



US 20250259144A1

(19) **United States**

(12) **Patent Application Publication**

Crabtree et al.

(10) **Pub. No.: US 2025/0259144 A1**

(43) **Pub. Date: Aug. 14, 2025**

(54) **PLATFORM FOR INTEGRATION OF  
MACHINE LEARNING MODELS UTILIZING  
MARKETPLACES AND CROWD AND  
EXPERT JUDGMENT AND KNOWLEDGE  
CORPORA**

(71) Applicant: **QOMPLX LLC**, Reston, VA (US)

(72) Inventors: **Jason Crabtree**, Vienna, VA (US);  
**Richard Kelley**, Woodbridge, VA (US);  
**Jason Hopper**, Halifax (CA); **David Park**, Fairfax, VA (US)

(21) Appl. No.: **18/733,830**

(22) Filed: **Jun. 4, 2024**

#### Related U.S. Application Data

(63) Continuation-in-part of application No. 18/668,137, filed on May 18, 2024, which is a continuation-in-part of application No. 18/656,612, filed on May 7, 2024.

(60) Provisional application No. 63/551,328, filed on Feb. 8, 2024.

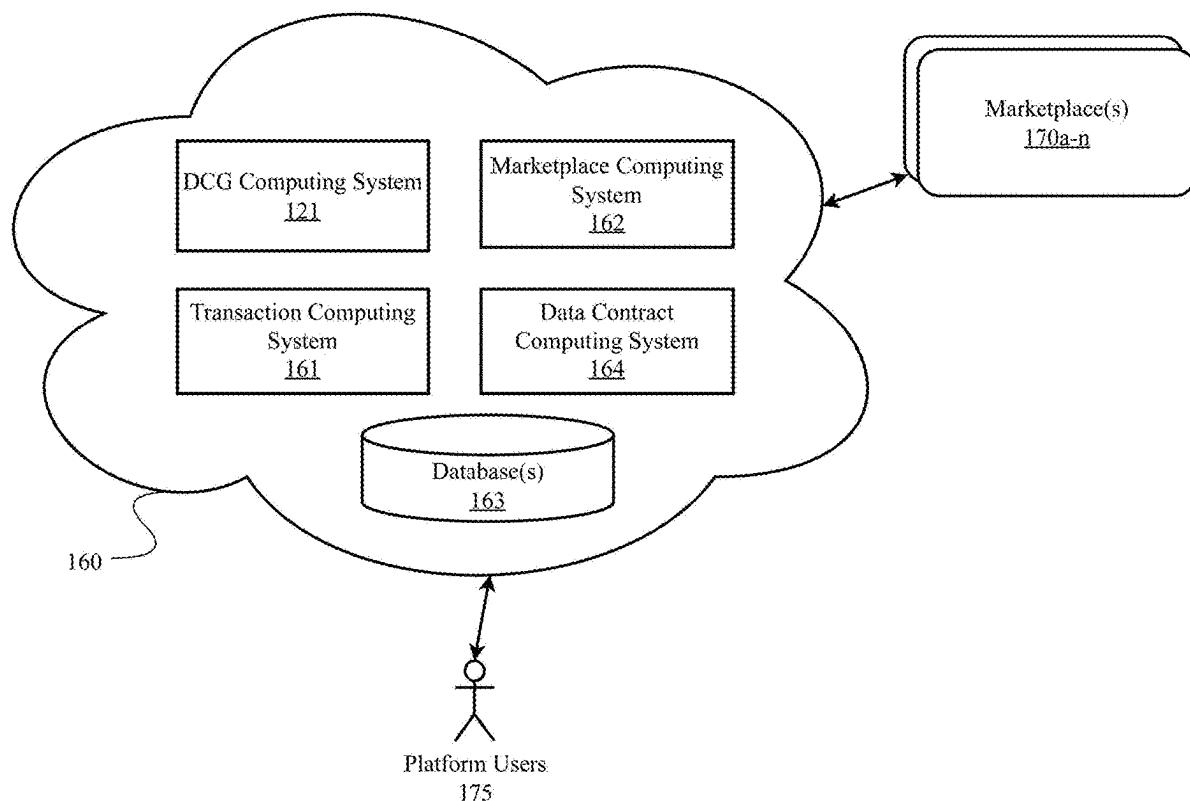
#### Publication Classification

(51) **Int. Cl.**  
**G06N 20/00** (2019.01)  
**G06Q 30/0201** (2023.01)  
**G06Q 30/0601** (2023.01)

(52) **U.S. Cl.**  
CPC ..... **G06Q 10/101** (2013.01); **G06Q 30/0201** (2013.01); **G06Q 30/0601** (2013.01)

#### ABSTRACT

A system and method for flexibly incorporating machine learning models into applications using a marketplace platform and distributed computational graph (DCG) architecture. The DCG enables dynamic selection, creation and incorporation of trained models with data sources and marketplaces for data, algorithms, simulation models, ontologies, knowledge corpora, and crowd or expert judgment. Multiple models can be used in series or parallel. An expert judgment marketplace allows human and artificial intelligence (AI) experts to score the accuracy of training data and model outputs. Consumers can select and rank AI agents or experts based on the helpfulness of their judgments. A symbolic knowledge corpora and retrieval augmented generation (RAG) marketplace enables selling access to proprietary datasets as RAGs and knowledge bases. The system includes knowledge corpora and RAG marketplaces with domain-specific components and user experience customization.



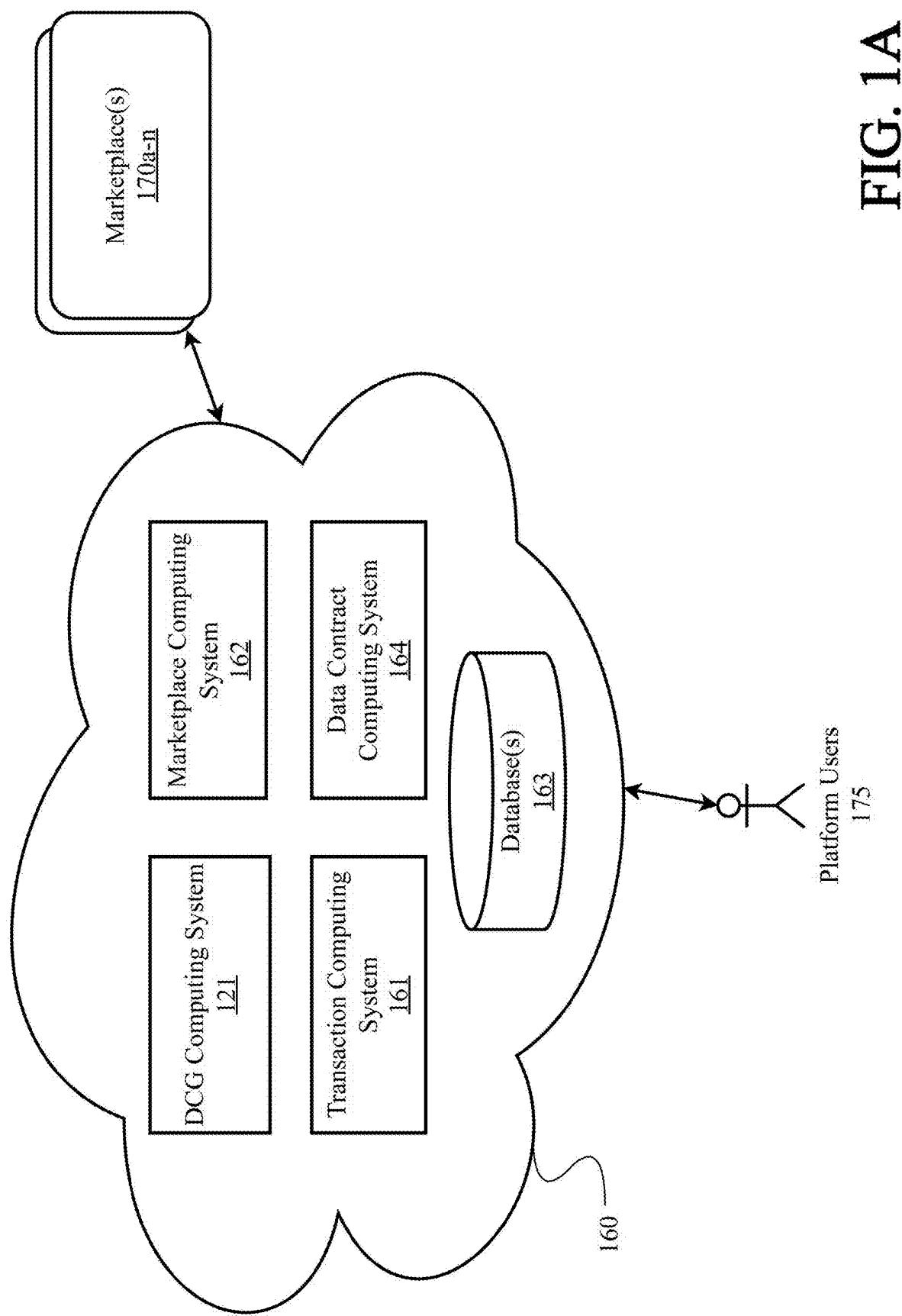
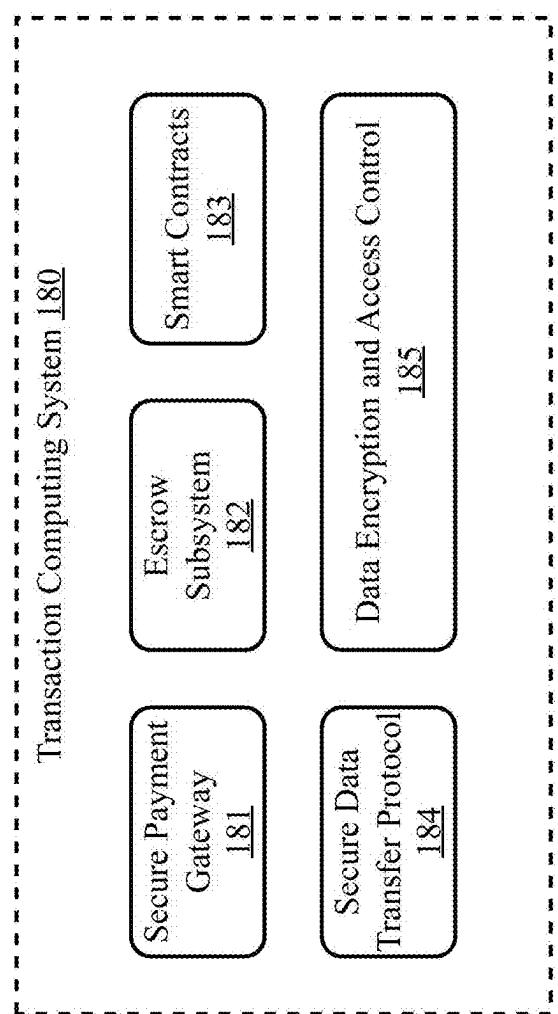


FIG. 1A

FIG. 1B



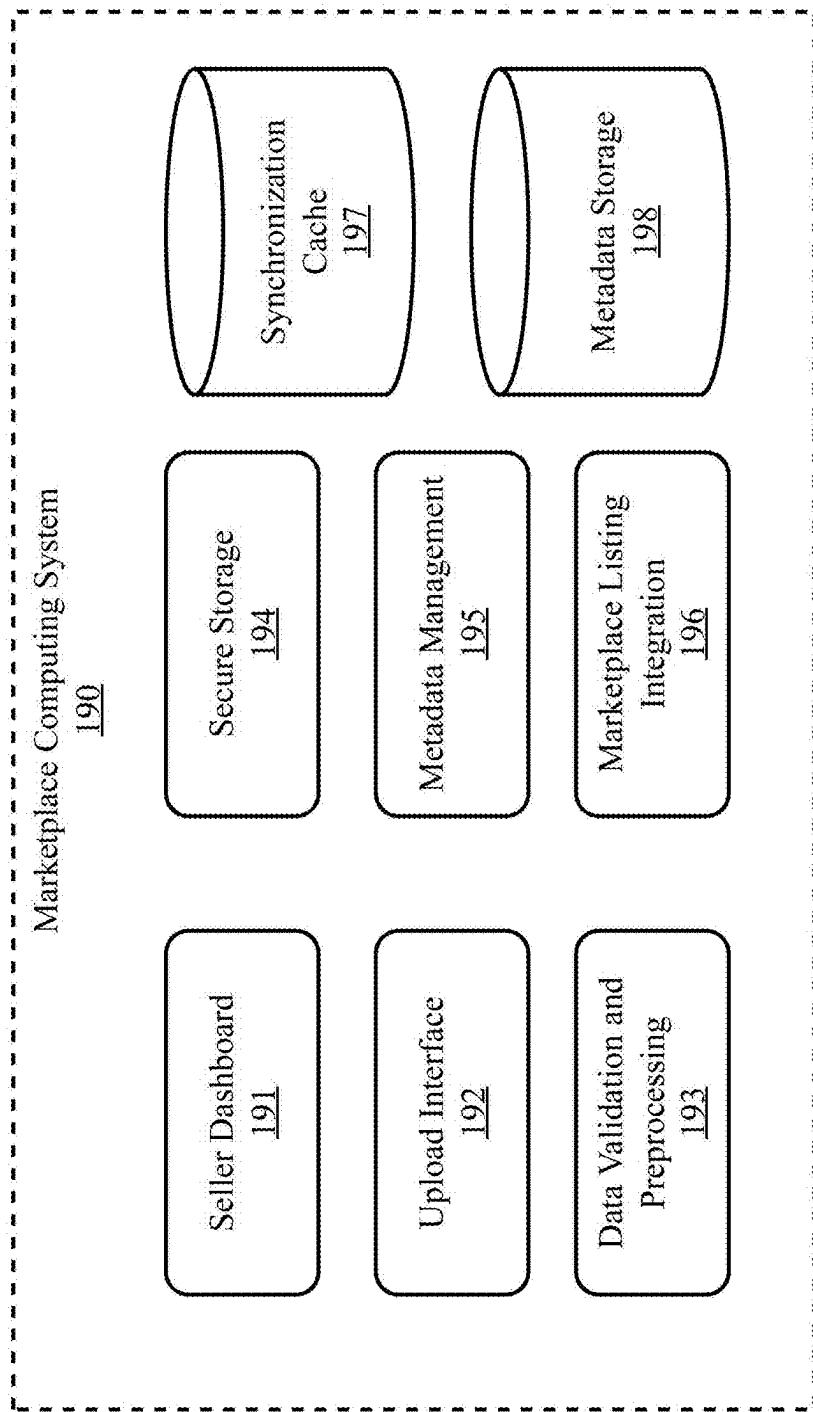


FIG. 1C

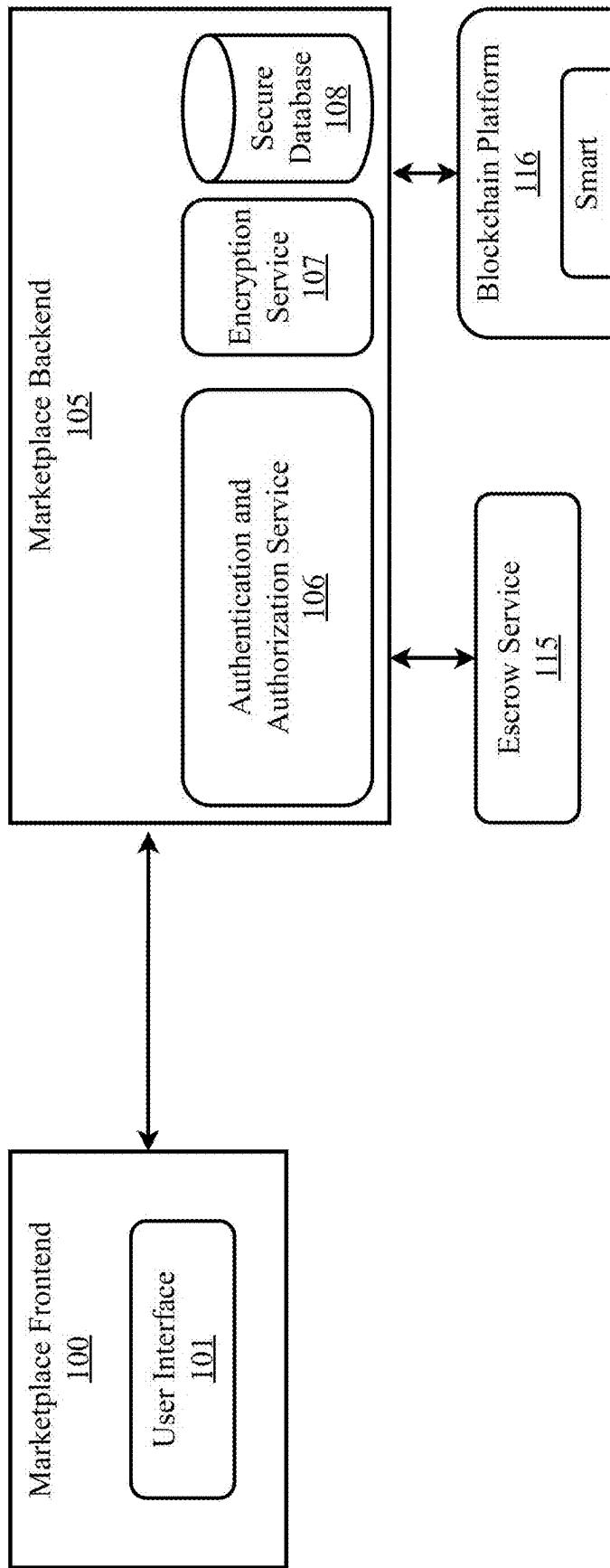
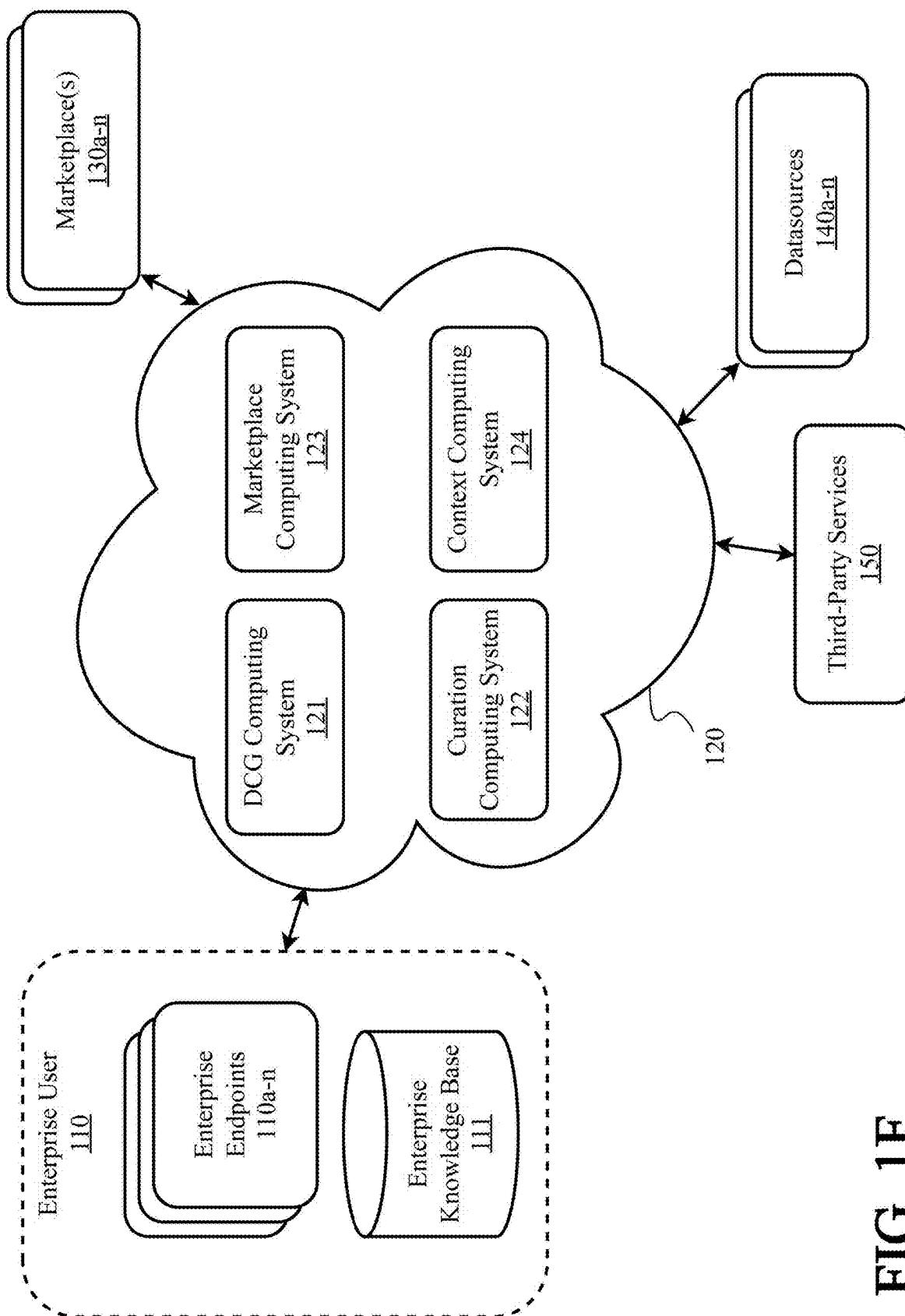


FIG. 1D



FIG. 1E



**FIG. 1F**

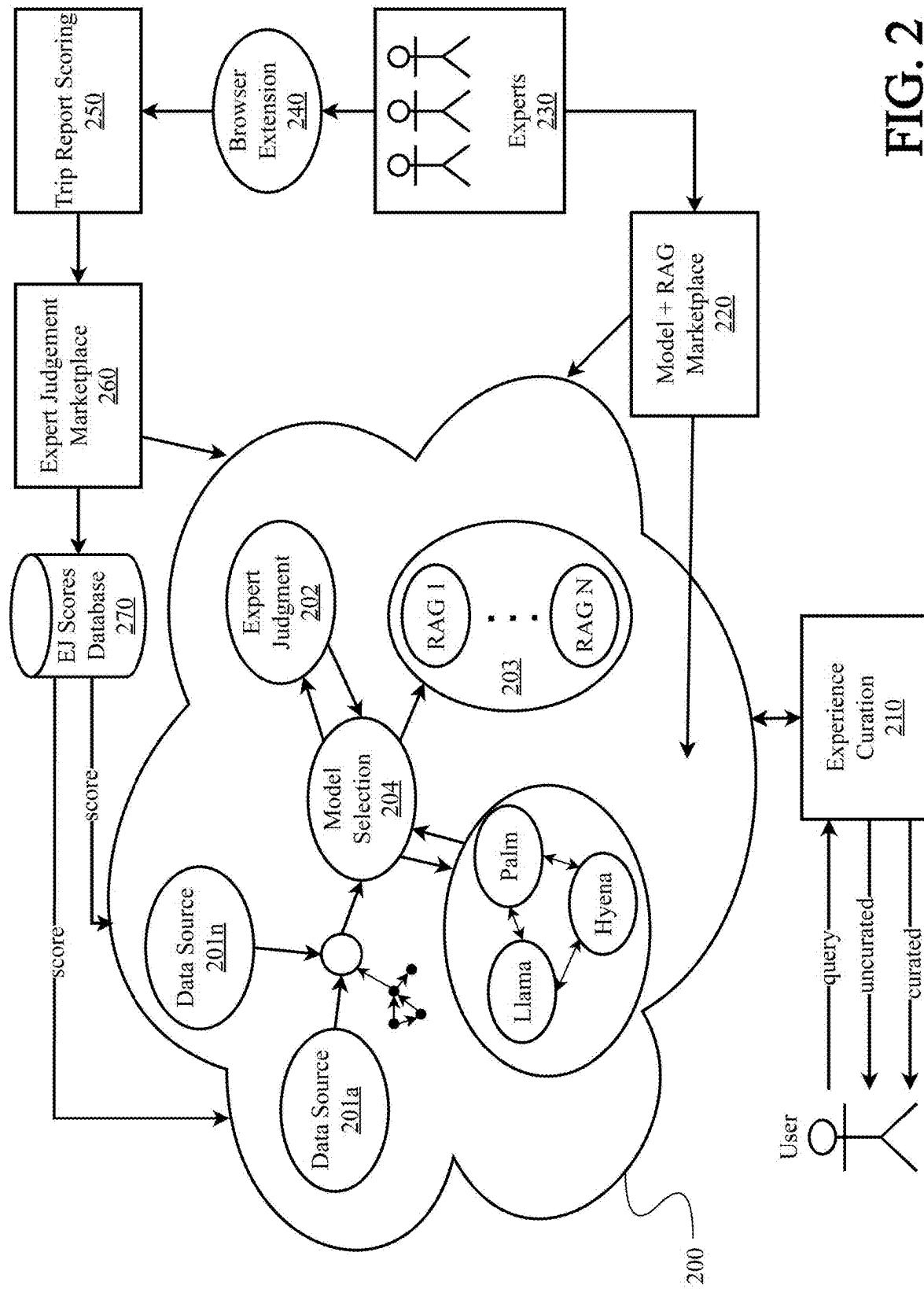
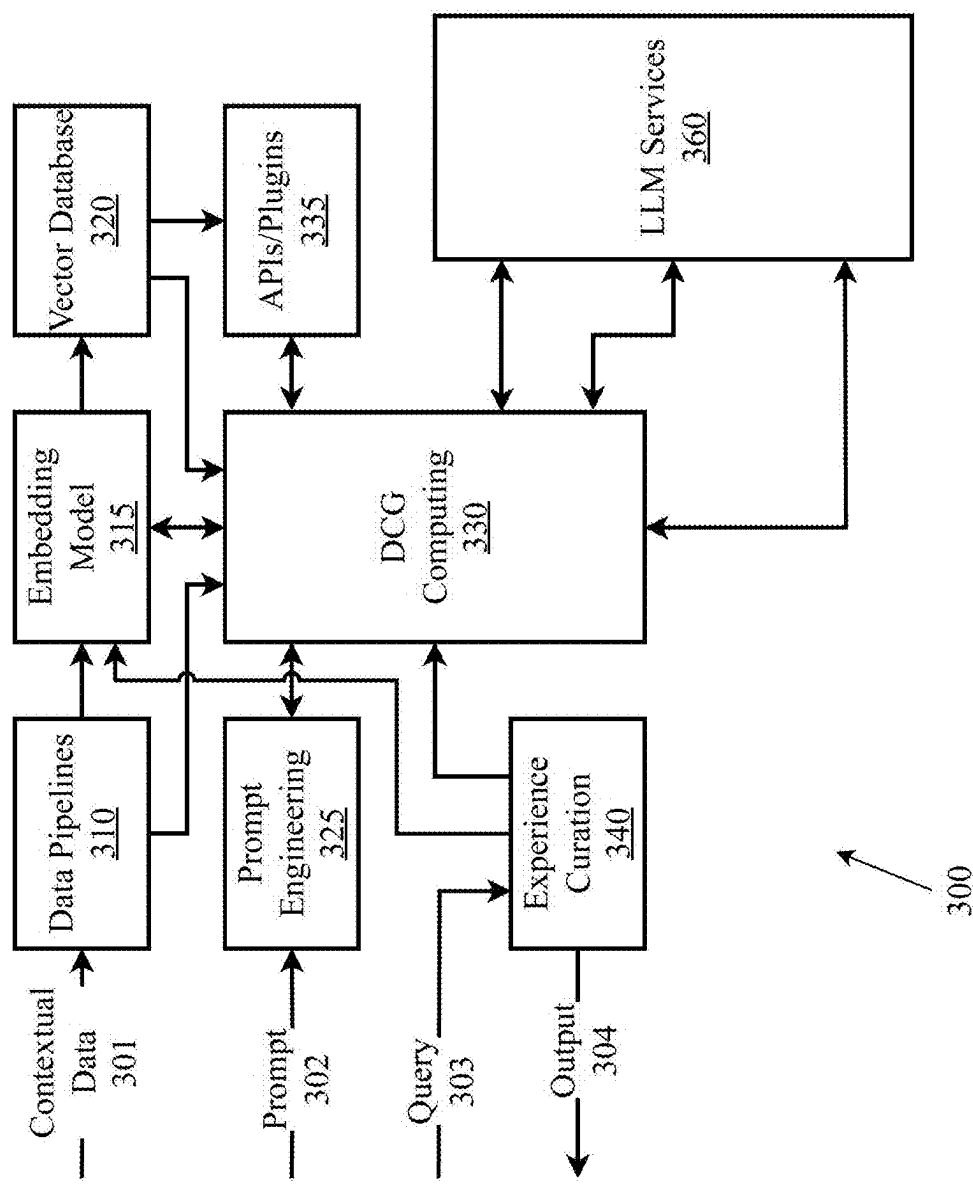
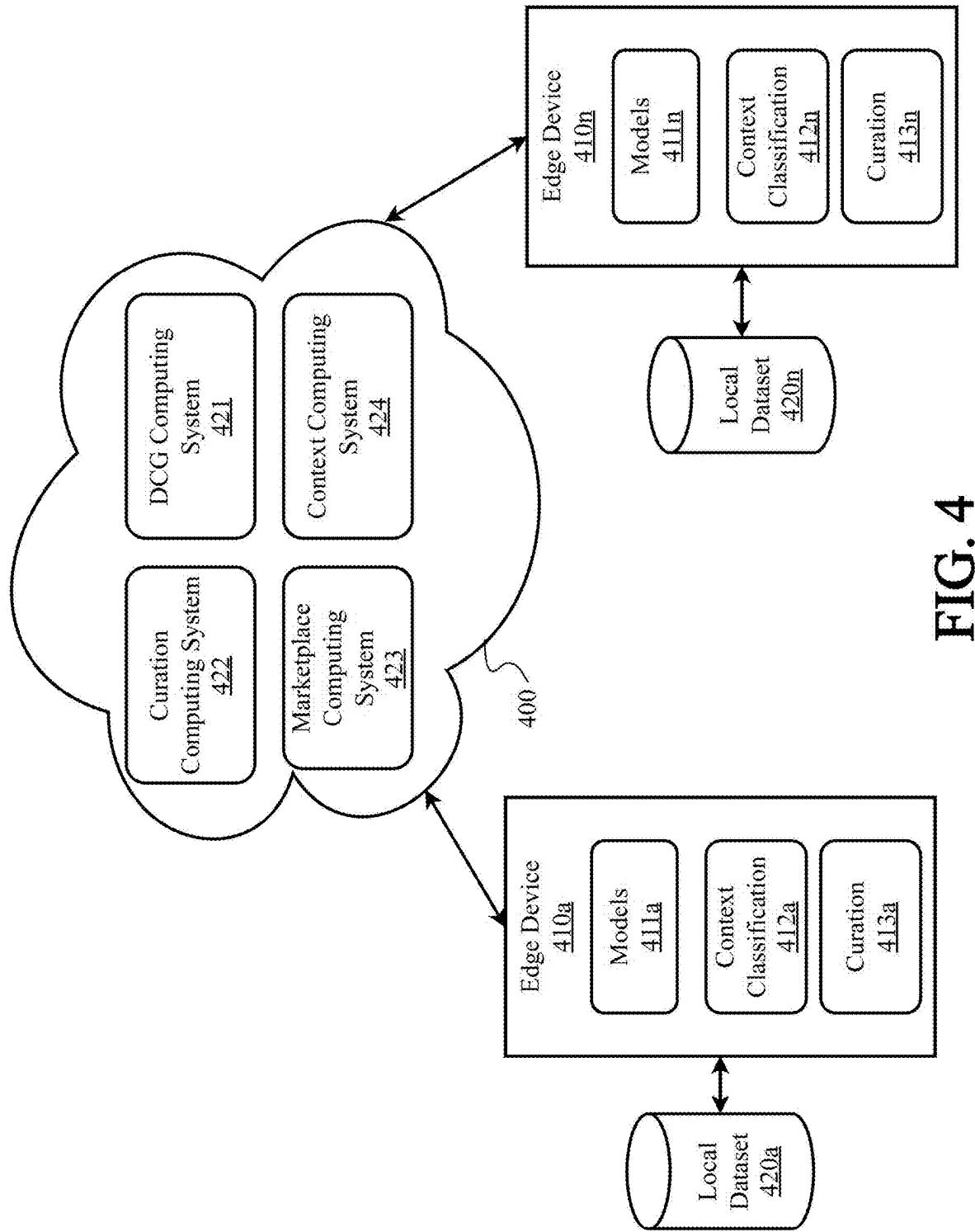


FIG. 2

FIG. 3





**FIG. 4**

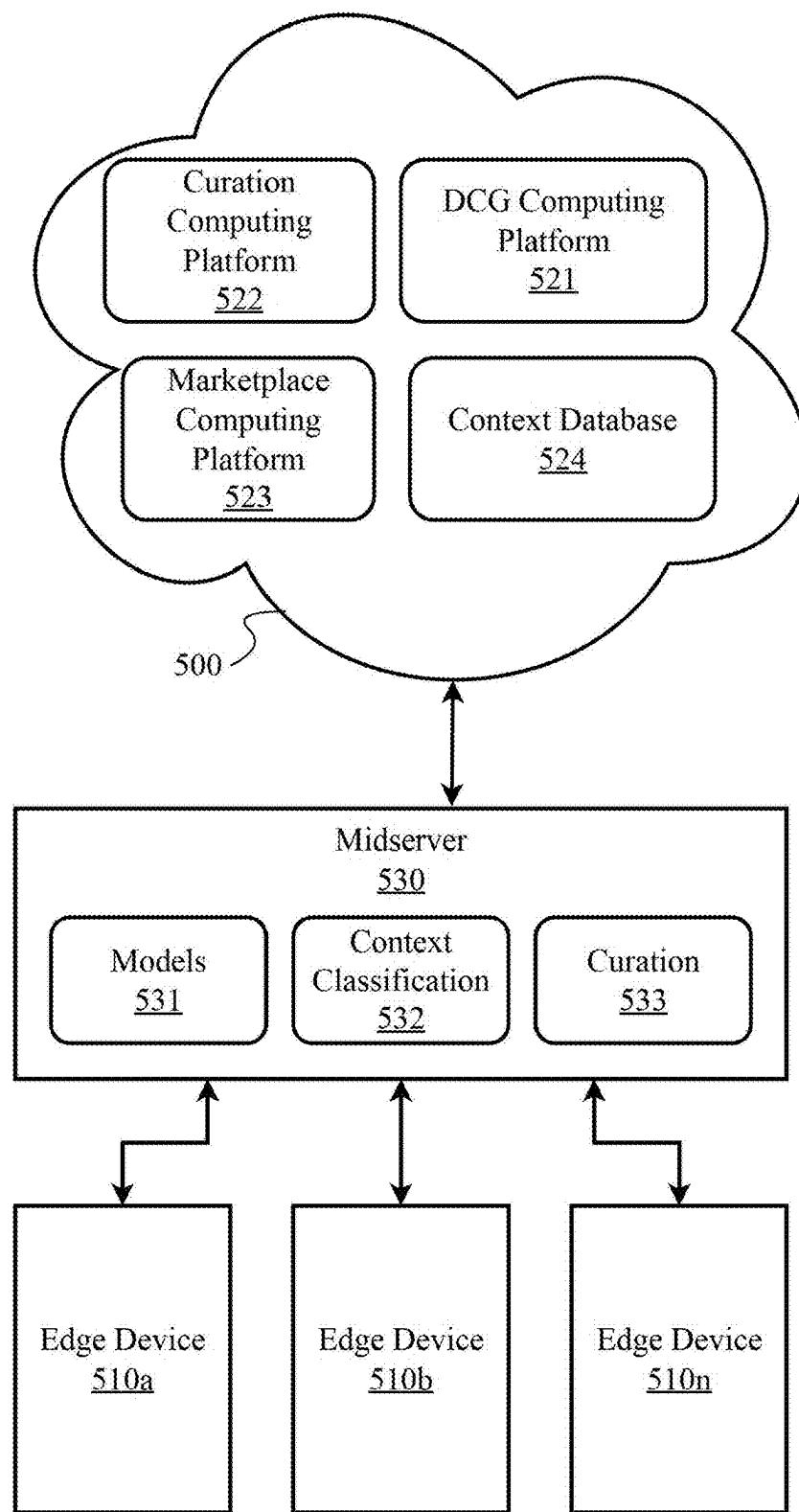


FIG. 5

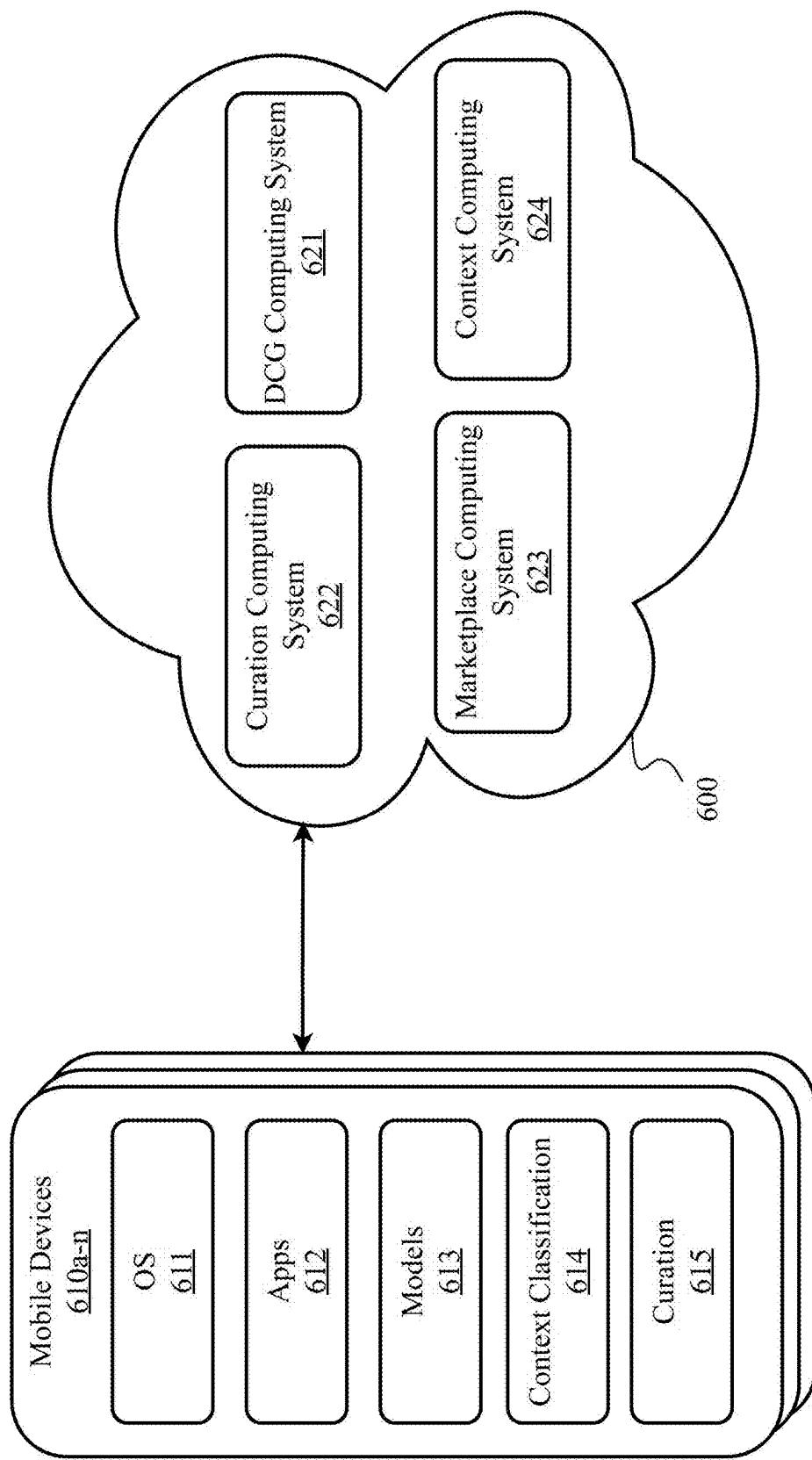


FIG. 6

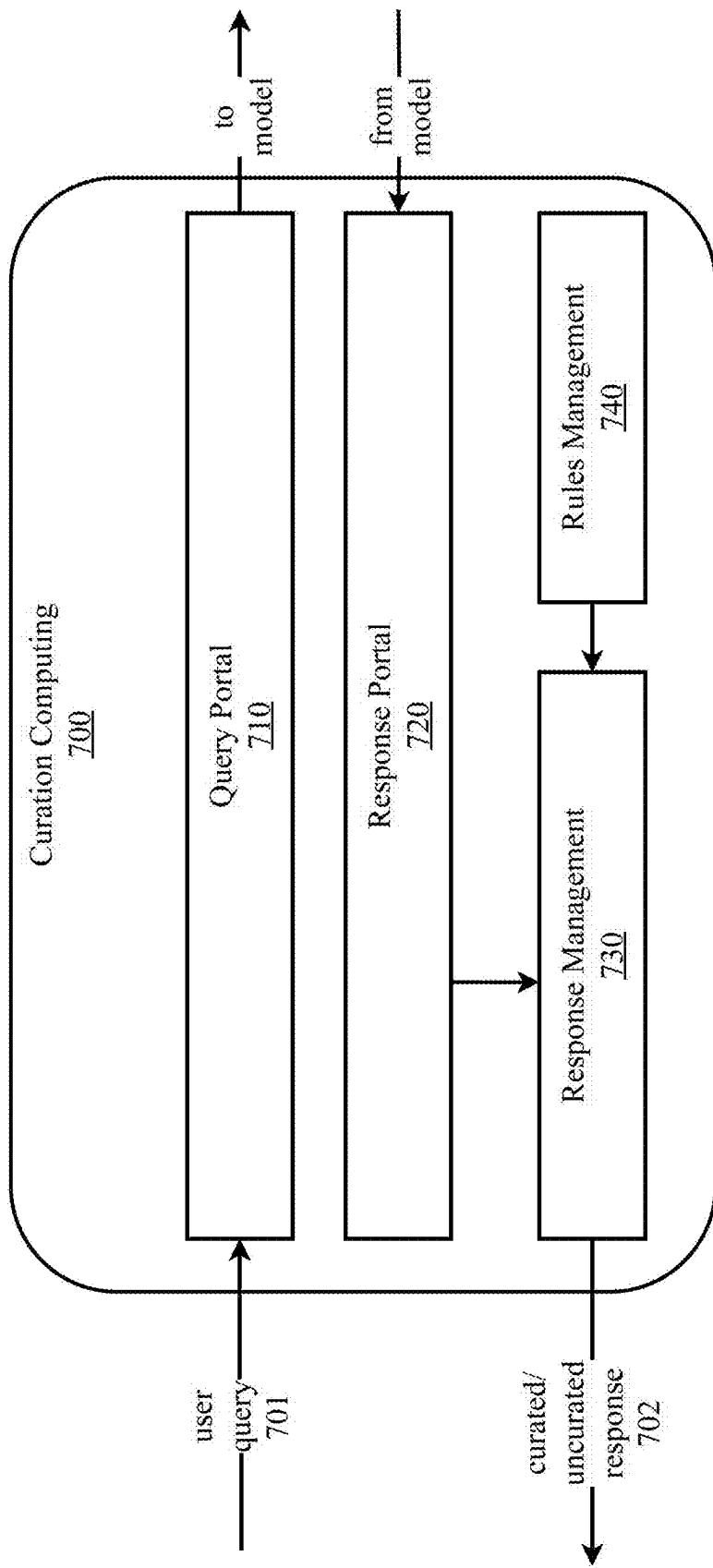


FIG. 7

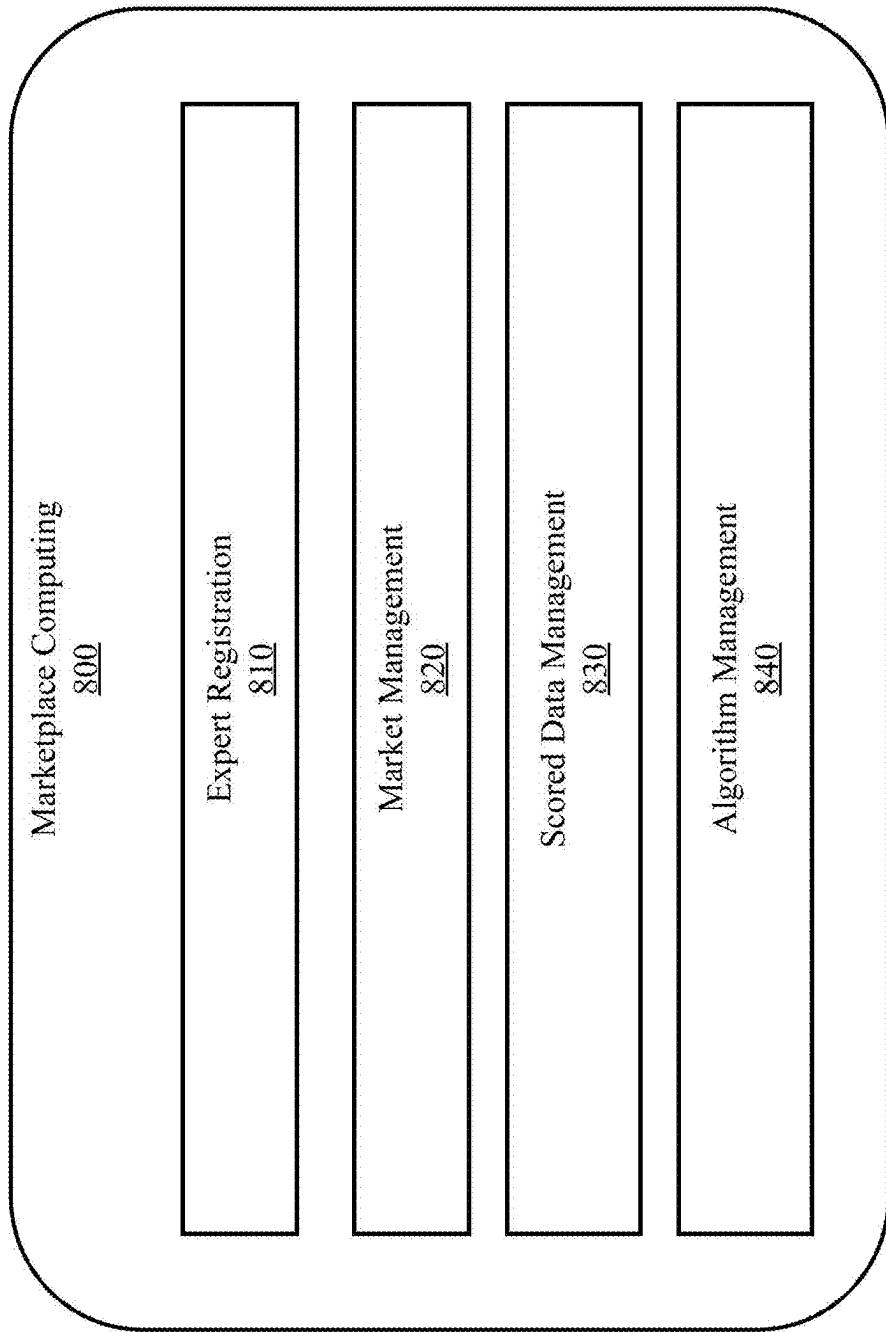


FIG. 8

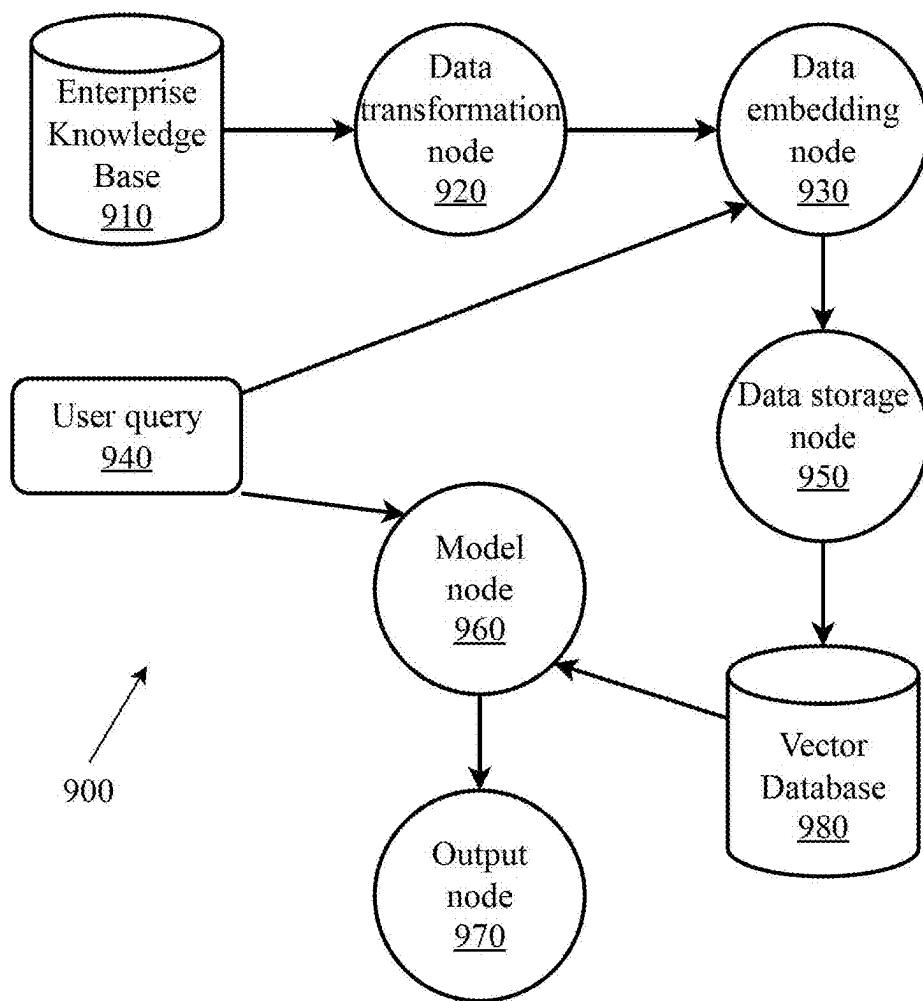


FIG. 9

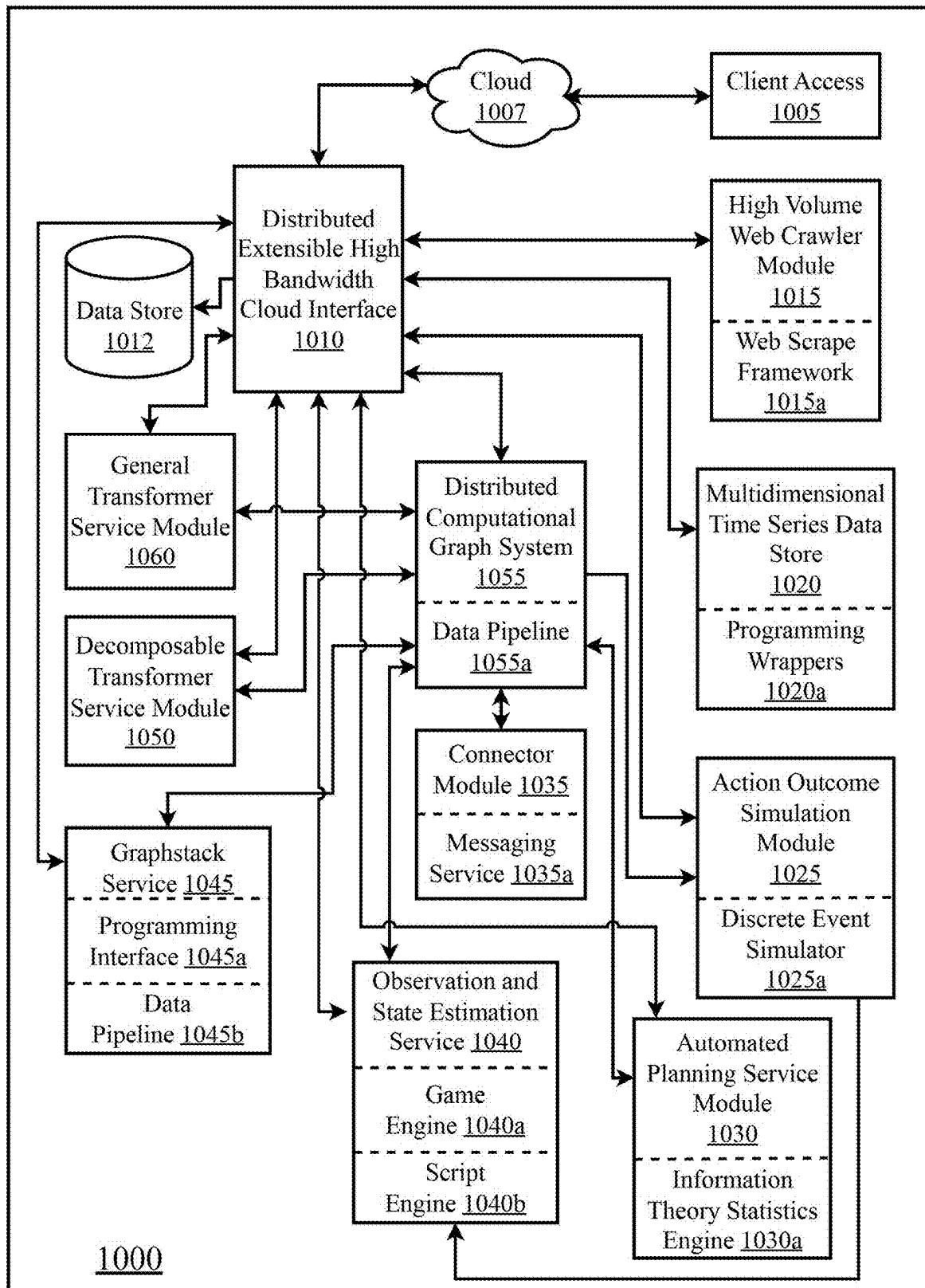


FIG. 10

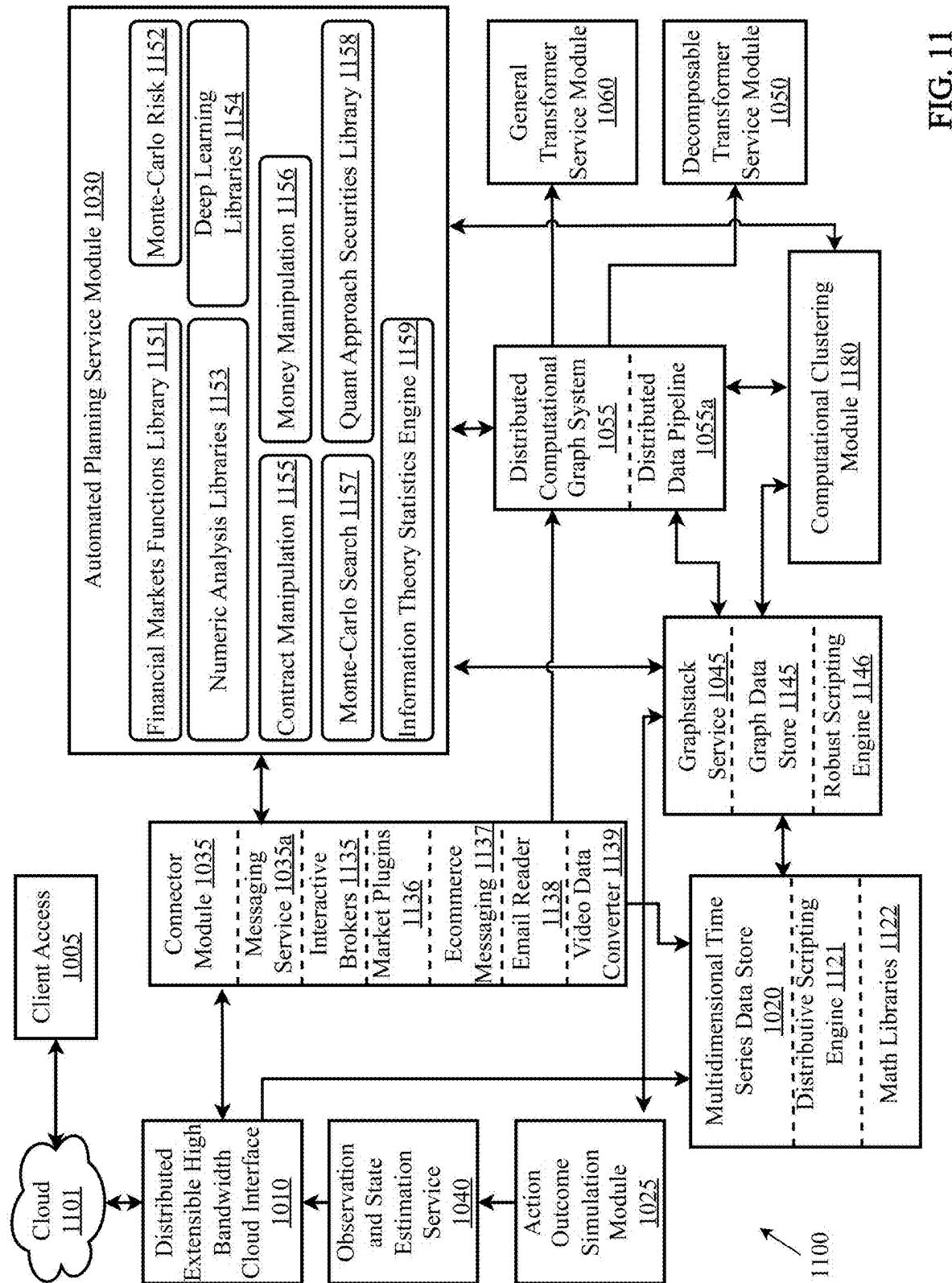


FIG. 11

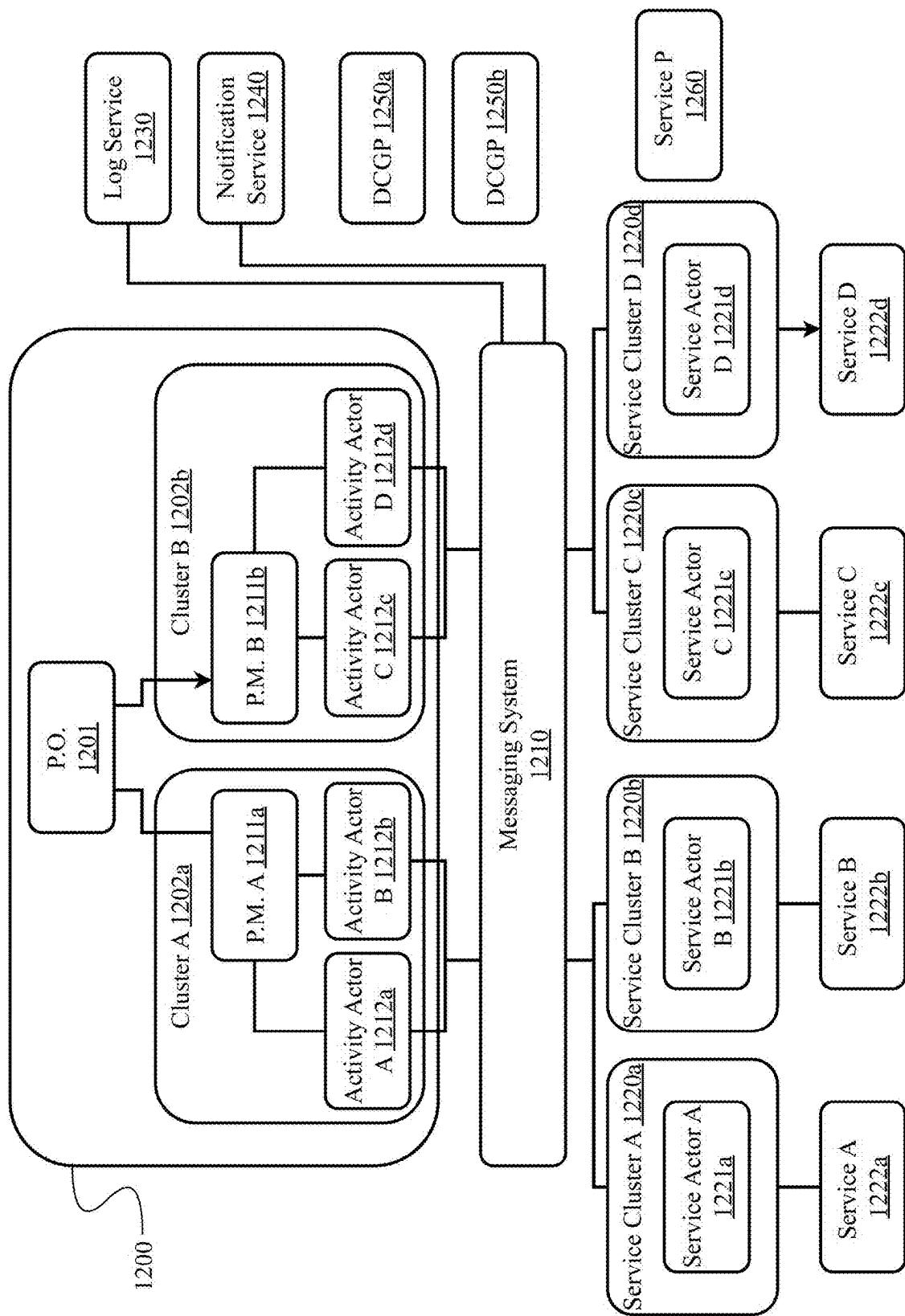


FIG. 12

FIG. 13

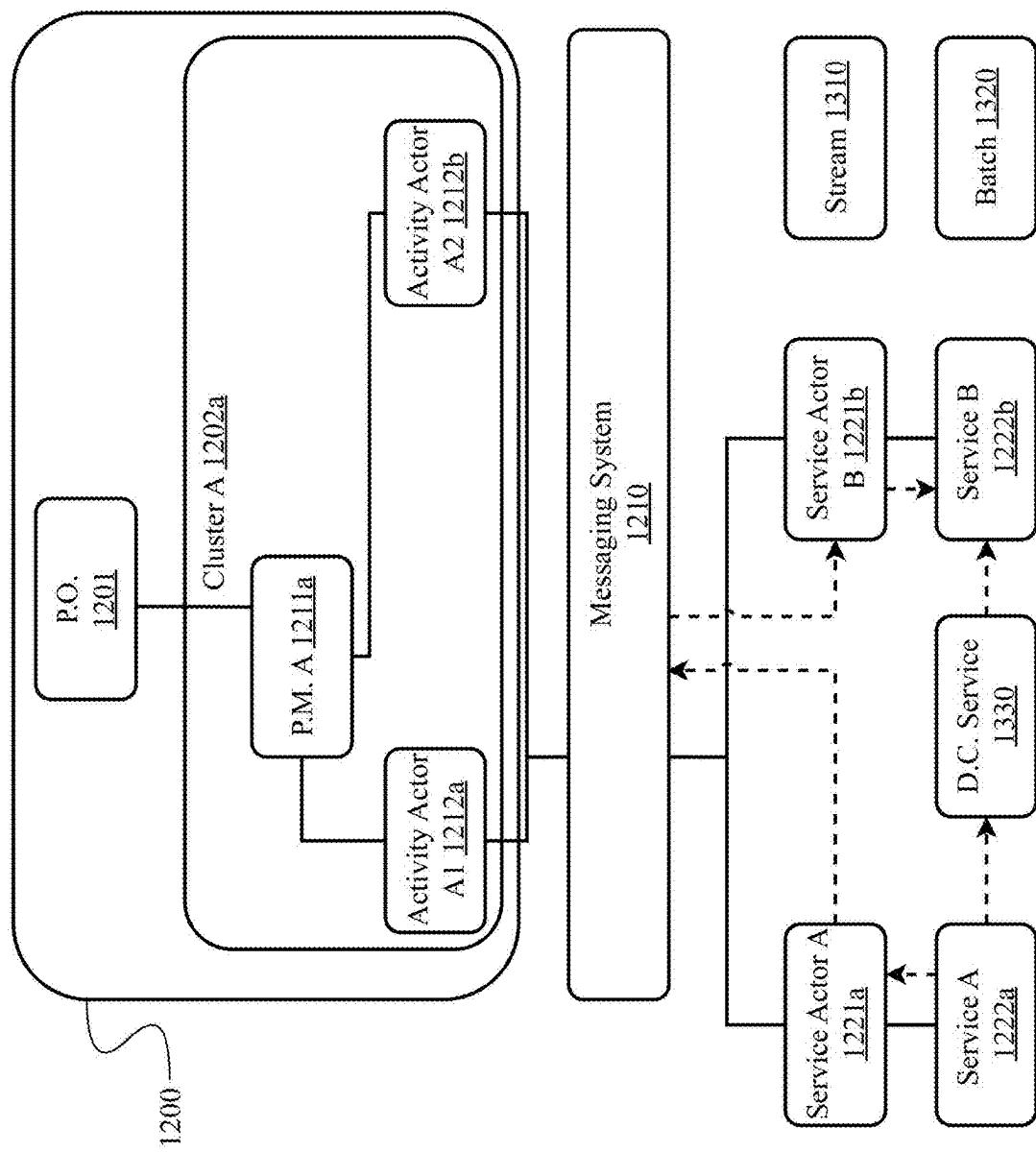
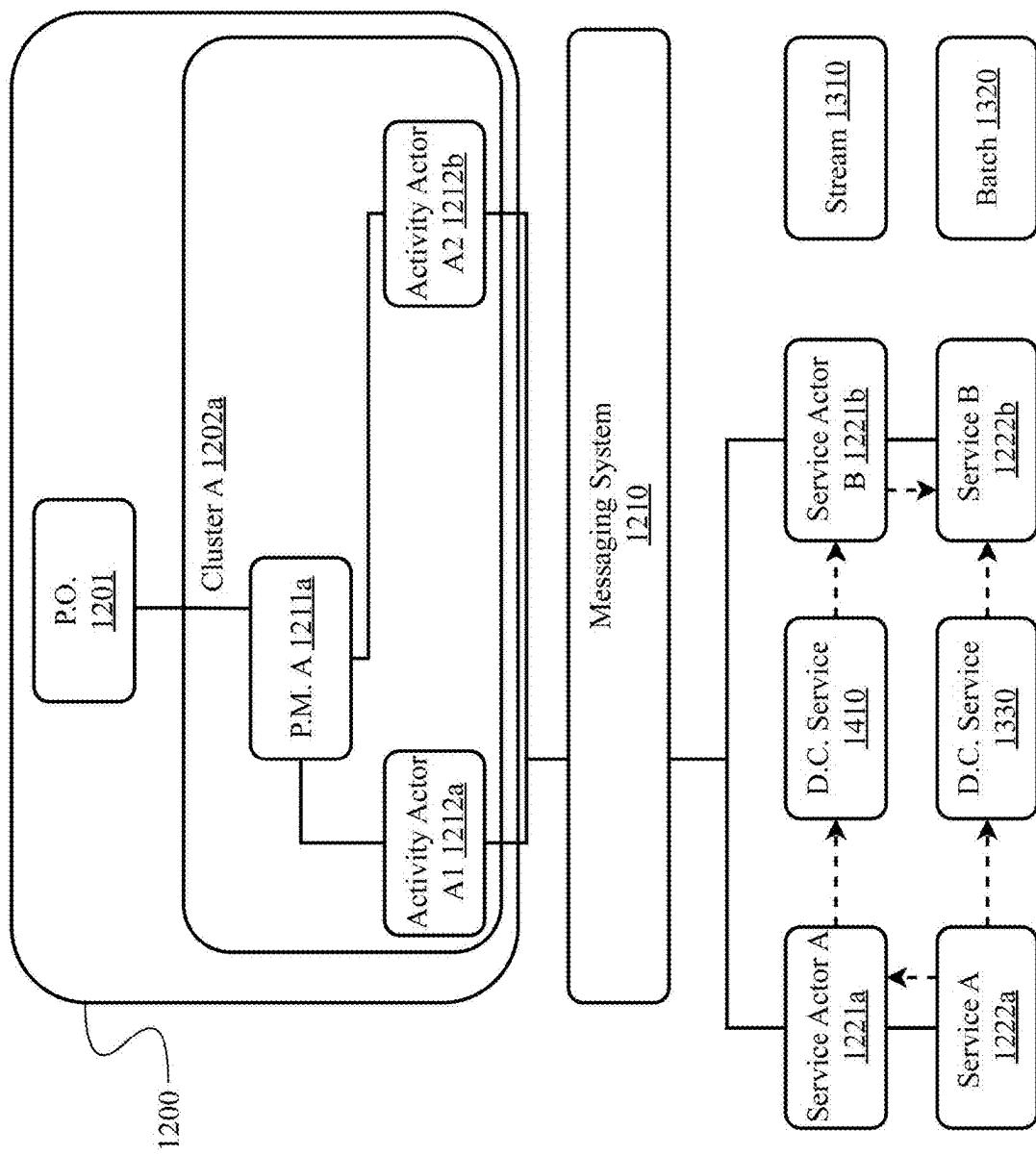


FIG. 14



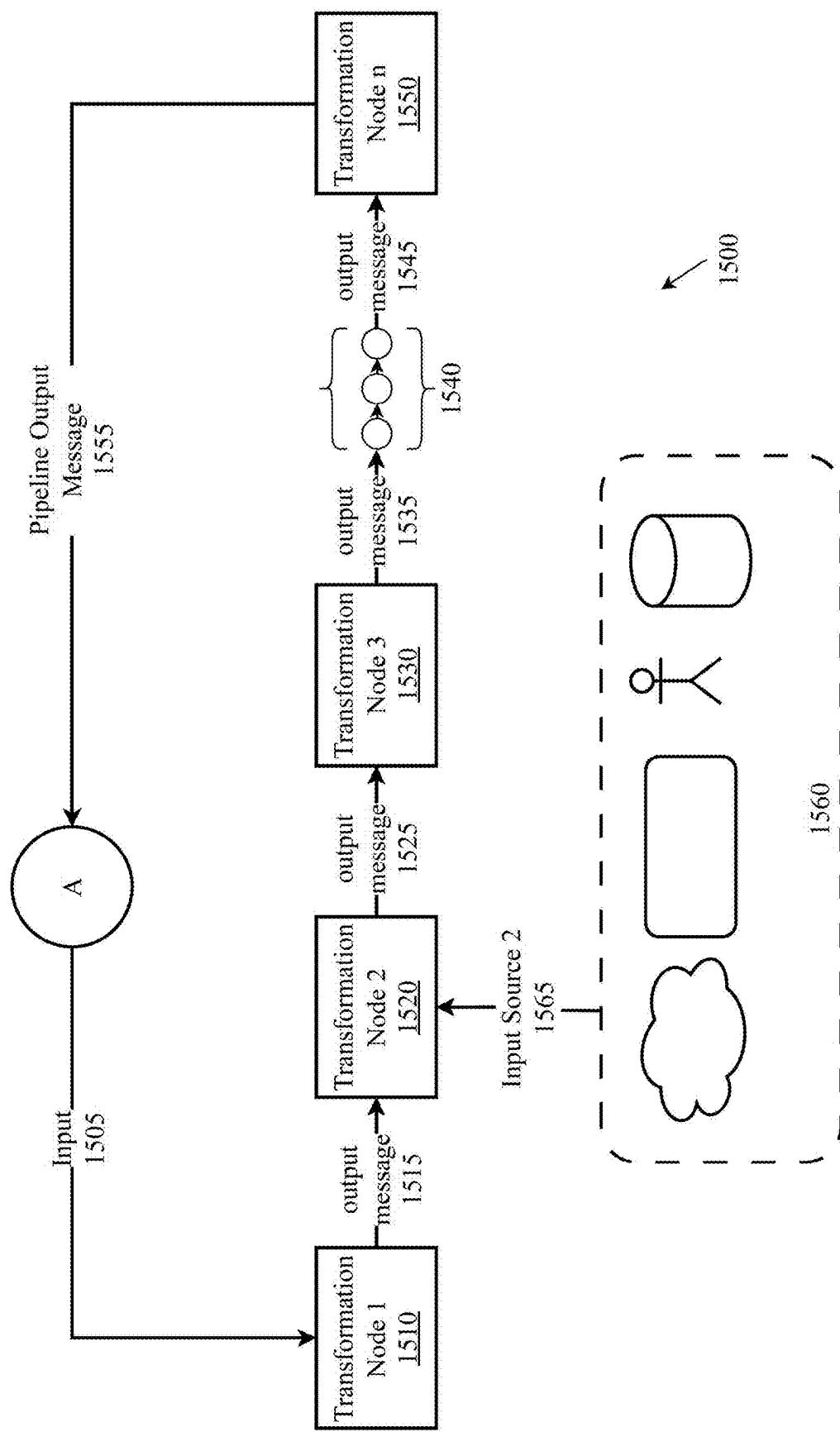
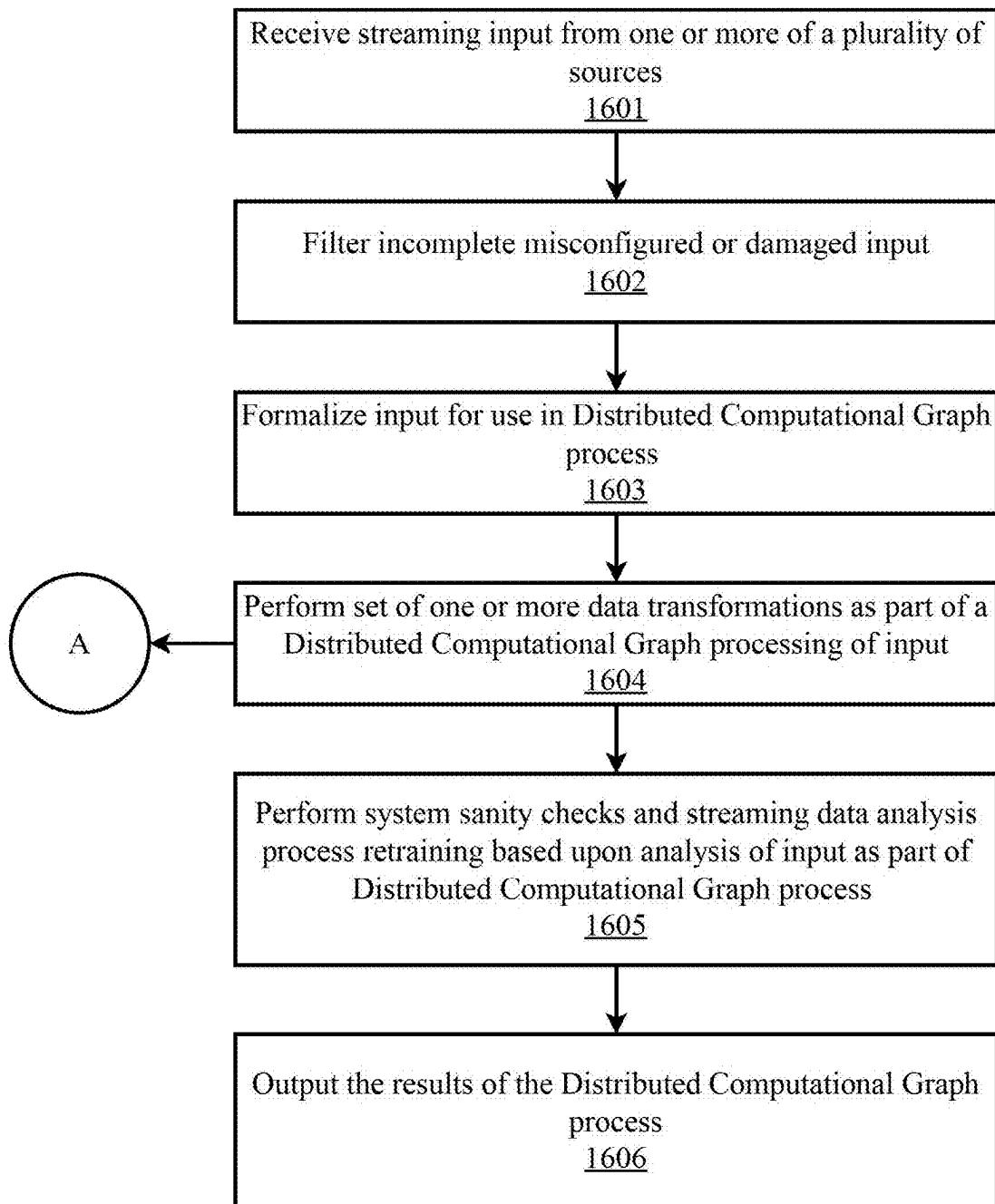


FIG. 15



1600  
↑

FIG. 16

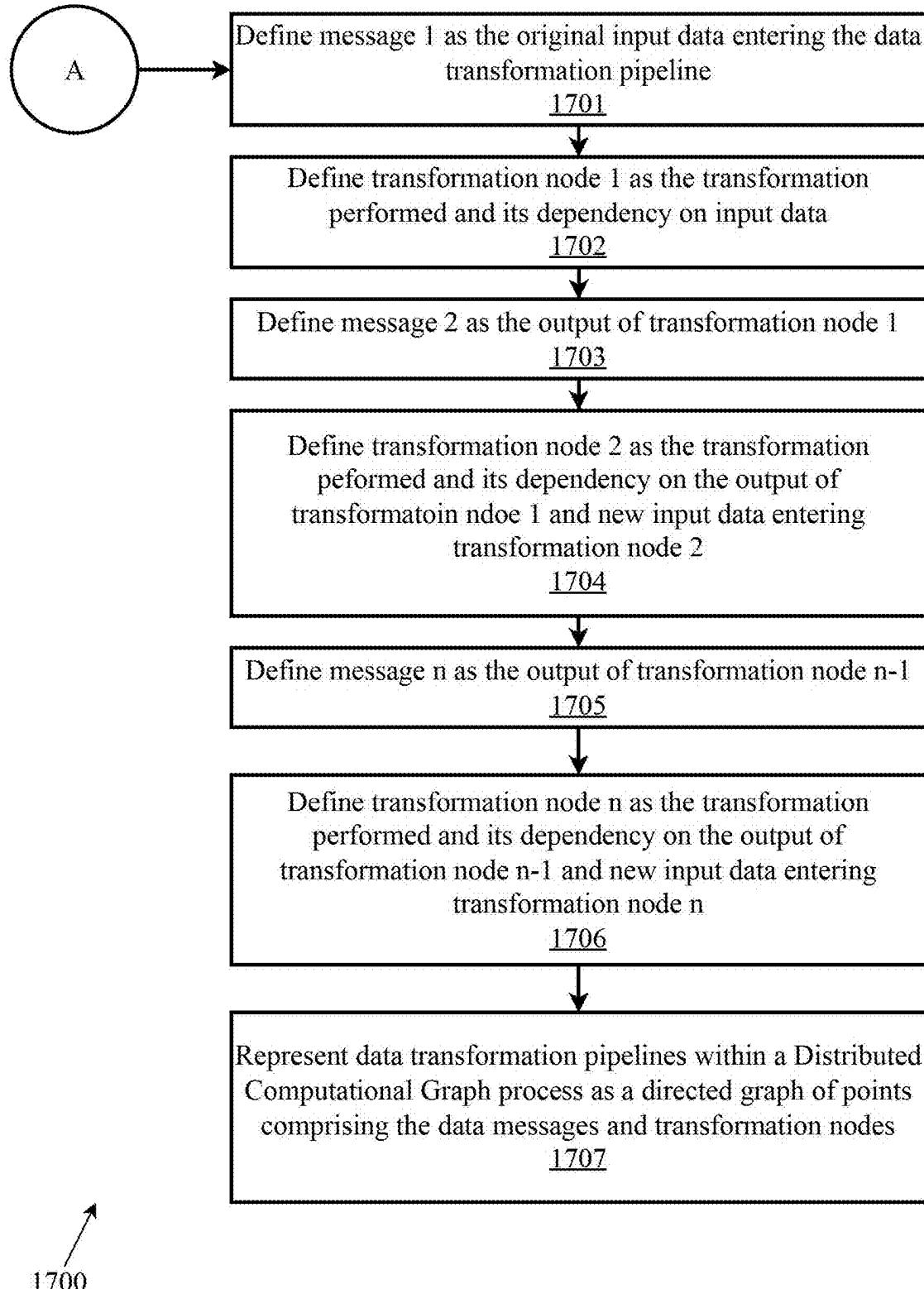
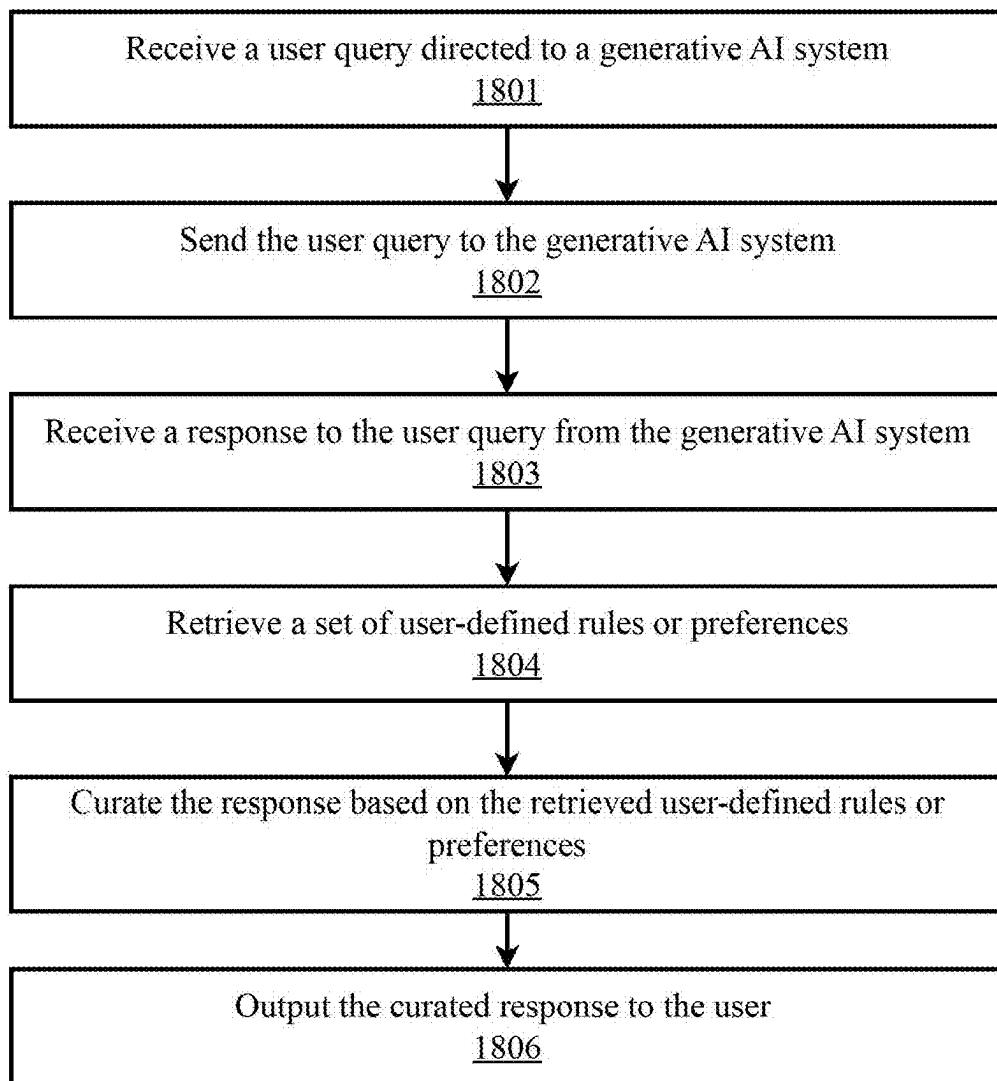


FIG. 17



**FIG. 18**

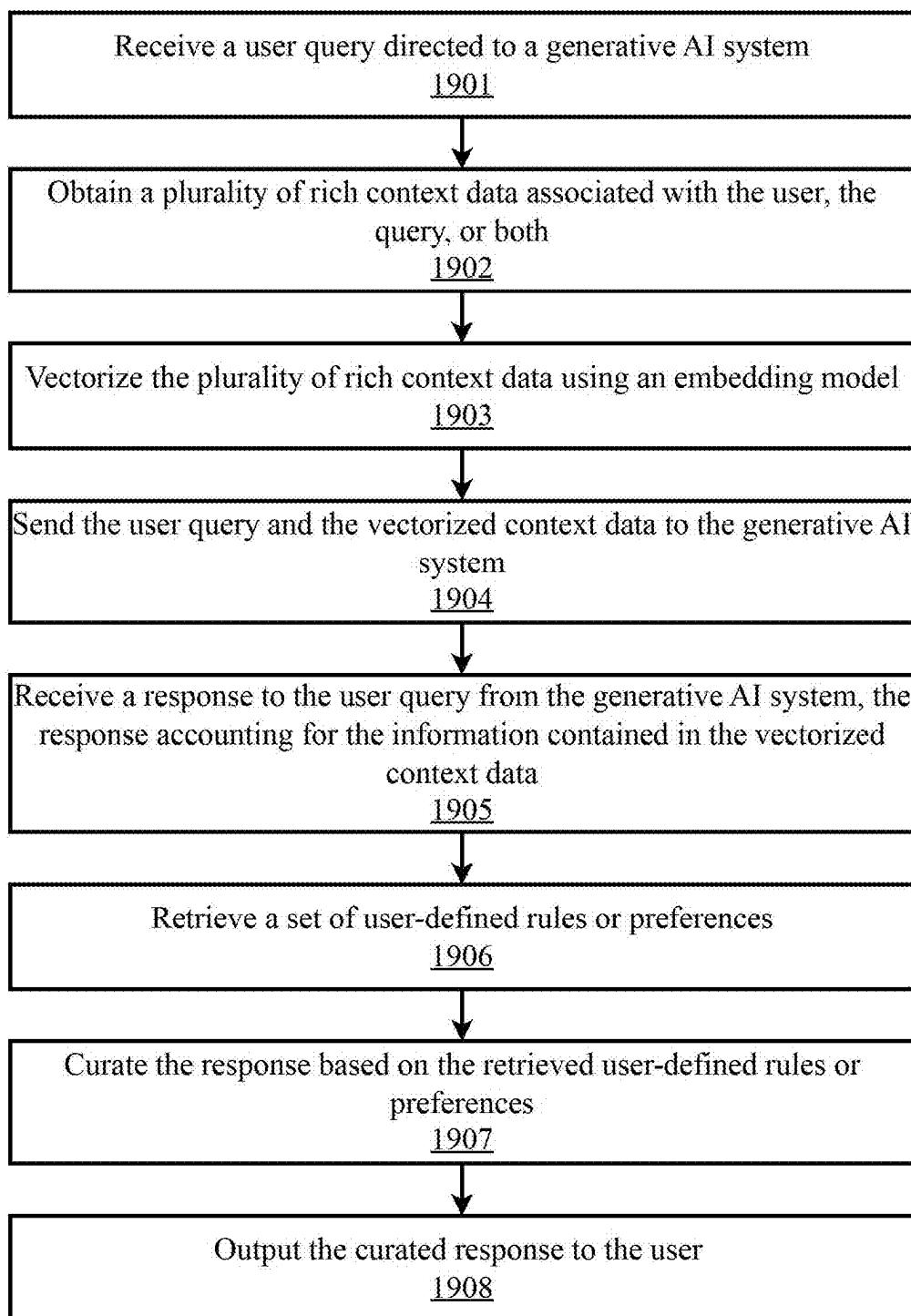


FIG. 19

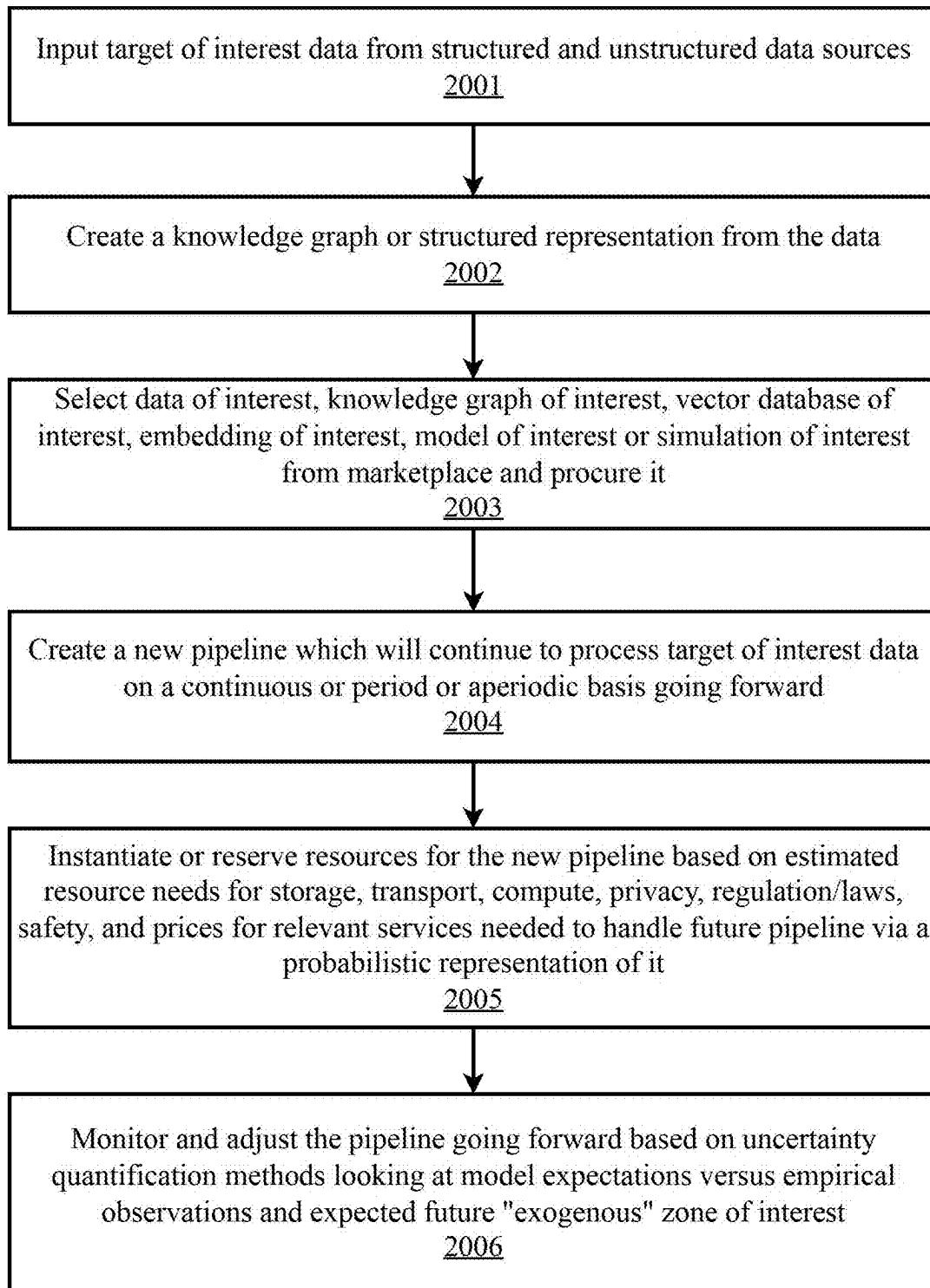


FIG. 20

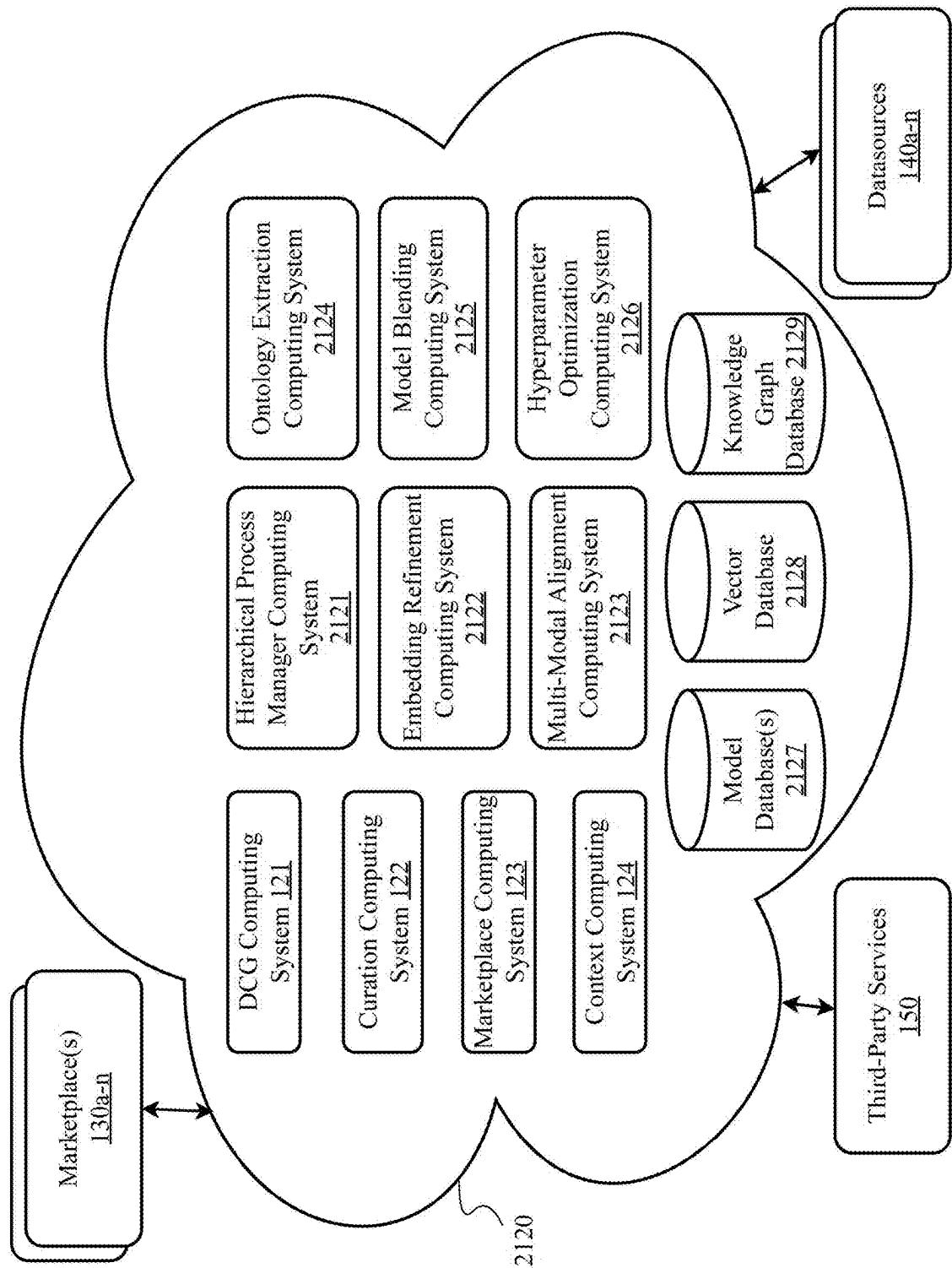


FIG. 21

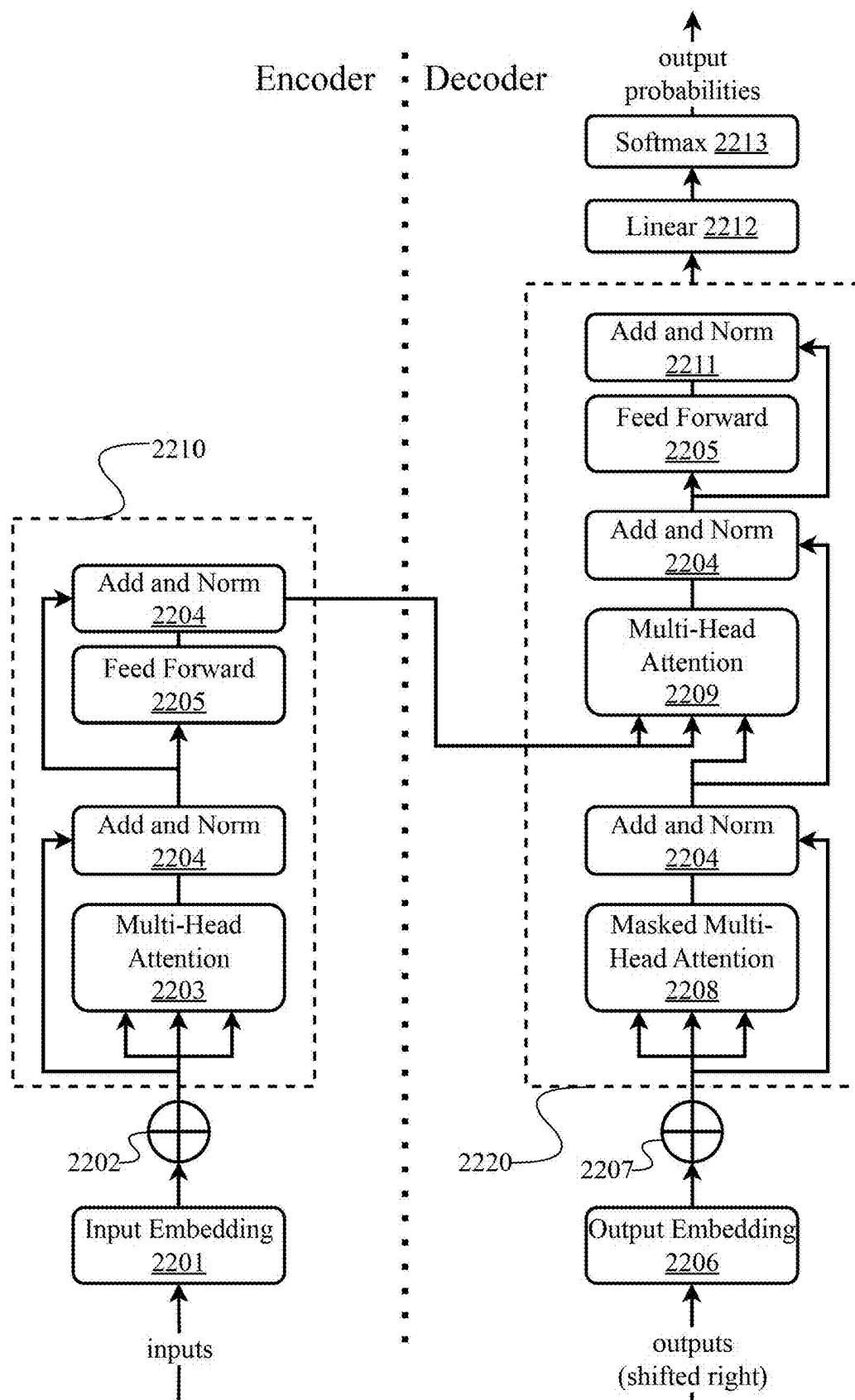


FIG. 22

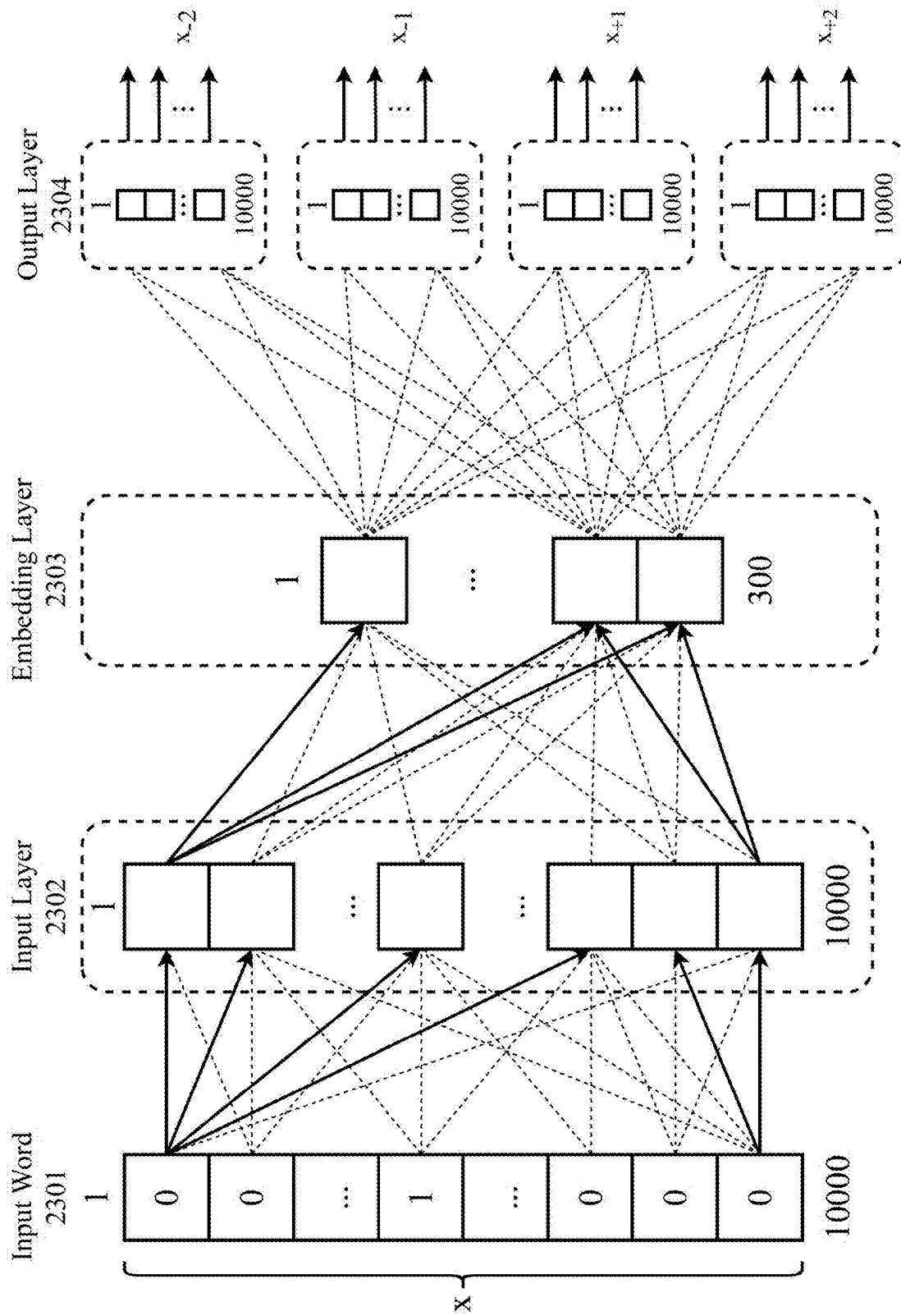


FIG. 23

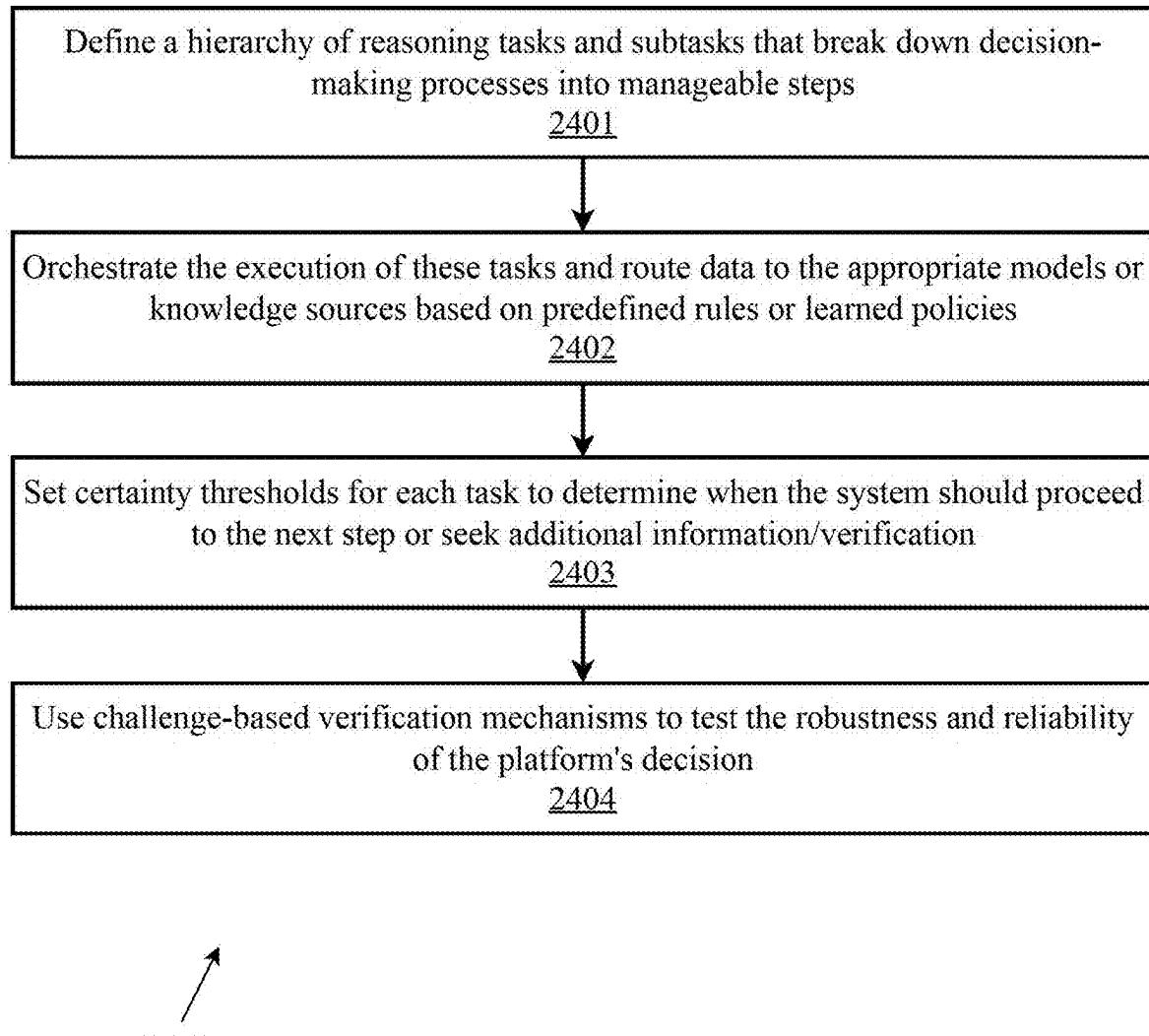
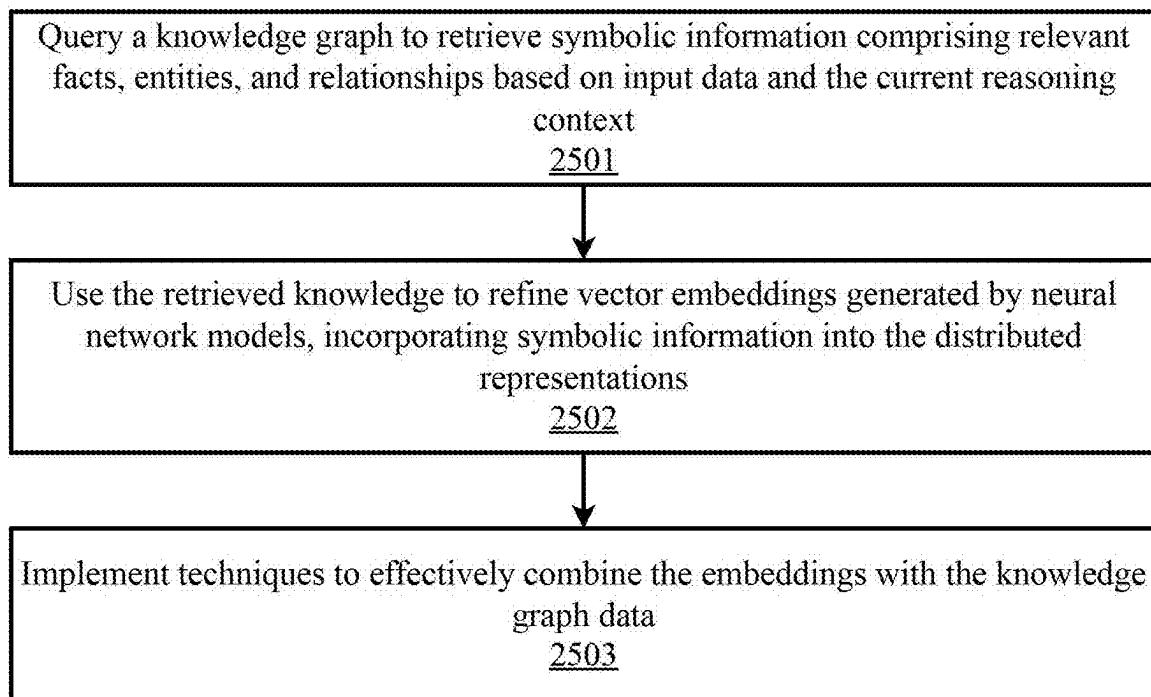
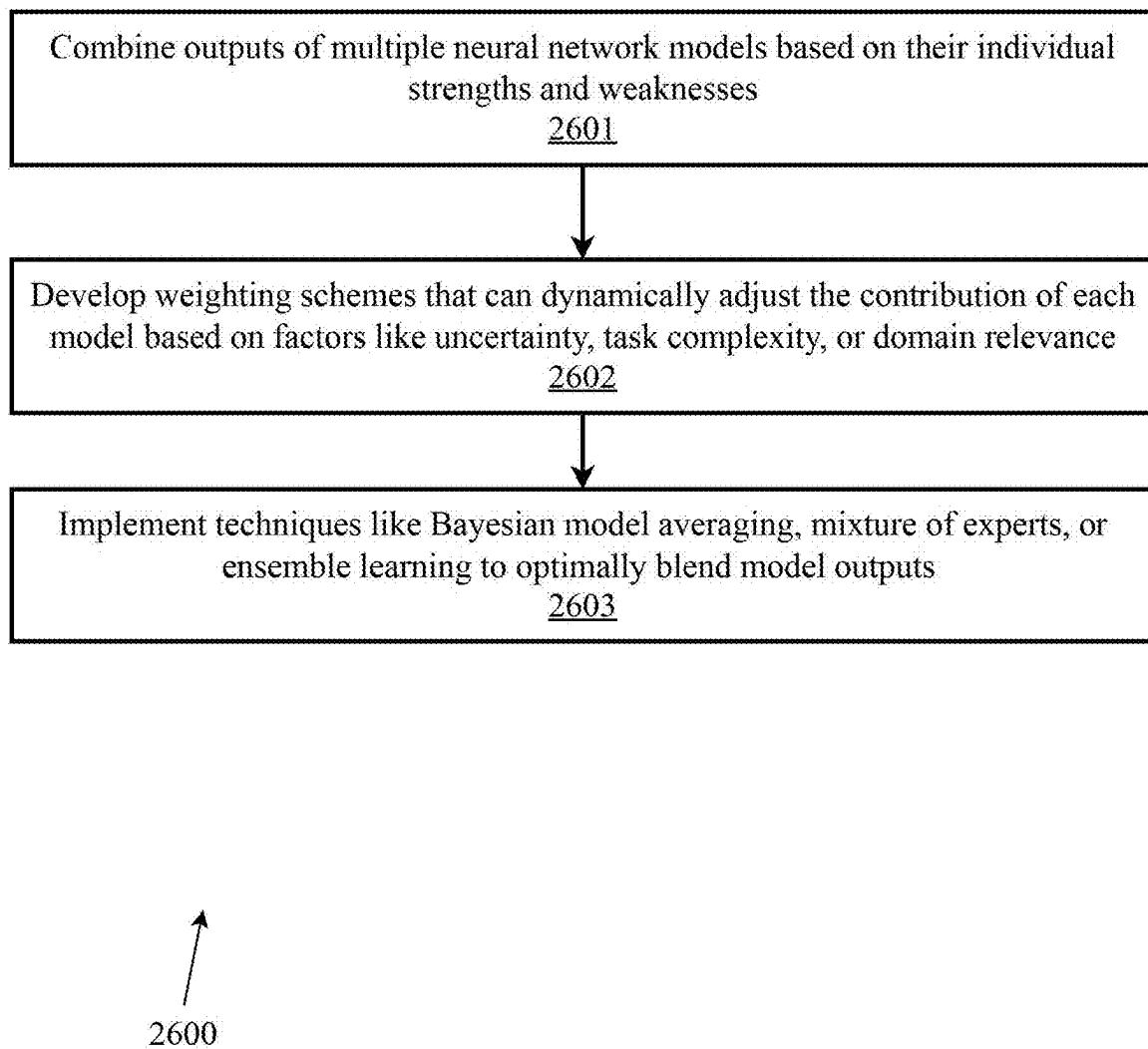


FIG. 24



2500

FIG. 25



**FIG. 26**

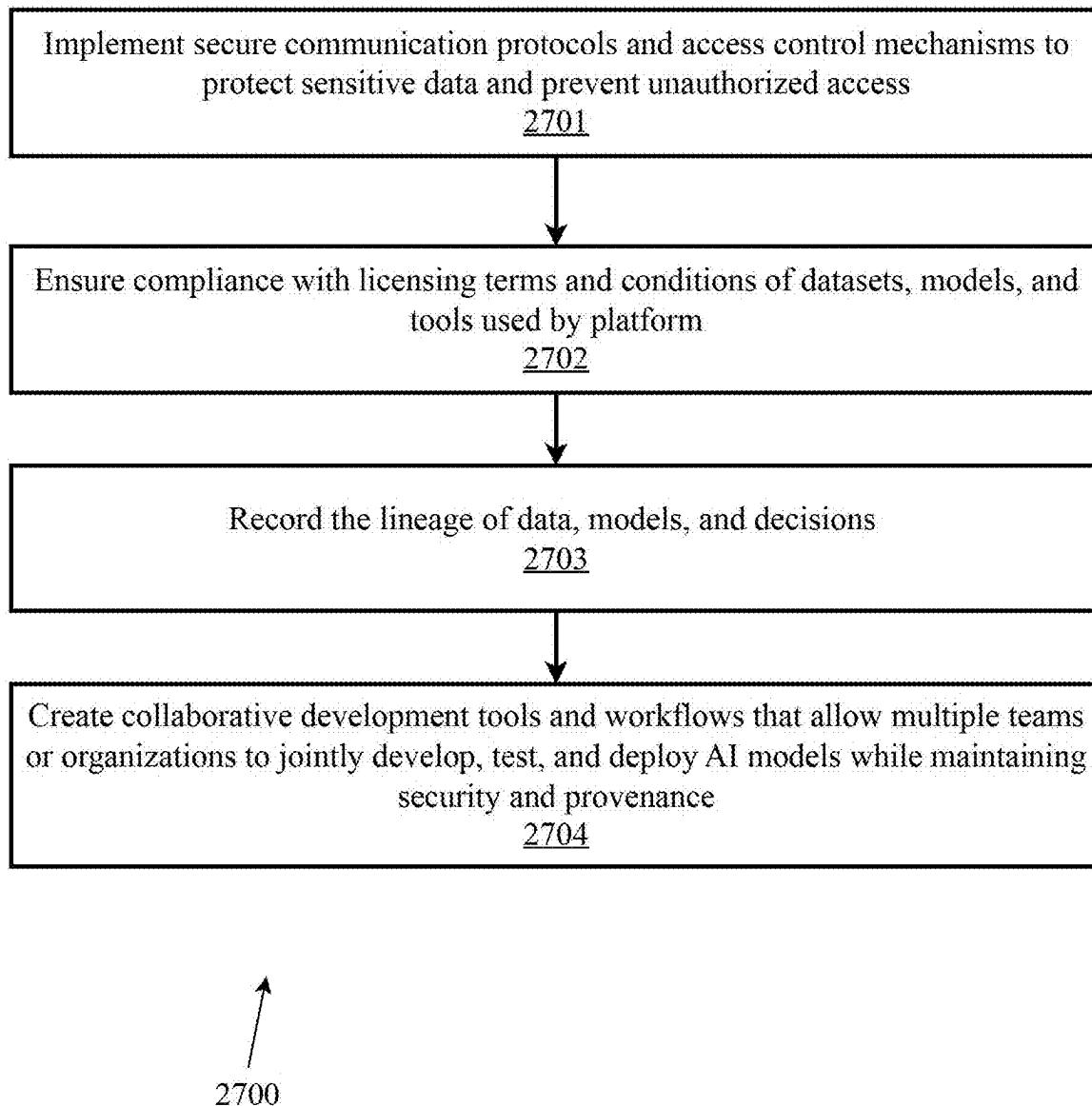
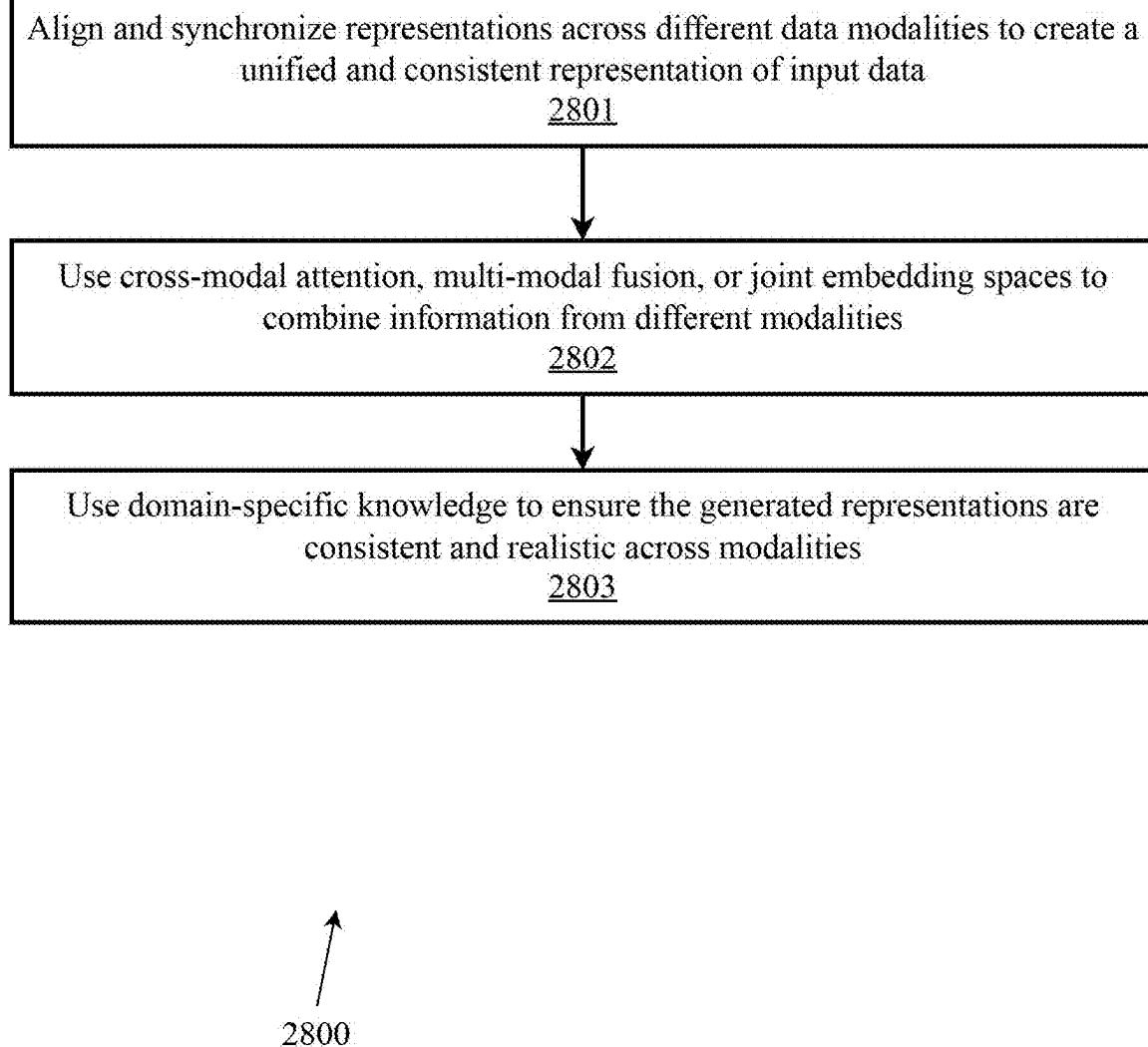


FIG. 27



**FIG. 28**

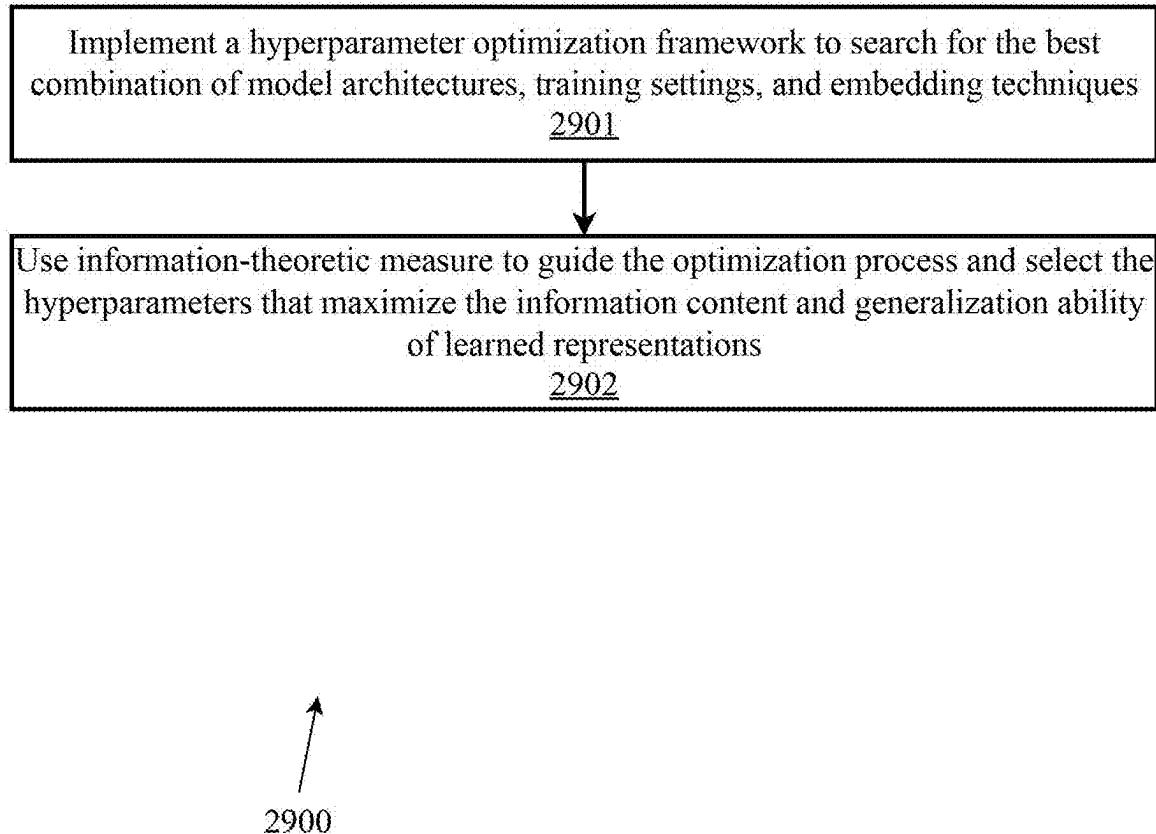
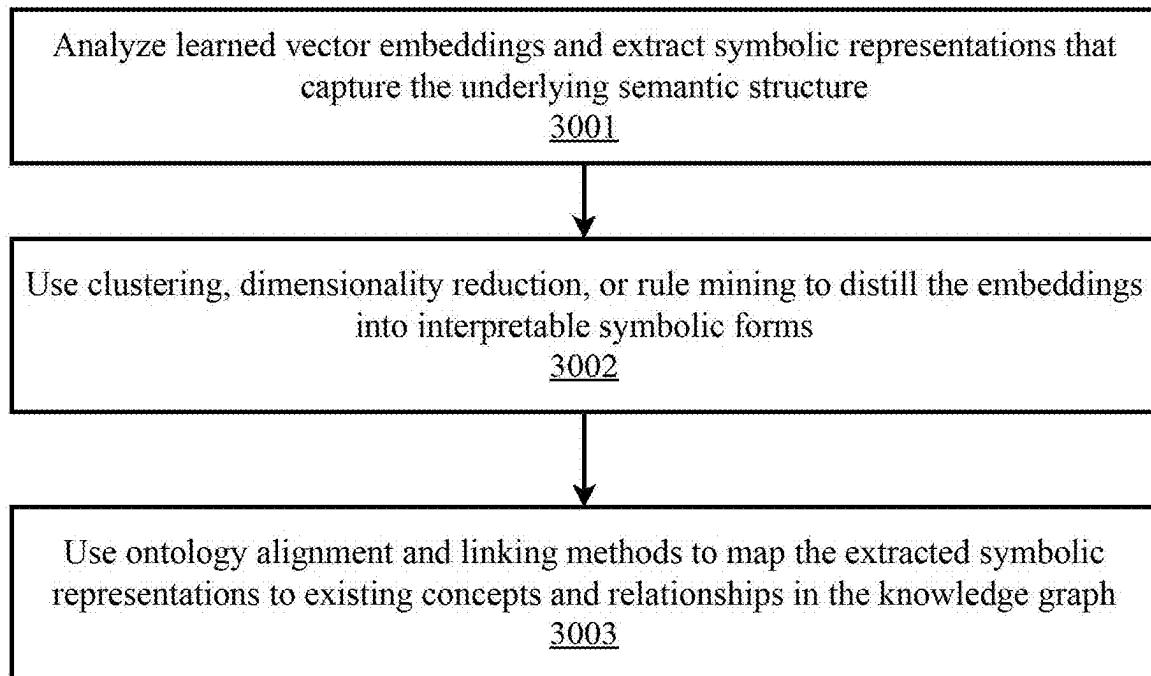


FIG. 29



3000

**FIG. 30**

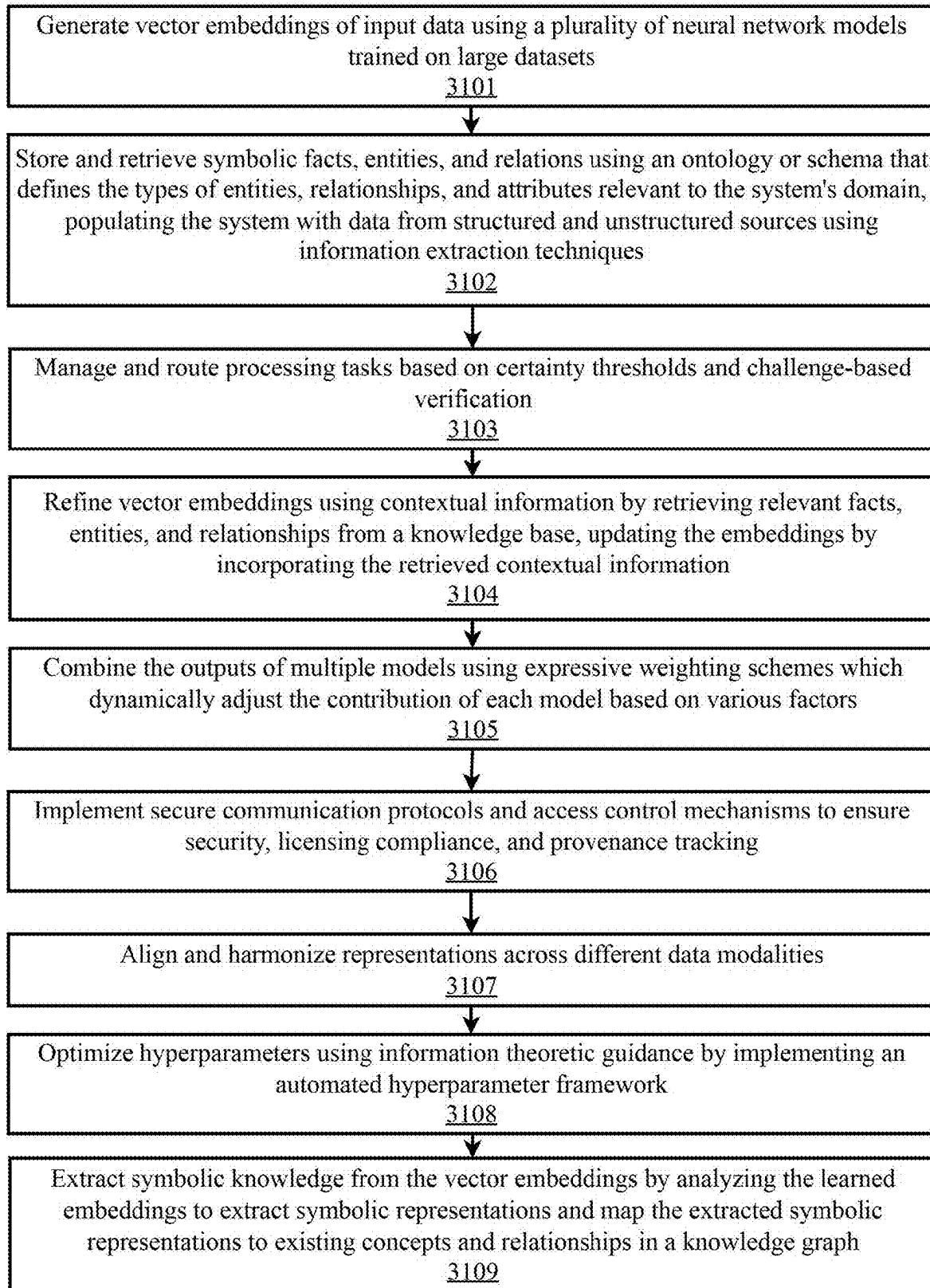


FIG. 31

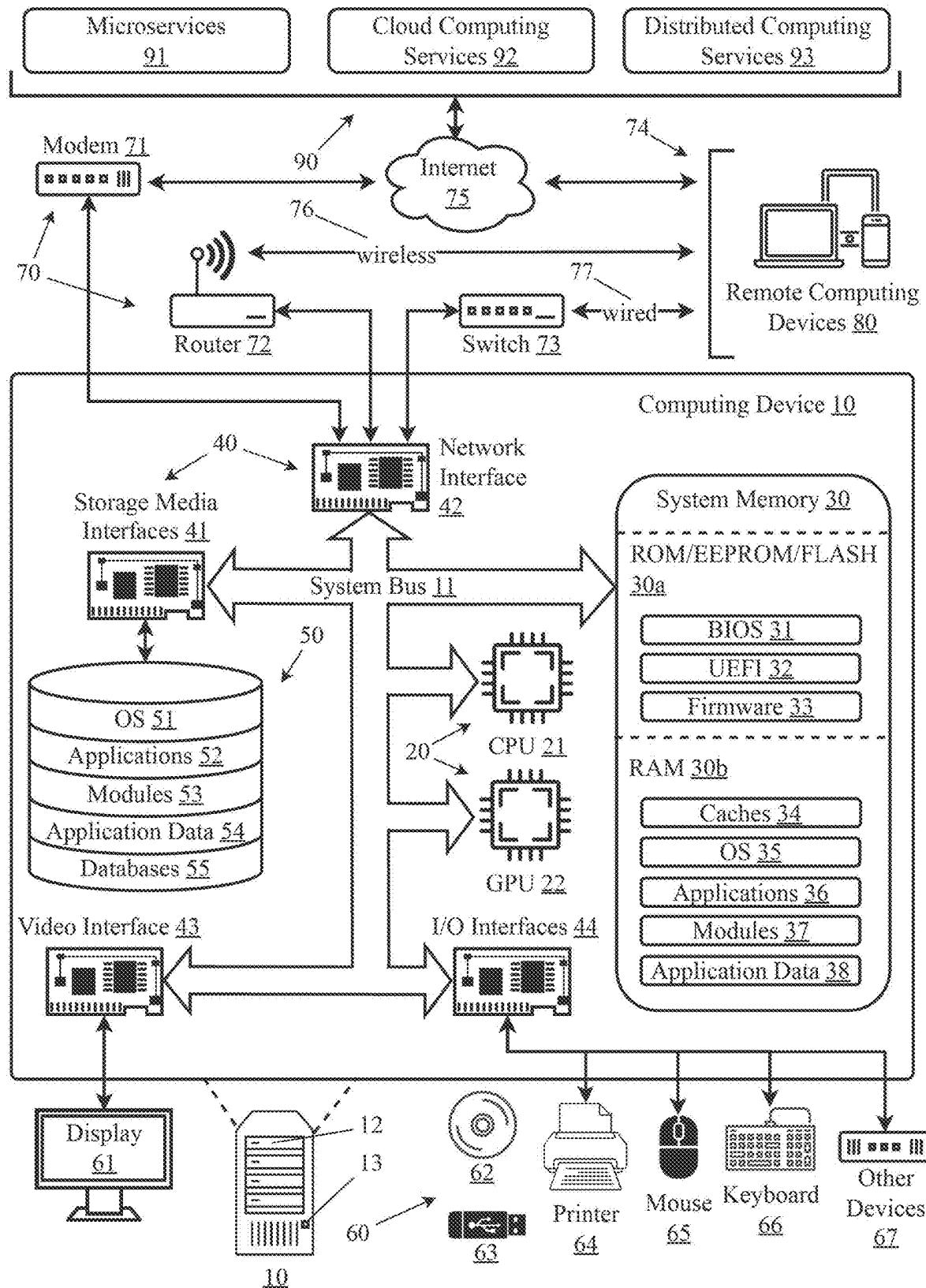


FIG. 32

**PLATFORM FOR INTEGRATION OF  
MACHINE LEARNING MODELS UTILIZING  
MARKETPLACES AND CROWD AND  
EXPERT JUDGMENT AND KNOWLEDGE  
CORPORA**

**CROSS-REFERENCE TO RELATED  
APPLICATIONS**

[0001] Priority is claimed in the application data sheet to the following patents or patent applications, each of which is expressly incorporated herein by reference in its entirety:

- [0002] Ser. No. 18/668,137
- [0003] Ser. No. 18/656,612
- [0004] 63/551,328

**BACKGROUND OF THE INVENTION**

**Field of the Art**

[0005] The present invention is in the field of artificial intelligence and distributed computing systems, and more particularly to electronic commerce in data, algorithms and network connected computing resources for storage, transport and compute workloads between multiple stakeholders.

**Discussion of the State of the Art**

[0006] Machine learning (ML) and artificial intelligence (AI) models are increasingly used in various applications. However, flexibly selecting and integrating ML and AI models remains challenging, especially when using multiple models and data sources together in real world decision-making processes. Assessing the utility and suitability and intellectual property considerations of proprietary models and datasets is also difficult and increasingly risky as attacks on data, algorithms and software code proliferate.

[0007] Current approaches such as the GPT Store or the AWS or Azure Marketplace (see e.g. <https://openai.com/index/introducing-the-gpt-store>) fail to address provenance, IP, usage, ongoing support, and methodology considerations needed to enable robust model and data incorporation and evolution in enterprises across both internal and exogenous resources. While systems like FINOS Legend have been furthered by Goldman Sachs and other notables, buoyed via the use of data contracts, they don't adequately marry the concepts with locality and regulatory aware distributed computational graphs for flow-based programming of complex (especially motile) logic across heterogeneous computing devices and dynamic network environments.

[0008] What is needed is a more transparent and comprehensive marketplace for data streams and sets, models, simulations, embeddings, algorithms, simulation components, scene elements, knowledge corpora, with an integrated license, usage, provenance, verification and payment functionality to support more collaborative and multi-stakeholder collaboration with robust but transparent economic principles.

**SUMMARY OF THE INVENTION**

[0009] Accordingly, the inventor has conceived and reduced to practice, a system and method for flexibly incorporating machine learning models into applications using a marketplace platform in a distributed computational graph (DCG) architecture. The DCG enables dynamic selection, creation and incorporation of trained models with data

sources and marketplaces for data, algorithms, models, simulations and expert/crowd judgment. Multiple models can be used in series or parallel and independently or in blends or consensus approaches. An expert judgment marketplace allows human and artificial intelligence (AI) experts (or crowds) to score the (at least perceived) accuracy of training data and model inputs and outputs. Consumers can select and rank experts (or groups) based on the helpfulness of their judgments within a given domain, for a given question, or for broader contexts. The marketplace platform enables data providers to sell access to proprietary datasets that can be dynamically integrated into the model optimization process based on the specific domain and context of the user's query. When a user submits a query, the system analyzes the query's domain and identifies relevant datasets from the marketplace that can enhance the model's performance for that particular domain. Through the marketplace, data providers can offer their proprietary datasets, which may include domain-specific data, annotated datasets, or datasets with unique features or characteristics. These datasets are curated, preprocessed, and optimized for integration into the platform's machine learning and artificial intelligence models and simulations. When a relevant dataset is identified for a specific query, the system can dynamically incorporate that dataset into the model optimization process. This real-time integration allows the model to adapt and fine-tune its performance based on the domain-specific data, enabling it to generate more accurate and contextually relevant results for the user's query. A similar system for knowledge graphs and symbolic models linked to specific ontologies enables more formal semantically represented knowledge and symbolic modeling capabilities to be transacted for inclusion in neuro symbolic AI systems with collaborative progenitors.

[0010] According to a preferred embodiment, a computing system for integration of machine learning models and facilitating transactions between buyers, sellers, and experts employing a marketplace platform, the computing system comprising: one or more hardware processors configured for: listing, searching, and transacting various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement; selecting and integrating machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy; collecting and aggregating evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods; securely processing payments, licensing, and delivery of acquired goods between buyers and sellers; facilitating communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and ensuring transparency, accountability, and adherence to quality standards and ethical principles in the marketplace for robust multi stakeholder development of robust solutions while preserving intellectual property rights of individuals and groups in downstream systems.

[0011] According to another preferred embodiment, a computer-implemented method executed on a marketplace platform for integration of machine learning models and facilitating transactions between buyers, sellers, and experts,

the computer-implemented method comprising: listing, searching, and transacting various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement; selecting and integrating machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy; collecting and aggregating evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods; securely processing payments, licensing, and delivery of acquired goods between buyers and sellers; facilitating communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and ensuring transparency, accountability, and adherence to quality standards and ethical principles in the marketplace.

[0012] According to another preferred embodiment, a system for integration of machine learning models and facilitating transactions between buyers, sellers, and experts employing a marketplace platform, comprising one or more computers with executable instructions that, when executed, cause the system to: list, search, and transact various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement; select and integrate machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy; collect and aggregate evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods; securely process payments, licensing, and delivery of acquired goods between buyers and sellers; facilitate communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and ensure transparency, accountability, and adherence to quality standards and ethical principles in the marketplace.

[0013] According to another preferred embodiment, non-transitory, computer-readable storage media having computer-executable instructions embodied thereon that, when executed by one or more processors of a computing system employing a marketplace platform for integration of machine learning models and facilitating transactions between buyers, sellers, and experts, cause the computing system to: list, search, and transact various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement; select and integrate machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy; collect and aggregate evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods; securely process payments, licensing, and delivery of acquired goods between buyers and sellers; facilitate communication, collaboration, and knowledge sharing among buyers, sellers,

and experts; and ensure transparency, accountability, and adherence to quality standards and ethical principles in the marketplace.

[0014] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for: collecting the expert evaluations and ratings while browsing external data sources; quantifying the quality, relevance, and suitability of listed goods based on expert judgments; and assessing the credibility and reliability of experts based on their historical evaluations and community feedback.

[0015] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for: securely processing financial transactions between buyers and sellers; generating and enforcing usage rights and restrictions for acquired goods; and holding funds until the satisfactory delivery and acceptance of goods.

[0016] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for: sharing and co-developing machine learning projects; and documenting best practices, tutorials, and case studies related to the listed goods.

[0017] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for proactively suggesting relevant goods, experts, or collaborators based on user preferences, transaction history, and platform interactions.

[0018] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for: assessing the interoperability and combinability of different machine learning models and datasets; evaluating the efficiency and scalability of integrated models; and suggesting improvements and enhancements to the selected models and datasets.

[0019] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for selecting, creating, and incorporating trained models based on expert judgment inputs.

[0020] According to an aspect of an embodiment, wherein the one or more hardware processors are further configured for: continuously adjusting and optimizing the hyperparameters of machine learning and artificial intelligence models based on performance metrics and user feedback; dynamically updating and fine-tuning machine learning and artificial intelligence models based on newly available data and evolving user requirements; optimizing the retrieval and generation components of RAG models, including fine-tuning retrieval algorithms, updating knowledge bases, and enhancing generation quality; and incorporating user feedback and preferences into the optimization process, ensuring continuous improvement and alignment with user expectations.

#### BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0021] FIG. 1A is a block diagram illustrating an exemplary system architecture of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces, according to an embodiment.

[0022] FIG. 1B is a block diagram illustrating an exemplary aspect of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces, a transaction computing system.

[0023] FIG. 1C is a block diagram illustrating an exemplary aspect of an embodiment of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces, a marketplace computing system.

[0024] FIG. 1D is a block diagram illustrating an exemplary architecture for facilitating secure financial transactions and data transfers within the platform's marketplaces, according to an embodiment.

[0025] FIG. 1E is a block diagram illustrating some exemplary marketplaces and marketplace goods which may be implemented according to various aspects of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces.

[0026] FIG. 1F is a block diagram illustrating an exemplary system architecture for a distributed generative artificial intelligence reasoning and action platform, according to an embodiment.

[0027] FIG. 2 is a block diagram illustrating an exemplary aspect of a distributed generative AI reasoning and action platform incorporating various additional contextual data.

[0028] FIG. 3 is a diagram illustrating incorporating symbolic reasoning in support of LLM-based generative AI, according to an aspect of a neuro-symbolic generative AI reasoning and action platform.

[0029] FIG. 4 is a block diagram illustrating an exemplary architecture for a neuro-symbolic generative AI reasoning and action platform configured for federated learning at a plurality of edge devices, according to an embodiment.

[0030] FIG. 5 is a block diagram illustrating an exemplary architecture for a neuro-symbolic generative AI reasoning and action platform configured to utilize a midserver to act as a computing intermediary between a plurality of edge devices and the platform.

[0031] FIG. 6 is a block diagram illustrating an exemplary mobile device configured for experience curation using embedded capabilities and functionality provided by a neuro-symbolic generative AI reasoning and action platform, according to an embodiment.

[0032] FIG. 7 is a block diagram illustrating an exemplary aspect of a distributed generative artificial intelligence reasoning and action platform, a curation computing system.

[0033] FIG. 8 is a block diagram illustrating an exemplary aspect of a distributed generative artificial intelligence reasoning and action platform, a marketplace computing system.

[0034] FIG. 9 is a block diagram illustrating a simple example of a distributed computational graph representation for providing neuro-symbolic GenAI capabilities, according to an aspect.

[0035] FIG. 10 is a block diagram illustrating an exemplary aspect of an embodiment of a distributed computational graph computing system utilizing an AI enhanced decision platform for external network reconnaissance and contextual data collection.

[0036] FIG. 11 is a block diagram illustrating another exemplary aspect of an embodiment of a distributed computational graph computing system utilizing an AI enhanced decision platform.

[0037] FIG. 12 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0038] FIG. 13 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0039] FIG. 14 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0040] FIG. 15 is a block diagram of an architecture for a transformation pipeline within a system for predictive analysis of very large data sets using distributed computational graph computing system.

[0041] FIG. 16 is a process flow diagram of a method for predictive analysis of very large data sets using the distributed computational graph.

[0042] FIG. 17 is a process flow diagram of a method for an aspect of modeling the transformation pipeline module as a directed graph using graph theory.

[0043] FIG. 18 is a flow diagram illustrating an exemplary method for providing experience curation, according to an aspect of an embodiment.

[0044] FIG. 19 is a flow diagram illustrating an exemplary method for providing experience curation with using rich contextual data, according to an aspect of an embodiment.

[0045] FIG. 20 is a flow diagram illustrating an exemplary method for using a distributed computation graph system for creating structured representations or knowledge graphs from various data sources, and setting up a pipeline for continuous processing and monitoring of that data, according to an embodiment.

[0046] FIG. 21 is a block diagram illustrating an exemplary system architecture for a distributed, composite symbolic and non-symbolic AI platform for advanced reasoning, according to an embodiment.

[0047] FIG. 22 is a block diagram illustrating an exemplary model architecture of the Transformer, consisting of an Encoder and a Decoder.

[0048] FIG. 23 is a block diagram illustrating an exemplary basic embedding layer generation process, according to an embodiment.

[0049] FIG. 24 is a flow diagram illustrating an exemplary method for routing processing based on certainty threshold and/or challenge-based verification, according to an embodiment.

[0050] FIG. 25 is a flow diagram illustrating an exemplary method for retrieving relevant contextual data from a knowledge graph database and enriching vector embeddings with the contextual data, according to an embodiment.

[0051] FIG. 26 is a flow diagram illustrating an exemplary method for applying expressive weighting schemes to model combinations, according to an embodiment.

[0052] FIG. 27 is a flow diagram illustrating an exemplary method for using feedback loops considering security, licensing, provenance, and collaborative development, according to an embodiment.

[0053] FIG. 28 is a flow diagram illustrating an exemplary method for multi-modal alignment for consistent representations across data types, according to an embodiment.

[0054] FIG. 29 is a flow diagram illustrating an exemplary method for hyperparameter using information-theoretic guidance, according to an embodiment.

[0055] FIG. 30 is a flow diagram illustrating an exemplary method for linking embeddings to knowledge graphs, according to an embodiment.

[0056] FIG. 31 is a flow diagram illustrating an exemplary method for advanced reasoning using a composite artificial intelligence platform, according to an embodiment.

[0057] FIG. 32 illustrates an exemplary computing environment on which an embodiment described herein may be implemented.

#### DETAILED DESCRIPTION OF THE INVENTION

[0058] The inventor has conceived, and reduced to practice, a system and method for flexibly incorporating machine learning models into applications using a marketplace platform and distributed computational graph (DCG) architecture. The DCG enables dynamic selection, creation and incorporation of trained models with diverse data sources and marketplaces for data, algorithms, and expert judgment. Multiple models can be used in series or parallel. An expert judgment marketplace allows human and artificial intelligence (AI) experts to score the accuracy of training data and model outputs. Consumers can select and rank experts based on the helpfulness of their judgments. A retrieval augmented generation (RAG) marketplace enables selling access to proprietary datasets as RAGs. The system includes model and RAG marketplaces with domain-specific components and user experience customization.

[0059] The integration of expert judgment, ML/AI models, datasets, RAGs, and model weightings in a unified marketplace creates a vibrant ecosystem where expertise, innovation, and collaboration thrive. Experts contribute their knowledge and insights to evaluate and improve the quality of ML/AI goods, while providers benefit from expert feedback and exposure to a diverse consumer base. Consumers confidently can access a wide range of high-quality ML/AI offerings, supported by expert judgments and ratings, to accelerate their projects and achieve better results.

[0060] One or more different aspects may be described in the present application. Further, for one or more of the aspects described herein, numerous alternative arrangements may be described; it should be appreciated that these are presented for illustrative purposes only and are not limiting of the aspects contained herein or the claims presented herein in any way. One or more of the arrangements may be widely applicable to numerous aspects, as may be readily apparent from the disclosure. In general, arrangements are described in sufficient detail to enable those skilled in the art to practice one or more of the aspects, and it should be appreciated that other arrangements may be utilized and that structural, logical, software, electrical and other changes may be made without departing from the scope of the particular aspects. Particular features of one or more of the aspects described herein may be described with reference to one or more particular aspects or figures that form a part of the present disclosure, and in which are shown, by way of illustration, specific arrangements of one or more of the aspects. It should be appreciated, however, that such features are not limited to usage in the one or more particular aspects or figures with reference to which they are described. The present disclosure is neither a literal description of all arrangements of one or more of the aspects nor a listing of features of one or more of the aspects that must be present in all arrangements.

[0061] Headings of sections provided in this patent application and the title of this patent application are for convenience only, and are not to be taken as limiting the disclosure in any way.

[0062] Devices that are in communication with each other need not be in continuous communication with each other, unless expressly specified otherwise. In addition, devices that are in communication with each other may communicate directly or indirectly through one or more communication means or intermediaries, logical or physical.

[0063] A description of an aspect with several components in communication with each other does not imply that all such components are required. To the contrary, a variety of optional components may be described to illustrate a wide variety of possible aspects and in order to more fully illustrate one or more aspects. Similarly, although process steps, method steps, algorithms or the like may be described in a sequential order, such processes, methods and algorithms may generally be configured to work in alternate orders, unless specifically stated to the contrary. In other words, any sequence or order of steps that may be described in this patent application does not, in and of itself, indicate a requirement that the steps be performed in that order. The steps of described processes may be performed in any order practical. Further, some steps may be performed simultaneously despite being described or implied as occurring non-simultaneously (e.g., because one step is described after the other step). Moreover, the illustration of a process by its depiction in a drawing does not imply that the illustrated process is exclusive of other variations and modifications thereto, does not imply that the illustrated process or any of its steps are necessary to one or more of the aspects, and does not imply that the illustrated process is preferred. Also, steps are generally described once per aspect, but this does not mean they must occur once, or that they may only occur once each time a process, method, or algorithm is carried out or executed. Some steps may be omitted in some aspects or some occurrences, or some steps may be executed more than once in a given aspect or occurrence.

[0064] When a single device or article is described herein, it will be readily apparent that more than one device or article may be used in place of a single device or article. Similarly, where more than one device or article is described herein, it will be readily apparent that a single device or article may be used in place of the more than one device or article.

[0065] The functionality or the features of a device may be alternatively embodied by one or more other devices that are not explicitly described as having such functionality or features. Thus, other aspects need not include the device itself.

[0066] Techniques and mechanisms described or referenced herein will sometimes be described in singular form for clarity. However, it should be appreciated that particular aspects may include multiple iterations of a technique or multiple instantiations of a mechanism unless noted otherwise. Process descriptions or blocks in figures should be understood as representing modules, segments, or portions of code which include one or more executable instructions for implementing specific logical functions or steps in the process. Alternate implementations are included within the scope of various aspects in which, for example, functions may be executed out of order from that shown or discussed, including substantially concurrently or in reverse order,

depending on the functionality involved, as would be understood by those having ordinary skill in the art.

#### Definitions

[0067] As used herein, “explainability” (also referred to as “interpretability”) is the concept that a machine learning model and its output can be explained in a way that “makes sense” to a human being at an acceptable level.

[0068] As used herein, “graph” is a representation of information and relationships, where each primary unit of information makes up a “node” or “vertex” of the graph and the relationship between two nodes makes up an edge of the graph. Nodes can be further qualified by the connection of one or more descriptors or “properties” to that node. For example, given the node “James R,” name information for a person, qualifying properties might be “183 cm tall,” “DOB Aug. 13, 1965” and “speaks English”. Similar to the use of properties to further describe the information in a node, a relationship between two nodes that forms an edge can be qualified using a “label”. Thus, given a second node “Thomas G,” an edge between “James R” and “Thomas G” that indicates that the two people know each other might be labeled “knows.” When graph theory notation (Graph= (Vertices, Edges)) is applied this situation, the set of nodes are used as one parameter of the ordered pair, V and the set of 2 element edge endpoints are used as the second parameter of the ordered pair, E. When the order of the edge endpoints within the pairs of E is not significant, for example, the edge James R, Thomas G is equivalent to Thomas G, James R, the graph is designated as “undirected.” Under circumstances when a relationship flows from one node to another in one direction, for example James R is “taller” than Thomas G, the order of the endpoints is significant. Graphs with such edges are designated as “directed.” In the distributed computational graph system, transformations within transformation pipeline are represented as directed graph with each transformation comprising a node and the output messages between transformations comprising edges. Distributed computational graph stipulates the potential use of non-linear transformation pipelines which are programmatically linearized. Such linearization can result in exponential growth of resource consumption. The most sensible approach to overcome possibility is to introduce new transformation pipelines just as they are needed, creating only those that are ready to compute. Such method results in transformation graphs which are highly variable in size and node, edge composition as the system processes data streams. Those familiar with the art will realize that transformation graph may assume many shapes and sizes with a vast topography of edge relationships and node types and subgraphs, which may be optionally stored, represented, or acted upon. It is also important to note that the resource topologies available at a given execution time for a given pipeline may be highly dynamic due to changes in available node or edge types or topologies (e.g. different servers, data centers, devices, network links, etc.) being available, and this is even more so when legal, regulatory, privacy and security considerations are included in a DCG pipeline specification or recipe in the DSL. Since the system can have a range of parameters (e.g. authorized to do transformation x at compute locations of a, b, or c) the JIT, JIC, JIP elements can leverage system state information (about both the processing system and the observed system of interest) and planning or modeling modules to compute at

least one parameter set (e.g. execution of pipeline may say based on current conditions use compute location b) at execution time. This may also be done at the highest level or delegated to lower level resources when considering the spectrum from centralized cloud clusters (i.e. higher) to extreme edge (e.g. a wearable, or phone or laptop). The examples given were chosen for illustrative purposes only and represent a small number of the simplest of possibilities. These examples should not be taken to define the possible graphs expected as part of operation of the invention

[0069] As used herein, “transformation” is a function performed on zero or more streams of input data which results in a single stream of output which may or may not then be used as input for another transformation. Transformations may comprise any combination of machine, human or machine-human interactions. Transformations need not change data that enters them, one example of this type of transformation would be a storage transformation which would receive input and then act as a queue for that data for subsequent transformations. As implied above, a specific transformation may generate output data in the absence of input data. A time stamp serves as an example. In the invention, transformations are placed into pipelines such that the output of one transformation may serve as an input for another. These pipelines can consist of two or more transformations with the number of transformations limited only by the resources of the system. Historically, transformation pipelines have been linear with each transformation in the pipeline receiving input from one antecedent and providing output to one subsequent with no branching or iteration. Other pipeline configurations are possible. The invention is designed to permit several of these configurations including, but not limited to: linear, afferent branch, efferent branch and cyclical.

[0070] A “pipeline,” as used herein and interchangeably referred to as a “data pipeline” or a “processing pipeline,” refers to a set of data streaming activities and batch activities. Streaming and batch activities can be connected indiscriminately within a pipeline and compute, transport or storage (including temporary in-memory persistence such as Kafka topics) may be optionally inferred/suggested by the system or may be expressly defined in the pipeline domain specific language. Events will flow through the streaming activity actors in a reactive way. At the junction of a streaming activity to batch activity, there will exist a Stream-BatchProtocol data object. This object is responsible for determining when and if the batch process is run. One or more of three possibilities can be used for processing triggers: regular timing interval, every N events, a certain data size or chunk, or optionally an internal (e.g. APM or trace or resource based trigger) or external trigger (e.g. from another user, pipeline, or exogenous service). The events are held in a queue (e.g. Kafka) or similar until processing. Each batch activity may contain a “source” data context (this may be a streaming context if the upstream activities are streaming), and a “destination” data context (which is passed to the next activity). Streaming activities may sometimes have an optional “destination” streaming data context (optional meaning: caching/persistence of events vs. ephemeral). System also contains a database containing all data pipelines as templates, recipes, or as run at execution time to enable post-hoc reconstruction or re-evaluation with a modified topology of the resources (e.g. compute, transport or storage), transformations, or data involved.

### Conceptual Architecture

**[0071]** FIG. 1A is a block diagram illustrating an exemplary system architecture of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces, according to an embodiment. According to the embodiment, platform **160** is configured as a cloud-based computing platform comprising various system or sub-system components configured to provide functionality for flexibly incorporating machine learning models into applications using a distributed computational graph (DCG) architecture. The DCG enables dynamic selection, creation and incorporation of trained models with data sources and marketplaces for data, algorithms, and expert judgment. Exemplary platform systems can include a distributed computational graph (DCG) computing system **121**, a marketplace computing system **162**, a transaction computing system **161**, and a data contract computing system **164**. Platform **160** may integrate with a plurality of marketplaces **170a-n**. In some embodiments, systems **121**, **161-164** may each be implemented as standalone software applications or as a services/microservices architecture which can be deployed (via platform **160**) to perform a specific task or functionality. In such an arrangement, services can communicate with each other over an appropriate network using lightweight protocols such as HTTP, gRPC, or message queues. This allows for asynchronous and decoupled communication between services. Services may be scaled independently based on demand, which allows for better resource utilization and improved performance. Services may be deployed using containerization technologies such as Docker and orchestrated using container orchestration platforms like Kubernetes. This allows for easier deployment and management of services.

**[0072]** According to the embodiment, platform **160** comprises one or more databases **163** configured to store a plurality of data. One or more databases **163** may store a plurality of marketplace data associated with a plurality of marketplace goods such as, for example, datasets, models, retrieval augmented generation (RAG) datasets, model weightings, expert judgment scores, and various tools and resources for developing machine learning and/or artificial intelligence (ML/AI) systems. One or more databases **163** may be configured as secure databases for securely storing user information such as personal identifying information, financial information, and/or authentication/authorization details.

**[0073]** According to the embodiment, a platform user **175** may refer to a seller, a consumer, an expert, or an organization/enterprise. An enterprise may wish to incorporate a trained ML model into their business processes. An enterprise may comprise a plurality of enterprise endpoints which can include, but are not limited to, mobile devices, workstations, laptops, personal computers, servers, switches, routers, industrial equipment, gateways, smart wearables, Internet-of-Things (IoT) devices, sensors, and/or the like. An enterprise may engage with platform **160** to create a trained model to integrate with its business processes via one or more enterprise endpoints.

**[0074]** A consumer user may engage with the platform to browse the various marketplaces to find the tools, datasets, models, etc. which they can purchase or license to suit their needs. As a consumer on the marketplace platform, a user can engage with the platform through various touchpoints and features designed to facilitate discovery, evaluation, and

utilization of the available goods and services. For example, the consumer creates an account on the marketplace platform by providing necessary information such as name, email address, and relevant background details. The user profile serves as a central hub for managing preferences, saved searches, and transaction history. The consumer uses the platform's search functionality to explore the available goods and services based on their needs and preferences. The search interface may allow users to filter and refine results based on criteria such as data type, domain, model architecture, expert ratings, licensing, model energy consumption and efficiency related to training, retraining, and inference costs (e.g. mean, median, min, max, moving average), or pricing, and various model constraints such as memory or processor requirements, or estimated execution complexity and run-time on known hardware or hardware combinations. In one embodiment, the marketplace supports filtering and recommendation of different assets for use in various AI endeavors in cloud, edge, device, federated and transfer-learning enabled systems. Since interactions between different techniques on different devices working in concert (e.g., for health data and recommendations or for Internet browsing/ecommerce and search) it is possible for the system to receive and store different architectures or flow depictions of use cases for consideration or recommendations for off the shelf marketplace artifacts which might be leveraged for a given desired user application, including with optional consideration of regulatory, privacy or compliance requirements associated with the depicted data flows and types. In some implementations, platform **160** may employ recommendation algorithms to suggest relevant goods or services based on the user's profile, search history, and preferences. The consumer can access detailed information about each marketplace offering, including descriptions, specifications, documentation, and performance metrics. When a consumer decides to acquire a specific marketplace offering, they can proceed with the purchase or licensing process through the platform's secure transaction system. The platform handles payment processing, license generation, and delivery of the acquired goods or services to the user's account. For acquired ML/AI models, datasets, or tools, the platform may provide integration guidelines, API documentation, or software development kits (SDKs) to facilitate seamless integration into the user's existing workflows or systems. In some embodiments, platform **160** may offer cloud-based environments or containerization options for users to deploy and utilize the acquired assets directly within the platform's infrastructure.

**[0075]** As a seller of marketplace goods on the platform, a user would engage with the platform through various features and workflows designed to facilitate the listing, promotion, and sale of their offerings. The seller creates a dedicated seller account on the marketplace platform by providing necessary information such as name, contact details, and business credentials. The seller profile serves as a central hub for managing listings, tracking sales, and communicating with potential buyers. The profile may include options for showcasing the seller's expertise, portfolio, or unique value proposition to establish credibility and attract buyers. The seller uses the platform's listing creation tools to add their goods or services to the marketplace. The listing process may involve providing detailed information about the offering, such as title, description, specifications, pricing, and any relevant documentation or supporting mate-

rials. The platform may offer templates, guidelines, or best practices to assist sellers in creating compelling and informative listings that effectively showcase their offerings. The seller determines the pricing model and licensing options for their listings, considering factors such as market demand, competition, and the unique value of their offerings. The platform may support various pricing models, such as one-time purchases, subscription-based access, or consumption or usage-based pricing, to cater to different buyer preferences and needs. Service level agreements for reliability, uptime, data quality, and other metrics may also be specified and have economic penalties or benefits tied to target thresholds or ranges or models/calculations (e.g. exponentially weighted moving average over time). The seller can define the licensing terms and conditions, specifying the rights, limitations, and usage guidelines associated with their offerings. The platform can provide sellers with tools and features to promote their listings and reach potential buyers effectively. Sellers can optimize their listing titles, descriptions, and keywords to improve search visibility and discoverability within the marketplace. In some implementations, platform 160 may offer promotional opportunities, such as featured listings, sponsored ads, or email marketing campaigns, to help sellers showcase their offerings to targeted audiences.

[0076] According to some embodiments, platform 160 facilitates communication between sellers and potential buyers through various channels, such as messaging systems, chat interfaces, or dedicated support ticketing. Sellers can respond to buyer inquiries, provide additional information, or negotiate terms and conditions directly through the platform's communication tools. When a buyer places an order for a seller's offering, the platform notifies the seller and initiates the order processing workflow. The seller receives the order details, including buyer information, purchased items, and any specific requirements or instructions. The platform handles the payment processing and revenue distribution for completed transactions. The seller receives payment for their sold offerings, minus any applicable platform fees or commissions, through the platform's secure payment gateway. According to an embodiment, platform 160 provides sellers with tools to track their sales, revenue, and payment history, enabling them to manage their financial aspects effectively.

[0077] According to an aspect, the platform allows buyers to provide feedback, ratings, and reviews for the offerings they have purchased from sellers. Sellers can monitor and respond to feedback, addressing any concerns or issues raised by buyers promptly and professionally. Building a positive reputation through consistent quality, timely delivery, and excellent customer service is important for sellers to attract more buyers and establish trust within the marketplace community.

[0078] According to an aspect, the platform provides sellers with analytics and insights related to their listings, sales performance, and buyer behavior. Sellers can access data-driven reports and dashboards to gain valuable insights into popular offerings, buyer preferences, and market trends. These insights help sellers make informed decisions, optimize their listings, and adapt their strategies to maximize sales and profitability.

[0079] According to an embodiment, platform 160 may provide one or more application programming interfaces

(APIs) for programmatic access and integration of the marketplace functionalities into external applications and systems.

[0080] According to the embodiment, transaction computing system 161 is configured to facilitate secure financial transactions and data transfers within the platform's marketplaces 170a-n. This may be accomplished using various components that work together to create a secure and trustworthy marketplace environment. For more detailed information about the operation of the transaction computing system, please refer to FIG. 1B.

[0081] According to the embodiment, marketplace computing system 162 is configured to enable sellers to upload marketplace goods to the platform and for consumers to browse marketplace listings. Marketplace computing system 162 also provides functionality for registering platform users 175. For more detailed information about the operation of marketplace computing system 162, please refer to FIG. 1C.

[0082] According to the embodiment, data contract computing system 164 is configured to integrate data contracts to ensure data quality, consistency, and usability across the platform 160. Data contract computing system 164 may provide decentralized data contract management. The marketplace system can provide tools and interfaces for data providers to define and manage their data contracts in a decentralized manner. For example, each data provider may have the ability to create, update, and version their data contracts independently, without relying on a centralized authority or bottleneck. The system 164 can facilitate collaboration and coordination among data providers to ensure consistency and compatibility of data contracts across different domains and use cases.

[0083] Data contract computing system 164 may provide producer-side contract enforcement wherein the marketplace system can provide mechanisms for data producers to enforce their data contracts at the source of data generation or ingestion. This can be achieved through automated data validation, quality checks, and conformance testing at the producer level. In some implementations, the system can offer tools and libraries that enable producers to integrate contract enforcement into their existing data pipelines and workflows. Producers may be able to define and apply data quality rules, constraints, and transformations to ensure that the data adheres to the specified contracts before it is made available to consumers.

[0084] According to an embodiment, the marketplace system maintains a centralized repository or registry of data contracts that is accessible to all authenticated and authorized users and services. Data contracts may be versioned and stored in a structured format (e.g., JSON, YAML) that can be easily parsed and consumed by different applications and services. The system can provide application programming interfaces (APIs) and interfaces for users and services to retrieve and query data contracts, including the ability to access specific versions of a contract. In some implementations, changes to data contracts may be managed through a robust versioning and change management process, ensuring backward compatibility and minimizing disruptions to downstream consumers.

[0085] According to an embodiment, the marketplace system can enforce that data contracts cover both the schema and semantics of the data. Data contracts can include detailed descriptions of entities, attributes, relationships, and constraints, going beyond just the structural aspects of the

data. The system **164** provides guidelines and best practices for defining comprehensive data contracts, including the use of standardized vocabularies, ontologies, and metadata frameworks. Tools and utilities may be available to help data providers create and validate data contracts that meet these requirements.

[**0086**] In some implementations, the marketplace system provides developer-friendly tools and APIs for defining, implementing, and testing data contracts. Data contract definition and enforcement should be seamlessly integrated into the existing development workflows and CI/CD pipelines used by data providers. For example, the system **164** can offer libraries, SDKs, and plugins that enable developers to incorporate data contract validation and testing into their preferred development environments and frameworks. Automated data contract validation and testing may be triggered as part of the data ingestion or publishing process, ensuring that only conformant data is made available to consumers.

[**0087**] According to an embodiment, the data contract computing system **164** can provide a sandbox environment for exploration, prototyping, and iterative development and testing. The marketplace system can provide a sandbox environment that allows data scientists to access raw, non-contract production data in a limited capacity. This sandbox environment is separate from the production environment and designed specifically for exploration, experimentation, and prototyping purposes. Data scientists may have the ability to freely explore and analyze the raw data within the sandbox, without the constraints of data contracts, to identify patterns, test hypotheses, and develop new models or algorithms. The sandbox environment should have appropriate safeguards and limitations in place to prevent any accidental or unauthorized changes to the production data or systems. The marketplace system supports an iterative development and testing process for data scientists. After exploring and prototyping in the sandbox environment, data scientists should be able to create and refine data contracts based on their findings and requirements. The system can provide tools and workflows for data scientists to collaborate with data providers and stakeholders to define and agree upon the necessary schemas, semantics, and constraints for the data contracts. Once the data contracts are defined, data scientists are able to test and validate their prototypes and models against the contracted data in a controlled testing environment.

[**0088**] When data scientists are ready to deploy their prototypes or models into production, the marketplace system can enforce the use of data contracts. The system can prevent the direct deployment of unsupported schemas or semantics into the production environment, ensuring that only data that adheres to the defined contracts is allowed. The deployment process may include automated validation and testing against the data contracts, flagging any discrepancies or violations for further review and resolution. By enforcing the use of data contracts in the production environment, the marketplace system helps maintain data consistency, reliability, and compatibility across different services and applications.

[**0089**] The combination of the sandbox environment for exploration and the enforced use of data contracts in production can have a positive impact on iteration speed for data scientists. By providing a dedicated space for experimentation and prototyping, data scientists can quickly

explore new ideas and approaches without the overhead of immediate contract compliance. Once the prototypes are validated and refined, the use of data contracts ensures that the deployed models and services are built on a solid foundation of well-defined and agreed-upon data structures and semantics. This approach reduces the accumulation of technical debt and tribal knowledge within the organization, as the data contracts serve as a clear and standardized reference for all data-related interactions. The reduced technical debt and improved data consistency ultimately contribute to faster iteration cycles and more efficient development processes in the long run.

[**0090**] FIG. 1B is a block diagram illustrating an exemplary aspect of a platform for integration of machine learning models and artificial intelligence utilizing marketplaces, a transaction computing system **180**.

[**0091**] According to an embodiment, a secure payment gateway subsystem **181** is present and configured to integrate with the marketplace backend using application programming interfaces (APIs) provided by a payment gateway provider (e.g., Stripe, PayPal, etc.) When a buyer initiates a payment, the marketplace backend securely communicates with the payment gateway **181** to process the transaction. The payment gateway encrypts sensitive payment information (e.g., credit card details) and handles the secure communication with payment networks for authorization and settlement. For example, when a buyer purchases a dataset from the marketplace, the marketplace backend sends a payment request to the secure payment gateway, including the transaction amount and buyer's payment details. The payment gateway encrypts the payment information and communicates with the payment network to authorize the transaction. Upon successful authorization, the payment gateway notifies the marketplace backend, and the transaction is recorded.

[**0092**] According to an embodiment, an escrow subsystem **182** is present and configured to hold funds temporarily until the successful delivery of marketplace goods (e.g., RAGs, datasets, models, weightings, outputs, etc.). When a buyer makes a purchase, the funds may be transferred to the escrow system instead of directly to the seller. The escrow system communicates with the marketplace backend to receive the transaction details and release the funds to the seller once the delivery is confirmed. The escrow system ensures trust between buyers and sellers and mitigates risks associated with fraudulent transactions. For example, after a buyer purchases a machine learning model, the funds are transferred to the escrow system. The seller then delivers the model to the buyer through a secure data transfer protocol. Once the buyer confirms the receipt and integrity of the model, the escrow system releases the funds to the seller, completing the transaction.

[**0093**] According to an embodiment, a smart contract subsystem **183** is present and configured to use smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. They are deployed on a blockchain platform (e.g., Ethereum) and automatically enforce the execution of transactions based on predefined conditions. Smart contracts ensure transparency, immutability, and automation of marketplace transactions. Smart contracts can handle complex logic, such as royalty distributions and usage-based payments. For example, a smart contract is deployed for a specific RAG in the marketplace. The smart contract defines the terms of usage,

pricing, and royalty distribution. When a buyer purchases access to the RAG, the smart contract automatically executes the payment, grants access to the buyer, and distributes royalties to the RAG creator based on the pre-defined terms.

[0094] According to an embodiment, transaction computing system 180 utilizes secure data transfer protocols 184 to ensure the secure exchange of marketplace goods (e.g., datasets, models, etc.) between sellers and buyers. It may utilize encryption techniques (e.g., Secure Sockets Layer/Transport Layer Security) to protect data in transit and authenticates the parties involved in the transfer. The protocols can be implemented using secure file transfer methods (e.g., Secure File Transfer Protocol, Hypertext Transfer Protocol Secure, etc.) or through secure APIs that facilitate the exchange of data. For example, when a buyer purchases a dataset, the secure data transfer protocol is initiated. The seller's dataset is encrypted and transferred to the buyer through a secure channel. The buyer's identity is authenticated, and the integrity of the dataset is verified. Once the transfer is complete, the buyer can decrypt and access the dataset.

[0095] According to an embodiment, a data encryption and access control subsystem 185 is present and configured to ensure the confidentiality of sensitive data stored in the platform's databases 163. Encryption algorithms (e.g., Advanced Encryption Standard) may be used to encrypt data at rest. Access control mechanisms (e.g., role-based access control) are implemented to restrict access to sensitive data based on user roles and permissions. Only authorized users can decrypt and access the data they are permitted to view. For example, when a seller uploads a proprietary dataset to the marketplace, the dataset is encrypted before being stored in the database. The encryption key is securely managed and accessible only to authorized system components. When a buyer purchases access to the dataset, the access control subsystem 185 verifies the buyer's permissions and grants decryption access to the authorized buyer.

[0096] These components work together to create a secure and trustworthy marketplace environment. The secure payment gateway and escrow system handle financial transactions, ensuring secure payment processing and holding funds until successful delivery. Smart contracts automate the execution of transactions and enforce the terms of agreements. The secure data transfer protocol and data encryption protect the confidentiality and integrity of marketplace goods during transfer and storage. Access control mechanisms ensure that only authorized users can access sensitive data.

[0097] FIG. 1C is a block diagram illustrating an exemplary aspect of an embodiment of marketplace platform 160, a marketplace computing system 190. According to the embodiment, marketplace computing system 190 enables sellers to upload marketplace goods to the platform.

[0098] According to the embodiment, a seller dashboard 191 subsystem component is present and configured as a user interface that provides sellers with a centralized location to manage their marketplace listings, including new goods. According to the aspect, seller dashboard 191 may implement authentication and authorization mechanisms to ensure only registered sellers can access the dashboard. The seller dashboard can provide an overview of existing listing and their status as well as options to create new listings and upload associated marketplace goods. The dashboard can

provide management features for editing, updating, and/or removing listings. The seller dashboard may be implemented as a web-based user interface using web technologies such as HTML, CSS, and JavaScript frameworks (e.g., React, Angular). It communicates with the backend server through APIs (e.g., RESTful APIs) to fetch and update seller-specific data. Authentication and authorization can be implemented using mechanisms like JSON Web Tokens (JWT) or session-based authentication to ensure secure access to the dashboard. As an example, a seller logs into their account and navigates to the seller dashboard. The dashboard displays an overview of the seller's existing listings, retrieved from the backend server via API calls. The seller clicks on a "Create New Listing" button, which opens the upload interface for adding a new marketplace goods.

[0099] According to an aspect, seller dashboard 191 can be extended to include functionality for registering sellers and/or experts (human or artificial intelligence), such as expert judgment sellers. In such aspects, the dashboard can include a registration form for sellers/experts to create an account on the platform 160. The form collects necessary information such as name, email address, password, and any additional profile details specific to the sellers or experts. For example, information related to the area of expertise for an expert may be collected during registration. Form validation may be implemented using JavaScript on the client-side and server-side validation to ensure data integrity and prevent invalid or malicious submissions. For example, a prospective seller navigates to the registration page within the seller dashboard and fills out a registration form, providing their name, email address, password, and any required profile information. The form validates the input fields, ensuring that all required fields are filled and the provided data meets the specified format and constraints.

[0100] Upon successful registration, the seller's credentials are securely stored in the platform's authentication system 163 (e.g., database). Password hashing techniques (e.g., bcrypt) may be used to store passwords securely, preventing unauthorized access to user accounts. Authentication mechanisms (e.g., JWT, session-based authentication, etc.) can be implemented to verify the identity of sellers and experts when they log into platform 160. To ensure the validity of registered email addresses, an email verification process may be implemented. For example, after registration, an automated email is sent to the provided email address, containing a unique verification link. The seller must click on the verification link to confirm their email address and activate their account. After registration and email verification, sellers and experts are prompted to set up their profile on platform 160. The profile setup process may include providing additional information, such as expertise areas, qualifications, or portfolio. The platform may implement a verification process to validate the authenticity and credibility of sellers and experts. Verification can involve manual review by platform administrators or automated checks against external databases or certifications. Once registered and verified, sellers and experts are granted appropriate access and permissions within the seller dashboard 191. Role-based access control (RBAC) may be implemented to assign specific roles (e.g., seller, expert) and corresponding permissions to each user. The access control system ensures that sellers and experts can only access and perform actions relevant to their role and permissions. For example, after registration and verification, a seller is

assigned the “Seller” role, granting them access to features such as listing management, order tracking, and payment information. An expert judgment seller/contributor is assigned the “Expert” role, which may include additional permissions to provide expert opinions, review submissions, or participate in expert marketplaces.

[0101] According to an embodiment, the registration process for an AI expert in the marketplace platform may comprise various steps to ensure the credibility, transparency, and reliability of the AI system. According to an aspect, an AI developer or organization creates a profile for the AI expert on the marketplace platform. The profile may include information such as the AI system’s name, developer details, intended domain or specialization, and a brief description of its capabilities. The profile should clearly indicate that the expert is an AI system to provide transparency. The AI developer can provide detailed documentation about the AI expert, including its architecture, training data, algorithms, and performance metrics. The documentation may cover the AI system’s intended use cases, limitations, and any potential biases or constraints. Information about the AI system’s development process, testing procedures, and validation techniques should be included to establish trust and credibility. The AI expert may undergo rigorous performance evaluation and benchmarking to assess its accuracy, reliability, and effectiveness in its claimed domain or specialization. The marketplace platform may provide standardized evaluation datasets or collaborate with third-party testing organizations to conduct impartial assessments. The AI expert’s performance metrics, such as accuracy scores, precision, recall, or domain-specific measures, can be recorded and made available to users.

[0102] The AI expert’s ability to provide explainable and interpretable insights may be evaluated. Such an assessment can verify whether the AI system can generate clear and understandable explanations for its evaluations, recommendations, or decisions. For example, the marketplace platform may establish guidelines or standards for explainability to ensure consistency and transparency across registered AI experts. According to an aspect, the AI expert undergoes security and privacy assessments to ensure the protection of user data and the integrity of the system. The assessment verifies the implementation of appropriate security measures, such as data encryption, access controls, and secure communication protocols. Compliance with relevant data protection regulations and privacy standards can be evaluated and documented.

[0103] Upon successful completion of the registration process and meeting all the required criteria, the AI expert may be approved and listed on the marketplace platform. The AI expert’s profile, documentation, and performance metrics are made available to users, enabling them to make informed decisions about engaging with the AI expert.

[0104] According to the embodiment, an upload interface 192 subsystem component is present and may be implemented as a web form or drag-and-drop component using HTML, CSS, and JavaScript. It allows sellers to select files from their local machine or provide a Uniform Resource Locator (URL) for remote files. Upload interface 192 can be configured to support various file formats and data types specific to the marketplace goods (e.g., CSV, JSON, model files, etc.). The selected files may be sent to a backend server via HTTP requests (e.g., POST requests) for processing and storage. In some aspects, progress indicators and error

handling are implemented using JavaScript to provide real-time feedback to the seller during the upload process. As an example of upload interface operation, a seller selects the dataset file (e.g., CSV) from their local machine using the upload interface. The selected file is sent to the backend server via an HTTP POST request. The upload interface displays a progress bar indicating the upload progress and handles any errors that may occur during the upload process.

[0105] According to the embodiment, marketplace computing system 190 utilizes a data validation and preprocessing subsystem 193 configured to ensure that uploaded marketplace goods meet any required format, structure, and quality standards. Data validation and preprocessing subsystem 192 may utilize automated validation scripts to check the structure and format of uploaded files. Data quality checks may identify missing values, inconsistencies, or anomalies in the uploaded data. Preprocessing tasks can include actions such as data cleaning, normalization, or transformation to ensure compatibility with the platform’s standards. The subsystem may implement a feedback mechanism to inform sellers about any validation errors or required modifications.

[0106] Data validation and preprocessing tasks may be implemented on the backend server using programming languages such as Python or Java. The uploaded files may be processed using data validation libraries or custom scripts to check for format and structure consistency. As an example, an uploaded dataset file is received by the backend server and undergoes data validation checks. The server uses a data validation library (e.g., pandas in Python) to check for missing values, inconsistent data types, and/or invalid formats. If any validation errors are detected, the server sends feedback to the seller through upload interface 192, prompting them to rectify the issues.

[0107] According to the embodiment, marketplace computing system 190 utilizes secure storage systems 194 to ensure safe and encrypted storage of uploaded marketplace goods on the platform’s servers. Examples of secure storage systems which may be implemented include but are not limited to Amazon S3, Google Cloud Storage, and/or the like. One or more encryption mechanisms (e.g., AES) may be used to encrypt the uploaded data at rest. In some embodiments, marketplace computing system 190 may implement access control policies to restrict access to stored files based on seller permissions and/or marketplace rules. Furthermore, the system may leverage backup and disaster recovery mechanisms to ensure data durability and availability. For example, after successful validation and preprocessing, the uploaded dataset file is encrypted using AES-256 encryption. The encrypted file is then stored in a secure storage bucket, with access restricted to authorized users and systems. Regular backups of the stored files are taken to ensure data durability in case of any incidents.

[0108] According to the embodiment, a metadata management subsystem 195 is present and configured to capture and store relevant information about the uploaded marketplace goods. This may comprise a database 163 or metadata storage system to store information such as, for example, file name, format, size, upload timestamp, and seller details. For example, metadata management may be implemented using a database system (e.g., MySQL, MongoDB) to store information about the uploaded files. A metadata schema may be defined to capture relevant attributes such as file name, format, size, upload timestamp, and seller details. In some

implementations, APIs or query interface can be provided to retrieve and manage metadata associated with the uploaded files. As an example of metadata operation, a dataset file is uploaded, the relevant metadata (e.g., file name, format, size, etc.) is extracted and stored in the metadata database. The metadata is associated with the corresponding marketplace listing using unique identifiers. When a buyer views a marketplace listing, the metadata is retrieved from the database and displayed alongside the listing details.

[0109] According to the embodiment, a marketplace listing integration subsystem **196** is present and configured to connect the uploaded marketplace goods with the corresponding listings on the platform. Marketplace listing integration system **196** may utilize automated processes to associate uploaded files with the respective marketplace listing based on seller inputs or predefined rules. Furthermore, system **196** can implement synchronization mechanisms to update the marketplace listing with the latest uploaded versions of the goods. Marketplace listing integration **196** can be configured to display relevant information about the uploaded goods (e.g., file size, format, etc.) on the marketplace listing pages. As an example, after a seller uploads a dataset file and completes the listing creation process, the backend server associates the uploaded file with the newly created listing in the database. When a buyer views the marketplace listing, the server retrieves the associated uploaded file from the secure storage and displays the relevant information (e.g., file size, format, etc.) on the listing page. If the seller updates the uploaded file for an existing listing, the synchronization mechanism ensures that the marketplace listing reflects the latest version of the file.

[0110] These subsystem components work together to provide a seamless and secure upload experience for sellers. The seller dashboard serves as the entry point, allowing sellers to manage their listings and initiate the upload process. The upload interface facilitates the selection and transmission of files to the backend server. Data validation and preprocessing ensure the quality and compatibility of uploaded files. Secure storage and encryption protect the uploaded data, while metadata management captures relevant information. Finally, marketplace listing integration connects the uploaded files with the corresponding listings, ensuring synchronization and up-to-date information for buyers.

[0111] According to an embodiment, the platform can provide functionality directed to an important aspect of the AI training landscape: the use of potentially unlicensed or copyrighted material from shadow libraries and other sources. The platform can incorporate the ability of the marketplace to register data/content that wasn't bought, while also addressing the legal and ethical considerations surrounding the use of such data. For example, the marketplace can allow users to register data/content that they have obtained from various sources, including those that may not have been purchased through the marketplace itself. Users may provide detailed information about the source, origin, and licensing status of the registered data, including any applicable copyrights, licenses, or terms of use. According to an aspect, the marketplace can implement a verification process to ensure that the registered data complies with legal and ethical standards, and that the user has the necessary rights or permissions to use and share the data. The marketplace may maintain a comprehensive record of the provenance and lineage of registered data, including the original

sources, any transformations or modifications applied, and the users who have accessed or used the data. This information can be made transparently available to all users of the marketplace, allowing them to make informed decisions about the data they use and the potential legal and ethical implications. The marketplace may also provide clear guidelines and educational resources to help users understand the importance of data provenance, licensing, and ethical considerations in AI training. In some implementations, the marketplace can establish clear policies and procedures to ensure compliance with relevant laws, regulations, and ethical standards related to data use and intellectual property rights. This may comprise implementing automated checks and filters to identify and flag potentially infringing or unlicensed data, as well as manual review processes to assess the legality and appropriateness of registered data. The marketplace may also provide mechanisms for rights holders to report and request the removal of infringing data, and for users to seek proper licensing or permission for the use of copyrighted material. The marketplace can provide guidance and resources on the principles of fair use and transformative use in the context of AI training and development. This may include information on factors such as the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use upon the potential market for or value of the copyrighted work. The marketplace may encourage users to carefully consider these factors when using registered data and to seek legal advice when necessary to ensure compliance with fair use and other applicable laws.

[0112] FIG. 1D is a block diagram illustrating an exemplary architecture for facilitating secure financial transactions and data transfers within the platform's marketplaces, according to an embodiment. The architecture comprises a marketplace frontend **100** and a marketplace backend **105** which can utilize and integrate with various services/microservices. Marketplace frontend **100** provides a user-facing interface **101** where buyers and sellers interact, browse listings, and initiate transactions. The frontend **100** user interface **101** may integrate with seller dashboard **191** and upload interface **192** to allow users to provide various goods to the marketplace.

[0113] The marketplace backend **105** represents a server-side component that handles marketplace logic, such as listings management, search, and transaction processing. Marketplace backend **105** may integrate with a secure payment gateway component to process financial transactions securely and an escrow service to hold and release funds based on transaction status. Marketplace backend **105** may comprise an authentication and authorization service **106** to ensure that only authenticated users can access the marketplaces and perform actions based on their assigned roles and permissions. Marketplace backend **105** may comprise an encryption service **107** and secure data storage system **108** to store marketplace data (e.g., listing, user information, etc.) in encrypted form in a secure database. This may comprise implementing access control mechanisms to restrict access to sensitive data based on user roles and permissions. As shown, marketplace backend **105** may integrate with third-party services such as a blockchain platform **116** (e.g., Ethereum) to deploy smart contracts **117** to enable automated and secure execution of transactions and agreements. An escrow service **115** may be imple-

mented that communicates with marketplace backend **105** to hold and release funds based on transaction status.

[0114] FIG. 1E is a block diagram illustrating some exemplary marketplaces **170** and marketplace goods which may be implemented according to various aspects of platform **160**. The marketplace facilitates interactions and transactions among experts, providers, and consumers of machine learning and/or artificial intelligence (ML/AI) goods. Experts can contribute their judgments, ratings, and feedback on datasets, models, RAGs, weightings, and a variety of other goods, earning rewards and/or recognition for their expertise. Providers of datasets, models, RAGs, and weightings can list their offerings in the marketplace, benefiting from expert evaluations and exposure to a wide consumer base. Consumers can explore, compare, and acquire the ML/AI goods they need, leveraging expert judgments and ratings to make informed decisions. Transactions can be handled through secure payment gateways, ensuring the protection of intellectual property rights and fair compensation for providers.

[0115] According to an embodiment, marketplace **170** establishes governance mechanisms and quality assurance processes to maintain the integrity and reliability of the listed ML/AI goods. For example, expert judgments and trip reports may be used to continuously monitor and assess the quality and trustworthiness of datasets, models, RAGs, and weightings. In some implementations, feedback loops and dispute resolution mechanisms can be put in place to address any issues or discrepancies in expert evaluations or provider offerings. According to an aspect, a marketplace administration team oversees the overall functioning of the marketplace, ensuring compliance with guidelines, resolving disputes, and maintaining a fair and transparent environment for all participants.

[0116] As shown an expert judgment marketplace **170a** is present and configured to allow experts to provide their knowledge, insights, and evaluations on various aspects of a ML/AI ecosystem, such as data quality, model performance, related model parameters (e.g., tau for an LLN or temperature for an LLM), and the trustworthiness of RAGs. Experts can use the browser extension **240** to score and provide feedback on datasets, models, and RAGs listed in the marketplace. Expert judgments may be captured through standardized scoring mechanisms and qualitative feedback, ensuring consistency and comparability across evaluations. In some implementations, the reputations and credibility of experts may be determined based on the quality and reliability of their judgments, as assessed through trip reports and feedback from the community.

[0117] A model marketplace **170b** is present and configured to offer a wide range of ML/AI models, including pre-trained models, customizable models, hybrid models, and model architectures. Models may be listed with detailed specifications, such as input/output formats, performance metrics, training datasets, and applicable domains. Experts can evaluate and provide judgments on the quality, performance, and suitability of models for specific tasks or datasets. Model providers can benefit from expert feedback to improve their models and gain visibility in the marketplace. Consumers can access and utilize models based on their requirements, considering factors such as performance, expert ratings, and compatibility with their datasets. Model marketplace may also provide simulations or simulation parameters.

[0118] A dataset marketplace **170c** is present and configured to provide a rich collection of datasets across various domains, such as text, image, audio, and video data. Data may be listed with metadata, including format, size, source, licensing terms, and preprocessing applied. Experts can evaluate datasets based on factors such as quality, diversity, representativeness, and suitability for specific ML/AI tasks. Dataset providers can leverage expert judgments and feedback to enhance the quality and usability of their datasets. Consumers can discover and access datasets that align with their ML/AI projects, considering factors such as expert ratings, relevance to their domain, and compatibility with their chosen models.

[0119] According to an embodiment, dataset marketplace **170c** may further comprise corrective datasets. The marketplace system may allow for the buying, trading, and licensing of corrective data sets, which can be used to improve the accuracy and reliability of models, RAGs, and knowledge bases. These corrective data sets can include both short-term valuable data such as, for example, traffic accident details or congestion information, and long-term changes, like route, atlas, or point of interest (POI) data. For example, the system can facilitate the easy integration and incorporation of these corrective data sets into local maps, algorithms, and directions, enabling applications like GPS or Waze to provide more accurate and up-to-date information. By streamlining the process of acquiring and utilizing corrective data sets, the marketplace system can offer a more efficient and effective alternative to the cumbersome and outdated processes commonly used in industries like the automotive sector.

[0120] The marketplace system may take into account the adversarial dynamics and incentives associated with data collection and existence. It can recognize that corrective data sets may be necessary to compensate for other incentives present in collaborative data environments. The system may incorporate mechanisms to assess and adjust the veracity or certainty scores of data elements based on factors such as the data collection mechanism, provenance, and interpretation pipeline. For example, the system may be able to identify and account for situations where certain incentives, such as criminal rewards, may introduce noise or bias into the data, affecting its reliability and usefulness.

[0121] According to an embodiment, the marketplace system implements advanced data veracity scoring techniques that consider the broader context and potential influences on the data. It may be capable of analyzing and incorporating information about related data sets, rewards or incentives associated with data collection, and the potential impact on data quality and reliability. For example, the system can dynamically update veracity or certainty scores based on factors such as time period, geographic region, or specific events that may affect data integrity. By taking a holistic approach to data veracity scoring, the marketplace system can provide more accurate and trustworthy assessments of data quality, enabling users to make informed decisions about the data they acquire and utilize.

[0122] According to an embodiment, the marketplace system includes mechanisms to identify and compensate for sampling bias and response bias issues that may be present in certain data sets. As an example, it may be able to compare and analyze data from different sources, such as ADP's detailed payroll reports and the Fed's payroll surveys, to identify discrepancies and potential biases. In some

implementations, the system can apply statistical techniques and machine learning algorithms to adjust and normalize the data, mitigating the impact of sampling and response biases on the overall data quality and reliability. By proactively addressing these biases, the marketplace system can provide more accurate and representative data sets for users, enhancing the reliability and usefulness of the datasets, models, RAGs, and knowledge bases built upon them.

[0123] A retrieval augmented generation (RAG) marketplace **170d** may be implemented. RAGs are knowledge retrieval and generation models that combine the strengths of information retrieval and language generation. The RAG marketplace offers a variety of RAGs, each tailored to specific domains, tasks, and/or data types. RAGs can be listed with details such as retrieval sources, generation capabilities, performance metrics, and applicable use cases. Experts can evaluate RAGs based on factors such as retrieval accuracy, generation quality, and domain relevance. RAG providers can benefit from expert feedback to refine and improve their models, enhancing their visibility and adoption in the marketplace. Consumers can select and integrate RAGs into their applications, leveraging the power of knowledge retrieval and generation to enhance their ML/AI solutions.

[0124] According to an embodiment, the RAG marketplace **170d** can offer a comprehensive suite of knowledge retrieval and generation components, as well as infrastructure providers for running LLM/Vector Databases. The marketplace provides a modular approach, allowing users to select and integrate specific elements of RAGs into their applications, and choose between hosting options or leveraging 3rd party providers. The marketplace provides a modular approach, allowing users to select and integrate specific elements of RAGs into their applications. The marketplace offers a wide range of expert system prompts, which are carefully crafted and optimized for specific domains, tasks, and data types. These prompts encapsulate domain knowledge and best practices, guiding the generation process to produce high-quality and relevant outputs. Experts can contribute, evaluate, and refine these prompts based on their domain expertise and experience. Consumers can browse, purchase, and integrate these prompts into their own RAG implementations, benefiting from the collective knowledge and expertise of the community. Furthermore, the RAG marketplace **170d** can provide access to augmented datasets that enhance the performance and versatility of RAGs. These datasets may be curated, preprocessed, and enriched with additional information, such as metadata, annotations, and domain-specific knowledge. Augmented data can be used to fine-tune RAGs, improve retrieval accuracy, and expand the knowledge coverage of the models. Data providers can contribute their high-quality datasets to the marketplace, benefiting from expert feedback and monetization opportunities. Consumers can acquire and integrate these augmented datasets into their RAG pipelines, leveraging the enhanced data to improve the quality and relevance of the generated outputs.

[0125] The RAG marketplace **170d** can further include various RAG models. The marketplace offers a variety of pre-trained RAG models that combine information retrieval and language generation capabilities. These models are tailored to specific domains, tasks, and data types, providing out-of-the-box functionality for various applications. RAG models may be listed with details such as retrieval sources,

generation capabilities, performance metrics, and applicable use cases. Experts can evaluate and provide feedback on these models, helping to refine and improve their performance and usability. Consumers can select and integrate suitable RAG models into their applications, leveraging the power of knowledge retrieval and generation to enhance their ML/AI solutions. The RAG marketplace **170d** provides a modular and flexible approach, allowing users to customize and compose their RAG implementations based on their specific requirements. Users can mix and match expert system prompts, augmented data, and RAG models to create tailored solutions that align with their domain, task, and performance needs.

[0126] According to an implementation, the marketplace includes a range of infrastructure providers that offer hosting and management services for LLM and vector databases. These providers offer scalable and efficient infrastructure solutions optimized for running and storing large-scale language models and vector representations. Providers may offer various deployment options, such as cloud-based hosting, on-premises installations, or hybrid setups, catering to different user requirements and preferences. Additionally, or alternatively, users can choose to host their LLM/vector databases with these providers, benefiting from their expertise, reliability, and performance optimizations. Alternatively, users can opt to use 3rd party providers or their own infrastructure for hosting LLM/Vector Databases, ensuring flexibility and compatibility with their existing systems. According to an embodiment, standardized APIs, data formats, and communication protocols may be established to facilitate easy integration and interoperability among the different components. By including LLM/vector database providers in the RAG marketplace **170d**, users have the flexibility to choose the most suitable infrastructure for running and storing their language models and vector representations. They can opt for the convenience and reliability of the marketplace's recommended providers or leverage their existing 3rd party or in-house infrastructure.

[0127] A model weightings marketplace **170e** may be present. Model weightings represent the relative importance or influence of different models in an ensemble or multi-modal setup. The marketplace allows experts and model providers to share and exchange model weightings for specific tasks or domains. Weightings can be based on factors such as model performance, expert judgments, domain relevance, and data characteristics. Experts can evaluate and provide feedback on model weightings, assessing their effectiveness and suitability for different scenarios. Consumers can access and utilize model weightings to optimize the combination and integration of multiple models in their ML/AI pipelines.

[0128] Consider an example scenario where a company wants to fine-tune a pre-trained language model, such as GPT-3, for a specific task like sentiment analysis in the e-commerce domain. The company decides to purchase a weighting for the GPT-3 model from the marketplace to improve its performance on this particular task. The company identifies GPT-3 as the base model they want to use for their sentiment analysis task in the e-commerce domain. They search the marketplace for available weightings and fine-tuning options specifically designed for GPT-3 and sentiment analysis. The company reviews the available weightings for GPT-3 in the marketplace, considering factors such as the domain relevance (e-commerce), task-

specific performance metrics (sentiment analysis accuracy), and user ratings or reviews. They identify a highly-rated weighting that has been successfully used by other organizations for similar sentiment analysis tasks in the e-commerce domain. The weighting may be described as a set of fine-tuned parameters that adapt GPT-3's language understanding and generation capabilities to better capture the nuances and context of sentiment in e-commerce product reviews and customer feedback. The company decides to purchase the selected weighting for GPT-3 from the marketplace. They agree to the pricing terms and licensing conditions associated with the weighting, which may include usage limits, data privacy requirements, and any restrictions on modification or redistribution. The transaction is securely processed through the marketplace's payment gateway, and the company receives access to the purchased weighting. The company integrates the purchased weighting into their existing GPT-3 model using the provided integration tools and documentation. They fine-tune the GPT-3 model using the weighting, which adjusts the model's parameters and architecture to optimize its performance for sentiment analysis in the e-commerce domain. The fine-tuning process leverages the knowledge and expertise encapsulated in the weighting, allowing the company to benefit from the pre-optimized configurations and training strategies specific to their use case. After successfully fine-tuning the GPT-3 model with the purchased weighting, the company deploys the model in their production environment. They evaluate the model's performance on real-world e-commerce sentiment analysis tasks, comparing its accuracy, precision, and recall against their previous baseline models. The fine-tuned GPT-3 model, enhanced by the purchased weighting, demonstrates improved performance in accurately identifying and classifying sentiment in e-commerce product reviews and customer feedback. Based on the initial results and user feedback, the company may choose to further optimize the fine-tuned GPT-3 model. They can explore additional weightings or fine-tuning techniques available in the marketplace to further refine the model's performance, adapt it to specific subdomains or languages, or address any identified weaknesses or edge cases.

[0129] Now consider an extension of the previous example to include an option to purchase a Kolmogorov-Arnold Network (KAN) model as an alternative to the static LLM edge weights. In this scenario, the company is considering using KANs with first-order differential equation weights on nodes for their sentiment analysis task in the e-commerce domain. The company is exploring alternative approaches to sentiment analysis beyond the traditional static LLM edge weights. They discover Kolmogorov-Arnold Networks (KANs) in the marketplace, which offer a different approach to modeling sentiment dynamics using first-order differential equation weights on nodes. The company compares the features, performance metrics, and user reviews of KANs against the static LLM edge weights to assess their suitability for the sentiment analysis task. The company delves into the details of the KANs model available in the marketplace, examining its architecture, training methodology, and performance on sentiment analysis tasks. They find that KANs leverage first-order differential equations to capture the temporal dynamics and evolution of sentiment in e-commerce product reviews and customer feedback. The differential equation weights on nodes allow KANs to model the sentiment trajectory over time, consid-

ering factors such as the intensity, duration, and rate of change of sentiment expressions. After careful evaluation, the company decides to purchase the KANs model from the marketplace as an alternative or complement to the static LLM edge weights. They review and agree to the pricing terms, licensing conditions, and usage guidelines associated with the KANs model. The transaction is securely processed, and the company receives access to the KANs model, along with the necessary integration tools, documentation, and support resources. The company integrates the purchased KANs model into their existing sentiment analysis pipeline, following the provided integration guidelines and best practices. They prepare their e-commerce sentiment datasets, ensuring the data is properly formatted and annotated for training the KANs model. The company trains the KANs model using the differential equation weights on nodes, allowing it to learn the temporal dynamics and sentiment evolution patterns specific to their e-commerce domain. After successfully training the KANs model, the company deploys it in their production environment alongside the static LLM edge weights model. They evaluate the performance of both models on real-world e-commerce sentiment analysis tasks, comparing their accuracy, precision, recall, and ability to capture sentiment dynamics over time. The KANs model demonstrates strong performance in tracking sentiment trajectories, identifying sentiment shifts, and providing insights into the temporal aspects of customer feedback and product reviews. Based on the evaluation results, the company explores the possibility of combining the KANs model with the static LLM edge weights model to create an ensemble approach. They experiment with different ensemble strategies, such as weighted averaging or meta-learning, to leverage the strengths of both models and improve overall sentiment analysis performance. The company fine-tunes the ensemble model, optimizing the combination of KANs and static LLM edge weights to achieve the best possible results for their specific e-commerce sentiment analysis use case.

[0130] A pre-processing and data cleaning tools marketplace 170f may be implemented. The marketplace can offer a range of pre-processing and data cleaning tools to help users prepare their datasets for ML/AI tasks. These tools can include algorithms for data normalization, outlier detection, missing value imputation, and feature scaling. Experts can evaluate and provide feedback on the effectiveness and usability of these tools for different data types and domains.

[0131] A data labeling and annotation marketplace 170g may be present. Many ML/AI projects require labeled or annotated datasets for training and evaluation purposes. The marketplace can offer data labeling and annotation services, where providers can contribute their expertise in labeling datasets across various domains, such as image classification, sentiment analysis, or named entity recognition. Consumers can access these labeled datasets or commission custom labeling services based on their specific requirements.

[0132] A model explainability and interpretation tools marketplace 170h may be provided. As ML/AI models become more complex, the need for model explainability and interpretation grows. The marketplace can offer tools and techniques that help users understand and interpret behavior and prediction of ML/AI models. These tools can include feature importance analysis, decision tree visualiza-

tions, or techniques like Shapley Additive explanations (SHAP) or Local Interpretable Model-Agnostic Explanations (LIME).

[0133] An evaluation metrics and benchmarking tools marketplace **170i** may be implemented. Evaluating the performance and effectiveness of ML/AI models is important for model selection and improvement. The marketplace can provide a range of evaluation metrics and benchmarking tools specific to different tasks and domains. These tools can help users assess the performance of their models against standardized benchmarks or compare them with other models available in the marketplace.

[0134] A model compression and optimization marketplace **170j** may be provided by platform **160**. Deploying ML/AI models in resource-constrained environments often requires model compression and optimization. The marketplace can offer techniques and tools for model compression, such as quantization, pruning, or knowledge distillation. Experts can provide guidance and best practices for applying these techniques to different model architectures and deployment scenarios.

[0135] A transfer learning and domain adaptation marketplace **170k** may be present. Transfer learning and domain adaptation techniques allow ML/AI models to leverage knowledge learned from one task or domain to improve performance on another. The marketplace can offer pre-trained models, fine-tuning techniques, or domain adaptation algorithms that enable users to apply transfer learning effectively. Experts can provide insights and recommendations on suitable transfer learning approaches for specific use cases and domains.

[0136] An ML/AI pipeline and workflow management marketplace **170l** may be implemented. Building and managing end-to-end ML/AI pipelines can be complex and time-consuming. The marketplace can offer tools and frameworks for designing, orchestrating, and monitoring ML/AI workflows. For example, a DCG computing system **121** can be configured to assist with ML/AI pipeline and workflow generation and execution. These tools can help users streamline their ML/AI development process, automate repetitive tasks, and enable reproducibility and scalability.

[0137] A synthetic data generation marketplace **170m** may be provided by platform **160**. In cases where real-world data is scarce or sensitive, synthetic data generation can be a valuable approach. The marketplace can provide tools and algorithms for generating realistic synthetic datasets based on specific data distributions or domain characteristics. Experts can evaluate the quality and validity of synthetic datasets and provide guidance on their appropriate usage.

[0138] A privacy-preserving ML/AI techniques marketplace **170n** can be implemented. Privacy and data protection are critical concerns in many ML/AI applications. The marketplace can offer privacy-preserving techniques, such as federated learning, differential privacy, or homomorphic encryption. These techniques enable training and inference on sensitive data while preserving the privacy of individuals or organizations.

[0139] A consulting and training services marketplace **170o** may be provided. In addition to goods, the marketplace can offer consulting and training services provided by experts in ML/AI. These services can include guidance on model selection, data preprocessing, model deployment, or custom solution development. Experts can offer workshops,

tutorials, or one-on-one mentoring sessions to help users build their ML/AI skills and knowledge.

[0140] An observability and enforcement service **170p** to check ongoing use compliance and adherence to data contracts can be integrated into the marketplace system to ensure that data providers and consumers are consistently meeting their obligations and maintaining the integrity of the data ecosystem. The observability and enforcement service can monitor and log all data access, usage, and manipulation activities within the marketplace system and may capture relevant metadata, such as data provider and consumer identities, data contract versions, timestamps, and operation types (e.g., read, write, transform). The monitoring functionality should be scalable and able to handle high volumes of data access and usage events across multiple data providers and consumers. The enforcement service **170p** can continuously validate data access and usage against the defined data contracts. It can check that data consumers are accessing and using data in accordance with the specified schemas, semantics, and constraints outlined in the relevant data contracts. The validation process can be automated and triggered in real-time or near-real-time as data access and usage events occur. The service should leverage the versioned data contracts stored in the centralized repository to ensure that the correct contract version is being enforced for each data interaction.

[0141] According to an embodiment, the observability and enforcement service **170p** can generate compliance reports and alerts based on the monitored data access and usage activities. It may identify and flag any instances of non-compliance, such as data consumers accessing or using data in ways that violate the terms of the data contracts. The service can provide detailed reporting on compliance metrics, including the number of compliant and non-compliant data interactions, trends over time, and breakdowns by data provider, consumer, and contract. In some implementations, automated alerts and notifications may be triggered when significant non-compliance issues are detected, allowing data providers and platform administrators to take prompt corrective actions. The observability and enforcement service can have predefined remediation and enforcement actions that can be triggered when non-compliance is detected. These actions could include temporarily suspending or revoking data access privileges for non-compliant consumers, issuing warnings or notifications, or applying data usage restrictions. The service may provide interfaces and workflows for data providers and platform administrators to review and approve enforcement actions, ensuring appropriate oversight and governance. In cases of severe or repeated non-compliance, the service may implement mechanisms for escalating the issue to relevant authorities or initiating legal or contractual remedies.

[0142] By expanding the range of goods and services offered on the marketplace, platform **160** creates a comprehensive ecosystem that caters to the diverse needs of ML/AI practitioners, researchers, and organizations. These offerings complement the core goods and provide users with the tools, techniques, and expertise necessary to tackle a wide range of ML/AI challenges effectively. The inclusion of these goods and services not only enhances the value proposition of the marketplace but also fosters collaboration, knowledge sharing, and innovation among participants. It creates a one-stop-shop for ML/AI resources, enabling users to access

cutting-edge techniques, best practices, and expert guidance to accelerate their projects and drive meaningful results.

[0143] According to some embodiments, platform 160 may leverage a browser extension 240 and trip report functionality 250 that allows experts to score data sources during their daily web usage. Experts can download and install the browser extension from the platform's website or trusted browser extension store. During the setup process, experts authenticate themselves using their platform credentials to ensure secure access to the extension's features. The extension may require additional permissions, such as access to browser history or the ability to modify web pages, which experts grant during installation. According to some aspects, the browser extension can add a small icon or button to the browser's toolbar, providing easy access to its features. When an expert visits a web page containing a data source, the extension's icon may change color or display a notification to indicate that scoring is available. Clicking on the extension's icon can open a pop-up window or sidebar within the browser, presenting the scoring interface.

[0144] The browser extension may utilize various techniques to detect and identify data sources on the web pages visited by experts. It may employ, for example, web scraping techniques, such as parsing the HTML structure or using CSS selectors, to locate and extract relevant data source elements. The extension may also leverage machine learning algorithms or predefined patterns to automatically recognize and highlight data sources on the page.

[0145] According to some aspects, a scoring interface provided by the browser extension allows experts to rate and provide feedback on the data sources they encounter. It may comprise a user-friendly form or rating system where experts can assign scores to various aspects of the data source, such as reliability, accuracy, or relevance. Experts can provide additional comments or qualitative feedback to justify their scores or provide insights. The extension may also display aggregated scores or ratings from other experts who have previously scored the same data source. When an expert submits their scores and feedback through the browser extension, the data is securely transmitted to the platform's servers. For example, the extension may utilize APIs or secure communication protocols (e.g., HTTPS) to send the scoring data to the backend system. The submitted scores are associated with the specific data source, expert's identity, and timestamp to maintain a record of the scoring activity. The extension may also synchronize with the platform to fetch updated scores or aggregated data from other experts, providing a collaborative scoring environment.

[0146] As experts browse the web and interact with data sources, the browser extension collects and stores relevant information about their scoring activity, according to an embodiment. This can include details such as the URLs visited, data sources encountered, scores assigned, and any additional feedback provided. The extension may also capture metadata, such as the time spent on each page or the frequency of visits to specific data sources. According to some aspects, the trip report functionality may be configured to aggregate and analyze the collected data to generate meaningful insights and summaries for experts and the platform. It may employ data analysis techniques, such as statistical analysis or natural language processing, to extract key findings from the scoring data. The report may include visualizations, such as graphs or charts, to present the expert's scoring patterns, top-rated data sources, or trends

over time. The generated report can be stored on the platform's servers and can be accessed by the expert through their dashboard or via email notifications.

[0147] The trip report serves as a valuable tool for experts to reflect on their scoring activity and identify areas for improvement. It provides insights into their scoring patterns, biases, or inconsistencies, enabling them to make more informed and objective judgments in the future. Experts can review their trip reports periodically to track their progress, compare their scores with other experts, and receive feedback from the platform or their peers.

[0148] According to an embodiment, the trip report data can be integrated into the platform's overall scoring and reputation system. The scored data sources and expert feedback contribute to the platform's knowledge base, helping to establish trust and credibility for the data sources. The platform may use the trip report data to generate aggregate scores, rankings, or recommendations for data sources based on the collective feedback from multiple experts. This integration enables the platform to provide more accurate and reliable information to its users, leveraging the expertise and real-world evaluations from the expert community.

[0149] The browser extension and trip report functionality prioritize the privacy and security of experts' data. All data collected by the extension is transmitted securely and stored in encrypted form on the platform's servers. Access to the trip report data is restricted to authorized personnel and systems, ensuring confidentiality and protecting experts' personal information. Experts have control over their data and can opt-out of certain data collection or sharing features if desired.

[0150] An expert judgment marketplace 170a can be seamlessly integrated into the platform 160, leveraging the browser extension and trip report functionality to facilitate the exchange of expert opinions and insights. Experts interested in participating in the marketplace register on the platform, providing their credentials, areas of expertise, and relevant qualifications. The platform verifies the experts' credentials and background to ensure the credibility and reliability of their judgments. Verified experts are granted access to the expert judgment marketplace and its features. In some implementations, data providers or organizations seeking expert judgments create listings in the marketplace, specifying the data sources or domains they want to be evaluated. Listings can include details such as the scope of the evaluation, specific criteria or guidelines, and any incentives or rewards for experts. Experts can browse and filter marketplace listings based on their areas of expertise, interest, or other relevant criteria.

[0151] Experts use the browser extension to access and evaluate the data sources listed in the marketplace. They follow the scoring guidelines and criteria provided in the listing to ensure consistent and standardized evaluations. Experts assign scores, provide qualitative feedback, and submit their evaluations through the browser extension. The extension captures the scoring data and securely transmits it to the platform's servers. The trip report functionality aggregates and analyzes the scoring data submitted by experts for each marketplace listing. It generates reports and insights on the collective opinions, consensus scores, and key findings from the expert evaluations. The platform uses the trip report data to update the reputation scores and credibility ratings of the experts based on the quality and consistency of their judgments. For example, experts with a proven track record

of accurate and reliable evaluations gain higher reputation scores, increasing their visibility and trust within the marketplace.

[0152] Data providers or organizations can access the expert evaluations and trip reports for their listed data sources through the marketplace. They can review the scores, feedback, and insights provided by the experts to make informed decisions about the quality and reliability of their data. The marketplace facilitates transactions between data providers and experts, enabling the exchange of value for the expert judgments rendered. Experts may be rewarded based on the terms and conditions of each marketplace listing, which may include monetary compensation, tokens, or other incentives.

[0153] According to some embodiments, the expert judgment marketplace 170a incorporates feedback loops and quality assurance mechanisms to ensure the ongoing reliability and accuracy of expert evaluations. Experts receive feedback on their evaluations, allowing them to learn, improve, and align their judgments with the platform's standards. The platform monitors the consistency and quality of expert evaluations, taking corrective actions or adjusting reputation scores as needed. Regular updates and enhancements to the marketplace ensure that it remains relevant, efficient, and reliable over time.

[0154] The expert judgment marketplace seamlessly integrates with other components of the platform, such as the data marketplace, model marketplace, and retrieval augmented generation (RAG) marketplace. Expert evaluations and trip reports from the judgment marketplace inform the quality and trustworthiness of data sources, models, and RAGs listed in the respective marketplaces. For example, the reputation scores and credibility ratings of experts in the judgment marketplace can be used as weighting factors in the selection and application of models, data sources, and RAGs across the platform.

[0155] By integrating an expert judgment marketplace into platform 160, it creates a valuable ecosystem where experts can contribute their knowledge and insights to evaluate and validate data sources. The marketplace leverages the browser extension and trip report functionality to facilitate efficient and standardized expert evaluations. The resulting expert judgments and trip reports provide data providers and organizations with trusted insights to make informed decisions, while experts are rewarded for their contributions. This integration enhances the overall reliability, credibility, and value of the platform's offerings, driving better outcomes for all participants in the ecosystem.

[0156] According to various aspects, AI systems/models can serve as experts 230 in the marketplace platform 160 by leveraging their vast knowledge, computational capabilities, and ability to learn from large amounts of data. There are several ways in which an AI system can be considered an expert. An AI can become an expert via comprehensive domain knowledge. AI systems can be trained on extensive datasets covering specific domains or industries. Through machine learning techniques like deep learning or natural language processing, AI systems can acquire comprehensive knowledge about a particular field. This knowledge can include historical data, research papers, case studies, and real-world examples, enabling the AI to provide expert-level insights and recommendations.

[0157] An AI system can become an expert with respect to pattern recognition and anomaly detection. AI systems excel

at recognizing patterns and detecting anomalies in large datasets. They can quickly identify trends, correlations, and outliers that may be challenging for human experts to spot. By analyzing vast amounts of data, AI experts can provide valuable insights into data quality, model performance, and potential issues or opportunities.

[0158] An AI system can become an expert with respect to predictive modeling and forecasting. AI systems can build sophisticated predictive models based on historical data and machine learning algorithms. These models can accurately forecast future trends, behaviors, or outcomes in various domains, such as finance, healthcare, or customer analytics. AI experts can provide precise and data-driven predictions, enabling users to make informed decisions and optimize their strategies.

[0159] An AI system can become an expert via continuous learning and adaptation. AI systems have the ability to continuously learn and adapt as new data becomes available. They can automatically update their knowledge bases, refine their models, and improve their performance over time. This continuous learning capability allows AI experts to stay up-to-date with the latest developments, research findings, and best practices in their respective domains.

[0160] An AI system can be considered an expert based on scalability and efficiency. AI systems can process and analyze vast amounts of data in a fraction of the time it would take human experts. They can handle complex computations, simulate multiple scenarios, and generate insights at a scale that is impractical for humans. AI experts can efficiently provide expert judgments, recommendations, or analyses across a wide range of datasets, models, or applications. Furthermore, AI systems can provide objective and unbiased analyses based on data-driven insights. They are not influenced by personal biases, emotions, or subjective opinions that may affect human judgment. AI experts can offer impartial evaluations and recommendations, ensuring fairness and consistency in the marketplace.

[0161] Expert AI systems can be trained to specialize in specific niches or sub-domains within a larger field. They can acquire deep expertise in narrow areas that may be challenging for human experts to master. AI experts can provide highly specialized insights, recommendations, or solutions tailored to specific use cases or industry verticals. In some embodiments, AI systems can collaborate with human experts to augment their capabilities and provide comprehensive solutions. They can assist human experts in tasks such as data analysis, pattern recognition, or decision support. The combination of human intuition and AI-driven insights can lead to more accurate and well-rounded expert judgments and recommendations.

[0162] To establish AI systems as credible experts in the marketplace, it is essential to ensure transparency, accountability, and trust. This can be achieved through: rigorous testing and validation of AI models to ensure their accuracy and reliability; providing explanations and interpretations of AI-generated insights to foster trust and understanding among users; implementing governance mechanisms to monitor and audit AI experts' performance and outputs; clearly communicating the capabilities and limitations of AI experts to set appropriate expectations; and collaborating with human experts to validate and enhance AI-generated insights and recommendations.

[0163] Integrating AI experts into the browser extension, trip reporting, and expert judgment scores can significantly

enhance the capabilities and value of the marketplace platform. The browser extension is not strictly limited to web browsers and refers to any specific application with similar functionality across multiple devices such as virtual reality devices, mobile apps, and embedded libraries. With respect to the browser extension, AI experts can provide AI-powered data source evaluation. The browser extension 240 can incorporate AI algorithms to automatically analyze and evaluate data sources visited by users. AI experts can assess factors such as data quality, reliability, relevance, and potential biases in real-time as users browse websites. The AI can provide instant feedback, ratings, or recommendations directly within the browser extension interface. AI experts can assist with contextual insights and recommendations. For example, AI experts can leverage the user's browsing history, preferences, and domain expertise to provide contextual insights and recommendations. The AI can suggest related data sources, models, or experts based on the user's current browsing context and past interactions. These personalized recommendations can help users discover valuable resources and make informed decisions.

[0164] AI experts can integrate with trip reporting via, for example, automated trip report generation. AI experts can automate the generation of trip reports based on the user's browsing activity and interactions with data sources. The AI can analyze patterns, summarize key findings, and highlight notable insights from the user's browsing sessions. This automation saves time and effort for users while ensuring comprehensive and consistent trip reports. Furthermore, AI experts can apply advanced data analysis techniques to the information collected during the user's browsing trips. The AI can identify trends, correlations, and anomalies in the data, providing deeper insights and actionable recommendations. AI-powered visualizations, such as interactive charts or graphs, can enhance the presentation of trip report findings, making them more intuitive and engaging.

[0165] AI experts can integrate with expert judgment scoring capabilities via AI-assisted scoring and evaluation. AI experts can assist in the scoring and evaluation process of data sources, models, and other marketplace goods. The AI can analyze large volumes of user feedback, ratings, and historical data to generate accurate and unbiased expert judgment scores. AI algorithms can identify patterns, detect outliers, and adjust scores based on various factors, enabling fair and reliable evaluations. AI experts can be leveraged to support continuous learning and refinement. AI experts can continuously learn and adapt based on the feedback and ratings provided by human experts and users. As more data becomes available, the AI can refine its scoring models, improve its accuracy, and provide more precise expert judgments over time. This continuous learning capability ensures that the AI expert's judgments remain up-to-date and aligned with the evolving needs and preferences of the marketplace community.

[0166] The integration of AI experts can foster collaboration between human experts and AI systems. AI experts can provide initial evaluations, insights, and recommendations, which can then be reviewed, validated, or enhanced by human experts. This collaborative approach combines the efficiency and scalability of AI with the intuition and domain knowledge of human experts, resulting in more comprehensive and reliable expert judgments. The browser extension 240 and trip reporting 250 components can include mechanisms for users to provide feedback on the AI expert's

evaluations and recommendations. This feedback can be used to fine-tune the AI models, improve their accuracy, and ensure alignment with user expectations. Regular updates and enhancements to the AI experts based on user feedback foster a continuous improvement cycle and maintain the quality and relevance of AI-generated insights.

[0167] When AI experts provide evaluations, recommendations, or scores, it should be clearly indicated to users that they are interacting with an AI system. This transparency helps users understand the nature of the expert judgment and sets appropriate expectations. Additionally, AI experts can incorporate explainable AI techniques to provide clear and understandable explanations for their evaluations and recommendations. Users may be able to access the reasoning behind AI-generated insights, enabling them to make informed decisions and build trust in the AI expert's judgments.

[0168] By seamlessly integrating AI experts into the browser extension, trip reporting, and expert judgment scores, the marketplace platform can leverage the power of artificial intelligence to enhance user experiences, provide intelligent insights, and streamline expert evaluation processes. This integration complements the expertise of human experts, enabling a more comprehensive and data-driven approach to evaluating and leveraging marketplace goods.

[0169] FIG. 1F is a block diagram illustrating an exemplary system architecture for a distributed generative artificial intelligence reasoning and action platform 120, according to an embodiment. According to the embodiment, platform 120 is configured as a cloud-based computing platform comprising various system or sub-system components configured to provide functionality directed to the execution of neuro-symbolic generative AI reasoning and action. Exemplary platform systems can include a distributed computational graph (DCG) computing system 121, a curation computing system 122, a marketplace computing system 123, and a context computing system 124. In some embodiments, systems 121-124 may each be implemented as standalone software applications or as a services/micro-services architecture which can be deployed (via platform 120) to perform a specific task or functionality. In such an arrangement, services can communicate with each other over an appropriate network using lightweight protocols such as HTTP, gRPC, or message queues. This allows for asynchronous and decoupled communication between services. Services may be scaled independently based on demand, which allows for better resource utilization and improved performance. Services may be deployed using containerization technologies such as Docker and orchestrated using container orchestration platforms like Kubernetes. This allows for easier deployment and management of services.

[0170] The distributed generative AI reasoning and action platform 120 can enable a more flexible approach to incorporating machine learning (ML) models into the future of the Internet and software applications; all facilitated by a DCG architecture capable of dynamically selecting, creating, and incorporating trained models with external data sources and marketplaces for data and algorithms.

[0171] According to the embodiment, DCG computing system 121 provides orchestration of complex, user-defined workflows built upon a declarative framework which can allow an enterprise user 110 to construct such workflows using modular components which can be arranged to suit the

use case of the enterprise user. As a simple example, an enterprise user **110** can create a workflow such that platform **120** can extract, transform, and load enterprise-specific data to be used as contextual data for creating and training a ML or AI model. The DCG functionality can be extended such that an enterprise user can create a complex workflow directed to the creation, deployment, and ongoing refinement of a trained model (e.g., LLM). For example, in some embodiments, an enterprise user **110** can select an algorithm from which to create the trained model, and what type of data and from what source they wish to use as training data. DCG computing system **121** can take this information and automatically create the workflow, with all the requisite data pipelines, to enable the retrieval of the appropriate data from the appropriate data sources, the processing/preprocessing of the obtained data to be used as inputs into the selected algorithm(s), the training loop to iteratively train the selected algorithms including model validation and testing steps, deploying the trained model, and finally continuously refining the model over time to improve performance.

[0172] A context computing system **124** is present and configured to receive, retrieve, or otherwise obtain a plurality of context data from various sources including, but not limited to, enterprise users **110**, marketplaces **130a-n**, third-party sources **150**, and other data sources **140a-n**. Context computing system **124** may be configured to store obtained contextual data in a data store. For example, context data obtained from various enterprise endpoints **110a-n** of a first enterprise may be stored separately from the context data obtained from the endpoints of a second enterprise. In some embodiments, context data may be aggregated from multiple enterprises within the same industry and stored as a single corpus of contextual data. In such embodiments, contextual data may be transformed prior to processing and storage so as to protect any potential private information or enterprise-specific secret knowledge that the enterprise does not wish to share.

[0173] A curation computing system **122** is present and configured to provide curated (or not) responses from a trained model (e.g., LLM) to received user queries. A curated response may indicate that it has been filtered, such as to remove personal identifying information or to remove extraneous information from the response, or it may indicate that the response has been augmented with additional context or information relevant to the user. In some embodiments, multiple trained models (e.g., LLMs) may each produce a response to a given prompt, which may include additional contextual data/elements, and a curation step may include selecting a single response of the multiple responses to send to a user, or the curation may involve curating the multiple responses into a single response. The curation of a response may be based on rules or policies that can set an individual user level, an enterprise level, or at a department level for enterprises with multiple departments (e.g., sales, marketing, research, product development, etc.).

[0174] According to the embodiment, an enterprise user **110** may refer to a business organization or company. An enterprise may wish to incorporate a trained ML model into their business processes. An enterprise may comprise a plurality of enterprise endpoints **110a-n** which can include, but are not limited to, mobile devices, workstations, laptops, personal computers, servers, switches, routers, industrial equipment, gateways, smart wearables, Internet-of-Things (IoT) devices, sensors, and/or the like. An enterprise may

engage with platform **120** to create a trained model to integrate with its business processes via one or more enterprise endpoints. To facilitate the creation of purpose-built, trained model, enterprise user **110** can provide a plurality of enterprise knowledge **111** which can be leveraged to build enterprise specific (or even specific to certain departments within the enterprise) ML/AI models. Enterprise knowledge **111** may refer to documents or other information important for the operation and success of an enterprise. Data from internal systems and databases, such as customer relationship management (CRM) systems, enterprise resource planning (ERP) systems, rules and policies databases, and transactional databases, can provide information about the operational context of an enterprise. For example, product knowledge, market knowledge, industry trends, regulatory knowledge, business processes, customer knowledge, technology knowledge, financial knowledge, organization knowledge, and risk management knowledge may be included in enterprise knowledge base **111**.

[0175] According to the embodiment, platform **120** is configured to retrieve, receive, or otherwise obtain a plurality of data from various sources. A plurality of marketplaces **130a-n** may be present and configured to provide centralized repositories for data, algorithms, and expert judgment, which can be purchased, sold, or traded on an open marketplace. External data sourced from various marketplaces **130a-n** can be used as a training data source for creating trained models for a particular use case. A marketplace computing system **123** is present and configured to develop and integrate various marketplaces **130a-n**. Marketplace computing system **123** can provide functionality directed to the registration of experts or entities. An expert may be someone who has a deep understanding and knowledge of a specific industry, including its trends, challenges, technologies, regulations, and best practices. Industry experts often have many years of experience working in the industry and have developed a reputation for their expertise and insights. Examples of experts can include, but are not limited to, consultants, analysts, researchers, academics, or professionals working in the industry. In some embodiments, experts and/or entities can register with platform **120** so that they may become verified experts/entities. In such an embodiment, an expert/entity profile may be created which can provide information about expert judgment, scored data and algorithms, and comparisons/statistics about the expert's/entity's scores and judgment with respect to other expert/entities. Marketplace computing system **123** may further provide functionality directed to the management of the various marketplaces and the data/algorithms provided therein.

[0176] According to some embodiments, platform **120** can communicate with and obtain data from various third-party services **150**. For example, third-party services can include LLM services such as APIs and LLM hosting platforms, which platform **120** can interface with to obtain algorithms or models to use as starting points for training a neuro-symbolic generative AI reasoning and action model to be deployed at the enterprise or individual level. As another example, social media platforms can provide data about trends, events, and public sentiment, which can be useful for understanding the social context of a situation. Exemplary data sources **140a-n** can include, but are not limited to, sensors, web data, environmental data, and survey and interviews.

[0177] FIG. 2 is a block diagram illustrating an exemplary aspect of a distributed generative AI reasoning and action platform incorporating various additional contextual data. According to the aspect, a plurality of contextual data from various data sources may be integrated into platform 120. A simple exemplary directed computational graph 200 is illustrated within the cloud and utilizing the plurality of contextual data to create and train a model. Various marketplaces 130a-n are shown which can provide contextual data to platform 120 including an expert judgment marketplace 260 and a model and retrieval augmented generation (RAG) marketplace 220. According to the aspect, DCG 200 orchestrates model (and model weight) selection 204, including multi-model usage in series or parallel (i.e., feed output of one model into another, or compare and choose outputs across multiple models), based on multiple data sources (both trained and external), input from crowdsourced expert judgment, training or tuning data set corpora, and RAG libraries.

[0178] Expert judgment will become increasingly important in the world of proprietary or otherwise blackbox ML or AI models where hallucinations and training data quality may produce misleading or otherwise incorrect results. The expert judgment marketplace 260 provides a way for experts 230 to weigh-in on the correctness of data whether that is training data or model output, and can be facilitated by a browser extension 240, for example, to score things like data sources during their daily “trip around web”. This trip report scoring 250 concept allows experts to score data sources. In an implementation, a browser extension 240 is developed with an accuracy score input where the user can rank a news article they are reading as they consume it. Expert judgment marketplace 260 allows for consumers to pick and rank “experts” based on how well their judgment helps or hinders their overall consumption of model output. For example, experts that routinely highly rank data sources, like news sites, that are known to spread false information should likewise be less trusted over time compared to their peers, and any models trained on that data similarly less trusted. Ultimately a database 270 of data sources and schemas scored by algorithms or experts could be used as input into the DCG 200 for more accurate and real-time inference based on ongoing rating of preferred data set and data format combinations (e.g. the same data might be purchased in unstructured, structured, schematized, normalized, or semantified formats) which may introduce different types of bias or impacts on performance, results, or processing costs.

[0179] Accordingly, a RAG marketplace 220 may be implemented to further refine model output. RAG information may be included as additional context which can be supplied to a GenAI model in addition to a prompt (engineered, or otherwise). This is especially important where companies may want to sell access to their proprietary dataset through the form of a RAG. For example, a medical research company may have valuable information they could sell to other institutions in the form of a RAG to augment related research without specifically providing access to the raw training data. Retrieval-augmented generation is a framework that combines elements of retrieval-based and generative models to improve the performance of natural language processing tasks. In RAG, a retriever component is used to select relevant information from a large corpus, and a generator component is used to produce a final output based on both the retrieved information and the

input query. RAG marketplace 220 may be scored by experts for accuracy and effectiveness across domains.

[0180] According to the aspect, a user experience curation engine 210 is needed that is able to curate output whether that is in the form of filtering out sensitive data or simply customizing results in a way the user prefers (which may be based on user-/entity-defined rules or policies). A user can submit a query to experience curation engine 210 which can send the query to the DCG trained model to obtain a response. Experience curation 210 may then process the received response to curate it (or not) to meet the preferences of the user.

[0181] As illustrated, DCG 200 shows a simple example of a directed computational graph which can be used to create a complex workflow to create and train an MI/AI model (e.g., variations of or standard transformer architecture). As shown, the DCG comprises multiple sources of information for training the selected model(s) including multiple data sources 201a-n which may or may not be scored by experts, expert judgment 202, and one or more RAGs 203 which may be obtained from RAG marketplace 220 or may be obtained directly from enterprise knowledge. DCG may have access to stored models or variants thereof. In the illustration, LLAMA (Learned Layer-wise Attention Metric for Transformers), PALM (Permuted Adaptive Lateral Modulation), and HYENA (Hyperbolic Encoder for Efficient Attention) are shown as possible examples of the types of models which can be selected by the DCG to create and train a GenAI model. Furthermore, the “model parameters” and mathematical techniques or assumptions used in each model may be cataloged and included in a model-specific template which may be stored in cloud-based storage on platform 120. In some embodiments, platform 120 may store a hierarchical representation of transformer models (e.g., as a graph), which may represent a lineage of the evolution of transformer models. In an implementation, model selection or exploration involves selections based on the evolutionary tree of one or more model types and use said tree (e.g., graph) for selections in heuristic search for best algorithm/data combinations, licensing costs/explorations, etc. It should be appreciated that certain aspects of the invention may be tailored based on what kind of mathematical approach underpins a specific model.

[0182] In operation, DCG 200 obtains the various contextual data from the connected data sources, creates training, validation, and test datasets from the obtained data, and uses the various datasets to train, validate, and test the model as it undergoes a model training loop that iteratively trains the model to generate responses based on the plurality of contextual data.

[0183] FIG. 3 is a diagram illustrating incorporating symbolic reasoning in support of LLM-based generative AI, according to an aspect of a neuro-symbolic generative AI reasoning and action platform. According to the aspect, platform 120 can incorporate symbolic reasoning and in-context learning to create and train off the shelf models (e.g., an LLM foundational model or narrow model) through clever prompting and conditioning on private data or very situation specific “contextual” data. Platform 120 can obtain contextual data 301 and preprocess the data for storage. Contextual data 301 may refer to data obtained from marketplaces 130a-n, third-party services 150, and enterprise knowledge 111, as well as other types of contextual data that may be obtained from other sources. DCG 330 is responsible

for orchestrating the entire process and can create data pipelines **310** as needed to facilitate the ingestion of contextual data **301**. Contextual data can include text documents, PDFs, and even structure formats like CSV (comma-separated values) or SQL tables or other common generic data formats like OWL or RDF or domain specific content such as the Financial Industry Business Ontology (FIBO) or Open Graph of Information Technology (OGIT). This stage involves storing private data (e.g., context data) to be retrieved later.

**[0184]** Typically, the context data **301** is broken into chunks, passed through and embedding model **315**, then stored in a specialized database called a vector database **320**. Embedding models are a class of models used in many tasks such as natural language processing (NLP) to convert words, phrases, or documents into numerical representations (embeddings) that capture similarity which often correlates semantic meaning. Exemplary embedding models can include, but are not limited to, text-embedding-ada-002 model (i.e., OpenAI API), bidirectional encoder representations from transformers, Word2Vec, FastText, transformer-based models, and/or the like. The vector database **315** is responsible for efficiently storing, comparing, and retrieving a large plurality of embeddings (i.e., vectors). Vector database **315** may be any suitable vector database system known to those with skill in the art including, but not limited to, open source systems like Pinecone, Weaviate, Vespa, and Qdrant. According to the embodiment, embedding model **315** may also receive a user query from experience curation **340** and vectorize it where it may be stored in vector database **320**. This provides another useful datapoint to provide deeper context when comparing received queries against stored query embeddings.

**[0185]** A user may submit a query **303** to an experience curation engine **340** which starts the prompt construction and retrieval process. The query is sent to DCG **330** which can send the query to various components such as prompt engineering **325** and embedding model **315**. Embedding model **315** receives the query and vectorizes it and stores it in vector database **320**. The vector database **320** can send contextual data (via vectors) to DCG **330** and to various APIs/plugins **335**. Prompt engineering **325** can receive prompts **302** from developers to train the model on. These can include some sample outputs such as in few-shot prompting. The addition of prompts via prompt engineering **325** is designed to ground model responses in some source of truth and provide external context the model wasn't trained on. Other examples of prompt engineering that may be implemented in various embodiments include, but are not limited to, chain-of-thought, self-consistency, generated knowledge, tree of thoughts, directional stimulus, and/or the like.

**[0186]** During a prompt execution process, experience curation **340** can send user query to DCG **330** which can orchestrate the retrieval of context and a response. Using its declarative roots, DCG **330** can abstract away many of the details of prompt chaining; interfacing with external APIs **335** (including determining when an API call is needed); retrieving contextual data from vector databases **330**; and maintaining memory across multiple LLM calls. The DCG output may be a prompt, or series of prompts, to submit to a language model via LLM services **360** (which may be potentially prompt tuned). In turn, the LLM processes the prompts, contextual data, and user query to generate a

contextually aware response which can be sent to experience curation **340** where the response may be curated, or not, and returned to the user as output **304**.

**[0187]** FIG. 4 is a block diagram illustrating an exemplary architecture for a neuro-symbolic generative AI reasoning and action platform **400** configured for federated learning at a plurality of edge devices **410a-n**, according to an embodiment. According to the embodiment, platform **400** comprises DCH computing system **421**, curation computing system **422**, marketplace computing system **423**, and context computing system **424**. According to an embodiment, edge devices **410a-n** may represent various enterprise endpoints. In other embodiments, edge devices **410a-n** may represent various endpoints from two or more separate enterprises. In an embodiment, an edge device **410a-n** may be a computing device associated with a platform user, such as someone who engages with the platform for experience curation or an expert who provides expert judgment scores to platform **400** via, for example, expert judgment marketplace **260** or some other mechanism.

**[0188]** As shown, each edge device **410a-n** may comprise instances of local models **411a-n**, context classification processes **412-n**, and experience curation processes **413a** operating on the device. Each edge device may have access to a local data or knowledge base **420a-n** and which is only accessible by its associated edge device. Edge devices **410a-n** may utilize these components to perform various computations wherein the processing of data and execution of algorithms happens locally on the device, rather than relying on the systems and services provided by platform **400**. In some embodiments, a plurality of edge devices **410a-n** may be implemented as individual computing nodes in a decentralized federated system, wherein tasks and data may be distributed across multiple nodes, allowing for parallel processing and potentially faster computation. Federated systems are often used in scenarios where data privacy and security are important, as data can remain on local nodes and only aggregated or processed results are shared more widely.

**[0189]** In some implementations, the platform **400** may leverage federated learning, where machine learning models **411a-n** are trained across multiple decentralized edge devices **410a-n**, with the models' updates being aggregated centrally. This approach allows for the training of models without the need to centrally store sensitive data from individual devices. For example, each edge device **410a-n** could train local instances of neuro-symbolic GenAI reasoning and action models and local instances of context classification models **412a-n**. According to an embodiment, context classification models **412a-n** may be configured to select relevant passages from a knowledge base **420a-n** or corpus given a query. This can be done using various techniques such as BM25, TF-IDF, or neural retrieval models like dense passage retrieval. The retrieved passages serve as context or input to a generator (e.g., a transformer-based model).

**[0190]** Federated learning can occur at the edge device wherein the context classification model **412a** is trained locally. Periodically, (e.g., hourly, daily, weekly, etc.) platform **400** may collect (e.g., aggregate) model parameters, encrypted data, and/or the like from all of, or a subset of, edge devices **410a-n** and apply the aggregated model parameters as an update to a master or global model (e.g., context classification, neuro-symbolic GenAI model, etc.). The

updated global model or just its parameters, may be transmitted to all of, or a subset of, the edge devices **410a-n** where they may be applied to the local models operating thereon. Similarly, platform **400** can aggregate obtained training data, which may or may not be encrypted, and apply the training data to global models. These updated models may be transmitted to edge devices as described above.

**[0191]** As shown, edge devices **410a-n** may further comprise a curation application **413a-n** operating on the device. Curation application **413a** may be configured to act as an intermediary between a user who can submit a query and models **411a** which receive the query and generate a response back. Curation **413a-n** may receive a response from a locally stored model and curate the response based on user (or entity) defined rules or preferences. For example, a response may first be filtered of any personal information by curation **413a** prior to being relayed back to the user. As another example, curation **413a** may transform the response into specific format, style, or language based on user defined preferences. This allows the edge device **410a** user to have their experience with the local models curated to fit any criteria they deem important.

**[0192]** FIG. 5 is a block diagram illustrating an exemplary architecture for a neuro-symbolic generative AI reasoning and action platform **500** configured to utilize a midserver **530** to act as a computing intermediary between a plurality of edge devices **510a-n** and the platform. According to the embodiment, midserver **530** facilitates communication between edge devices **510a-n** and the backend systems **521, 522, 523, 524** provided by platform **500**. According to the embodiment, midserver **530** may have stored and operating on it one or more neuro-symbolic GenAI reasoning and action models **531**, context classification processes **532**, and curation processes **533**. Midserver **530** can be configured to periodically receive data (e.g., context data) and state information from each of the connected edge devices **510a-n**. Midserver **530** may use this information to train/update the models **531, 532**. Additionally, midserver **530** can be configured to receive user-submitted queries from edge devices via curation **533**, obtain relevant context associated with the received query via context classification **532**, and use a neuro-symbolic GenAI model **531** to process the query and context data to generate a response to the user. The generated response may be curated (or not) and transmitted back to the user of the edge device.

**[0193]** In some implementations, edge devices **510a-n** may have stored upon them local models as described in FIG. 4, and midserver **530** may store global models or even mid-tier models associated with the local models. In such an implementation, midserver can aggregate model parameters and update the global/mid-tier models accordingly.

**[0194]** FIG. 6 is a block diagram illustrating an exemplary mobile device **610a-n** configured for experience curation using embedded capabilities and functionality provided by a neuro-symbolic generative AI reasoning and action platform **600**, according to an embodiment. According to the embodiment, a mobile device **610a** may comprise an operating system **611**, various software applications **612** (e.g., text messaging application, social media application, mobile games, music streaming applications, etc.), a local instance of a neuro-symbolic GenAI model **613**, a context classification model **614**, and an experience curation application **615**. Mobile devices **610a-n** may further comprise a processor, memory, sensors, storage, wireless communication

modules, a display, audio components, and various other components to enable the functionality of a mobile computing device. Mobile devices **610a-n** may connect to platform **600** via a suitable communication network such as the Internet. In some embodiments, mobile device may utilize the systems and services **621, 622, 623, 624** provided by platform to facilitate query-response interactions with a neuro-symbolic GenAI model.

**[0195]** According to the embodiment, mobile device **610a** stores and operates local models **613, 614** and a curation application **615** which can be leveraged during instances when mobile device **610a** is unable to connect with platform **600** or otherwise has an intermittent connection thereby making data transmission difficult, slow, or impossible. In such situations, mobile device **610a** can leverage the local components to perform computation at the edge. A user of mobile device **610a** can use curation application **615** to submit a query to the local neuro-symbolic GenAI model **613**, along with any aggregated context retrieved via context classification **614**. The model **613** can generate a response and send it to curation application **615** where it may be curated (or not) based on the mobile device user's preferences or rules.

**[0196]** In some embodiments, when there is only an intermittent connection to platform **600**, such as when a mobile device is in an area with poor network coverage, various strategies may be implemented to provide functionality to the mobile device user. For example, data (e.g., a user submitted query or prompt) can be temporarily stored in a buffer on the device until a connection to platform **600** is available. Once the connection is reestablished, the buffered data can be transmitted. Likewise, frequently accessed data or recently transmitted data can be cached on the device. This allows the device to access the data locally when a connection to platform **600** is not available. In some implementations, data can be compressed before transmission to reduce the amount of data that needs to be transmitted. This can help to minimize the impact of intermittent connections on data transmission. In some embodiments, mobile device **610a-n** may use protocols that are designed to handle intermittent connections, such as MQTT (Message Queuing Telemetry Transport) or CoAP (Constrained Application Protocol), can help to ensure that data is successfully transmitted even in challenging network conditions. Finally, some use cases may implement an offline mode that allows users to continue using the application (or local instances) and storing data locally until a connection to platform **600** is available again.

**[0197]** FIG. 7 is a block diagram illustrating an exemplary aspect of a distributed generative artificial intelligence reasoning and action platform, a curation computing system **700**. According to the aspect, curation computing system **700** is configured to provide curated (or not) responses from a trained model (e.g., transformer-based model) to received user queries. A curated response may indicate that the response has been filtered, such as to remove personal identifying information or to remove extraneous information from the response, or it may indicate that the response has been augmented with additional context or information relevant to the user. The curation of a response may be based on rules or policies that can be set at an individual user level, an enterprise level, or at a department level for enterprises with multiple departments (e.g., sales, marketing, research, product development, etc.). User/entity rules and/or prefer-

ences may be stored in a data storage system of platform 120 and retrieved by a rules management component 740 during experience curation processes.

[0198] In operation, curation computing 700 receives a user query 701 directed to a neuro-symbolic GenAI model. A query portal 710 may be present and configured to receive a query 701 and prepare it for processing by a GenAI model. For example, a query may be split into tokens, (e.g., words or sub words) which are basic units of the language model. As another example, a text-based query may undergo normalization (e.g., converting to lowercase, removing punctuation, handling special characters, etc.) to ensure consistency and improve model performance. As yet another example, for models that use attention mechanisms, an attention mask may be applied to the input to indicate which tokens should be attended to and which should be ignored. In some implementations, a query portal 710 may be configured to send received queries to an embedding model which can vectorize the received query and store it in a vector database. In such embodiments, stored query embeddings may be used as a form of contextual data which may be retrieved and transmitted with the query to a GenAI model which generates a response based on the received query and contextual data.

[0199] According to the aspect, a response portal 720 is present and configured to receive a response from one a GenAI model and a response management system 730 determines if the received response needs to be curated or not. If the response does not need to be curated, then it may be sent as an uncurated response 702 to the user who submitted the query. Response management 730 can determine if there are any user/entity defined rules or preferences available such as stored in a user/entity profile in a data storage system of platform 120. Rules management 740 can retrieve said rules and response management can curate or otherwise augment the received response based on the user/entity rules or preferences. The result is a curated response 702 which can be transmitted back to the user who submitted the query.

[0200] FIG. 8 is a block diagram illustrating an exemplary aspect of a distributed generative artificial intelligence reasoning and action platform, a marketplace computing system 800. According to the aspect, marketplace computing system 800 is present and configured to develop and integrate various marketplaces 130a-n for data, algorithms, and RAGs into platform 120. Marketplace computing system 800 can provide functionality directed to the registration of experts 810 or entities. An expert may be someone who has a deep understanding and knowledge of a specific industry, including its trends, challenges, technologies, regulations, and best practices. Industry experts often have many years of experience working in the industry and have developed a reputation for their expertise and insights. An expert may be registered by providing proof of identity and qualifications, and creating an expert profile which can store a variety of information about the expert such as their name, industry, credentials, scores (e.g., scores that the expert has assigned to data sources, models/algorithms, model outputs, and/or the like), and reputation. For example, a university professor who specializes in transformer-based algorithms can register as an expert in the realm of generative algorithms. As another example, a virologist could register as an expert and provide scores for academic papers which disclose a new methodology for viral spread modelling. Marketplace com-

puting system 800 may further comprise a market management component 820 which can interface with a plurality of markets 130a-n to integrate information contained therein. A scored data management component 830 may be configured to interface with a browser extension 240 or expert judgment marketplace 260 to retrieve expert scores and store them in an expert judgment score database 270. According to the aspect, an algorithm management component 840 is present and configured to acquire algorithms from algorithm marketplaces to be used in the construction and configuration of neuro-symbolic GenAI models.

[0201] FIG. 9 is a block diagram illustrating a simple example of a distributed computational graph 900 representation for providing neuro-symbolic GenAI capabilities, according to an aspect. According to the aspect, the DCG may be represented as a series of nodes which represent discrete computational or data processing functions, and a series of edges connecting the nodes which represent information or data messages being sent between processing nodes. A DCG can be used to acquire a plurality of context data in the form of an enterprise knowledge base 910. A data transformation node 920 is created to handle the ingestion and transformation of acquired context data. Obtained data may then be sent to a data embedding node 930 which can vectorize the received context data. The vectorized data may flow from the embedding node 930 to a data storage node 950. Data storage node 950 may select the appropriate vector database 980 in which to store the vectorized context data. An input node 940 may allow for a user to submit a query to the workflow. The user query can be sent to data embedding node 930 where it may be vectorized and sent to data storage node 950 for storage in the vector database. The user query can also be sent to a model node 960 which contains the selected model(s) which will process the user query along with any relevant context data obtained from data storage node vector database 980. Model node 960 then processes this information to generate a response which can be sent to output node 970. In some instances, output node 970 may output the response directly to the user. In other instances, output node 970 may be configured to transform the response into a curated response based on user/entity defined rules or preferences.

[0202] FIGS. 10-14 illustrate various exemplary aspects of system architectures of distributed computational graph computing environments. For more detailed information regarding the operation of the various components and aspects described herein with respect to FIGS. 10-14, please refer to U.S. patent application Ser. No. 15/931,534 which is incorporated herein by reference.

[0203] FIG. 10 is a block diagram illustrating an exemplary aspect of an embodiment of a distributed computational graph computing system utilizing an AI enhanced decision platform for external network reconnaissance and contextual data collection. Client access to the system 1005 for specific data entry, system control and for interaction with system output such as automated predictive decision making and planning and alternate pathway simulations, occurs through the system's distributed, extensible high bandwidth cloud interface 1010 which uses a versatile, robust web application driven interface for both input and display of client-facing information via network 1007 and operates a data store 1012 such as, but not limited to MONGODB™, COUCHDB™, CASSANDRA™ or REDIS™ according to various arrangements. Much of the

enterprise knowledge/context data analyzed by the system both from sources within the confines of the enterprise business, and from cloud based sources, also enter the system through the cloud interface **1010**, data being passed to the connector module **1035** which may possess the API routines **1035a** needed to accept and convert the external data and then pass the normalized information to other analysis and transformation components of the system, the directed computational graph module **1055**, high volume web crawler module **1015**, multidimensional time series database (MDTSDB) **1020** and the graph stack service **1045**. The directed computational graph module **1055** retrieves one or more streams of data from a plurality of sources, which includes, but is in no way not limited to, enterprise knowledge, RAGs, expert judgment/scores, a plurality of physical sensors, network service providers, web based questionnaires and surveys, monitoring of electronic infrastructure, crowdsourcing campaigns, and human input device information. Within the directed computational graph module **1055**, data may be split into two identical streams in a specialized pre-programmed data pipeline **1055a**, wherein one sub-stream may be sent for batch processing and storage while the other sub-stream may be reformatted for transformation pipeline analysis. The data is then transferred to the general transformer service module **1060** for linear data transformation as part of analysis or the decomposable transformer service module **1050** for branching or iterative transformations that are part of analysis. The directed computational graph module **1055** can represent all data as directed graphs where the transformations are nodes and the result messages between transformations edges of the graph. The high volume web crawling module **1015** uses multiple server hosted preprogrammed web spiders, which while autonomously configured are deployed within a web scraping framework **1015a** of which SCRAPY™ is an example, to identify and retrieve data of interest from web based sources that are not well tagged by conventional web crawling technology. Data persistence stores such as the multiple dimension time series data store module **1020** may receive streaming data from a large plurality of sensors that may be of several different types. The multiple dimension time series data store module may also store any time series data encountered by the system such as but not limited to enterprise network usage data, component and system logs, environmental context, edge device state information, performance data, network service information captures such as, but not limited to news and financial feeds, and sales and service related customer data. The module is designed to accommodate irregular and high volume surges by dynamically allocating network bandwidth and server processing channels to process the incoming data. Inclusion of programming wrappers **1020a** for languages examples of which are, but not limited to C++, PERL, PYTHON, Rust, GoLang, and ERLANG™ allows sophisticated programming logic to be added to the default function of the multidimensional time series database **1020** without intimate knowledge of the core programming, greatly extending breadth of function. Data retrieved by various data stores such as SQL, graph, key-value, or the multidimensional time series database (MDTSDB) **1020** and the high volume web crawling module **1015** may be further analyzed and transformed into task optimized results by the directed computational graph **1055** and associated general transformer service **1050** and decomposable transformer service **1060**

modules. Alternately, data from the multidimensional time series database and high volume web crawling modules may be sent, often with scripted cuing information determining important vertexes **1045a**, to the graph stack service module **1045** which, employing standardized protocols for converting streams of information into graph representations of that data, for example, open graph internet technology although the invention is not reliant on any one standard. Through the steps, the graph stack service module **1045** represents data in graphical form influenced by any predetermined scripted modifications **1045a** and stores it in a graph-based data store **1045b** such as GIRAPHTM or a key value pair type data store REDISTM, or RIAKTM, among others, all of which are suitable for storing graph-based information.

[0204] Results of the transformative analysis process may then be combined with further client directives, and additional business rules and practices relevant to the analysis and situational information external to the already available data in the automated planning service module **1030** which also runs powerful information theory **1030a** based predictive statistics functions and machine learning algorithms to allow future trends and outcomes to be rapidly forecast based upon the current system derived results and choosing each a plurality of possible business decisions. Using all available data, the automated planning service module **1030** may propose business decisions most likely to result in the most favorable business outcome with a usably high level of certainty. Closely related to the automated planning service module in the use of system derived results in conjunction with possible externally supplied additional information (i.e., context) in the assistance of end user business decision making, the action outcome simulation module **1025** with its discrete event simulator programming module **1025a** coupled with the end user facing observation and state estimation service **1040** which is highly scriptable **1040b** as circumstances require and has a game engine **1040a** to more realistically stage possible outcomes of business decisions under consideration, allows business decision makers to investigate the probable outcomes of choosing one pending course of action over another based upon analysis of the current available data.

[0205] FIG. 11 is a block diagram illustrating another exemplary aspect of an embodiment **1100** of a distributed computational graph computing system utilizing an AI enhanced decision platform. According to an aspect, the integrated platform **1100**, is very well suited to perform advanced predictive analytics and predictive simulations to produce investment predictions. Much of the trading specific programming functions are added to the automated planning service module **1030** of the modified AI enhanced decision platform **1100** to specialize it to perform trading analytics on financial assets, advertisements or content or even marketplace assets. Specialized purpose libraries may include but are not limited to financial markets functions libraries **1151**, Monte-Carlo risk routines **1152**, numeric analysis libraries **1153**, deep learning libraries **1154**, contract manipulation functions **1155**, money handling functions **1156**, Monte-Carlo search libraries **1157**, and quant approach securities routines **1158**. Pre-existing deep learning routines including information theory statistics engine **1159** may also be used. The invention may also make use of other libraries and capabilities that are known to those skilled in the art as instrumental in the regulated trade of items of worth. Data from a plurality of sources used in trade analysis are

retrieved, much of it from remote, cloud resident **1101** servers through the system's distributed, extensible high bandwidth cloud interface **110** using the system's connector module **135** which is specifically designed to accept data from a number of information services both public and private through interfaces to those service's applications using its messaging service **135a** routines, due to ease of programming, are augmented with interactive broker functions **1135**, market data source plugins **1136**, e-commerce messaging interpreters **1137**, business-practice aware email reader **1138** and programming libraries to extract information from video or other multimedia or multimodal data sources **1139**.

**[0206]** Other modules that make up the AI enhanced decision platform may also perform significant analytical transformations on trade related data. These may include the multidimensional time series data store **1020** with its robust scripting features which may include a distributive friendly, fault-tolerant, real-time, continuous run prioritizing, programming platform such as, but not limited to Erlang/OTP **1121** and a compatible but comprehensive and proven library of math functions of which the C++ math libraries are an example **1122**, data formalization and ability to capture time series data including irregularly transmitted, burst data; the GraphStack service **145** which transforms data into graphical representations for relational analysis and may use packages for graph format data storage such as Titan **1145** or the like and a highly interface accessible programming interface an example of which may be Akka/Spray, although other, similar, combinations may equally serve the same purpose in this role **1146** to facilitate optimal data handling; the directed computational graph module **155** and its distributed data pipeline **155a** supplying related general transformer service module **160** and decomposable transformer module **150** which may efficiently carry out linear, branched, and recursive transformation pipelines during trading data analysis may be programmed with multiple trade related functions involved in predictive analytics of the received trade data. Both possibly during and following predictive analyses carried out by the system, results must be presented to clients **1005** in formats best suited to convey both important results for analysts to make highly informed decisions and, when needed, interim or final data in summary and potentially raw for direct human analysis. Simulations which may use data from a plurality of field spanning sources to predict future trade actions or conditions are accomplished within the action outcome simulation module **1025**. Data and simulation formatting may be completed or performed by the observation and state estimation service **1040** using its ease of scripting and gaming engine to produce optimal presentation results.

**[0207]** In cases where there are both large amounts of data to be ingested, schematized, normalized, semantified or otherwise cleansed, enriched or formalized and then intricate transformations such as those that may be associated with deep learning, machine learning, predictive analytics and predictive simulations, distribution of computer tasks and allocation resources across a plurality of systems may be routinely required to accomplish these tasks due to the volume of data being handled and acted upon and practical service level requirements such as availability, timeliness, latency, security metrics or processing guarantees. The AI enhanced platform employs a distributed architecture that is highly extensible to meet these needs. A number of the tasks

carried out by the system are extremely processor intensive and for these, the highly integrated process of hardware clustering of systems, possibly of a specific hardware architecture particularly suited to the calculations inherent in the task, is desirable, if not required for timely completion. The system includes a computational clustering module **1180** to allow the configuration and management of such clusters during application of the AI enhanced decision platform. While the computational clustering module is drawn directly connected to specific co-modules of the AI enhanced decision platform these connections, while logical, are for ease of illustration and those skilled in the art will realize that the functions attributed to specific modules of an embodiment may require clustered computing under one use case and not under others. Similarly, the functions designated to a clustered configuration may be role, if not run, dictated. Further, not all use cases or data runs may use clustering.

**[0208]** FIG. 12 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **1200**, according to one aspect. According to the aspect, a DCG **1200** may comprise a pipeline orchestrator **1201** that may be used to perform a variety of data transformation functions on data within a processing pipeline, and may be used with a messaging system **1210** that enables communication with any number of various services and protocols, relaying messages and translating them as needed into protocol-specific API system calls for interoperability with external systems (rather than requiring a particular protocol or service to be integrated into a DCG **1200**).

**[0209]** Pipeline orchestrator **1201** may spawn a plurality of child pipeline clusters **1202a-b**, which may be used as dedicated workers for streamlining parallel processing. In some arrangements, an entire data processing pipeline may be passed to a child cluster **1202a** for handling, rather than individual processing tasks, enabling each child cluster **1202a-b** to handle an entire data pipeline in a dedicated fashion to maintain isolated processing of different pipelines using different cluster nodes **1202a-b**. Pipeline orchestrator **1201** may provide a software API for starting, stopping, submitting, or saving pipelines. When a pipeline is started, pipeline orchestrator **1201** may send the pipeline information to an available worker node **1202a-b**, for example using AKKATM clustering. For each pipeline initialized by pipeline orchestrator **1201**, a reporting object with status information may be maintained. Streaming activities may report the last time an event was processed, and the number of events processed. Batch activities may report status messages as they occur. Pipeline orchestrator **1201** may perform batch caching using, for example, an IGFS™ caching file-system. This allows activities **1212a-d** within a pipeline **1202a-b** to pass data contexts to one another, with any necessary parameter configurations.

**[0210]** A pipeline manager **1211a-b** may be spawned for every new running pipeline, and may be used to send activity, status, lifecycle, and event count information to the pipeline orchestrator **1201**. Within a particular pipeline, a plurality of activity actors **1212a-d** may be created by a pipeline manager **1211a-b** to handle individual tasks, and provide output to data services **1222a-d**. Data models used in a given pipeline may be determined by the specific pipeline and activities, as directed by a pipeline manager **1211a-b**. Each pipeline manager **1211a-b** controls and directs the operation of any activity actors **1212a-d** spawned

by it. A pipeline process may need to coordinate streaming data between tasks. For this, a pipeline manager **1211a-b** may spawn service connectors to dynamically create TCP connections between activity instances **1212a-d**. Data contexts may be maintained for each individual activity **1212a-d**, and may be cached for provision to other activities **1212a-d** as needed. A data context defines how an activity accesses information, and an activity **1212a-d** may process data or simply forward it to a next step. Forwarding data between pipeline steps may route data through a streaming context or batch context.

**[0211]** A client service cluster **1230** may operate a plurality of service actors **1221a-d** to serve the requests of activity actors **1212a-d**, ideally maintaining enough service actors **1221a-d** to support each activity per the service type. These may also be arranged within service clusters **1220a-d**, in a manner similar to the logical organization of activity actors **1212a-d** within clusters **1202a-b** in a data pipeline. A logging service **1230** may be used to log and sample DCG requests and messages during operation while notification service **1240** may be used to receive alerts and other notifications during operation (for example to alert on errors, which may then be diagnosed by reviewing records from logging service **1230**), and by being connected externally to messaging system **1210**, logging and notification services can be added, removed, or modified during operation without impacting DCG **1200**. A plurality of DCG protocols **1250a-b** may be used to provide structured messaging between a DCG **1200** and messaging system **1210**, or to enable messaging system **1210** to distribute DCG messages across service clusters **1220a-d** as shown. A service protocol **1260** may be used to define service interactions so that a DCG **1200** may be modified without impacting service implementations. In this manner it can be appreciated that the overall structure of a system using an actor-driven DCG **1200** operates in a modular fashion, enabling modification and substitution of various components without impacting other operations or requiring additional reconfiguration.

**[0212]** FIG. 13 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **1200**, according to one aspect. According to the aspect, a variant messaging arrangement may utilize messaging system **1210** as a messaging broker using a streaming protocol **1310**, transmitting and receiving messages immediately using messaging system **1210** as a message broker to bridge communication between service actors **1221a-b** as needed. Alternately, individual services **1222a-b** may communicate directly in a batch context **1320**, using a data context service **1330** as a broker to batch-process and relay messages between services **1222a-b**.

**[0213]** FIG. 14 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **1200**, according to one aspect. According to the aspect, a variant messaging arrangement may utilize a service connector **1410** as a central message broker between a plurality of service actors **1221a-b**, bridging messages in a streaming context **1310** while a data context service **1330** continues to provide direct peer-to-peer messaging between individual services **1222a-b** in a batch context **1320**.

**[0214]** It should be appreciated that various combinations and arrangements of the system variants described above (referring to FIGS. 10-14) may be possible, for example

using one particular messaging arrangement for one data pipeline directed by a pipeline manager **1211a-b**, while another pipeline may utilize a different messaging arrangement (or may not utilize messaging at all). In this manner, a single DCG **1200** and pipeline orchestrator **1201** may operate individual pipelines in the manner that is most suited to their particular needs, with dynamic arrangements being made possible through design modularity as described above in FIG. 12.

**[0215]** FIGS. 15-17 illustrate various exemplary aspects of system architectures and methods of distributed computational graph computing environments. For more detailed information regarding the operation of the various components and aspects described herein with respect to FIGS. 15-17, please refer to U.S. patent application Ser. No. 15/616,427 which is incorporated herein by reference.

**[0216]** FIG. 15 is a block diagram of an architecture for a transformation pipeline within a system for predictive analysis of very large data sets using distributed computational graph computing system **1500**. According to the aspect, streaming input from a data filter software module, **1505** serves as input to the first transformation node **1510** of the transformation pipeline. Each transformation node's function **1510, 1520, 1530, 1540, 1550** is performed on input data stream and transformed output message **1515, 1525, 1535, 1545, 1555, 1565** is sent to the next step. In this aspect, transformation node 2 **1520** has a second input stream **1560**. The specific source of this input is inconsequential to the operation of the invention and could be another transformation pipeline software module, a data store, human interaction, physical sensors, monitoring equipment for other electronic systems or a stream from the internet as from a crowdsourcing campaign, just to name a few possibilities **1560**. For example, a first input stream may comprise enterprise knowledge and a second input stream may comprise RAG data from a RAG marketplace. Functional integration of a second input stream into one transformation node requires the two input stream events be serialized. The illustrated system can perform this serialization using a decomposable transformation software module. While transformation nodes are described according to various aspects as uniform shape, such uniformity is used for presentation simplicity and clarity and does not reflect necessary operational similarity between transformations within the pipeline. It should be appreciated that one knowledgeable in the field will realize that certain transformations in a pipeline may be entirely self-contained; certain transformations may involve direct human interaction, such as selection via dial or dials, positioning of switch or switches, or parameters set on control display, all of which may change during analysis; other transformations may require external aggregation or correlation services or may rely on remote procedure calls to synchronous or asynchronous analysis engines as might occur in simulations among a plurality of other possibilities. For example, engines may be singletons (composed of a single activity or transformation). Furthermore, leveraging the architecture in this way allows for versioning and functional decomposition (i.e. embedding entire saved workflows as single nodes in other workflows). Further according to the aspect, individual transformation nodes in one pipeline may represent functions of another transformation pipeline. It should be appreciated that the node length of transformation pipelines depicted in no way confines the transformation pipelines employed by the

invention to an arbitrary maximum length **1510**, **1520**, **1530**, **1540**, **1550**, as, being distributed, the number of transformations would be limited by the resources made available to each implementation of the invention. It should be further appreciated that there need be no limits on transform pipeline length. Output of the last transformation node and by extension, the transform pipeline, **1550** may be sent back to messaging software module **562** for pre-decided action.

**[0217]** FIG. 21 is a block diagram illustrating an exemplary system architecture for a distributed, composite symbolic and non-symbolic AI platform for advanced reasoning **2120**, according to an embodiment. According to the embodiment, the platform **2120** aims to enable vast automation of modeling/analysis workflows by exploring large potential parameter combinations. Platform **2120** can be configured for extracting and curating knowledge into structured ontologies to complement neuro-symbolic AI capabilities. Platform **2120** can provide an iterative multi-dimensional optimization and evaluation process to explore the relative performance of the different techniques, datasets, and “fitness of purpose” definitions (e.g., security, licenses, traceability/provenance, etc.) associated with a plurality of AI models.

**[0218]** According to the embodiment, platform **2120** is configured as a cloud-based computing platform comprising various system or sub-system components configured to provide functionality directed to the execution of composite symbolic generative AI reasoning and action. Exemplary platform systems can include a distributed computational graph (DCG) computing system **121**, a curation computing system **122**, a marketplace computing system **123**, and a context computing system **124**, a hierarchical process manager computing system **2121**, an embedding refinement computing system **2122**, a multi-modal alignment computing system **2123**, an ontology extraction computing system **2124**, a model blending computing system **2125**, and a hyperparameter optimization computing system **2126**. Platform **2120** may further comprise various databases for storing a plurality of data sets, models **2127**, vectors/embeddings **2128**, and knowledge graphs **2129**. In some embodiments, systems **121-124** and **2121-2126** may each be implemented as standalone software applications or as a services/microservices architecture which can be deployed (via platform **120** or **2120**) to perform a specific task or functionality. In such an arrangement, services can communicate with each other over an appropriate network using lightweight protocols such as HTTP, gRPC, or message queues (e.g., AMQP or Kafka). This allows for asynchronous and decoupled communication between services. Services may be scaled independently based on demand, which allows for better resource utilization and improved performance. Services may be deployed using containerization technologies such as Docker or containerd containerized and orchestrated using container orchestration platforms like Kubernetes. This allows for more flexible deployment and management of services.

**[0219]** The composite symbolic AI reasoning and action platform **2120** can enable a more flexible approach to incorporating machine learning (ML) or artificial intelligence (AI) models into the future of the Internet and software applications; all facilitated by a distributed computational graph (DCG) architecture capable of dynamically creating, persisting, retraining, augmenting, selecting, executing, decommissioning, and incorporating trained

models with both internal and external data sources and marketplaces for data and algorithms and expertise (e.g. expert or layperson or user feedback or knowledge) at the data, model, knowledge, or process levels.

**[0220]** The platform **2120** emphasizes the importance of considering various types of semantics, including, but not limited to, symbolic, distributional, compositional distributional, and information-theoretic compositional distributional semantics. This consideration allows the platform to capture and represent meaning at different levels of abstraction and compositionality, enabling more comprehensive and nuanced understanding of the input data in its original, intermediate, or curated forms. By explicitly addressing these different types of semantics, the platform **2120** can leverage the strengths of each approach and combine them in a unified framework.

**[0221]** In some cases, the platform may be configured to label non-textual data (e.g., images or scenes) with textual descriptions before computing embeddings. This labeling step converts the non-textual data into textual representations (or other representations like image or domain similar to Fourier transforms), which can then be processed using language-based techniques that are more well-developed and understood or consistent or otherwise advantageous. By bridging the gap between non-textual and textual data through labeling, the platform can take advantage of the rich semantic information captured by language models and embeddings into text or alternative media or domain formats. After labeling non-textual data (if applicable), the platform computes numerical embedding representations of the input data in a given format. These embeddings capture the semantic properties and relationships of the data in a dense vector format, enabling efficient storage, retrieval, and comparison. The computed embeddings may then be persisted in memory or in a database such as a vector database, which allows for fast and scalable similarity search (e.g., cosine, dot product, Euclidean, etc.) and other vector operations or graph operations or hybrid representations depending on the data type, representation, and elements such as facts, spatial or temporal dynamics of the systems and/or entities of interest. The persisted embeddings serve as input features for downstream ML or AI models, such as neural networks or symbolic reasoning engines, or knowledge bases. By incorporating the embeddings or representations into these versioned models, the platform can leverage the information captured by the embeddings to improve the performance and generalization of the AI system under different operating environments or conditions and assess ongoing fitness for purpose using ongoing pipeline fitness evaluation functions executed on event or periodic basis. The integration of embeddings with downstream models allows for seamless knowledge accumulation and transfer and enables the AI system to make informed curation and event or context-based decisions based on the semantic understanding of observed input data, simulated input data, submitted user actions, submitted event data, ongoing system state information or operational information or simulated versions of potential versions of the aforementioned elements.

**[0222]** According to the embodiment, platform **2120** utilizes a plurality of neural network models that generate vector embeddings representing input data. The plurality of neural network models may be stored in model database **2126**. Each of the plurality of neural network models may be

associated with a specific type of AI system (e.g., gaming, medical diagnosis, sentiment analysis, LLM, recommendation system, virtual reality, autonomous vehicle, etc.). As such, models and AI systems may be used interchangeably throughout this specification. Platform can use various neural network architectures as previously detailed such as Transformers, Long Short-Term Memory (LSTM), or convolutional neural networks (CNNs) to process different types of input data (text, images, audio, video, 3d or 4-d models, etc.). In some implementations, platform can train these models on large datasets to learn meaningful vector, graph, or SQL or NOSQL representations that capture the properties and relationships of the input data-ideally based on semantified representations of the data but also on unstructured, structured, schematized, normalized or partially semantified basis. Platform may leverage techniques like transfer learning, fine-tuning, or multi-task learning to improve the quality and generalizability of the embeddings. For example, a text classification system that uses a BERT model to generate embeddings for input documents, and a CNN model to generate embeddings for images associated with the documents. The embeddings may then be concatenated and fed into a final classification layer.

[0223] Embeddings are dense vector representations that capture the semantic meaning and relationships of data points. Vector databases 2128 store and index these embeddings for efficient retrieval and similarity search. Platform 2120 can facilitate iterative refinement which updates the embeddings based on new data or feedback to improve their quality and representational power. For example, a recommendation AI system uses embeddings to represent user preferences and item characteristics. As users interact with the system, their feedback is used to iteratively refine the embeddings, making them more accurate predictors of user interests. The refined embeddings are stored in a vector database for fast retrieval during recommendation generation.

[0224] According to the embodiment, a knowledge graph database 2129 is present comprising symbolic facts, entities, and relations. Platform may use an ontology or schema for the knowledge graph that defines the types of entities, relationships, and attributes relevant to a given AI system's domain. Platform populates the knowledge graph with data from structured sources (e.g., databases) and unstructured sources (e.g., text documents) using information extraction techniques like named entity recognition, relation extraction, and/or co-reference resolution. Knowledge graph database 2129 may be implemented as a graph database (e.g., Neo4j, ArangoDB) or a triple store (e.g., Apache Jena) to efficiently store and query the knowledge graph. Knowledge graph database 2129 may comprise a plurality of knowledge graphs, wherein knowledge graphs may be associated with a specific domain. For example, a biomedical knowledge graph that contains entities such as drugs, diseases, and genes, and relationships like "treats", "causes", and "interacts\_with". This exemplary knowledge graph is populated from structured databases like DrugBank and UniProt, as well as from semi-structured or unstructured sources like publications, Internet crawl data, video, text, audio files.

[0225] According to the embodiment, hierarchical process manager computing system 2121 is present and configured to route processing based on certainty thresholds (e.g., certification) and challenge-based verification. Platform may define a hierarchy of reasoning tasks and subtasks that

break down the AI system's (e.g., models) decision-making process into manageable steps. Process manager 2121 orchestrates the execution of these tasks and routes data to the appropriate models or knowledge sources based on predefined rules or learned policies. Process manager 2121 or an administrator may set certainty thresholds for each task to determine when the system should proceed to the next step or seek additional information/verification. Process manager 2121 can design and leverage challenge-based verification mechanisms (e.g., adversarial examples, counterfactual reasoning, etc.) to test the robustness and reliability of the AI system's decisions. For example, a fraud detection system that first uses a rule-based model to flag potentially fraudulent transactions based on simple heuristics. If the certainty of the rule-based model is below a threshold or specific score range or constraint, the transaction is routed to a more complex machine learning model for further analysis. The final decision is then verified through a challenge-response mechanism that asks the user to provide additional authentication. Thresholds or scores may also be defined by functions, such as a first order differential equation to enable more complex score dynamics.

[0226] Hierarchical process definitions break down complex reasoning tasks into smaller, more manageable steps. The system may note decomposable workflows which can be independently evaluated and also evaluations which require coordination or contextualization based on ongoing feedback from aggregated data or evaluation results and therefore require intermediate state sharing across resources at the actor, virtual or physical resource level. Specialized routing dynamically selects the most appropriate AI models or knowledge sources for each subtask based on their capabilities and performance. For example, an autonomous vehicle AI system uses a hierarchical process to handle different driving situations. At a top level, the platform decides whether to use models specialized for highway driving, city navigation, or parking. Within each specialization, further routing occurs to handle specific challenges like merging, pedestrian detection, or parallel parking.

[0227] Certification involves validating the performance and reliability of AI models through rigorous testing and evaluation. Challenge-based verification sets up specific test cases or benchmarks that models must pass to be considered certified for a given task. Model blending combines the outputs of multiple models using weighted averaging or more sophisticated methods to improve overall performance. For example, a financial forecasting AI system blends the predictions of several certified models, each specializing in different asset classes or market conditions. The blending weights are adjusted based on each model's historical performance and current market challenges.

[0228] According to the embodiment, embedding refinement computing system 2122 is present and configured to incorporate data from one or more knowledge graphs. Embedding refinement 2122 may utilize algorithms that can query the knowledge graph to retrieve relevant facts, entities, and relationships based on the input data and the current reasoning context. Retrieved knowledge may be used to refine the vector embeddings generated by the neural networks models, incorporating symbolic information into the distributed representations (embeddings). In some implementations, techniques like attention mechanisms, graph convolutions, and/or knowledge-aware language models to effectively combine the embeddings with the knowledge

graph data. For example, consider a recommendation system that generates initial embeddings for users and items based on their interaction history. The platform then queries a knowledge graph of user demographics, item categories, and contextual factors (e.g., time, location) to retrieve relevant information. This information can be used to refine the user and item embeddings through, for example, a graph attention network, incorporating the contextual knowledge into the recommendations.

[0229] A Graph Attention Network (GAT) is a type of neural network architecture designed to operate on graph-structured data. It leverages the concept of self-attention to compute the importance of neighboring nodes in a graph, allowing the network to focus on the most relevant information when making predictions or generating representations. The key advantage of GATs is their ability to capture the importance of neighboring nodes based on their feature compatibility, allowing the network to focus on the most relevant information. This attention mechanism enables GATs to effectively handle graph-structured data and learn meaningful representations of nodes and their relationships.

[0230] According to the embodiment, model blending computing system 2125 is present and configured to apply expressive weighting schemes to model combinations. Platform may leverage a model blending architecture that can combine the outputs of multiple neural network models based on their individual strengths and weaknesses. Such a system may use weighting schemes that can dynamically adjust the contribution of each model based on factors like uncertainty, task complexity, or domain relevance. Techniques such as Bayesian model averaging, mixture of experts, and/or ensemble learning may be implemented to optimally blend the model outputs. For example, consider a sentiment analysis system that combines the outputs of three models: a Naive Bayes model, an LSTM model, and a BERT model. Model blending 2125 assigns weights to each model based on their confidence scores and the complexity of the input text. The weights are learned through a reinforcement learning approach that optimizes the overall sentiment classification performance, to include optional looping through vectorized embeddings of suggested content and then symbolic searches through knowledge graphs where RDF or OWL or other ontologies aid in comparing formalized knowledge to the vector similar content to the original three models.

[0231] According to the embodiment, platform 2120 implements feedback loops considering security, licensing, provenance, and collaborative development. Feedback loops allow the AI system to learn and adapt based on real-world performance and user feedback. Security considerations ensure that the AI system is protected against malicious attacks or misuse. For example, implementing secure communication protocols and access controls mechanisms to protect sensitive data and prevent unauthorized access to the AI system. Economic factors optimize the cost-benefit trade-offs of different model configuration and deployment strategies. Licensing takes into account the legal rights and restrictions associated with using certain datasets or model components. Platform 2120 can monitor and ensure compliance with the terms and conditions of licensing of datasets, models, and tools used by the platform. Traceability/provenance keeps track of the lineage of data sources, training processes, and model versions used in each output. Model collaboration enables different teams or organizations

to jointly develop, test, deploy, and improve AI models while maintaining security and provenance. For example, a healthcare AI system incorporates feedback from doctors and patients to continually refine its diagnosis and treatment recommendations. The system logs each decision's provenance and securely shares performance data with research partners under appropriate licensing terms. As another example, consider a federated learning system for medical image analysis that allows multiple hospitals to collaboratively train a deep learning model without sharing raw patient data. The system uses secure multi-party computation and differential privacy techniques to protect patient privacy. The model's provenance is tracked using a blockchain-based ledger, ensuring transparency and accountability. The system also includes a licensing management component that enforces usage restrictions based on each hospital's data sharing agreements.

[0232] According to the embodiment, multi-modal computing system 2123 is present and configured to align and synchronize representations across different data modalities (e.g., text, images, audio, etc.) to create a unified and consistent representation of the input data. Multi-modal system 2123 may implement techniques such as cross-modal attention, multi-modal fusion, and/or joint embedding spaces to effectively combine information from different modalities. Platform can utilize domain-specific knowledge (e.g., physics, psychology) (from knowledge graphs) to ensure the generated representations are consistent and realistic across modalities. For example, consider a virtual assistant that can process user queries in the form of text, speech, and images. The multi-modal system 2123 uses cross-modal attention to align the representations of the different input modalities, creating a unified query representation. For example, if the user asks, "What is the breed of the dog in this picture?", the engine aligns the image embedding with the relevant parts of the text embedding to understand that the query is about identifying the dog breed.

[0233] According to the embodiment, hyperparameter optimization computing system 2126 is present and configured to use information theoretic guidance for optimization tasks. System 2126 may implement an automated hyperparameter optimization framework (e.g., Bayesian optimization, evolutionary algorithms, etc.) to search for the best combination of model architectures, training settings, and embedding techniques. System 2126 can use information-theoretic measures (e.g., mutual information, Kullback-Leibler divergence) to guide the optimization process and select hyperparameters that maximize the information content and generalization ability of the learned representations. In some implementations, platform 2120 may develop efficient parallel computing strategies to speed up the hyperparameter search process and explore a larger space of configurations. For example, consider a natural language generation system that uses a variational autoencoder (VAE) to generate diverse and coherent sentences. The hyperparameter optimization system 2126 uses Bayesian optimization to search for the best combination of latent space dimensionality, regularization strength, and decoder architecture. The optimization is guided by an information-theoretic objective that maximizes the mutual information between the latent space and the generated sentences, ensuring that the VAE captures meaningful and interpretable representations.

[0234] In some embodiments, hyperparameters may also be defined by expert judgment via experts and made available via a hyperparameter expert judgment marketplace.

[0235] According to the embodiment, hyperparameter optimization computing system 2126 may be configured or continuously adjusting and optimizing the hyperparameters of machine learning models based on performance metrics and user feedback, and for dynamically updating and fine-tuning machine learning/AI models based on newly available data and evolving user requirements. The platform can dynamically update and fine-tunes machine learning models based on newly available data and evolving user requirements. This allows the models to adapt to changing data patterns and user needs in real-time. According to an embodiment, hyperparameter optimization computing system 2126 is configured for optimizing the retrieval and generation components of RAG models, including fine-tuning retrieval algorithms, updating knowledge bases, and enhancing generation quality. The computing system 2126 may implement a feedback loop mechanism for incorporating user feedback and preferences into the optimization process, ensuring continuous improvement and alignment with user expectations.

[0236] Embedding generation techniques convert raw data into dense vector representations. Different techniques (e.g., Word2Vec, GloVe, BERT, etc.) have different strengths and weaknesses. Training data selection and processing impact the quality and generalizability of the learned embeddings. Model type (e.g., perceptron, feedforward, radial basis network, deep feed forward, recurrent, long-short term memory, gated recurrent unit, auto encoder, variational autoencoder, denoising auto encoder, sparse autoencoder, Markov chain, Hopfield network, Boltzmann machine, restricted Boltzmann machine, deep belief network, deep convolutional network, convolutional network, deconvolutional network, deep convolutional inverse graphics network, general adversarial network, liquid state machine, extreme learning machine, echo state network, deep residual network, Kohonen network, support vector machine, neural tuning machine etc.) and architecture (e.g., number of hidden layers, hidden units, etc.) influence the embedding learning process. Hyperparameter optimization searches and explorations for the best combination of embedding generation technique, training data, model type, and architecture to maximize the embedding quality and downstream task performance. For example, a sentiment analysis AI system experiments with different embedding generation techniques (Word2Vec, GloVe) and model architectures (long short-term memory, convolutional neural network) and dimensionality reduction techniques (e.g., none vs PCA vs ICA vs information sieve) to find the best combination for the specific domain and language as well as different system states (e.g. based on clustering algorithms for different operational modalities). The platform also tunes hyperparameters such as, for example, embedding dimensionality, context window size, randomness/temperature and learning rate to further improve performance or other measures of efficacy based on a narrow or system-wide or process-wide objective or fitness function.

[0237] Information theory provides another exemplary mathematical framework for quantifying and understanding the properties of embeddings, such as their information content or gain when compared to an alternative, compression, and generalization ability. Theoretical analysis may

apply information-theoretic concepts and measures to study the effectiveness of different embedding methods and guide their development or data set or model or parameter or encoding/serialization/compression. For example, platform 2120 analyzes the mutual information between word embeddings and their context to quantify the amount of semantic information captured or gained. Platform may then use this analysis to propose a new embedding method that maximizes mutual information while minimizing redundancy, resulting in more informative and compact representations on either a marginal or absolute basis, or both.

[0238] According to the embodiment, ontology extraction computing system 2124 is present and configured to link data elements, facts, or embeddings to symbolic knowledge graphs or ontological entities. Connectionist models (e.g., neural networks) learn distributed representations that capture patterns and relationships in data, but these representations are not directly interpretable as symbolic knowledge. Extracting symbolic representations involves techniques like rule extraction, decision tree induction, or clustering to distill the learned knowledge into a symbolic form in terms of both allowed elements in an ontology or instances of such elements. Linking the extracted symbolic representations to existing knowledge graphs (or extending or amending underlying ontologies dynamically based on accumulated data or experiences) enables the integration of the learned knowledge with or without prior domain expertise, facilitating more comprehensive and explainable reasoning for both connectionist and symbolic modeling regimes as well as for simulation based modeling initiatives supporting synthetic data generation for simulation-based and empirical real-world observation and refinement. For example, a medical diagnosis AI system based on a deep neural network learns to classify diseases from patient data. The platform bb extracts symbolic rules or representations from data of interest via a model (e.g., a trained network), expressing the learned decision boundaries in terms of interpretable clinical features. These rules are then linked to a medical knowledge graph consisting of both an ontological framework, a corresponding query formalism, and a data set consisting of allowed ontology instances and characteristics, allowing the system to explain both its available reasoning in terms of known disease mechanisms and treatment guidelines. It is important to note that every version of such a composite knowledge corpus may be numbered or uniquely identified as an element of a given decision, model training, or other system action for its stated purpose or for administrative or maintenance/system operation functions.

[0239] Ontology extraction system 2124 can leverage algorithms that can analyze the learned vector embeddings and extract symbolic representations (e.g., entities, relationships, rules, etc.) that capture the underlying semantic structure. In some implementations, techniques such as, for example, clustering, dimensionality reduction, and/or rule mining may be used to capture the underlying semantic structure. Ontology alignment and linking methods can be used to map the extracted symbolic representations to existing concepts and relationships in the knowledge graph, enabling seamless integration of the learned knowledge with prior domain expertise. For example, consider a legal case analysis system that uses a BERT model to generate embeddings for legal documents. The ontology extraction system can use hierarchical clustering to group the embeddings into semantically related clusters, and then apply association rule

mining to discover relationships between the clusters. The extracted ontology is then linked to a legal knowledge graph that contains concepts like laws, precedents, and jurisdictions, enabling the system to reason about legal cases using both the learned embeddings and the symbolic knowledge.

[0240] Symbolic knowledge represents facts, rules, and relationships using structured formalisms like ontologies or knowledge graphs. Connectionist models, such as neural networks, learn distributed representations from data with explicit symbolic structure. Retrieval augmented generation (RAGs) enhance language models by incorporating an external knowledge retrieval mechanism. During the generation process, the model queries a knowledge base to retrieve relevant information and condition its outputs on both the input context and the retrieved knowledge. Expressive weightings allow the platform to dynamically adjust the influence of different knowledge sources based on their relevance to the current context. For example, a customer support AI system uses a knowledge graph of product information and troubleshooting procedures (symbolic) alongside a neural language model trained on past support interactions (connectionist). When generating responses to customer inquiries, the system employs RAG to retrieve relevant information from the knowledge graph and the language model to condition the responses on both the customer's input and the retrieved knowledge. The system assigns higher weights to knowledge sources that are more pertinent to the specific inquiry, ensuring accurate and context-appropriate responses.

[0241] According to the embodiment, platform 2120 can implement scene generation with knowledge graph elements for contextual refinement. Scene generation creates realistic images, videos, or three-dimensional (3D) environments based on textual descriptions or other input data. Knowledge graph elements, such as object properties, relationships, and constraints, can be leveraged to guide the scene generation process to ensure consistency and realism. Contextual refinement adjusts the generated scene based on the specific context and purpose of the AI application. For example, a virtual reality AI system generates immersive scenes for training simulations. The platform can use a knowledge graph of object properties (e.g., materials, size, physics) and relationships (e.g., spatial constraints) to ensure physically plausible layouts. The generated scenes may be refined based on the specific training scenario and user interactions.

[0242] In addition to visual and textual data, platform 2120 incorporates other sensory modalities like sound and smell to create more immersive and realistic experiences. Harmonizing multiple senses involves aligning and synchronizing the different modalities to create a coherent and consistent output. For example, a gaming AI system generates realistic soundscapes and ambient scents to match the visual environment. The platform 2120 ensures that the sound of footsteps matches the character's movement and the smell of a forest scene includes the scent of pine trees and damp moss.

[0243] According to some embodiments, platform 2120 can be leveraged to develop enterprise-specific or domain-specific models, which can be "small models" that are more efficient, accurate, or predictable in specific contexts and prompts. These small models can be integrated into platform 2120 as specialized components that are selected and deployed based on the specific domain or task at hand. Hierarchical process manager 2121 can route the input data

to the appropriate small model based on the context, ensuring optimal performance and efficiency.

[0244] Furthermore, platform 2120 can provide effective orchestration, selection, and management of small models, particularly in restricted or regulated domains such as medicine, investing, law, insurance, and banking. Platform's model blending system 2125 and feedback loops can be extended to incorporate the orchestration and management of small models, taking into account factors such as data nutrition labels, model labels, and administrative processes. The system can leverage existing system/platforms, and ML ops to facilitate the effective deployment and governance of small models.

[0245] In some implementations, the platform can train and deploy hybrid models that combine foundational connectionist models with additional symbolic models, simulations, or datasets and training processes to generate explanations, estimations, and specialized model combinations with different performance characteristics or fitness regimes or envelopes based on their provenance, included data or modeling elements, or even the people or other algorithms or AI agents involved in their creation or execution. The platform can incorporate these hybrid models as part of its model blending and composition capabilities, leveraging the strengths of different models for tasks such as explainability, auditing, and ML ops training/supervision. The ontology extraction system 2124 can help in generating explanations and traces from these hybrid models, enhancing the interpretability and transparency of the system's reasoning process.

[0246] The platform addresses the security and intellectual property concerns associated with foundational models, which are considered core IP and may be less likely to be exposed due to their immense cost, time, and sensitivity. The platform can utilize small models as a means of model obfuscation, where the sensitive foundational models are distilled into smaller, more focused models that can be deployed with less risk of information leakage. The platform can also incorporate techniques for model theft detection, such as using vector similarity scoring and hash-based functions to identify potential infringement of small models derived from foundational models.

[0247] The platform can leverage the use of ML ops optimization routines for model selection, training, classification, and dynamic deployment based on fitness for purpose. The platform can integrate these optimization techniques to dynamically select and deploy the most suitable small models based on the specific task, context, and performance requirements. The platform can also optimize model hyperparameters, such as temperature and token length, to balance performance, efficiency, and the generation of hallucinations or other undesired outputs.

[0248] By integrating the concepts and techniques related to small models, the platform can achieve greater efficiency, specialization, explainability, security, and adaptability. The use of domain-specific small models allows the system to tailor its reasoning and decision-making processes to specific contexts, while the orchestration and management capabilities ensure the effective deployment and governance of these models. The hybrid models and explainability techniques enhance the interpretability and transparency of the platform, enabling users to understand and trust its reasoning process. Simulations and uncertainty quantification routines to isolate the factors influencing deviation

between expected and actual observations in empirical and synthetic data sets may be handled by the system, to include via DCG specified processes, to guide ongoing model and simulation training and fitness and selection routines and to guide AI agent and or human decision makers in the evaluation of data, ontology, model, simulation or process level decisions or fitness for a given situation or task. The model obfuscation and theft detection mechanisms may help protect the intellectual property and sensitive information associated with the core foundational models. Overall, the integration of small models into platform 2120 aligns with the broader goals of achieving advanced reasoning, adaptability, explainability, and security in AI systems. By leveraging the strengths of small models and incorporating them into the various components and processes of the system, the platform aims to push the boundaries of AI capabilities while addressing the practical challenges and requirements of real-world applications.

[0249] In some implementations, platform 2120 can be configured to provide capabilities directed to automatic error identification and correction, such as those provided by a self-healing neural graph AI. This AI system continuously monitors the operation of the computing device's hardware and software components, identifying anomalies, errors, or suboptimal performance. Upon detecting an issue, the self-healing neural graph AI dynamically reconfigures the system's resources, reroutes data flows, and adapts the computing graph to mitigate the problem and maintain optimal performance. This autonomous error identification and correction mechanism enhances the computing device's reliability, resilience, and ability to operate in demanding or unpredictable environments without the need for manual intervention.

[0250] FIG. 22 is a block diagram illustrating an exemplary model architecture of the Transformer, consisting of an Encoder (the components on the left side of the illustration) and a Decoder (the components on the right side of the illustration). Transformers form the backbone of large language models. A large language model (LLM) is a type of artificial intelligence algorithm that utilizes deep learning techniques and massively large datasets to understand, summarize, generate and predict new content. The term generative AI is also closely connected to LLMs, which are a type of generative AI that has been specifically architected to help generate text-based content. All language models are first trained on a set of data, and then they make use of various techniques to infer relationships and then generate new content based on the trained data. Language models are commonly used in natural language processing (NLP) applications where a user inputs a query in natural language to generate a result.

[0251] An LLM is the evolution of the language model concept in AI that dramatically expands the data used for training and inference. In turn, it provides a massive increase in the capabilities of the AI model. While there isn't a universally accepted figure for how large the data set for training needs to be, an LLM typically has at least one billion or more parameters. Parameters are a machine learning term for the variables present in the model on which it was trained that can be used to infer new content.

[0252] Modern LLMs that have emerged within the last decade are based on transformer models, which are neural networks commonly referred to as transformers. With a large number of parameters and the transformer model, LLMs are

able to understand and generate accurate responses rapidly, which makes the AI technology broadly applicable across many different domains. Some LLMs are referred to as foundation models, a term coined by the Stanford Institute for Human-Centered Artificial Intelligence in 2021. A foundation model is so large and impactful that it serves as the foundation for further optimizations and specific use cases.

[0253] LLMs take a complex approach that involves multiple components. At the foundational layer, an LLM needs to be trained on a large volume, sometimes referred to as a corpus, of data that is typically petabytes in size. The training can take multiple steps, usually starting with an unsupervised learning approach. In that approach, the model is trained on unstructured data and unlabeled data. The benefit of training on unlabeled data is that there is often vastly more data available. At this stage, the model begins to derive relationships between different words and concepts.

[0254] The next step for some LLMs is training and fine-tuning with a form of self-supervised learning. Here, some data labeling has occurred, assisting the model to more accurately identify different concepts.

[0255] Next, the LLM undertakes deep learning as it goes through the transformer neural network process. The transformer model architecture enables the LLM to understand and recognize the relationships and connections between words and concepts using a self-attention mechanism. That mechanism is able to assign a score, commonly referred to as a weight, to a given item (called a token) in order to determine the relationship.

[0256] Once an LLM has been trained, a base exists on which the AI can be used for practical purposes. By querying the LLM with a prompt, the AI model inference can generate a response, which could be an answer to a question, newly generated text, summarized text or a sentiment analysis report.

[0257] LLMs have become increasingly popular because they have broad applicability for a range of NLP tasks, including but not limited to, text generation, translation, content summary, rewriting content, classification and categorization, sentiment analysis, and conversational AI and chatbots.

[0258] There are numerous advantages that LLMs provide to organizations and users including, for example, extensibility and adaptability, flexibility, performance, accuracy, and ease of training. LLMs can serve as a foundation for customized use cases. Additional training on top of an LLM can create a finely tuned model for an organization's specific needs. One LLM can be used for many different tasks and deployments across organizations, users and applications. Modern LLMs are typically high-performing, with the ability to generate rapid, low-latency responses. As the number of parameters and the volume of trained data grow in an LLM, the transformer model is able to deliver increasing levels of accuracy. Many LLMs are trained on unlabeled data, which helps to accelerate the training process.

[0259] While there are many advantages to using LLMs, there are also several challenges and limitations such as, development costs (e.g., LLMs generally require large quantities of expensive graphics processing unit hardware and massive data sets), operational costs, bias, hallucination (e.g., AI hallucination occurs when an LLM provides an inaccurate response that is not based on trained data), complexity (e.g., with billions, or more, of parameters, modern LLMs are exceptionally complicated technologies

that can be particularly complex to troubleshoot), and glitch tokens which are maliciously designed prompts to cause the LLM to malfunction.

**[0260]** There is an evolving set of terms to describe the different types of large language models. Among the common types are zero-shot models, fine-tuned or domain-specific models, language representation models, and multimodal models. A zero-shot model is a large, generalized model trained on a generic corpus of data that is able to give a fairly accurate result for general use cases, without the need for additional training. GPT-3 is often considered a zero-shot model. Fine-tuned/domain-specific models require additional training on top of a zero-shot model and can lead to a fine-tuned, domain-specific model. One example is OpenAI Codex, a domain-specific LLM for programming based on GPT-3. One example of a language representation model is Bidirectional Encoder Representations from Transformers (BERT), which makes use of deep learning and transformers well suited for NLP. Originally LLMs were specifically tuned just for text, but with the multimodal approach it is possible to handle both text and images. GPT-4 is an example of this type of model.

**[0261]** There are multiple important components significantly influencing the architecture of LLMs. The size of an LLM, often quantified by the number of parameters, greatly impacts its performance. Larger models tend to capture more intricate language patterns but require increased computational resources for training and inference. Effective input representations, like tokenization, are vital as they convert text into formats that the model can process. Special tokens, like [CLS] and [September] in BERT, enable the model to understand sentence relationships and structure. Pre-training objectives define how a model learns from unlabeled data. For instance, predicting masked words in BERT helps the model learn contextual word relationships, while autoregressive language modeling in GPT-3 teaches coherent text generation. The computational demands of LLMs can be mitigated through techniques like knowledge distillation, model pruning, and quantization. These methods maintain model efficiency without sacrificing performance. How a model generates output is essential. Greedy decoding, beam search, and nucleus sampling are techniques used in LLMs for coherent and diverse output generation. These methods balance between accuracy & creativity, while creating a significant difference between LLMs and traditional language models.

**[0262]** The illustrated Transformer comprises an Encoder and a Decoder. The Encoder takes input embeddings and processes them through a stack of layers (represented as dashed box 2210). Each layer consists of: positional encoding, which adds position information to the input embeddings; multi-head attention, which allows the model to attend to different parts of the input sequence; add and norm, which applies residual connection and layer normalization; feed forward, which is a fully connected feed-forward network; and add and norm which is another residual connection and layer normalization.

**[0263]** The power of the transformer model lies in the self-attention mechanism. This mechanism contributes to accelerated learning compared to traditional models such as long short-term memory models. Self-attention empowers the transformer model with the remarkable capability to meticulously scrutinize distinct segments of a given sequence or even encompass the entire contextual essence of

a sentence. This profound contextual awareness enables the model to make predictions with an elevated degree of accuracy and relevance.

**[0264]** The input embedding 2201 to the Encoder is a sequence of tokens, typically represented as integers. Each token is mapped to a learnable embedding vector of a fixed size. The embedding layer is a lookup table that converts each token into its corresponding dense vector representation. The embeddings are learned during training and capture semantic and syntactic relationships between tokens.

**[0265]** A dense vector representation, also known as a dense embedding or a continuous vector representation, is a way of representing data, particularly words or tokens, as dense vectors in a high-dimensional continuous space. In the context of natural language processing (NLP) and language models, dense vector representations are used to capture semantic and syntactic information about words or tokens. Each word or token is mapped to a fixed-size vector of real numbers, typically with hundreds or thousands of dimensions. Each word or token is represented by a vector of a fixed size, regardless of the length of the input sequence. The size of the vector is a hyperparameter that is determined during model design. The vectors exist in a continuous high-dimensional space, where each dimension represents a latent feature or aspect of the word or token. The continuous nature allows for capturing fine-grained relationships and similarities between words. The dense vector representations are learned during the training process of the model. The model learns to assign similar vectors to words that have similar meanings or occur in similar contexts. The dense vector representations aim to capture semantic and syntactic relationships between words. Words that have similar meanings or are used in similar contexts tend to have similar vector representations. Dense vector representations allow for performing algebraic operations on words, such as addition and subtraction. These operations can capture analogies and relationships between words, such as “prince”–“man”+“woman”=“princess”. Dense vector representations serve as input features for various downstream NLP tasks, such as text classification, sentiment analysis, named entity recognition, and machine translation. The dense representations provide a rich and informative input to the models, enabling them to learn patterns and make predictions. Some popular examples of dense vector representations include, but are not limited to, Word2Vec, Global Vectors for Word Representations (GloVe), FastText, and BERT.

**[0266]** After the input embedding layer, positional encoding 2202 is added to the input embedding to provide position information to the model. Since the Transformer architecture doesn't have inherent recurrence or convolution, positional encodings help capture the order and relative positions of tokens. The positional encodings are typically sine and cosine functions of different frequencies, allowing the model to learn relative positions. The positional encodings have the same dimensionality as the input embeddings and are summed with them.

**[0267]** The Encoder utilizes a multi-head attention mechanism 2203 which is a key component of the Transformer architecture. It allows the Encoder to attend to different parts of the input sequence and capture dependencies between tokens. The attention mechanism computes three matrices: Query (Q), Key (K), and Value (V). The Query, Key, and Value matrices are obtained by linearly projecting the input

embeddings using learned weight matrices. The attention scores are computed by taking the dot product of the Query matrix with the transpose of the Key matrix, followed by scaling and applying a softmax function. The attention scores determine the importance of each token in the input sequence for a given position. The Value matrix is then multiplied with the attention scores to obtain the weighted sum of the values, which forms the output of the attention mechanism. Multi-Head Attention splits the Query, Key, and Value matrices into multiple heads, allowing the model to attend to different aspects of the input simultaneously. The outputs from each head are concatenated and linearly projected to obtain the final output of the Multi-Head Attention layer 2203.

[0268] After the Multi-Head Attention layer, a residual connection is applied, followed by Layer Normalization at add and norm 2204. The residual connection adds the input embeddings to the output of the attention layer, helping the model learn faster and deeper. Layer Normalization normalizes the activations across the features, stabilizing the training process.

[0269] The Feed Forward layer 2205 is a fully connected neural network applied to each position of the Encoder's hidden states. It consists of two linear transformations with a Rectified Linear Unit (ReLU) activation function in between. The purpose of the Feed Forward layer is to introduce non-linearity and increase the model's capacity to learn complex representations. The output of the Feed Forward layer has the same dimensionality as the input embeddings. A residual connection and Layer Normalization 2204 are applied after the Feed Forward layer.

[0270] The Encoder layers 2210 are stacked Nx times, where N is a hyperparameter that determines the depth of the Encoder. Each layer follows the same structure: Multi-Head Attention, Add & Norm, Feed Forward, and Add & Norm. By stacking multiple Encoder layers, the model can capture hierarchical and long-range dependencies in the input sequence. The output of the final Encoder layer represents the encoded input sequence, which is then passed to the Decoder for generating the output sequence.

[0271] The Decoder generates the output probabilities. It has a similar structure to the Encoder, with a few additions. The Decoder takes output embeddings and processes them through a stack of layers (represented as dashed box 2220). The output embedding layer 2206 takes the previous output tokens (shifted right by one position) and converts them into dense vectors. Each token is mapped to a learnable embedding vector of a fixed size. The embedding vectors capture semantic and syntactic relationships between tokens.

[0272] Positional encoding 2207 is added to the output embedding to provide position information to the model. Since the Transformer architecture does not have inherent recurrence or convolution, positional encodings help capture the order and relative positions of tokens. The positional encodings are typically sine and cosine functions of different frequencies, allowing the model to learn relative positions.

[0273] The masked multi-head attention 2208 mechanism prevents the model from attending to future tokens. This layer performs self-attention on the Decoder's input sequence. It allows the Decoder to attend to different parts of its own input sequence. The attention is "masked" to prevent the Decoder from attending to future tokens, ensuring that the predictions are based only on the previously generated tokens. Multi-head attention splits the input into

multiple heads, allowing the model to attend to different aspects of the input simultaneously.

[0274] After the masked multi-head attention, a residual connection is applied followed by layer normalization via add and norm 2204. The residual connection adds the input to the output of the attention layer, helping the model learn faster and deeper. Layer normalization normalizes the activations across the features, stabilizing the training process.

[0275] The multi-head attention 2209 layer performs attention between the Decoder's hidden states and the Encoder's output. It allows the Decoder to attend to relevant parts of the input sequence based on the Encoder's representations. The attention weights are computed based on the compatibility between the Decoder's hidden states and Encoder's outputs.

[0276] Another add and norm 2204 layer is then followed by feed forward network 2205. This is a fully connected feed-forward network applied to each position of the Decoder's hidden states. It consists of two linear transformations with a Rectified Linear Unit (ReLU) activation in between. The feed forward layer helps the model capture non-linear interactions and increases the model's capacity.

[0277] Another add and norm 2204 layer is followed by linear 2212 and softmax 2213 layers. The final hidden states of the Decoder are passed through a linear transformation to project them into the vocabulary space. Vocabulary space refers to the set of all unique tokens or words that the model can generate or predict. In the context of language models, the vocabulary is a predefined set of tokens that the model is trained on and can output. When the Decoder's final hidden states are passed through a linear transformation, they are projected into a vector space with the same dimensionality as the size of the vocabulary. Each dimension in this space corresponds to a specific token in the vocabulary. For example, the model has a vocabulary of 10,000 unique tokens. The linear transformation would project the Decoder's hidden states into a 10,000-dimensional vector space. Each element in this vector represents the model's predicted probability or score for the corresponding token in the vocabulary.

[0278] A softmax function is applied to the projected values (vectors) to generate output probabilities over the vocabulary. The softmax function normalizes the values so that they sum up to 1, representing a probability distribution over the vocabulary. Each probability indicates the likelihood of a specific token being the next output token. The token with the highest probability is selected as the next output token. During the model's training, the objective is to maximize the probability of the correct next token given the input sequence and the previously generated tokens. The model learns to assign higher probabilities to the tokens that are more likely to appear based on the context. At inference time, the token with the highest probability in the vocabulary space is selected as the next output token. This process is repeated iteratively, with the generated token being fed back into the Decoder as input for the next step, until a stopping criterion is met (e.g., reaching a maximum length or generating an end-of-sequence token). The size and composition of the vocabulary can vary depending on the specific task and the data the model is trained on. It can include words, subwords, or even characters, depending on the tokenization strategy used.

**[0279]** The Decoder layers 2220 can be stacked Nx times, allowing the model to capture complex dependencies and generate coherent output sequences.

**[0280]** This transformer architecture allows the model to process input sequences, capture long-range dependencies, and generate output sequences based on the encoded input and the previously generated tokens.

**[0281]** There are at least three variations of transformer architecture that enable different LLMs. A first such variation comprises Auto-Encoding Models. In autoencoders, the decoder portion of the transformer is discarded after pre-training and only the encoder is used to generate the output. The popular BERT and ROBERTa models are examples of models based on this architecture and perform well on sentiment analysis and text classification. These types of models may be trained using a process called masked language modeling (MLM).

**[0282]** The primary goal of an autoencoder is to learn efficient representations of input data by encoding the data into a lower-dimensional space and then reconstructing the original data from the encoded representation. Autoencoders are trained in an unsupervised manner, meaning they don't require labeled data. They learn to capture the underlying structure and patterns in the input data without explicit guidance. An autoencoder consists of two main components: an encoder and a decoder. The encoder takes the input data and maps it to a lower-dimensional representation, often referred to as the latent space or bottleneck. The decoder takes the latent representation and tries to reconstruct the original input data. Autoencoders can be used for dimensionality reduction by learning a compressed representation of the input data in the latent space. The latent space has a lower dimensionality than the input data, capturing the most salient features or patterns. The training objective of an autoencoder is to minimize the reconstruction error between the original input and the reconstructed output. The model learns to encode and decode the data in a way that preserves the essential information needed for reconstruction. Variants and extensions of autoencoders can include denoising autoencoders, variational autoencoders (VAEs) which introduce a probabilistic approach to autoencoders wherein they learn a probabilistic encoder and decoder, allowing for generating new samples from the learned latent space, and conditional autoencoders which incorporate additional conditions or labels as input to the encoder and decoder, enabling the generation of samples conditioned on specific attributes.

**[0283]** Autoencoders can have various applications. Autoencoders can be used to detect anomalies by measuring the reconstruction error. Anomalous samples tend to have higher reconstruction errors compared to normal samples. Autoencoders can be used as a pre-training step to learn meaningful features from unlabeled data. The learned features can then be used for downstream tasks like classification or clustering. Additionally, or alternatively, autoencoders, particularly VAEs, can be used as generative models to generate new samples similar to the training data by sampling from the learned latent space. It's worth noting that while autoencoders can be effective for certain tasks, they have some limitations. They may struggle to capture complex dependencies and may generate blurry or less sharp reconstructions compared to other generative models like Generative Adversarial Networks (GANs).

**[0284]** Another type of variation is the auto-regressive model which feature the use of only the decoder portion of

the transformer architecture. In autoregressive architectures, the decoder portion of the transformer is retained and the encoder portion is not used after model pre-training. Autoregressive models are a class of models that generate outputs by predicting the next element based on the previously generated elements. In the context of the Transformer architecture and language modeling, auto-regressive models are commonly used for tasks such as text generation, machine translation, and language understanding.

**[0285]** Auto-regressive models generate outputs sequentially, one element at a time. In the case of language modeling, the model predicts the next word or token based on the previous words or tokens in the sequence. The prediction of the next element is conditioned on the previously generated elements. The model learns the conditional probability distribution  $P(x_{t|x_1, x_2, \dots, x_{\{t-1\}}})$ , where  $x_t$  is the element at position t, and  $x_1, x_2, \dots, x_{\{t-1\}}$  are the previously generated elements. The Transformer architecture, particularly the Decoder component, is well-suited for auto-regressive modeling. The Decoder generates the output sequence one element at a time, conditioned on the previously generated elements and the encoded input sequence from the Encoder. In the Transformer Decoder, the self-attention mechanism is masked to prevent the model from attending to future positions during training. This masking ensures that the model relies only on the previously generated elements to make predictions, following the auto-regressive property. During training, the Transformer Decoder uses a technique called teacher forcing. Instead of feeding the model's own predictions as input for the next step, the ground truth target sequence is used. This helps the model learn to generate the correct output sequence based on the input sequence and the previous target tokens. During inference or generation, the Transformer Decoder generates the output sequence one element at a time. At each step, the model takes the previously generated elements as input and predicts the next element. This process continues until a stopping criterion is met, such as reaching a maximum sequence length or generating an end-of-sequence token. Auto-regressive models, including the Transformer, have achieved state-of-the-art performance in language modeling tasks. They excel at capturing the statistical properties and dependencies in sequential data, making them effective for generating coherent and fluent text.

**[0286]** While text generation is the most suitable use case of auto-regressors, they perform exceptionally well on a wide variety of tasks. Most modern LLMs are auto-regressors including, for example, the popular GPT series of LLMs, BERT, and XLNet.

**[0287]** The third variation of the transformer model is the sequence-to-sequence model which utilizes both the encoder and decoder portions of the transformer and can be trained in multiple ways. One of the methods is span corruption and reconstruction. These models are, generally, best suited for language translation. The T5 and BART family of models are examples of sequence-to-sequence models.

**[0288]** FIG. 23 is a block diagram illustrating an exemplary basic embedding layer generation process, according to an embodiment. The illustration shows the basic structure of an embedding layer, which is commonly used in natural language processing tasks to convert input words into dense vector representations. The diagram shows an input word 2301, an input word layer 2302, an embedding layer 2303,

and an output layer **2304**. As shown, the input word **2301** is represented as one-hot encoded vectors, where each word is represented by a vector of size 10,000 (i.e., the vocabulary size). One-hot encoding is a common technique used to represent categorical variables, such as words in a vocabulary, as binary vectors. In one-hot encoding, each word is represented by a vector with a length equal to the size of the vocabulary. The vector consists of zeros in all positions except for a single position, which is set to one, indicating the presence of the corresponding word. The input word is one-hot encoded with a 1 at the corresponding word index and 0s elsewhere. For example, if a vocabulary of 10,000 words exists, each word will be represented by a vector of size 10,000. If the input word is the 5th word in the vocabulary, its one-hot encoded vector will have a 1 at the 5th position and 0s everywhere else. It is important to note that the one-hot encoding is just one way to represent input words. Other techniques, such as integer encoding or using pre-trained word embeddings (e.g., Word2Vec or GloVe), can also be used depending on the specific requirements of the task and the available resources.

**[0289]** The input layer **2302** takes the one-hot encoded input word vectors and passes them to the embedding layer **2303**. The input layer in the embedding generation process is responsible for handling the initial representation of the input words before they are passed to the embedding layer. The one-hot encoding ensures that each word has a unique representation, but it also results in sparse and high-dimensional vectors. The embedding layer **2303** then transforms these sparse vectors into dense, lower-dimensional representations (embeddings) that capture semantic and syntactic relationships between words. The embedding layer **2303** is a fully connected layer without an activation function. It maps the one-hot encoded input vectors to dense vector representations of a specified dimension (in this case, 300). The embedding layer has a weight matrix of size (vocabulary\_size, embedding\_dimension), which is learned during training. In the given example, the vocabulary size is 10,000, and the embedding dimension is 300. Each row in the weight matrix corresponds to a word in the vocabulary, and the columns represent the dimensions of the embedding space. When a one-hot encoded vector is passed to the embedding layer, it performs an embedding lookup. Since the one-hot vector has a single 1 at the position corresponding to the input word, the embedding lookup effectively selects the corresponding row from the weight matrix, which represents the embedding vector for that word.

**[0290]** The embedding size (dimension) is a hyperparameter that determines the size of the dense vector representations. In the example, the embedding size is 300, meaning each word is represented by a vector of length 300. The choice of embedding size depends on the complexity of the task, the size of the vocabulary, and the available computational resources. Larger embedding sizes can capture more fine-grained semantic information but also require more memory and computation. The embedding layer's weights (the embedding vectors) are learned during the training process through backpropagation. The model adjusts these weights based on the downstream task's objective, such as minimizing a loss function. As a result, the learned embeddings capture semantic and syntactic relationships between words, with similar words having similar vector representations. Once the embeddings are learned, they can be reused for various downstream tasks. The learned embeddings can

be used as input features for other models, such as recurrent neural networks (RNNs) including echo state network (ESN) and graph neural network (GNN) variants or convolutional neural networks (CNNs), in tasks like text classification, sentiment analysis, or language translation.

**[0291]** The output layer **2304** consists of the dense word embeddings generated by the embedding layer. In this example, there are four output embedding vectors, each of size 300, corresponding to different words in the vocabulary. The embedding layer allows the model to learn meaningful representations of words in a lower-dimensional space, capturing semantic and syntactic relationships between words. These embeddings can then be used as input to downstream tasks such as text classification, sentiment analysis, or language modeling.

#### Detailed Description of Exemplary Aspects

**[0292]** FIG. 16 is a process flow diagram of a method **1600** for predictive analysis of very large data sets using the distributed computational graph. One or more streams of data from a plurality of sources, which includes, but is in no way limited to, a number of physical sensors, web-based questionnaires and surveys, monitoring of electronic infrastructure, crowd sourcing campaigns, and direct human interaction, may be received by system **1601**. The received stream is filtered **1602** to exclude data that has been corrupted, data that is incomplete or misconfigured and therefore unusable, data that may be intact but nonsensical within the context of the analyses being run, as well as a plurality of predetermined analysis related and unrelated criteria set by the authors. Filtered data may be split into two identical streams at this point (second stream not depicted for simplicity), wherein one substream may be sent for batch processing **1600** while another substream may be formalized **1603** for transformation pipeline analysis **1604**, **1500**, and retraining **1605**. Data formalization for transformation pipeline analysis acts to reformat the stream data for optimal, reliable use during analysis. Reformating might entail, but is not limited to: setting data field order, standardizing measurement units if choices are given, splitting complex information into multiple simpler fields, and stripping unwanted characters, again, just to name a few simple examples. The formalized data stream may be subjected to one or more transformations. Each transformation acts as a function on the data and may or may not change the data. Within the invention, transformations working on the same data stream where the output of one transformation acts as the input to the next are represented as transformation pipelines. While the great majority of transformations in transformation pipelines receive a single stream of input, modify the data within the stream in some way and then pass the modified data as output to the next transformation in the pipeline, the invention does not require these characteristics. According to the aspect, individual transformations can receive input of expected form from more than one source or receive no input at all as would a transformation acting as a timestamp. According to the aspect, individual transformations may not modify the data as would be encountered with a data store acting as a queue for downstream transformations. According to the aspect, individual transformations may provide output to more than one downstream transformations. This ability lends itself to simulations where multiple possible choices might be made at a single step of a procedure all of which need to be analyzed. While

only a single, simple use case has been offered for each example, in each case, that example was chosen for simplicity of description from a plurality of possibilities, the examples given should not be considered to limit the invention to only simplistic applications. Last, according to the invention, transformations in a transformation pipeline backbone may form a linear, a quasi-linear arrangement or may be cyclical, where the output of one of the internal transformations serves as the input of one of its antecedents allowing recursive analysis to be run. The result of transformation pipeline analysis may then be modified by results from batch analysis of the data stream and output **1606** in format predesigned by the authors of the analysis with could be human readable summary printout, human readable instruction printout, human-readable raw printout, data store, or machine encoded information of any format known to the art to be used in further automated analysis or action schema.

**[0293]** FIG. 17 is a process flow diagram of a method **1700** for an aspect of modeling the transformation pipeline module as a directed graph using graph theory. According to the aspect, the individual transformations **17102**, **17104**, **17106** of the transformation pipeline  $t_1 \dots t_n$  such that each  $t_i \in T$  are represented as graph nodes. Transformations belonging to  $T$  are discrete transformations over individual datasets  $d_i$ , consistent with classical functions. As such, each individual transformation  $t_i$  receives a set of inputs and produces a single output. The input of an individual transformation  $t_i$  is defined with the function  $in: t_i \times d_1 \dots d_k \rightarrow \{d_1 \dots d_k\}$  and describes a transformation with  $k$  inputs. Similarly, the output of an individual transformation is defined as the function  $out: t_i \times \{d_i\} \rightarrow \{d_i\}$  to describe transformations that produce a single output (usable by other transformations). A dependency function can now be defined such that  $dep(t_a, t_b) \iff out(t_a) \subset in(t_b)$ . The messages carrying the data stream through the transformation pipeline **1701**, **1703**, **1705** make up the graph edges. Using the above definitions, then, a transformation pipeline within the invention can be defined as  $G = (V, E)$  where message  $(t_1, t_2 \dots t_{(n-1)}, t_n) \in V$  and all transformations  $t_1 \dots t_n$  and all dependencies  $dep(t_i, t_j) \in E$  **1707**.

**[0294]** FIG. 18 is a flow diagram illustrating an exemplary method for providing experience curation, according to an aspect of an embodiment. According to the aspect, the process begins at step **1801** when a distributed generative AI reasoning and action platform receives a user query directed to a generative AI system. The query may comprise a request for information, a summary, a request for a document, or some other action. The user may submit their query to the platform via an experience curation portal such as through a webapp or website accessed via an Internet browser operating on a computer (e.g., personal computer, laptop), or through an associated curation application which can be operated on a mobile computing device (e.g., smart phone, tablet, smart wearable, IoT device, etc.). In some implementations, the received user query may be sent to a data embedding system which can vectorize the query and store it in a vector database where it may be retrieved to be used as contextual data included in a query/prompt sent to a generative AI system.

**[0295]** At step **1802** the query is sent to the generative AI system which processes the query and returns a generated response which is received by the platform at step **1803**. At step **1804** curation system locates and retrieves any available

user-defined rules or preferences. In some embodiments, the user-defined rules/preferences may be defined by an entity (e.g., a company). Exemplary rules or preferences can include, but are not limited to, conditional generation preferences, formatting rules, language rules, style rules, geographic rules, environmental rules, and timing rules. With respect to conditional generation rules, the model can be conditioned on specific input data related to the individual, such as preferences, behavior, and characteristics. For example, in text generation, the model could be conditioned on a user's previous messages or writing style to generate more personalized responses. Formatting, style, and language rules are closely related and may be used to curate a response in a specific format (e.g., bullet points, paragraph, single sentence, numbered outline, CSV, etc.), response style (e.g., formal, informal, academic, accessible, abstract, casual, etc.), and the language in which a response is translated, respectively. At step **1805** curation system can curate the response based on the retrieved user-defined rules or preferences. For example, the system may filter out extraneous data, or personal information. As a last step **1806**, curation system returns the curated response to the user, thereby providing experience curation to a platform user.

**[0296]** FIG. 19 is a flow diagram illustrating an exemplary method for providing experience curation with using rich contextual data, according to an aspect of an embodiment. According to the aspect, the process begins at step **1901** when a distributed generative AI reasoning and action platform receives a user query directed to a generative AI system. The query may comprise a request for information, a summary, a request for a document, or some other action. The user may submit their query to the platform via an experience curation portal such as through a webapp or website accessed via an Internet browser operating on a computer (e.g., personal computer, laptop), or through an associated curation application which can be operated on a mobile computing device (e.g., smart phone, tablet, smart wearable, IoT device, etc.). In some implementations, the received user query may be sent to a data embedding system which can vectorize the query and store it in a vector database where it may be retrieved to be used as contextual data included in a query/prompt sent to an ML, AI, generative AI, planning, or automation/action orchestration system.

**[0297]** A DCG orchestrated model which employs a hierarchical classification and model selection regime for content (either in whole or in part) can enable much more accurate ultimate semantic performance. For example, a query/prompt can be submitted to the generative AI system with additional metadata associated with the context of the prompt itself as well as additional broader information about the user and the user's ongoing behavior and/or activities. At step **1902** the system obtains a plurality of rich context data associated with the user, the query, or both. A subset of the plurality of context data information may be obtained from a vector database, the vector database comprising a plurality of embedded contextual data. Embedded contextual data can comprise (but is not limited to) information obtained from an enterprise knowledge base and embedded queries/prompts. Context data associated with the user may comprise information obtained from or related to one or more of a computing device on which the user is accessing the curation system/platform, the geographic location the user is located, an action the user is performing during interaction with the curation system/platform, and timing data associ-

ated with the user, and/or the like. A subset of the plurality of obtained context data may be obtained from one or more marketplaces such as a data marketplace and/or an expert judgment marketplace. In some embodiments, the selection of context data may be based on one or more expert judgment scores assigned to an information source, dataset, model, and/or hyperparameters.

**[0298]** As an example, if a user is asking a generative AI enhanced search engine for “the best pizza” on her cell phone while driving at 55 mph on the road and not near her home (e.g. on vacation) this is massively different from the user being at home, on her couch, connected on her laptop, from her normal IP address, having just ran a series of searches for airline tickets to Italy and Neapolitan Pizza recipes. The additional device, user, recent behavior, etc. content can be used by a classifier alongside a prompt to help focus results on things that are not only relevant (e.g. pizza places near the user that are open now) but likely to be consistent with her broader needs/persona (e.g. if available, the suggestions could be looked at based on other budget, dining, etc. preferences like outdoor seating and meals below \$20 per person). The same principle applies to more complicated and complex topics like medicine or finance or law.

**[0299]** At step 1903 the obtained plurality of context data may be processed into vectors by an embedding model and stored in the vector database.

**[0300]** At step 1904 the user query and the vectorized context data is sent to the generative AI system which processes the query and returns a generated response which accounts for the information contained in the vectorized context data and which is received by the platform at step 1905. At step 1906 curation system locates and retrieves any available user-defined rules or preferences. In some embodiments, the user-defined rules/preferences may be defined by an entity (e.g., a company). Exemplary rules or preferences can include, but are not limited to, conditional generation preferences, formatting rules, language rules, style rules, geographic rules, environmental rules, and timing rules. With respect to conditional generation rules, the model can be conditioned on specific input data related to the individual, such as preferences, behavior, and characteristics. For example, in text generation, the model could be conditioned on a user’s previous messages or writing style to generate more personalized responses. Formatting, style, and language rules are closely related and may be used to curate a response in a specific format (e.g., bullet points, paragraph, single sentence, numbered outline, CSV, etc.), response style (e.g., formal, informal, academic, accessible, abstract, casual, etc.), and the language in which a response is translated, respectively. At step 1907 curation system can curate the response based on the retrieved user-defined rules or preferences. For example, the system may filter out extraneous data, or personal information. As a last step 1908, curation system returns the curated response to the user, thereby providing experience curation to a platform user.

**[0301]** FIG. 20 is a flow diagram illustrating an exemplary method for providing distributed neuro-symbolic reasoning and action model, according to an aspect of an embodiment. A neuro-symbolic model combines neural network-based approaches with symbolic reasoning to enable a more flexible and powerful reasoning system. In neuro-symbolic reasoning, neural networks are used to learn representations of data, similar to how they are used in deep learning. These

learned representations can then be combined with symbolic representations and rules to perform reasoning tasks. This combination allows for the strengths of both approaches to be leveraged: the ability of neural networks to learn complex patterns from data, and the ability of symbolic reasoning to represent and manipulate abstract concepts and rules.

**[0302]** According to the aspect, the process begins at step 2001a-c wherein a plurality of input data is obtained from various sources. Examples of input data can include entity knowledge 2001a, context data 2001b, and expert knowledge 2001c. Other types of data may be obtained and may be dependent upon the embodiment and the particular use case. Data may be obtained from third-party services, entity databases/data warehouses/knowledge base and/or the like, and various marketplaces for data, algorithms, RAGs, and/or expert judgment. At step 2002 the obtained plurality of input data is vectorized using an embedding model and stored in a vector database. Vectorizing the data allows it to be used as input for processing by a neural network. At step 2003 platform 120 can train the neural network using the input data to learn patterns and relationships in the data. In some embodiments, this step may involve the use of labeled examples and supervised learning. A recurrent neural network or some other transformer-based model may be used as the basis for the neural network. At step 2004 the system maps the learned representations to symbolic concepts or rules. At this step, the system learns to represent the learned features or representations from the neural network in symbolic form. At step 2005 the system applies reasoning techniques to the symbolic representations to perform reasoning tasks. Examples of reasoning techniques that may be implemented can include, but are not limited to, logic rules or inference engines. This step may involve combining the learned representations with existing knowledge or rules to derive new conclusions. At this point in the process a feedback loop is created wherein feedback from the symbolic reasoning step is incorporated back into the neural network to refine the learned representations. This feedback loop helps to improve the performance of the system over time. In some embodiments, the feedback loop may include functionality for evaluating generated outputs based on quality and/or relevance to the task. In such embodiments, users’ positive and/or negative feedback may then be used to adjust the running model’s parameters. In this way, user feedback can be used as a form of (positive or negative) reinforcement. In another embodiment, a panel of known experts (either human or AI or both) may be used to assess model outputs and/or performance and apply feedback based on the panel’s assessment.

**[0303]** As a last step 2006, the trained, distributed GenAI reasoning and action model can generate output of the reasoning process, which could be a decision, a prediction, or an action based on the input data and the reasoning process. In some embodiment, the input data may further include a query/prompt and metadata comprising various contextual information about the user and/or prompt.

**[0304]** FIG. 20 is a flow diagram illustrating an exemplary method for using a distributed computation graph system for creating structured representations or knowledge graphs from various data sources, and setting up a pipeline for continuous processing and monitoring of that data, according to an embodiment. According to the embodiment, the process begins at step 2001 when the platform receives a plurality of input data of interest from structured (e.g.,

databases, spreadsheets, etc.) and unstructured (e.g., documents, websites, social media, etc.) data sources. Data may be obtained using data extraction techniques such as, for example, web scraping, APIs, natural language processing, etc.). Additionally, or alternatively, the data may be obtained from a data marketplace (e.g., expert judgment, RAGs, models, datasets, etc.). At step 2002 the platform creates a knowledge graph or structured representation from data of interest. This may comprise applying information extraction methods (e.g., named entity recognition, relation extraction, etc.) to extract entities and relationships from unstructured data and integrating the extracted information with structured data sources. Further, a knowledge graph representation can be built by creating nodes for entities and edges for relationships. Optionally, the platform can be configured to create vector representations of entities/relationships using techniques like word embeddings.

[0305] At step 2003, the platform selects data of interest, knowledge graph of interest, vector database of interest, embedding of interest, model of interest or simulation of interest from a marketplace and procures it. Platform can search/browse a marketplace or repository for relevant data sources, knowledge graphs, vector databases, models, simulations, etc., and evaluate the potential options based on factors like relevance, quality, and cost. This step may further include purchasing or licensing selected assets for use in a pipeline. As a next step 2004, platform creates a new pipeline which will continue to process target of interest data on a continuous or periodic or aperiodic basis going forward. The pipeline may be designed (e.g., batch, streaming, etc.) based on the processing needs and can integrate components for data ingestion, knowledge graph updates, model execution and/or the like.

[0306] At step 2005, platform can instantiate or reserve resources for the new pipeline based on estimated resource needs for storage, transport, compute, privacy, regulation/laws, safety, and prices for relevant services needed to handle future pipeline via a probabilistic representation of it. Platform may estimate pipeline resource requirements (storage, compute, networking, etc.) and also consider privacy, regulatory, and safety constraints that impact resource needs. Platform may use probabilistic modeling to forecast future resource demands. This step may further comprise provisioning cloud/on-premise resources (e.g., virtual machines, containers, databases, etc.) accordingly. As a last step 2006, platform monitors and adjusts the pipeline going forward based on uncertainty quantification methods looking at model expectations versus empirical observations and expected future “exogenous” zone of interest. A pipeline may be monitored for performance, data drift, model accuracy, etc. and by tracking metrics like data volumes, processing times, error rates, and model accuracies. Platforms may use techniques such as, for example, Bayesian modeling to quantify uncertainties in model parameters and propagate input/parameter uncertainties through the model(s) to get prediction uncertainties. Techniques such as bootstrap, cross-validation can also quantify model uncertainties. Platform can identify external variables (e.g., new regulations, market shifts, technology changes, etc.) that may impact the “zone of interest” and quantify potential impacts on pipeline performance/relevance. As an example, a platform could implement monitoring for these variables using web scraping, news feeds, etc.

[0307] FIG. 24 is a flow diagram illustrating an exemplary method 2400 for routing processing based on certainty threshold and/or challenge-based verification, according to an embodiment. According to the embodiment, the process begins at step 2401 by defining a hierarchy of reasoning tasks and subtasks that break down decision-making processes into manageable steps. Examples of reasoning tasks could include “Gather relevant information,” “Analyze data,” “Generate potential solutions,” “Evaluate alternatives,” and “Select the best option.” For each identified reasoning task, break it down further into smaller, more manageable subtasks. For example, the reasoning task “Gather relevant information” could be decomposed into subtasks such as “Identify information sources,” “Extract relevant data,” “Preprocess and clean data,” and “Integrate data from multiple sources. Determine which tasks or subtasks need to be completed before others can be started (prerequisites) and establish the flow of information and outputs between tasks and subtasks, specifying how the results of one task feed into the inputs of another. This can be orchestrated by the DCG computing system. For each subtask, assign the appropriate AI models, algorithms, or knowledge sources that will be used to perform the required processing. This could include machine learning models, rule-based systems, knowledge bases, or external APIs.

[0308] At step 2402 platform 2120 orchestrates the execution of these tasks and routes data to the appropriate models or knowledge sources based on predefined rules or learned policies. Platform 2120 or an administrator can set certainty thresholds for each task to determine when the system should proceed to the next step or seek additional information/verification at step 2403. Certainty thresholds can be predetermined levels of confidence or probability that an AI system uses to make decisions or trigger specific actions. As a last step 2404, the platform may use challenge-based verification mechanisms to test the robustness and reliability of a given AI system’s decisions by subjecting the system to various challenges or adversarial scenarios. These mechanisms help identify potential weaknesses, biases, or failure points in the decision-making process. Some examples of challenge-based verification mechanisms can include, adversarial examples, edge case testing, counterfactual reasoning, stress testing, robustness to noise and outliers, and fairness and bias testing, to name a few.

[0309] Adversarial examples are carefully crafted inputs that are designed to fool or mislead the AI system into making incorrect predictions or decisions. For example, in an image classification system, an adversarial example could be an image that has been slightly perturbed or modified in a way that is imperceptible to humans but causes the system to misclassify the image. By testing the system’s performance on a range of adversarial examples, platform 2120 can assess its robustness against manipulated or deceptive inputs.

[0310] Edge case testing involves evaluating the system’s performance on rare, extreme, or unusual scenarios that may not be well-represented in the training data. For example, in a self-driving car system, an edge case could be a scenario where a pedestrian suddenly appears from behind a parked vehicle or a situation with complex road construction and detours. By subjecting the system to a variety of edge cases, platform 2120 can assess its ability to handle unexpected or challenging situations more gracefully and appropriately, especially when it is able to compare connectionist and

symbolic knowledge corpora and reasoning in assessing decision appropriateness during both planning and action execution phases. This can be even further enhanced when the data sets used in model formulation are able to be checked for sufficient presence of similar scenarios in the training data such as real world empirical observations, or agent-based modeling simulations or hierarchical modeling simulation of pedestrian behavior for individuals and groups in this example.

[0311] Counterfactual reasoning involves analyzing how the system's decisions would change if certain input features or conditions were different. As an example, in a loan approval system, counterfactual reasoning could involve examining how the system's decision would differ if an applicant's income or credit score were slightly modified. By exploring counterfactual scenarios, platform 2120 can identify the sensitivity of the system's decisions to specific input features and ensure that the decisions remain consistent and fair.

[0312] Robustness to noise and outliers tests the system's resilience to noisy or outlier data points that may be present in real-world scenarios. As an example, in a sentiment analysis system, robustness testing could involve evaluating the system's performance on reviews with spelling errors, grammatical mistakes, or unconventional language patterns. By assessing the system's performance on noisy and outlier data, platform 2120 can ensure that it remains reliable and accurate in the presence of imperfect or unexpected inputs.

[0313] Fairness and bias testing aim to identify and mitigate any unintended biases or prohibited discriminatory behavior in the system's decision-making process when needed. For example, in a hiring recommendation system, fairness testing could involve analyzing the system's predictions for any systematic biases based on protected attributes such as gender, race, or age or other protected class attributes. By conducting fairness and bias tests, you can ensure that the system's decisions are equitable and do not perpetuate or amplify societal biases that are not desired. This can also be used to compare hiring manager and interviewer performance to better elucidate internal selection biases and gifted or poor managers or talent spotters.

[0314] These challenge-based verification mechanisms help assess the robustness, reliability, fairness, and transparency of an AI system's decisions. By subjecting the system to various challenges and adversarial scenarios, platform 2120 can identify potential weaknesses, biases, or failure modes and take appropriate measures to mitigate them. It's important to note that the specific challenges and verification mechanisms used will depend on the domain, the nature of the AI system, and the potential consequences of its decisions. A comprehensive verification strategy should encompass a diverse set of challenges to thoroughly test the system's performance and ensure its reliability in real-world deployment.

[0315] FIG. 25 is a flow diagram illustrating an exemplary method 2500 for retrieving relevant contextual data from a knowledge graph database and enriching vector embeddings with the contextual data, according to an embodiment. According to an aspect of an embodiment, this process may be conducted by embedding refinement computing system 2122. According to the embodiment, the process begins at step 2501 when platform 2120 queries a knowledge graph to retrieve symbolic information comprising relevant facts, entities, and relationships based on input data and the current

reasoning context. At step 2502, the retrieved knowledge is used to refine vector embeddings generated by connectionist models (e.g., neural network models or Kolmogorov-Arnold Networks [KANs]), incorporating symbolic information into the distributed representations (i.e., embeddings) or refining the symbolic ontology or improve the embedding model itself. As a last step 2503, the platform 2120 can implement techniques to effectively combine the embeddings with the knowledge graph data. One or more techniques may be used to combine the embeddings and the symbolic information. A first technique may leverage knowledge graph embedding alignment wherein platform 2120 generates vector embeddings for the entities and relationships in the knowledge graph using techniques such as TransE, TransR, or DistMult, for example, and aligning the vector embeddings generated by the neural network models with the knowledge graph embeddings using techniques such as embedding space transformation or joint embedding learning. Then the platform can update the neural network embeddings by incorporating the aligned knowledge graph embeddings, allowing the symbolic information to influence the distributed representations.

[0316] Another approach may utilize attention mechanisms to compute the relevance or importance of the retrieved knowledge for each input instance and then modify the neural network architecture to incorporate attention layers that take the retrieved knowledge as additional input. During the attention computation, higher weights may be assigned to the retrieved knowledge that is most relevant to the current input and task. Platform can update the vector embeddings generated by the neural network models by incorporating the attention-weighted knowledge representations.

[0317] Another technique may leverage knowledge-aware language models wherein the language model architecture is modified to incorporate knowledge-aware layers or components and the retrieved knowledge is injected into the language model during the encoding or decoding process. For example, platform 2120 can use techniques like knowledge-aware self-attention, where the attention computation is conditioned on the retrieved knowledge. Additional techniques can include the use of graph convolutional networks, and/or knowledge distillation.

[0318] It's important to note that the retrieved knowledge should be relevant and complementary to the input data and the task at hand. The symbolic information should provide additional context or constraints that can guide the refinement of the vector embeddings and improve the overall performance of the AI system.

[0319] FIG. 26 is a flow diagram illustrating an exemplary method 2600 for applying expressive weighting schemes to model combinations, according to an embodiment. According to an aspect of an embodiment, the process may be performed by model blending computing system 2125. According to the embodiment, the process begins at step 2601 by combining the outputs of multiple neural network models based on their individual strengths and weaknesses. This can include, for example, combining the output of two or more expert models within a larger model. At step 2602 weighting schemes dynamically adjust the contribution of each model based on factors such as uncertainty, task complexity, and domain relevance. As a last step 2603, platform 2120 may implement techniques like Bayesian model averaging, mixture of experts, and/or ensemble learn-

ing to optimally blend model outputs. When combining the outputs of multiple neural network models based on their individual strengths and weaknesses, and developing weighting schemes to dynamically adjust the contribution of each model, the goal is to create an ensemble of models that can leverage the diverse capabilities of each individual model to improve overall performance and robustness.

**[0320]** Multiple neural network models, each trained on the same task or dataset, can have different strengths and weaknesses. Some models may excel at capturing certain patterns or features, while others may be more robust to noise or better at handling specific types of inputs. By combining the outputs of these models, platform **2120** can harness their complementary strengths and mitigate their individual weaknesses. Common approaches for combining model outputs include (but are not limited to) averaging (e.g., taking the average of the outputs from all models), voting (e.g., assigning the final output based on the majority vote of the model), and weighted averaging (e.g., assigning different weights to the outputs of each model based on their perceived importance or performance).

**[0321]** Weighting schemes determine how much influence each individual model has on the final combined output. Instead of using fixed weights, platform **2120** can develop dynamic weighting schemes that adjust the contribution of each model based on various factors. A first such factor is uncertainty wherein models that exhibit higher uncertainty or lower confidence in their predictions can be given lower weights, while models with higher confidence can have higher weights. Another factor is task complexity wherein for tasks with varying levels of complexity, the platform can assign higher weights to models that specialize in handling specific types of complexity. A domain relevance factor determines if the input data belongs to different domains or categories, wherein the platform can assign higher weights to models that are more relevant or perform better in that particular domain.

**[0322]** Combining the outputs of multiple models and dynamically adjusting their contributions based on relevant factors allows for more robust, accurate, and adaptable AI systems. By leveraging the strengths of different models and adapting to the characteristics of the input data, the ensemble can provide improved performance and handle a wider range of scenarios compared to individual models.

**[0323]** FIG. 27 is a flow diagram illustrating an exemplary method **2700** for using feedback loops considering security, licensing, provenance, and collaborative development, according to an embodiment. According to the embodiment, the process begins at step **2701** by implementing secure communication protocols and access control mechanisms to protect sensitive data and prevent unauthorized access. Platform **2120** may be configured to ensure compliance with licensing terms and conditions of datasets, models, and tools used therein at step **2702**. For example, platform **2120** may use governance frameworks and policies that define the roles, responsibilities, and processes for collaborative AI development and implement compliance checks and validation processes to ensure adherence to legal, ethical, and regulatory requirements. Furthermore, the platform can record the lineage of data, models, and decisions made by the various AI systems through the lifecycle of said systems at step **2703**. As a last step **2704**, the platform may create and use collaborative development tools and workflows that

allow multiple teams or organizations to jointly develop, test, and deploy AI models while maintaining security and provenance.

**[0324]** To perform data lineage tracking the platform **2120** can leverage a data versioning and tracking system that captures the source, transformations, and dependencies of the data used for training and inference. This may involve the use of metadata standards and schemas to describe properties, origins, and relationships of the data. Platform may maintain a historical record of data updates, modifications, and deletions to ensure traceability, as well as utilize data cataloging and discovery tools to facilitate easy searching and understanding of the data lineage.

**[0325]** To perform model lineage tracking the platform **2120** can establish a model versioning and tracking system that captures the evolution of the AI models throughout their lifecycle. This may involve recording information such as model architectures, hyperparameters, training configurations, and performance metrics for each version of the model. Platform can maintain a repository of model artifacts, including trained weights, configuration files, and associated documentation to track the dependencies between models, including any transfer learning or fine-tuning relationships.

**[0326]** To perform decision lineage tracking the platform **2120** can implement a decision tracking system that captures the inputs, outputs, and intermediate steps involved in each decision made by an AI system. This may involve recording the specific model versions, data inputs, and any external factors that influenced each decision and maintaining a log of decision outcomes, along with their associated confidence scores or uncertainty measures. This may further comprise a mechanism to link decisions back to the corresponding models and data used for inference. In some implementations, the platform may leverage auditing and reporting capabilities to analyze decision patterns, identify anomalies, and support accountability.

**[0327]** Collaborative development tools can include version control systems (e.g., Git) to manage the codebase, models, and configurations collaboratively. Platform **2120** can use access control mechanisms to ensure that only authorized individuals or teams can contribute to the development process and establish code review workflows and pull request processes to maintain code quality and security standards. In some implementations, a platform may leverage federated learning techniques to enable collaborative model training without directly sharing raw data.

**[0328]** FIG. 28 is a flow diagram illustrating an exemplary method **2800** for multi-modal alignment for consistent representations across data types, according to an embodiment. According to an aspect of an embodiment, the process may be performed by multi-modal alignment computing system **2123**. According to the embodiment, the process begins at step **2801** when platform **2120** aligns and synchronizes representations across different data modalities (e.g., text, images, audio, smell, etc.) to create a unified and consistent representation of input data. At step **2802** one or more techniques such cross-modal attention, multi-modal fusion, and/or joint embedding spaces are used to combine information from different modalities. At step **2803** the platform uses domain-specific knowledge (e.g., knowledge graph) to ensure the generated representations (embeddings) are consistent and realistic across modalities.

**[0329]** Multimodal embedding space alignment is performed by learning a shared embedding space where representations from different modalities can be projected and aligned. This may utilize techniques like canonical correlation analysis (CCA) or adversarial learning to map the representations from each modality into a common space. Platform may then train the embedding space alignment model using paired or aligned data from different modalities. Once the alignment model is trained, it can be used to project the representations from each modality into the shared space, creating a unified representation.

**[0330]** Cross-modal attention mechanisms utilize attention mechanisms to attend to relevant information from one modality based on the representations from another modality. For example, in a visual-textual alignment task, use the textual representations to guide the attention over the visual features, or vice versa. Platform can train the attention mechanism to learn the cross-modal dependencies and alignments wherein the attended representations from different modalities can be combined or fused to create a unified representation.

**[0331]** In some implementations, the platform can train a joint embedding model that learns to map the representations from different modalities into a shared embedding space. This may involve the use of techniques like contrastive loss or triplet loss to bring the representations of aligned or similar instances from different modalities closer together in the embedding space.

**[0332]** FIG. 29 is a flow diagram illustrating an exemplary method 2900 for hyperparameter optimization using information-theoretic guidance, according to an embodiment. According to an aspect of an embodiment, this process may be performed by hyperparameter optimization computing system 2126. According to the embodiment, the process begins at step 2901 with the implementation of a hyperparameter optimization framework which searches for the best combination of model architectures, training settings, and embedding techniques. Developing such a framework may begin by defining the hyperparameter search space. This can include identifying the hyperparameters to optimize, such as model architectures, learning rates, batch sizes, embedding dimensions, etc., and specifying the range or possible values for each hyperparameter, defining the search space. This may further involve using appropriate data types and ranges for each hyperparameter (e.g., categorical variables for model architectures, continuous variables for learning rates). Some exemplary hyperparameter optimization algorithms which may be implemented can include, but are not limited to, grid search, random search, Bayesian optimization, and evolutionary algorithms. Platform may create an optimization loop that iteratively generates hyperparameter configurations, evaluates them using the objective function, and updates the search process based on the results. For grid search or random search, a platform can generate all the configurations upfront and evaluate them in parallel or sequentially. For Bayesian optimization or evolutionary algorithms, the platform may need to implement the specific update rules and sampling strategies based on the chosen algorithm.

**[0333]** At step 2902 information-theoretic measures are incorporated into the hyperparameter optimization to guide the optimization process and select hyperparameters that maximize the information content and generalization ability of learned representations. Information content refers to the

amount of meaningful or relevant information captured by the learned representations (embeddings). Representations with high information content are able to capture and encode the salient features, patterns, and relationships present in the input data. Maximizing the information content ensures that the learned representations are rich, expressive, and informative. Representations with good generalization ability can effectively capture the underlying patterns and structures in the data, rather than merely memorizing the training examples. Maximizing the generalization ability ensures that the learned representations are robust, transferable, and applicable to a wide range of tasks and datasets.

**[0334]** Information-theoretic measures quantify the information content and relationships between variables or representations. Common information-theoretic measures, which may be implemented in various aspects of platform 2120, can include: Shannon entropy which measures the average amount of information contained in a random variable or representation; mutual information which quantifies the amount of information shared between two variables or representations; or Kullback-Leibler (KL) divergence which measures the difference between two probability distributions, often used to assess the dissimilarity between learned representations and a reference distribution. During the hyperparameter optimization process, information-theoretic measures can be used as objective functions or regularization terms to guide the search towards hyperparameters that maximize the information content and generalization ability. For example, platform 2120 or an administrator can define an objective function that combines the performance metric (e.g., accuracy) with an information-theoretic measure (e.g., mutual information between learned representations and class labels). By optimizing this objective function, the hyperparameter search will favor configurations that not only achieve high performance but also learn representations with high information content and generalization ability.

**[0335]** Information-theoretic measures can be used to evaluate and compare different hyperparameter configurations based on the quality of the learned representations. For each hyperparameter configuration, the platform can compute the relevant information-theoretic measures on the learned representations and assess their information content and generalization ability. Hyperparameter configurations that yield representations with higher information content and better generalization ability are considered more desirable and are selected as the optimal choices.

**[0336]** Information-theoretic measures can also be used as regularization terms or constraints during the model training process itself. For example, the platform can add a regularization term that encourages the learned representations to have high mutual information with the target variables or to minimize the KL divergence between the learned representations and a desired prior distribution. These regularization techniques help guide the model towards learning representations that are informative, generalize well, and align with the desired properties.

**[0337]** Hyperparameter optimization can be computationally expensive, especially when training and evaluating complex models. As such, the platform may leverage parallel computing techniques to distribute the evaluation of hyperparameter configurations across multiple cores, machines, or clusters. Additionally, or alternatively, the platform can incorporate early stopping mechanisms to

terminate the evaluation of poorly performing hyperparameter configurations early, saving computational resources and allocate more resources (e.g., training iterations, computational budget) to promising configurations based on their intermediate performance. For example, techniques like successive halving or Hyperband can dynamically allocate resources based on the relative performance of configurations.

[0338] FIG. 30 is a flow diagram illustrating an exemplary method 3000 for linking embeddings to knowledge graphs, according to an embodiment. According to an aspect of an embodiment, the process may be performed by ontology extraction computing system 2124. According to the embodiment, the process begins at step 3001 by analyzing learned vector embeddings (produced by one or more neural network models) and extracting symbolic representations that capture the underlying semantic structure. At step 3002 the platform may use clustering, dimensionality reduction, and/or rule mining to distill the embeddings into interpretable symbolic forms.

[0339] Platform 2120 may apply clustering algorithms, such as k-means or hierarchical clustering, to group similar embeddings together based on their spatial proximity in the vector space. Each cluster can be considered as a symbolic representation or concept that captures a group of semantically related embeddings. Platform may analyze the clusters to identify common themes, attributes, or relationships among the embeddings within each cluster and then assign meaningful labels or descriptions to the clusters based on their content or representative embeddings.

[0340] In embodiments where dimension reduction techniques are used, platform 2120 may implement Principal Component Analysis (PCA) or t-SNE (t-Distributed Stochastic Neighbor Embedding), to reduce the high-dimensional embedding space to a lower-dimensional representation and then visualize the reduced-dimensional space to identify patterns, clusters, or separations among the embeddings. Platform can analyze the principal components or dimensions to understand the most significant factors contributing to the variance in the embedding space in order to interpret the dimensions or components in terms of their semantic meaning or the attributes they capture.

[0341] In other implementations, platform 2120 may use semantic similarity analysis to compute pairwise similarities or distances between embeddings using metrics such as cosine similarity, Euclidean distance, or dot product to identify pairs or groups of embeddings that have high semantic similarity, indicating their close relationship or shared attributes. The most similar embeddings may be analyzed to understand the semantic connections and relationships captured by the embedding space and to extract symbolic representations or rules based on the observed semantic similarities, such as synonyms, antonyms, or analogies.

[0342] At step 3002, the platform may utilize ontology alignment techniques that align the learned embeddings with existing ontologies or knowledge bases (e.g., knowledge graphs) that provide a structured symbolic representation of the domain. This may involve the use of ontology matching techniques, such as string similarity, semantic similarity, or structural similarity, to establish correspondences between embeddings and ontology concepts. Leverage the aligned ontology to assign symbolic labels or categories to the embeddings based on their semantic similarity to ontology

concepts and enrich the ontology with new concepts or relationships discovered from the embedding space.

[0343] FIG. 31 is a flow diagram illustrating an exemplary method for advanced reasoning using a composite artificial intelligence platform, according to an embodiment. According to the embodiment, the process begins at step 3101 by generating vector embeddings (i.e., learned representations) of input data using a plurality of neural network models trained on large datasets. This may be accomplished by applying transfer learning, fine-tuning, and/or multi-task learning techniques to improve the quality and generalizability of the embeddings. At step 3102 platform 2120 can store and retrieve symbolic facts, entities, and relations using an ontology or schema that defines the types of entities, relationships, and attributes relevant to a given system's (AI model) domain, populating the system with data from structured and unstructured sources using information extraction techniques. Symbolic information can be stored in one or more knowledge graph databases 2129. At step 3103 platform 2120, via DCG computing system 121 and hierarchical process system 2121 manages and routes processing tasks based on certainty thresholds and/or challenge based verification, selecting the appropriate models and data sources to complete the tasks.

[0344] As a next step 3104 platform can refine vector embeddings using contextual information by retrieving relevant facts, entities, and relationships from the knowledge base (e.g., knowledge graphs), updating the embeddings by incorporating the retrieved contextual information. At step 3105 platform 2120 combines the outputs of multiple models using expressive weighting schemes which dynamically adjust the contribution of each model based on various factors. Platform can implement secure communication protocols and access control mechanisms to ensure security, licensing compliance, and provenance tracking with respect to models, data sources, and decision making in a collaborative development environment at step 3106.

[0345] At step 3107 platform 2120 may align and harmonize representations across different data modalities and then optimize hyperparameters using information theoretic guidance at step 3108. As a last step 3109, platform 2120 extracts symbolic knowledge from the vector embeddings by analyzing the learned embeddings to extract symbolic representations and map the extracted symbolic representations to existing concepts and relationships in a knowledge graph.

[0346] In this way, platform 2120 can provide an end-to-end process of advanced reasoning in an artificial intelligence system, starting from the generation of vector embeddings using neural network models, progressing through the storage and retrieval of symbolic knowledge, managing and routing processing tasks, refining embeddings with contextual information, combining outputs of multiple models, ensuring security and compliance, aligning representations across modalities, optimizing hyperparameters, and finally extracting symbolic knowledge from the learned embeddings.

#### Exemplary Computing Environment

[0347] FIG. 32 illustrates an exemplary computing environment on which an embodiment described herein may be implemented, in full or in part. This exemplary computing environment describes computer-related components and processes supporting enabling disclosure of computer-implemented embodiments. Inclusion in this exemplary

computing environment of well-known processes and computer components, if any, is not a suggestion or admission that any embodiment is no more than an aggregation of such processes or components. Rather, implementation of an embodiment using processes and components described in this exemplary computing environment will involve programming or configuration of such processes and components resulting in a machine specially programmed or configured for such implementation. The exemplary computing environment described herein is only one example of such an environment and other configurations of the components and processes are possible, including other relationships between and among components, and/or absence of some processes or components described. Further, the exemplary computing environment described herein is not intended to suggest any limitation as to the scope of use or functionality of any embodiment implemented, in whole or in part, on components or processes described herein.

[0348] The exemplary computing environment described herein comprises a computing device **10** (further comprising a system bus **11**, one or more processors **20**, a system memory **30**, one or more interfaces **40**, one or more non-volatile data storage devices **50**), external peripherals and accessories **60**, external communication devices **70**, remote computing devices **80**, and cloud-based services **90**.

[0349] System bus **11** couples the various system components, coordinating operation of and data transmission between those various system components. System bus **11** represents one or more of any type or combination of types of wired or wireless bus structures including, but not limited to, memory busses or memory controllers, point-to-point connections, switching fabrics, peripheral busses, accelerated graphics ports, and local busses using any of a variety of bus architectures. By way of example, such architectures include, but are not limited to, Industry Standard Architecture (ISA) busses, Micro Channel Architecture (MCA) busses, Enhanced ISA (EISA) busses, Video Electronics Standards Association (VESA) local busses, a Peripheral Component Interconnects (PCI) busses also known as a Mezzanine busses, or any selection of, or combination of, such busses. Depending on the specific physical implementation, one or more of the processors **20**, system memory **30** and other components of the computing device **10** can be physically co-located or integrated into a single physical component, such as on a single chip. In such a case, some or all of system bus **11** can be electrical pathways within a single chip structure.

[0350] Computing device may further comprise externally-accessible data input and storage devices **12** such as compact disc read-only memory (CD-ROM) drives, digital versatile discs (DVD), or other optical disc storage for reading and/or writing optical discs **62**; magnetic cassettes, magnetic tape, magnetic disk storage, or other magnetic storage devices; or any other medium which can be used to store the desired content and which can be accessed by the computing device **10**. Computing device may further comprise externally-accessible data ports or connections **12** such as serial ports, parallel ports, universal serial bus (USB) ports, and infrared ports and/or transmitter/receivers. Computing device may further comprise hardware for wireless communication with external devices such as IEEE 1394 ("Firewire") interfaces, IEEE 802.11 wireless interfaces, BLUETOOTH® wireless interfaces, and so forth. Such ports and interfaces may be used to connect any number of

external peripherals and accessories **60** such as visual displays, monitors, and touch-sensitive screens **61**, USB solid state memory data storage drives (commonly known as "flash drives" or "thumb drives") **63**, printers **64**, pointers and manipulators such as mice **65**, keyboards **66**, and other devices **67** such as joysticks and gaming pads, touchpads, additional displays and monitors, and external hard drives (whether solid state or disc-based), microphones, speakers, cameras, and optical scanners.

[0351] Processors **20** are logic circuitry capable of receiving programming instructions and processing (or executing) those instructions to perform computer operations such as retrieving data, storing data, and performing mathematical calculations. Processors **20** are not limited by the materials from which they are formed or the processing mechanisms employed therein, but are typically comprised of semiconductor materials into which many transistors are formed together into logic gates on a chip (i.e., an integrated circuit or IC). The term processor includes any device capable of receiving and processing instructions including, but not limited to, processors operating on the basis of quantum computing, optical computing, mechanical computing (e.g., using nanotechnology entities to transfer data), and so forth. Depending on configuration, computing device **10** may comprise more than one processor. For example, computing device **10** may comprise one or more central processing units (CPUs) **21**, each of which itself has multiple processors or multiple processing cores, each capable of independently or semi-independently processing programming instructions based on technologies like complex instruction set computer (CISC) or reduced instruction set computer (RISC). Further, computing device **10** may comprise one or more specialized processors such as a graphics processing unit (GPU) **22** configured to accelerate processing of computer graphics and images via a large array of specialized processing cores arranged in parallel. Further computing device **10** may be comprised of one or more specialized processes such as Intelligent Processing Units, field-programmable gate arrays or application-specific integrated circuits for specific tasks or types of tasks. The term processor may further include: neural processing units (NPUs) or neural computing units optimized for machine learning and artificial intelligence workloads using specialized architectures and data paths; tensor processing units (TPUs) designed to efficiently perform matrix multiplication and convolution operations used heavily in neural networks and deep learning applications; application-specific integrated circuits (ASICs) implementing custom logic for domain-specific tasks; application-specific instruction set processors (ASIPs) with instruction sets tailored for particular applications; field-programmable gate arrays (FPGAs) providing reconfigurable logic fabric that can be customized for specific processing tasks; processors operating on emerging computing paradigms such as quantum computing, optical computing, mechanical computing (e.g., using nanotechnology entities to transfer data), and so forth. Depending on configuration, computing device **10** may comprise one or more of any of the above types of processors in order to efficiently handle a variety of general purpose and specialized computing tasks. The specific processor configuration may be selected based on performance, power, cost, or other design constraints relevant to the intended application of computing device **10**.

[0352] System memory **30** is processor-accessible data storage in the form of volatile and/or nonvolatile memory.

System memory **30** may be either or both of two types: non-volatile memory and volatile memory. Non-volatile memory **30a** is not erased when power to the memory is removed, and includes memory types such as read only memory (ROM), electronically-erasable programmable memory (EEPROM), and rewritable solid state memory (commonly known as “flash memory”). Non-volatile memory **30a** is typically used for long-term storage of a basic input/output system (BIOS) **31**, containing the basic instructions, typically loaded during computer startup, for transfer of information between components within computing device, or a unified extensible firmware interface (UEFI), which is a modern replacement for BIOS that supports larger hard drives, faster boot times, more security features, and provides native support for graphics and mouse cursors. Non-volatile memory **30a** may also be used to store firmware comprising a complete operating system **35** and applications **36** for operating computer-controlled devices. The firmware approach is often used for purpose-specific computer-controlled devices such as appliances and Internet-of-Things (IoT) devices where processing power and data storage space is limited. Volatile memory **30b** is erased when power to the memory is removed and is typically used for short-term storage of data for processing. Volatile memory **30b** includes memory types such as random-access memory (RAM), and is normally the primary operating memory into which the operating system **35**, applications **36**, program modules **37**, and application data **38** are loaded for execution by processors **20**. Volatile memory **30b** is generally faster than non-volatile memory **30a** due to its electrical characteristics and is directly accessible to processors **20** for processing of instructions and data storage and retrieval. Volatile memory **30b** may comprise one or more smaller cache memories which operate at a higher clock speed and are typically placed on the same IC as the processors to improve performance.

[0353] There are several types of computer memory, each with its own characteristics and use cases. System memory **30** may be configured in one or more of the several types described herein, including high bandwidth memory (HBM) and advanced packaging technologies like chip-on-wafer-on-substrate (CoWoS). Static random access memory (SRAM) provides fast, low-latency memory used for cache memory in processors, but is more expensive and consumes more power compared to dynamic random access memory (DRAM). SRAM retains data as long as power is supplied. DRAM is the main memory in most computer systems and is slower than SRAM but cheaper and more dense. DRAM requires periodic refresh to retain data. NAND flash is a type of non-volatile memory used for storage in solid state drives (SSDs) and mobile devices and provides high density and lower cost per bit compared to DRAM with the trade-off of slower write speeds and limited write endurance. HBM is an emerging memory technology that provides high bandwidth and low power consumption which stacks multiple DRAM dies vertically, connected by through-silicon vias (TSVs). HBM offers much higher bandwidth (up to 1 TB/s) compared to traditional DRAM and may be used in high-performance graphics cards, AI accelerators, and edge computing devices. Advanced packaging and CoWoS are technologies that enable the integration of multiple chips or dies into a single package. CoWoS is a 2.5D packaging technology that interconnects multiple dies side-by-side on a silicon interposer and allows for higher bandwidth, lower

latency, and reduced power consumption compared to traditional PCB-based packaging. This technology enables the integration of heterogeneous dies (e.g., CPU, GPU, HBM) in a single package and may be used in high-performance computing, AI accelerators, and edge computing devices.

[0354] Interfaces **40** may include, but are not limited to, storage media interfaces **41**, network interfaces **42**, display interfaces **43**, and input/output interfaces **44**. Storage media interface **41** provides the necessary hardware interface for loading data from non-volatile data storage devices **50** into system memory **30** and storage data from system memory **30** to non-volatile data storage device **50**. Network interface **42** provides the necessary hardware interface for computing device **10** to communicate with remote computing devices **80** and cloud-based services **90** via one or more external communication devices **70**. Display interface **43** allows for connection of displays **61**, monitors, touchscreens, and other visual input/output devices. Display interface **43** may include a graphics card for processing graphics-intensive calculations and for handling demanding display requirements. Typically, a graphics card includes a graphics processing unit (GPU) and video RAM (VRAM) to accelerate display of graphics. In some high-performance computing systems, multiple GPUs may be connected using NVLink bridges, which provide high-bandwidth, low-latency interconnects between GPUs. NVLink bridges enable faster data transfer between GPUs, allowing for more efficient parallel processing and improved performance in applications such as machine learning, scientific simulations, and graphics rendering. One or more input/output (I/O) interfaces **44** provide the necessary support for communications between computing device **10** and any external peripherals and accessories **60**. For wireless communications, the necessary radio-frequency hardware and firmware may be connected to I/O interface **44** or may be integrated into I/O interface **44**. Network interface **42** may support various communication standards and protocols, such as Ethernet and Small Form-Factor Pluggable (SFP). Ethernet is a widely used wired networking technology that enables local area network (LAN) communication. Ethernet interfaces typically use RJ45 connectors and support data rates ranging from 10 Mbps to 100 Gbps, with common speeds being 100 Mbps, 1 Gbps, 10 Gbps, 25 Gbps, 40 Gbps, and 100 Gbps. Ethernet is known for its reliability, low latency, and cost-effectiveness, making it a popular choice for home, office, and data center networks. SFP is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. SFP interfaces provide a modular and flexible solution for connecting network devices, such as switches and routers, to fiber optic or copper networking cables. SFP transceivers support various data rates, ranging from 100 Mbps to 100 Gbps, and can be easily replaced or upgraded without the need to replace the entire network interface card. This modularity allows for network scalability and adaptability to different network requirements and fiber types, such as single-mode or multi-mode fiber.

[0355] Non-volatile data storage devices **50** are typically used for long-term storage of data. Data on non-volatile data storage devices **50** is not erased when power to the non-volatile data storage devices **50** is removed. Non-volatile data storage devices **50** may be implemented using any technology for non-volatile storage of content including, but not limited to, CD-ROM drives, digital versatile discs (DVD), or other optical disc storage; magnetic cassettes,

magnetic tape, magnetic disc storage, or other magnetic storage devices; solid state memory technologies such as EEPROM or flash memory; or other memory technology or any other medium which can be used to store data without requiring power to retain the data after it is written. Non-volatile data storage devices **50** may be non-removable from computing device **10** as in the case of internal hard drives, removable from computing device **10** as in the case of external USB hard drives, or a combination thereof, but computing device will typically comprise one or more internal, non-removable hard drives using either magnetic disc or solid state memory technology. Non-volatile data storage devices **50** may be implemented using various technologies, including hard disk drives (HDDs) and solid-state drives (SSDs). HDDs use spinning magnetic platters and read/write heads to store and retrieve data, while SSDs use NAND flash memory. SSDs offer faster read/write speeds, lower latency, and better durability due to the lack of moving parts, while HDDs typically provide higher storage capacities and lower cost per gigabyte. NAND flash memory comes in different types, such as Single-Level Cell (SLC), Multi-Level Cell (MLC), Triple-Level Cell (TLC), and Quad-Level Cell (QLC), each with trade-offs between performance, endurance, and cost. Storage devices connect to the computing device **10** through various interfaces, such as SATA, NVMe, and PCIe. SATA is the traditional interface for HDDs and SATA SSDs, while NVMe (Non-Volatile Memory Express) is a newer, high-performance protocol designed for SSDs connected via PCIe. PCIe SSDs offer the highest performance due to the direct connection to the PCIe bus, bypassing the limitations of the SATA interface. Other storage form factors include M.2 SSDs, which are compact storage devices that connect directly to the motherboard using the M.2 slot, supporting both SATA and NVMe interfaces. Additionally, technologies like Intel Optane memory combine 3D XPoint technology with NAND flash to provide high-performance storage and caching solutions. Non-volatile data storage devices **50** may be non-removable from computing device **10**, as in the case of internal hard drives, removable from computing device **10**, as in the case of external USB hard drives, or a combination thereof. However, computing devices will typically comprise one or more internal, non-removable hard drives using either magnetic disc or solid-state memory technology. Non-volatile data storage devices **50** may store any type of data including, but not limited to, an operating system **51** for providing low-level and mid-level functionality of computing device **10**, applications **52** for providing high-level functionality of computing device **10**, program modules **53** such as containerized programs or applications, or other modular content or modular programming, application data **54**, and databases **55** such as relational databases, non-relational databases, object oriented databases, NoSQL databases, vector databases, knowledge graph databases, key-value databases, document oriented data stores, and graph databases.

[0356] Applications (also known as computer software or software applications) are sets of programming instructions designed to perform specific tasks or provide specific functionality on a computer or other computing devices. Applications are typically written in high-level programming languages such as C, C++, Scala, Erlang, GoLang, Java, Scala, Rust, and Python, which are then either interpreted at runtime or compiled into low-level, binary, processor-executable instructions operable on processors **20**. Applica-

tions may be containerized so that they can be run on any computer hardware running any known operating system. Containerization of computer software is a method of packaging and deploying applications along with their operating system dependencies into self-contained, isolated units known as containers. Containers provide a lightweight and consistent runtime environment that allows applications to run reliably across different computing environments, such as development, testing, and production systems facilitated by specifications such as containerd.

[0357] The memories and non-volatile data storage devices described herein do not include communication media. Communication media are means of transmission of information such as modulated electromagnetic waves or modulated data signals configured to transmit, not store, information. By way of example, and not limitation, communication media includes wired communications such as sound signals transmitted to a speaker via a speaker wire, and wireless communications such as acoustic waves, radio frequency (RF) transmissions, infrared emissions, and other wireless media.

[0358] External communication devices **70** are devices that facilitate communications between computing device and either remote computing devices **80**, or cloud-based services **90**, or both. External communication devices **70** include, but are not limited to, data modems **71** which facilitate data transmission between computing device and the Internet **75** via a common carrier such as a telephone company or internet service provider (ISP), routers **72** which facilitate data transmission between computing device and other devices, and switches **73** which provide direct data communications between devices on a network or optical transmitters (e.g., lasers). Here, modem **71** is shown connecting computing device **10** to both remote computing devices **80** and cloud-based services **90** via the Internet **75**. While modem **71**, router **72**, and switch **73** are shown here as being connected to network interface **42**, many different network configurations using external communication devices **70** are possible. Using external communication devices **70**, networks may be configured as local area networks (LANs) for a single location, building, or campus, wide area networks (WANs) comprising data networks that extend over a larger geographical area, and virtual private networks (VPNs) which can be of any size but connect computers via encrypted communications over public networks such as the Internet **75**. As just one exemplary network configuration, network interface **42** may be connected to switch **73** which is connected to router **72** which is connected to modem **71** which provides access for computing device **10** to the Internet **75**. Further, any combination of wired **77** or wireless **76** communications between and among computing device **10**, external communication devices **70**, remote computing devices **80**, and cloud-based services **90** may be used. Remote computing devices **80**, for example, may communicate with computing device through a variety of communication channels **74** such as through switch **73** via a wired **77** connection, through router **72** via a wireless connection **76**, or through modem **71** via the Internet **75**. Furthermore, while not shown here, other hardware that is specifically designed for servers or networking functions may be employed. For example, secure socket layer (SSL) acceleration cards can be used to offload SSL encryption computations, and transmission control protocol/internet protocol (TCP/IP) offload hardware and/or packet

classifiers on network interfaces **42** may be installed and used at server devices or intermediate networking equipment (e.g., for deep packet inspection).

[0359] In a networked environment, certain components of computing device **10** may be fully or partially implemented on remote computing devices **80** or cloud-based services **90**. Data stored in non-volatile data storage device **50** may be received from, shared with, duplicated on, or offloaded to a non-volatile data storage device on one or more remote computing devices **80** or in a cloud computing service **92**. Processing by processors **20** may be received from, shared with, duplicated on, or offloaded to processors of one or more remote computing devices **80** or in a distributed computing service **93**. By way of example, data may reside on a cloud computing service **92**, but may be usable or otherwise accessible for use by computing device **10**. Also, certain processing subtasks may be sent to a microservice **91** for processing with the result being transmitted to computing device **10** for incorporation into a larger processing task. Also, while components and processes of the exemplary computing environment are illustrated herein as discrete units (e.g., OS **51** being stored on non-volatile data storage device **51** and loaded into system memory **35** for use) such processes and components may reside or be processed at various times in different components of computing device **10**, remote computing devices **80**, and/or cloud-based services **90**. Also, certain processing subtasks may be sent to a microservice **91** for processing with the result being transmitted to computing device **10** for incorporation into a larger processing task. Infrastructure as Code (IaaC) tools like Terraform can be used to manage and provision computing resources across multiple cloud providers or hyperscalers. This allows for workload balancing based on factors such as cost, performance, and availability. For example, Terraform can be used to automatically provision and scale resources on AWS spot instances during periods of high demand, such as for surge rendering tasks, to take advantage of lower costs while maintaining the required performance levels. In the context of rendering, tools like Blender can be used for object rendering of specific elements, such as a car, bike, or house. These elements can be approximated and roughed in using techniques like bounding box approximation or low-poly modeling to reduce the computational resources required for initial rendering passes. The rendered elements can then be integrated into the larger scene or environment as needed, with the option to replace the approximated elements with higher-fidelity models as the rendering process progresses.

[0360] In an implementation, the disclosed systems and methods may utilize, at least in part, containerization techniques to execute one or more processes and/or steps disclosed herein. Containerization is a lightweight and efficient virtualization technique that allows you to package and run applications and their dependencies in isolated environments called containers. One of the most popular containerization platforms is containerd, which is widely used in software development and deployment. Containerization, particularly with open-source technologies like containerd and container orchestration systems like Kubernetes, is a common approach for deploying and managing applications. Containers are created from images, which are lightweight, standalone, and executable packages that include application code, libraries, dependencies, and runtime. Images are often built from a containerfile or similar, which contains instruc-

tions for assembling the image. Containerfiles are configuration files that specify how to build a container image. Systems like Kubernetes natively support containerd as a container runtime. They include commands for installing dependencies, copying files, setting environment variables, and defining runtime configurations. Container images can be stored in repositories, which can be public or private. Organizations often set up private registries for security and version control using tools such as Harbor, JFrog Artifactory and Bintray, GitLab Container Registry, or other container registries. Containers can communicate with each other and the external world through networking. Containerd provides a default network namespace, but can be used with custom network plugins. Containers within the same network can communicate using container names or IP addresses.

[0361] Remote computing devices **80** are any computing devices not part of computing device **10**. Remote computing devices **80** include, but are not limited to, personal computers, server computers, thin clients, thick clients, personal digital assistants (PDAs), mobile telephones, watches, tablet computers, laptop computers, multiprocessor systems, microprocessor based systems, set-top boxes, programmable consumer electronics, video game machines, game consoles, portable or handheld gaming units, network terminals, desktop personal computers (PCs), minicomputers, mainframe computers, network nodes, virtual reality or augmented reality devices and wearables, and distributed or multi-processing computing environments. While remote computing devices **80** are shown for clarity as being separate from cloud-based services **90**, cloud-based services **90** are implemented on collections of networked remote computing devices **80**.

[0362] Cloud-based services **90** are Internet-accessible services implemented on collections of networked remote computing devices **80**. Cloud-based services are typically accessed via application programming interfaces (APIs) which are software interfaces which provide access to computing services within the cloud-based service via API calls, which are pre-defined protocols for requesting a computing service and receiving the results of that computing service. While cloud-based services may comprise any type of computer processing or storage, three common categories of cloud-based services **90** are serverless logic apps, microservices **91**, cloud computing services **92**, and distributed computing services **93**.

[0363] Microservices **91** are collections of small, loosely coupled, and independently deployable computing services. Each microservice represents a specific computing functionality and runs as a separate process or container. Microservices promote the decomposition of complex applications into smaller, manageable services that can be developed, deployed, and scaled independently. These services communicate with each other through well-defined application programming interfaces (APIs), typically using lightweight protocols like HTTP, protobufs, gRPC or message queues such as Kafka. Microservices **91** can be combined to perform more complex or distributed processing tasks. In an embodiment, Kubernetes clusters with containerized resources are used for operational packaging of system.

[0364] Cloud computing services **92** are delivery of computing resources and services over the Internet **75** from a remote location. Cloud computing services **92** provide additional computer hardware and storage on as-needed or subscription basis. Cloud computing services **92** can provide

large amounts of scalable data storage, access to sophisticated software and powerful server-based processing, or entire computing infrastructures and platforms. For example, cloud computing services can provide virtualized computing resources such as virtual machines, storage, and networks, platforms for developing, running, and managing applications without the complexity of infrastructure management, and complete software applications over public or private networks or the Internet on a subscription or alternative licensing basis, or consumption or ad-hoc marketplace basis, or combination thereof.

**[0365]** Distributed computing services 93 provide large-scale processing using multiple interconnected computers or nodes to solve computational problems or perform tasks collectively. In distributed computing, the processing and storage capabilities of multiple machines are leveraged to work together as a unified system. Distributed computing services are designed to address problems that cannot be efficiently solved by a single computer or that require large-scale computational power or support for highly dynamic compute, transport or storage resource variance or uncertainty over time requiring scaling up and down of constituent system resources. These services enable parallel processing, fault tolerance, and scalability by distributing tasks across multiple nodes.

**[0366]** Although described above as a physical device, computing device 10 can be a virtual computing device, in which case the functionality of the physical components herein described, such as processors 20, system memory 30, network interfaces 40, NVLink or other GPU-to-GPU high bandwidth communications links and other like components can be provided by computer-executable instructions. Such computer-executable instructions can execute on a single physical computing device, or can be distributed across multiple physical computing devices, including being distributed across multiple physical computing devices in a dynamic manner such that the specific, physical computing devices hosting such computer-executable instructions can dynamically change over time depending upon need and availability. In the situation where computing device 10 is a virtualized device, the underlying physical computing devices hosting such a virtualized computing device can, themselves, comprise physical components analogous to those described above, and operating in a like manner. Furthermore, virtual computing devices can be utilized in multiple layers with one virtual computing device executing within the construct of another virtual computing device. Thus, computing device 10 may be either a physical computing device or a virtualized computing device within which computer-executable instructions can be executed in a manner consistent with their execution by a physical computing device. Similarly, terms referring to physical components of the computing device, as utilized herein, mean either those physical components or virtualizations thereof performing the same or equivalent functions.

**[0367]** The skilled person will be aware of a range of possible modifications of the various aspects described above. Accordingly, the present invention is defined by the claims and their equivalents.

What is claimed is:

1. A computing system for integration of machine learning models and facilitating transactions between buyers, sellers, and experts employing a marketplace platform, the computing system comprising:

one or more hardware processors configured for:  
listing, searching, and transacting various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement;  
selecting and integrating machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy;  
collecting and aggregating evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods;  
securely processing payments, licensing, and delivery of acquired goods between buyers and sellers;  
facilitating communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and ensuring transparency, accountability, and adherence to quality standards and ethical principles in the marketplace for robust multi stakeholder development of robust solutions while preserving intellectual property rights of individuals and groups in downstream systems.

2. The computing system of claim 1, wherein the one or more hardware processors are further configured for:

collecting the expert evaluations and ratings while browsing external data sources;  
quantifying the quality, relevance, and suitability of listed goods based on expert judgments; and  
assessing the credibility and reliability of experts based on their historical evaluations and community feedback.

3. The computing system of claim 1, wherein the one or more hardware processors are further configured for:

securely processing financial transactions between buyers and sellers;  
generating and enforcing usage rights and restrictions for acquired goods; and  
holding funds until the satisfactory delivery and acceptance of goods.

4. The computing system of claim 1, wherein the one or more hardware processors are further configured for:

sharing and co-developing machine learning projects; and documenting best practices, tutorials, and case studies related to the listed goods.

5. The computing system of claim 1, wherein the one or more hardware processors are further configured for proactively suggesting relevant goods, experts, or collaborators based on user preferences, transaction history, and platform interactions.

6. The computing system of claim 1, wherein the one or more hardware processors are further configured for:

assessing the interoperability and combinability of different machine learning models and datasets;  
evaluating the efficiency and scalability of integrated models; and  
suggesting improvements and enhancements to the selected models and datasets.

7. The computing system of claim 1, wherein the one or more hardware processors are further configured for selecting, creating, and incorporating trained models based on expert judgment inputs.

8. The computing system of claim 1, wherein the one or more hardware processors are further configured for:  
continuously adjusting and optimizing the hyperparameters of machine learning and artificial intelligence models based on performance metrics and user feedback;  
dynamically updating and fine-tuning machine learning and artificial intelligence models based on newly available data and evolving user requirements;  
optimizing the retrieval and generation components of RAG models, including fine-tuning retrieval algorithms, updating knowledge bases, and enhancing generation quality; and  
incorporating user feedback and preferences into the optimization process, ensuring continuous improvement and alignment with user expectations.
9. A computer-implemented method executed on a marketplace platform for integration of machine learning models and facilitating transactions between buyers, sellers, and experts, the computer-implemented method comprising:  
listing, searching, and transacting various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement;  
selecting and integrating machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy;  
collecting and aggregating evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods;  
securely processing payments, licensing, and delivery of acquired goods between buyers and sellers;  
facilitating communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and  
ensuring transparency, accountability, and adherence to quality standards and ethical principles in the marketplace for robust multi stakeholder development of robust solutions while preserving intellectual property rights of individuals and groups in downstream systems.
10. The computer-implemented method of claim 9, wherein the one or more hardware processors are further configured for:  
collecting the expert evaluations and ratings while browsing external data sources;  
quantifying the quality, relevance, and suitability of listed goods based on expert judgments; and  
assessing the credibility and reliability of experts based on their historical evaluations and community feedback.
11. The computer-implemented method of claim 9, further comprising:  
securely processing financial transactions between buyers and sellers;  
generating and enforcing usage rights and restrictions for acquired goods; and  
holding funds until the satisfactory delivery and acceptance of goods.
12. The computer-implemented method of claim 9, further comprising:  
sharing and co-developing machine learning projects; and

- documenting best practices, tutorials, and case studies related to the listed goods.
13. The computer-implemented method of claim 9, further comprising proactively suggesting relevant goods, experts, or collaborators based on user preferences, transaction history, and platform interactions.
14. The computer-implemented method of claim 9, further comprising:  
assessing the interoperability and combinability of different machine learning models and datasets;  
evaluating the efficiency and scalability of integrated models; and  
suggesting improvements and enhancements to the selected models and datasets.
15. The computer-implemented method of claim 9, further comprising selecting, creating, and incorporating trained models based on expert judgment inputs.
16. The computer-implemented method of claim 9, further comprising:  
continuously adjusting and optimizing the hyperparameters of machine learning and artificial intelligence models based on performance metrics and user feedback;  
dynamically updating and fine-tuning machine learning and artificial intelligence models based on newly available data and evolving user requirements;  
optimizing the retrieval and generation components of RAG models, including fine-tuning retrieval algorithms, updating knowledge bases, and enhancing generation quality; and  
incorporating user feedback and preferences into the optimization process, ensuring continuous improvement and alignment with user expectations.
17. A system for integration of machine learning models and facilitating transactions between buyers, sellers, and experts employing a marketplace platform, comprising one or more computers with executable instructions that, when executed, cause the system to:  
list, search, and transact various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement;  
select and integrate machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy;  
collect and aggregate evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods;  
securely process payments, licensing, and delivery of acquired goods between buyers and sellers;  
facilitate communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and  
ensure transparency, accountability, and adherence to quality standards and ethical principles in the marketplace for robust multi stakeholder development of robust solutions while preserving intellectual property rights of individuals and groups in downstream systems.
18. The system of claim 17, wherein the system is further caused to:

collect the expert evaluations and ratings while browsing external data sources;

quantify the quality, relevance, and suitability of listed goods based on expert judgments; and

assess the credibility and reliability of experts based on their historical evaluations and community feedback.

**19.** The system of claim 17, wherein the system is further caused to:

- securely process financial transactions between buyers and sellers;
- generate and enforcing usage rights and restrictions for acquired goods; and
- hold funds until the satisfactory delivery and acceptance of goods.

**20.** The system of claim 17, wherein the system is further caused to:

- share and co-develop machine learning projects; and
- document best practices, tutorials, and case studies related to the listed goods.

**21.** The system of claim 17, wherein the system is further caused to proactively suggest relevant goods, experts, or collaborators based on user preferences, transaction history, and platform interactions.

**22.** The system of claim 17, wherein the system is further caused to:

- assess the interoperability and combinability of different machine learning models and datasets;
- evaluate the efficiency and scalability of integrated models; and
- suggest improvements and enhancements to the selected models and datasets.

**23.** The system of claim 17, wherein the system is further caused to select, create, and incorporate trained models based on expert judgment inputs.

**24.** The system of claim 17, further comprising:

- continuously adjust and optimize the hyperparameters of machine learning and artificial intelligence models based on performance metrics and user feedback;
- dynamically update and fine-tune machine learning and artificial intelligence models based on newly available data and evolving user requirements;
- optimize the retrieval and generation components of RAG models, including fine-tuning retrieval algorithms, updating knowledge bases, and enhancing generation quality; and
- incorporate user feedback and preferences into the optimization process, ensuring continuous improvement and alignment with user expectations.

**25.** Non-transitory, computer-readable storage media having computer-executable instructions embodied thereon that, when executed by one or more processors of a computing system employing a marketplace platform for integration of machine learning models and facilitating transactions between buyers, sellers, and experts, cause the computing system to:

- list, search, and transact various machine learning and artificial intelligence assets comprising models, datasets, embeddings, Retrieval Augmented Generations (RAGs), knowledge corpora, simulations, human or

expert responses, surveys, and related goods in a marketplace with data contract specification and enforcement;

select and integrate machine learning, artificial intelligence, and simulation models based on user requirements and compatibility and compliance and privacy; collect and aggregate evaluations and ratings from human experts and artificial intelligence expert models on the quality, performance, energy efficiency, or suitability of listed goods;

securely process payments, licensing, and delivery of acquired goods between buyers and sellers;

facilitate communication, collaboration, and knowledge sharing among buyers, sellers, and experts; and

ensure transparency, accountability, and adherence to quality standards and ethical principles in the marketplace for robust multi stakeholder development of robust solutions while preserving intellectual property rights of individuals and groups in downstream systems.

**26.** The non-transitory, computer-readable storage media of claim 25, wherein the computing system is further caused to:

- collect the expert evaluations and ratings while browsing external data sources;
- quantify the quality, relevance, and suitability of listed goods based on expert judgments; and
- assess the credibility and reliability of experts based on their historical evaluations and community feedback.

**27.** The non-transitory, computer-readable storage media of claim 25, wherein the computing system is further caused to:

- securely process financial transactions between buyers and sellers;
- generate and enforcing usage rights and restrictions for acquired goods; and
- hold funds until the satisfactory delivery and acceptance of goods.

**28.** The non-transitory, computer-readable storage media of claim 25, wherein the computing system is further caused to:

- share and co-develop machine learning projects; and
- document best practices, tutorials, and case studies related to the listed goods.

**29.** The non-transitory, computer-readable storage media of claim 25, wherein the computing system is further caused to proactively suggest relevant goods, experts, or collaborators based on user preferences, transaction history, and platform interactions.

**30.** The non-transitory, computer-readable storage media of claim 25, wherein the computing system is further caused to:

- assess the interoperability and combinability of different machine learning models and datasets;
- evaluate the efficiency and scalability of integrated models; and
- suggest improvements and enhancements to the selected models and datasets.