuitry”) **4402**, an input/output (I/O) subsystem **4408**, data storage **4410**, a communication circuitry subsystem **4412**, and, optionally, one or more peripheral devices **4414**. In other examples, a respec-

tive compute device may include other or additional components, such as those used in personal or server computing systems (e.g., a display, peripheral devices, etc.). Additionally, in some examples, one or more of the illustrative components may be incorporated in, or otherwise form a portion of, another component.

[0292] The compute node **4400** may be embodied as any type of engine, device, or collection of devices capable of performing various compute functions. In some examples, the compute node **4400** may be embodied as a single device such as an integrated circuit, an embedded system, a field-programmable gate array (FPGA), a system-on-a-chip (SOC), or other integrated system or device. In the illustrative example, the compute node **4400** includes or is embodied as a processor **4404** and a memory **4406**. The processor **4404** may be embodied as any type of processor capable of performing the functions described herein (e.g., executing an application). For example, the processor **4404** may be embodied as a multi-core processor(s), a microcontroller, a processing unit, a specialized or special purpose processing unit, or other processor or processing/controlling circuit. In some examples, the processor **4404** may be embodied as, include, or be coupled to an FPGA, an application-specific integrated circuit (ASIC), reconfigurable hardware or hardware circuitry, or other specialized hardware to facilitate performance of the functions described herein. Also in some examples, the processor **4404** may be embodied as a specialized x-processing unit (xPU) also known as a data processing unit (DPU), infrastructure processing unit (IPU), or network processing unit (NPU). Such an xPU may be embodied as a standalone circuit or circuit package, integrated within an SOC, or integrated with networking circuitry (e.g., in a SmartNIC, or enhanced SmartNIC), dedicated compute circuitry, storage devices, or AI or specialized hardware (e.g., GPUs, programmed FPGAs, Network Processing Units (NPU), Infrastructure Processing Units (IPUs), Storage Processing Units (SPUs), AI Processors (APUs), Data Processing Units (DPUs), Edge Processing Units (EPUs), or other specialized compute units such as a cryptographic processing unit/accelerator). Such an xPU may be designed to receive programming to process one or more data streams and perform specific tasks and actions for the data streams (such as hosting microservices, performing service management or orchestration, organizing or managing server or data center hardware, managing service meshes, or collecting and distributing telemetry), outside of the CPU or general purpose processing hardware. Thus, any of the C2E techniques described herein and their accompanying attestation, trust, security, provisioning, testing, simulation, or orchestration functions may be coordinated by an xPU. However, it will be understood that an xPU, a SOC, a CPU, and other variations of the processor **4404** may work in coordination with each other to execute many types of operations and instructions within and on behalf of the compute node **4400**.

[0293] The main memory **4406** may be embodied as any type of volatile (e.g., dynamic random access memory (DRAM), etc.) or non-volatile memory or data storage capable of performing the functions described herein. Volatile memory may be a storage medium that requires power to maintain the state of data stored by the medium. Non-limiting examples of volatile memory may include various types of random access memory (RAM), such as DRAM or static random access memory (SRAM). One particular type

of DRAM that may be used in a memory module is synchronous dynamic random access memory (SDRAM).

[0294] In one example, the memory device is a block addressable memory device, such as those based on NAND or NOR technologies. A memory device may also include a three-dimensional crosspoint memory device (e.g., Intel 3D XPoint™ memory), or other byte-addressable write-in-place nonvolatile memory devices. The memory device may refer to the die itself and/or to a packaged memory product. In some examples, 3D crosspoint memory (e.g., Intel 3D XPoint™ memory) may comprise a transistor-less stackable cross-point architecture in which memory cells sit at the intersection of word lines and bit lines and are individually addressable and in which bit storage is based on a change in bulk resistance. In some examples, all or a portion of the main memory **4406** may be integrated into the processor **4404**. The main memory **4406** may store various software and data used during operation such as one or more applications, data operated on by the application(s), libraries, and drivers. The compute circuitry **4402** is communicatively coupled to other components of the compute node **4400** via the I/O subsystem **4408**, which may be embodied as circuitry and/or components to facilitate input/output operations with the compute circuitry **4402** (e.g., with the processor **4404** and/or the main memory **4406**) and other components of the compute circuitry **4402**. For example, the I/O subsystem **4408** may be embodied as, or otherwise include memory controller hubs, input/output control hubs, integrated sensor hubs, firmware devices, communication links (e.g., point-to-point links, bus links, wires, cables, light guides, printed circuit board traces, etc.), and/or other components and subsystems to facilitate the input/output operations. In some examples, the I/O subsystem **4408** may form a portion of a system-on-a-chip (SoC) and be incorporated, along with one or more of the processor **4404**, the main memory **4406**, and other components of the compute circuitry **4402**, into the compute circuitry **4402**.

[0295] The one or more illustrative data storage devices **4410** may be embodied as any type of device configured for short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. A respective data storage device **4410** may include a system partition that stores data and firmware code for the data storage device **4410**. A respective data storage device **4410** may also include one or more operating system partitions that store data files and executables for operating systems depending on, for example, the type of compute node **4400**.

[0296] The communication circuitry **4412** may be embodied as any communication circuit, device, or collection thereof, capable of enabling communications over a network between the compute circuitry **4402** and another compute device (e.g., an edge gateway node **4312** of the edge computing system **4300**). The communication circuitry **4412** may be configured to use any one or more communication technology (e.g., wired or wireless communications) and associated protocols (e.g., a cellular networking protocol such as 3GPP 4G or 5G standard, a wireless local area network protocol such as IEEE 802.11/Wi-Fi®, a wireless wide area network protocol, Ethernet, Bluetooth®, Bluetooth Low Energy, an IoT protocol such as IEEE 802.15.4 or ZigBee®, low-power wide-area network (LPWAN) or low-power wide-area (LPWA) protocols, etc.) to effect such communication.

[0297] The illustrative communication circuitry **4412** includes a network interface controller (NIC) **4420**, which may also be referred to as a host fabric interface (HFI). The NIC **4420** may be embodied as one or more add-in-boards, daughter cards, network interface cards, controller chips, chipsets, or other devices that may be used by the compute node **4400** to connect with another compute device (e.g., an edge gateway node **4312**). In some examples, the NIC **4420** may be embodied as part of a system-on-a-chip (SoC) that includes one or more processors or included on a multichip package that also contains one or more processors. In some examples, the NIC **4420** may include a local processor (not shown) and/or a local memory and storage (not shown) that are local to the NIC **4420**. In such examples, the local processor of the MC **4420** (which can include general-purpose accelerators or specific accelerators) may be capable of performing one or more of the functions of the compute circuitry **4402** described herein. Additionally, or alternatively, the local memory of the NIC **4420** may be integrated into one or more components of the client compute node at the board level, socket level, chip level, and/or other levels.

[0298] Additionally, in some examples, a respective compute node **4400** may include one or more peripheral devices **4414**. Such peripheral devices **4414** may include any type of peripheral device found in a compute device or server such as audio input devices, a display, other input/output devices, interface devices, and/or other peripheral devices, depending on the particular type of the compute node **4400**. In further examples, the compute node **4400** may be embodied by a respective edge compute node in an edge computing system (e.g., client compute node **4302**, edge gateway node **4312**, edge aggregation node **4322**) or like forms of appliances, computers, subsystems, circuitry, or other components.

[0299] In a more detailed example, FIG. 45 illustrates a block diagram of an example of components that may be present in an edge computing device (or node) **4550** for implementing the techniques (e.g., operations, processes, methods, and methodologies) described herein. The edge computing node **4550** provides a closer view of the respective components of node **4400** when implemented as or as part of a computing device (e.g., as a mobile device, a base station, server, gateway, etc.). The edge computing node **4550** may include any combinations of the components referenced above, and it may include any device usable with an edge communication network or a combination of such networks. The components may be implemented as integrated circuits (ICs), portions thereof, discrete electronic devices, or other modules, logic, instruction sets, programmable logic or algorithms, hardware, hardware accelerators, software, firmware, or a combination thereof adapted in the edge computing node **4550**, or as components otherwise incorporated within a chassis of a larger system.

[0300] The edge computing node **4550** may include processing circuitry in the form of a processor **4552**, which may be a microprocessor, a multi-core processor, a multithreaded processor, an ultra-low voltage processor, an embedded processor, an xPU/DPU/IPU/NPU, special purpose processing unit, specialized processing unit, or other known processing elements. The processor **4552** may be a part of a system on a chip (SoC) in which the processor **4552** and other components are formed into a single integrated circuit, or a single package, such as the Edison™ or Galileo™ SoC

boards from Intel Corporation, Santa Clara, California. As an example, the processor **4552** may include an Intel® Architecture Core™ based processor, such as a Quark™, an Atom™, an i3, an i5, an i7, an i9, or an MCU-class processor, or another such processor available from Intel®. However, any number other processors may be used, such as available from Advanced Micro Devices, Inc. (AMD) of Sunnyvale, California, a MIPS-based design from MIPS Technologies, Inc. of Sunnyvale, California, an ARM-based design licensed from ARM Holdings, Ltd. or a customer thereof, or their licensees or adopters. The processors may include units such as an A5-A14 processor from Apple® Inc., a Snapdragon™ processor from Qualcomm® Technologies, Inc., or an OMAP™ processor from Texas Instruments, Inc. The processor **4552** and accompanying circuitry may be provided in a single socket form factor, multiple socket form factor, or a variety of other formats, including in limited hardware configurations or configurations that include fewer than all elements shown in FIG. 45.

[0301] The processor **4552** may communicate with a system memory **4554** over an interconnect **4556** (e.g., a bus). Any number of memory devices may be used to provide for a given amount of system memory. As examples, the memory may be random access memory (RAM) in accordance with a Joint Electron Devices Engineering Council (JEDEC) design such as the DDR or mobile DDR standards (e.g., LPDDR, LPDDR2, LPDDR3, or LPDDR4). In particular examples, a memory component may comply with a DRAM standard promulgated by JEDEC, such as JESD79F for DDR SDRAM, JESD79-2F for DDR2 SDRAM, JESD79-3F for DDR3 SDRAM, JESD79-4A for DDR4 SDRAM, JESD209 for Low Power DDR (LPDDR), JESD209-2 for LPDDR2, JESD209-3 for LPDDR3, and JESD209-4 for LPDDR4. Such standards (and similar standards) may be referred to as DDR-based standards and communication interfaces of the storage devices that implement such standards may be referred to as DDR-based interfaces. In various implementations, the individual memory devices may be of any number of different package types such as single die package (SDP), dual die package (DDP), or quad die package (Q17P). These devices, in some examples, may be directly soldered onto a motherboard to provide a lower profile solution, while in other examples the devices are configured as one or more memory modules that in turn couple to the motherboard by a given connector. Any number of other memory implementations may be used, such as other types of memory modules, e.g., dual inline memory modules (DIMMs) of different varieties including but not limited to microDIMMs or MiniDIMMs.

[0302] To provide for persistent storage of information such as data, applications, operating systems, and so forth, a storage **4558** may also couple to the processor **4552** via the interconnect **4556**. In an example, the storage **4558** may be implemented via a solid-state disk drive (SSDD). Other devices that may be used for the storage **4558** include flash memory cards, such as SD cards, microSD cards, XD picture cards, and the like, and USB flash drives. In an example, the memory device may be or may include memory devices that use chalcogenide glass, multi-threshold level NAND flash memory, NOR flash memory, single or multi-level Phase Change Memory (PCM), a resistive memory, nanowire memory, ferroelectric transistor random access memory (FeTRAM), anti-ferroelectric memory, magnetoresistive random access memory (MRAM) memory that incorporates

memristor technology, resistive memory including the metal oxide base, the oxygen vacancy base and the conductive bridge Random Access Memory (CB-RAM), or spin-transfer torque (STT)-MRAM, a spintronic magnetic junction memory-based device, a magnetic tunneling junction (MTJ) based device, a DW (Domain Wall) and SOT (Spin-Orbit Transfer) based device, a thyristor-based memory device, or a combination of any of the above, or other memory.

[0303] In low power implementations, the storage **4558** may be on-die memory or registers associated with the processor **4552**. However, in some examples, the storage **4558** may be implemented using a micro hard disk drive (HDD) or solid-state drive (SSD). Further, any number of new technologies may be used for the storage **4558** in addition to, or instead of, the technologies described, such resistance change memories, phase change memories, holographic memories, or chemical memories, among others.

[0304] The components may communicate over the interconnect **4556**. The interconnect **4556** may include any number of technologies, including industry-standard architecture (ISA), extended ISA (EISA), peripheral component interconnect (PCI), peripheral component interconnect extended (PCI-X), PCI express (PCIe), or any number of other technologies. The interconnect **4556** may be a proprietary bus, for example, used in an SoC based system. Other bus systems may be included, such as an I2C interface, an SPI interface, point to point interfaces, and a power bus, among others.

[0305] The interconnect **4556** may couple the processor **4552** to a transceiver **4566**, for communications with the connected edge devices **4562**. The transceiver **4566** may use any number of frequencies and protocols, such as 2.4 Gigahertz (GHz) transmissions under the IEEE 802.15.4 standard, using the Bluetooth® low energy (BLE) standard, as defined by the Bluetooth® Special Interest Group, or the ZigBee® standard, among others. Any number of radios, configured for a particular wireless communication protocol, may be used for the connections to the connected edge devices **4562**. For example, a wireless local area network (WLAN) unit may be used to implement Wi-Fi® communications in accordance with the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. In addition, wireless wide area communications, e.g., according to a cellular or other wireless wide area protocol, may occur via a wireless wide area network (WWAN) unit.

[0306] The wireless network transceiver **4566** (or multiple transceivers) may communicate using multiple standards or radios for communications at a different range. For example, the edge computing node **4550** may communicate with close devices, e.g., within about 10 meters, using a local transceiver based on BLE, or another low power radio, to save power. More distant connected edge devices **4562**, e.g., within about 50 meters, may be reached over ZigBee or other intermediate power radios. Both communications techniques may take place over a single radio at different power levels or may take place over separate transceivers, for example, a local transceiver using BLE and a separate mesh transceiver using ZigBee®.

[0307] A wireless network transceiver **4566** (e.g., a radio transceiver) may be included to communicate with devices or services in the edge cloud **4590** via local or wide area network protocols. The wireless network transceiver **4566** may be an LPWA transceiver that follows the IEEE 802.15.4, or IEEE 802.15.4g standards, among others. The edge

computing node **4550** may communicate over a wide area using LoRaWAN™ (Long Range Wide Area Network) developed by Semtech and the LoRa Alliance. The techniques described herein are not limited to these technologies but may be used with any number of other cloud transceivers that implement long-range, low bandwidth communications, such as Sigfox, and other technologies. Further, other communications techniques, such as time-slotted channel hopping, described in the IEEE 802.15.4e specification may be used.

[0308] Any number of other radio communications and protocols may be used in addition to the systems mentioned for the wireless network transceiver **4566**, as described herein. For example, the transceiver **4566** may include a cellular transceiver that uses spread spectrum (SPA/SAS) communications for implementing high-speed communications. Further, any number of other protocols may be used, such as Wi-Fi® networks for medium speed communications and provision of network communications. The transceiver **4566** may include radios that are compatible with any number of 3GPP (Third Generation Partnership Project) specifications, such as Long Term Evolution (LTE) and 5th Generation (5G) communication systems, discussed in further detail at the end of the present disclosure. A network interface controller (NIC) **4568** may be included to provide a wired communication to nodes of the edge cloud **4590** or other devices, such as the connected edge devices **4562** (e.g., operating in a mesh). The wired communication may provide an Ethernet connection or may be based on other types of networks, such as Controller Area Network (CAN), Local Interconnect Network (LIN), DeviceNet, ControlNet, Data Highway+, PROFIBUS, or PROFINET, Time Sensitive Networks (TSN), among many others. An additional NIC **4568** may be included to enable connecting to a second network, for example, a first NIC **4568** providing communications to the cloud over Ethernet, and a second NIC **4568** providing communications to other devices over another type of network.

[0309] Given the variety of types of applicable communications from the device to another component or network, applicable communications circuitry used by the device may include or be embodied by any one or more of components **4564**, **4566**, **4568**, or **4570**. Accordingly, in various examples, applicable means for communicating (e.g., receiving, transmitting, etc.) may be embodied by such communications circuitry.

[0310] The edge computing node **4550** may include or be coupled to acceleration circuitry **4564**, which may be embodied by one or more AI accelerators, a neural compute stick, neuromorphic hardware, an FPGA, an arrangement of GPUs, an arrangement of xPUs/DPUs/IPU/NPUs, one or more SoCs, one or more CPUs, one or more digital signal processors, dedicated ASICs, or other forms of specialized processors or circuitry designed to accomplish one or more specialized tasks. These tasks may include AI processing (including machine learning, training, inferencing, and classification operations), visual data processing, network data processing, object detection, rule analysis, or the like. Accordingly, in various examples, applicable means for acceleration may be embodied by such acceleration circuitry.

[0311] The interconnect **4556** may couple the processor **4552** to a sensor hub or external interface **4570** that is used to connect additional devices or subsystems. The devices

may include sensors **4572**, such as accelerometers, level sensors, flow sensors, optical light sensors, camera sensors, temperature sensors, a global navigation system (e.g., GPS) sensors, pressure sensors, barometric pressure sensors, and the like. The hub or interface **4570** further may be used to connect the edge computing node **4550** to actuators **4574**, such as power switches, valve actuators, an audible sound generator, a visual warning device, and the like.

[0312] In some optional examples, various input/output (I/O) devices may be present within or connected to, the edge computing node **4550**. For example, a display or other output device **4584** may be included to show information, such as sensor readings or actuator position. An input device **4586**, such as a touch screen or keypad may be included to accept input. An output device **4584** may include any number of forms of audio or visual display, including simple visual outputs such as binary status indicators (e.g., LEDs) and multi-character visual outputs, or more complex outputs such as display screens (e.g., LCD screens), with the output of characters, graphics, multimedia objects, and the like being generated or produced from the operation of the edge computing node **4550**. A display or console hardware, in the context of the present system, may be used to provide output and receive input of an edge computing system; to manage components or services of an edge computing system; identify a state of an edge computing component or service; or to conduct any other number of management or administration functions or service use cases.

[0313] A battery **4576** may power the edge computing node **4550**, although, in examples in which the edge computing node **4550** is mounted in a fixed location, it may have a power supply coupled to an electrical grid, or the battery may be used as a backup or for temporary capabilities. The battery **4576** may be a lithium-ion battery, or a metal-air battery, such as a zinc-air battery, an aluminum-air battery, a lithium-air battery, and the like.

[0314] A battery monitor/charger **4578** may be included in the edge computing node **4550** to track the state of charge (SoCh) of the battery **4576**. The battery monitor/charger **4578** may be used to monitor other parameters of the battery **4576** to provide failure predictions, such as the state of health (SoH) and the state of function (SoF) of the battery **4576**. The battery monitor/charger **4578** may include a battery monitoring integrated circuit, such as an LTC4020 or an LTC2990 from Linear Technologies, an ADT7488A from ON Semiconductor of Phoenix Arizona, or an IC from the UCD90xxx family from Texas Instruments of Dallas, TX. The battery monitor/charger **4578** may communicate the information on the battery **4576** to the processor **4552** over the interconnect **4556**. The battery monitor/charger **4578** may also include an analog-to-digital (ADC) converter that enables the processor **4552** to directly monitor the voltage of the battery **4576** or the current flow from the battery **4576**. The battery parameters may be used to determine actions that the edge computing node **4550** may perform, such as transmission frequency, mesh network operation, sensing frequency, and the like.

[0315] A power block **4580**, or other power supply coupled to a grid, may be coupled with the battery monitor/charger **4578** to charge the battery **4576**. In some examples, the power block **4580** may be replaced with a wireless power receiver to obtain the power wirelessly, for example, through a loop antenna in the edge computing node **4550**. A wireless battery charging circuit, such as an LTC4020 chip from

Linear Technologies of Milpitas, California, among others, may be included in the battery monitor/charger **4578**. The specific charging circuits may be selected based on the size of the battery **4576**, and thus, the current required. The charging may be performed using the Airfuel standard promulgated by the Airfuel Alliance, the Qi wireless charging standard promulgated by the Wireless Power Consortium, or the Rezence charging standard, promulgated by the Alliance for Wireless Power, among others.

[0316] The storage **4558** may include instructions **4582** in the form of software, firmware, or hardware commands to implement the techniques described herein. Although such instructions **4582** are shown as code blocks included in the memory **4554** and the storage **4558**, it may be understood that any of the code blocks may be replaced with hardwired circuits, for example, built into an application-specific integrated circuit (ASIC).

[0317] Also in a specific example, the instructions **4582** on the processor **4552** (separately, or in combination with the instructions **4582** of the machine readable medium **4560**) may configure execution or operation of a trusted execution environment (TEE) **4595**. In an example, the TEE **4595** operates as a protected area accessible to the processor **4552** for secure execution of instructions and secure access to data. Various implementations of the TEE **4595**, and an accompanying secure area in the processor **4552** or the memory **4554** may be provided, for instance, through use of Intel® Software Guard Extensions (SGX), AMD® Secure Encrypted Virtualization (SEV), or ARM® TrustZone® hardware security extensions, Intel® Management Engine (ME), or Intel® Converged Security Manageability Engine (CSME). Other aspects of security hardening, hardware roots-of-trust, and trusted or protected operations may be implemented in the edge computing node **4550** through the TEE **4595** and the processor **4552**.

[0318] In an example, the instructions **4582** provided via memory **4554**, the storage **4558**, or the processor **4552** may be embodied as a non-transitory, machine-readable medium **4560** including code to direct the processor **4552** to perform electronic operations in the edge computing node **4550**. The processor **4552** may access the non-transitory, machine-readable medium **4560** over the interconnect **4556**. For instance, the non-transitory, machine-readable medium **4560** may be embodied by devices described for the storage **4558** or may include specific storage units such as optical disks, flash drives, or any number of other hardware devices. The non-transitory, machine-readable medium **4560** may include instructions to direct the processor **4552** to perform a specific sequence or flow of actions, for example, as described with respect to the flowchart(s) and block diagram(s) of operations and functionality depicted above. As used herein, the terms “machine-readable medium,” “computer-readable medium,” “machine-readable storage,” and “computer-readable storage” are interchangeable.

[0319] In an example embodiment, the edge computing node **4550** can be implemented using components/modules/blocks **4552-4586** which are configured as IP Blocks. An individual IP Block may contain a hardware RoT (e.g., device identifier composition engine, or DICE), where a DICE key may be used to identify and attest the IP Block firmware to a peer IP Block or remotely to one or more of components/modules/blocks **4562-4580**. Thus, it will be understood that the node **4550** itself may be implemented as a SoC or standalone hardware package.

[0320] In further examples, a machine-readable medium also includes any tangible medium that is capable of storing, encoding or carrying instructions for execution by a machine and that cause the machine to perform any one or more of the methodologies of the present disclosure or that is capable of storing, encoding or carrying data structures utilized by or associated with such instructions. A “machine-readable medium” thus may include but is not limited to, solid-state memories, and optical and magnetic media. Specific examples of machine-readable media include non-volatile memory, including but not limited to, by way of example, semiconductor memory devices (e.g., electrically programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM)) and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The instructions embodied by a machine-readable medium may further be transmitted or received over a communications network using a transmission medium via a network interface device utilizing any one of a number of transfer protocols (e.g., HTTP).

[0321] A machine-readable medium may be provided by a storage device or other apparatus which is capable of hosting data in a non-transitory format. In an example, information stored or otherwise provided on a machine-readable medium may be representative of instructions, such as instructions themselves or a format from which the instructions may be derived. This format from which the instructions may be derived may include source code, encoded instructions (e.g., in compressed or encrypted form), packaged instructions (e.g., split into multiple packages), or the like. The information representative of the instructions in the machine-readable medium may be processed by processing circuitry into the instructions to implement any of the operations discussed herein. For example, deriving the instructions from the information (e.g., processing by the processing circuitry) may include: compiling (e.g., from source code, object code, etc.), interpreting, loading, organizing (e.g., dynamically or statically linking), encoding, decoding, encrypting, unencrypting, packaging, unpackaging, or otherwise manipulating the information into the instructions.

[0322] In an example, the derivation of the instructions may include assembly, compilation, or interpretation of the information (e.g., by the processing circuitry) to create the instructions from some intermediate or preprocessed format provided by the machine-readable medium. The information, when provided in multiple parts, may be combined, unpacked, and modified to create the instructions. For example, the information may be in multiple compressed source code packages (or object code, or binary executable code, etc.) on one or several remote servers. The source code packages may be encrypted when in transit over a network and decrypted, uncompressed, assembled (e.g., linked) if necessary, and compiled or interpreted (e.g., into a library, stand-alone executable, etc.) at a local machine, and executed by the local machine.

[0323] The block diagrams of FIGS. 44 and 45 are intended to depict a high-level view of components of a device, subsystem, or arrangement of an edge computing node. However, it will be understood that some of the components shown may be omitted, additional components may be present, and a different arrangement of the components shown may occur in other implementations.

[0324] FIG. 46 illustrates an example software distribution platform 4605 to distribute software, such as the example computer readable instructions 4582 of FIG. 45, to one or more devices, such as example processor platform(s) 46 and/or other example connected edge devices or systems discussed herein. The example software distribution platform 4605 may be implemented by any computer server, data facility, cloud service, etc., capable of storing and transmitting software to other computing devices. Example connected edge devices may be customers, clients, managing devices (e.g., servers), third parties (e.g., customers of an entity owning and/or operating the software distribution platform 4605). Example connected edge devices may operate in commercial and/or home automation environments. In some examples, a third party is a developer, a seller, and/or a licensor of software such as the example computer readable instructions 4582 of FIG. 45. The third parties may be consumers, users, retailers, OEMs, etc. that purchase and/or license the software for use and/or re-sale and/or sub-licensing. In some examples, distributed software causes display of one or more user interfaces (UIs) and/or graphical user interfaces (GUIs) to identify the one or more devices (e.g., connected edge devices) geographically and/or logically separated from each other (e.g., physically separated IoT devices chartered with the responsibility of water distribution control (e.g., pumps), electricity distribution control (e.g., relays), etc.).

[0325] In the illustrated example of FIG. 46, the software distribution platform 4605 includes one or more servers and one or more storage devices that store the computer readable instructions 4582. The one or more servers of the example software distribution platform 4605 are in communication with a network 4615, which may correspond to any one or more of the Internet and/or any of the example networks described above. In some examples, the one or more servers are responsive to requests to transmit the software to a requesting party as part of a commercial transaction. Payment for the delivery, sale and/or license of the software may be handled by the one or more servers of the software distribution platform and/or via a third-party payment entity. The servers enable purchasers and/or licensors to download the computer readable instructions 4582 from the software distribution platform 4605. For example, the software, which may correspond to example computer readable instructions 4582, may be downloaded to the example processor platform(s), which is/are to execute the computer readable instructions 4582. In some examples, one or more servers of the software distribution platform 4605 are communicatively connected to one or more security domains and/or security devices through which requests and transmissions of the example computer readable instructions 4582 must pass. In some examples, one or more servers of the software distribution platform 4605 periodically offer, transmit, and/or force updates to the software (e.g., the example computer readable instructions 4582 of FIG. 45) to ensure improvements, patches, updates, etc. are distributed and applied to the software at the end user devices.

[0326] In the illustrated example of FIG. 46, the computer readable instructions 4582 are stored on storage devices of the software distribution platform 4605 in a particular format. A format of computer readable instructions includes, but is not limited to a particular code language (e.g., Java, JavaScript, Python, C, C #, SQL, HTML, etc.), and/or a particular code state (e.g., uncompiled code (e.g., ASCII),

interpreted code, linked code, executable code (e.g., a binary), etc.). In some examples, the computer readable instructions **4582** stored in the software distribution platform **4605** are in a first format when transmitted to the example processor platform(s) **4610**. In some examples, the first format is an executable binary in which particular types of the processor platform(s) **4610** can execute. However, in some examples, the first format is uncompiled code that requires one or more preparation tasks to transform the first format to a second format to enable execution on the example processor platform(s) **4610**. For instance, the receiving processor platform(s) **4600** may need to compile the computer readable instructions **4582** in the first format to generate executable code in a second format that is capable of being executed on the processor platform(s) **4510**. In still other examples, the first format is interpreted code that, upon reaching the processor platform(s) **4610**, is interpreted by an interpreter to facilitate execution of instructions.

[0327] Implementation of the preceding techniques may be accomplished through any number of specifications, configurations, or example deployments of hardware and software. It should be understood that the functional units or capabilities described in this specification may have been referred to or labeled as components or modules, to more particularly emphasize their implementation independence. Such components may be embodied by any number of software or hardware forms. For example, a component or module may be implemented as a hardware circuit comprising custom very-large-scale integration (VLSI) circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A component or module may also be implemented in programmable hardware devices such as field-programmable gate arrays, programmable array logic, programmable logic devices, or the like. Components or modules may also be implemented in software for execution by various types of processors. An identified component or module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions, which may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified component or module need not be physically located together but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the component or module and achieve the stated purpose for the component or module.

[0328] Indeed, a component or module of executable code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices or processing systems. In particular, some aspects of the described process (such as code rewriting and code analysis) may take place on a different processing system (e.g., in a computer in a data center), than that in which the code is deployed (e.g., in a computer embedded in a sensor or robot). Similarly, operational data may be identified and illustrated herein within components or modules and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices, and may exist, at least partially, merely as electronic signals on a system or network. The components or modules may be passive or active, including agents operable to perform desired functions.

[0329] In the above Detailed Description, various features may be grouped to streamline the disclosure. However, claims may not set forth every feature disclosed herein as embodiments may feature a subset of said features. Further, embodiments may include fewer features than those disclosed in a particular example. Thus, the following claims are hereby incorporated into the Detailed Description, with a claim standing on its own as a separate embodiment.

1. A computing system configured to manage distributed workloads, comprising:

processing circuitry; and

a memory device including instructions embodied thereon, wherein the instructions, which when executed by the processing circuitry, configure the processing circuitry to cause operations that:

identify characteristics of a distributed workload from an ongoing execution of the distributed workload, the distributed workload being partitioned among multiple computing nodes;

evaluate a trust status of the distributed workload in response to a change in the execution of the distributed workload, including verifying resources to execute the distributed workload and verifying security policies associated with the resources; and

control the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status.

2. The computing system of claim 1, wherein the characteristics of the distributed workload include expected trust properties to exist between a workload execution environment and respective infrastructure resources, and

wherein the control of the execution of the distributed workload is based on use of a token that includes security intents metadata to describe the expected trust properties.

3. The computing system of claim 1, wherein the operations to evaluate the trust status are performed by a trust coordination framework service, and wherein the instructions further configure the processing circuitry to cause operations that:

evaluate data provenance of data associated with the distributed workload, attestation properties of the resources to execute the distributed workload, and workload provenance of respective portions of the distributed workload, using the trust coordination framework service.

4. The computing system of claim 1, wherein the distributed workload is associated with an attestation workload, and wherein the instructions further configure the processing circuitry to cause operations that:

distribute the attestation workload by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload.

5. The computing system of claim 1, wherein the change in the execution of the distributed workload is provided from a software or firmware update to at least one of the multiple computing nodes.

6. The computing system of claim 5, wherein the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource.

7. The computing system of claim 5, wherein the software or firmware update is coordinated by a workload update

manager, and wherein the workload update manager is to coordinate distribution of the software or firmware update.

8. The computing system of claim 1, wherein the multiple computing nodes are provided by a cloud repository infrastructure, and wherein the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

9. The computing system of claim 1, wherein the characteristics of the distributed workload are based on results from a resource simulation performed on the distributed workload, and wherein the resource simulation includes testing of resource bindings to be used by the distributed workload.

10. The computing system of claim 1, wherein the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, wherein the operations of the computing system are coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload.

11. At least one non-transitory machine-readable storage medium comprising instructions stored thereupon, which when executed by processing circuitry of a computing machine, cause the processing circuitry to:

identify characteristics of a distributed workload from an ongoing execution of the distributed workload, the distributed workload being partitioned among multiple computing nodes;

evaluate a trust status of the distributed workload in response to a change in the execution of the distributed workload, including verifying resources to execute the distributed workload and verifying security policies associated with the resources; and

control the execution of the distributed workload among the multiple computing nodes, based on the characteristics and the evaluated trust status.

12. The machine-readable storage medium of claim 11, wherein the characteristics of the distributed workload include expected trust properties to exist between a workload execution environment and respective infrastructure resources, and

wherein the control of the execution of the distributed workload is based on use of a token that includes security intents metadata to describe the expected trust properties.

13. The machine-readable storage medium of claim 11, wherein operations to evaluate the trust status are performed by a trust coordination framework service, and wherein the instructions cause the processing circuitry to:

evaluate data provenance of data associated with the distributed workload, attestation properties of the resources to execute the distributed workload, and workload provenance of respective portions of the distributed workload, using the trust coordination framework service.

14. The machine-readable storage medium of claim 11, wherein the distributed workload is associated with an attestation workload, and wherein the instructions further cause the processing circuitry to:

distribute the attestation workload by co-locating execution of portions of the attestation workload onto the resources that are to execute portions of the distributed workload.

15. The machine-readable storage medium of claim 11, wherein the change in the execution of the distributed workload is provided from a software or firmware update to at least one of the multiple computing nodes.

16. The machine-readable storage medium of claim 15, wherein the software or firmware update includes moving a provisioned workload to a migration target workload, and moving a provisioned resource to a migration target resource.

17. The machine-readable storage medium of claim 15, wherein the software or firmware update is coordinated by a workload update manager, and wherein the workload update manager is to coordinate distribution of the software or firmware update.

18. The machine-readable storage medium of claim 11, wherein the multiple computing nodes are provided by a cloud repository infrastructure, and wherein the cloud repository infrastructure operates a trusted repository cloud agent service to verify operations that execute the distributed workload.

19. The machine-readable storage medium of claim 11, wherein the characteristics of the distributed workload are based on results from a resource simulation performed on the distributed workload, and wherein the resource simulation includes testing of resource bindings to be used by the distributed workload.

20. The machine-readable storage medium of claim 11, wherein the multiple computing nodes are provided by a platform-as-a-service (PaaS) configuration, wherein operations of the computing machine are coordinated by an infrastructure-as-a-service (IaaS) configuration to execute the distributed workload.

* * * * *