FORM 2

THE PATENT ACT 1970

(39 OF 1970)

&

The Patents Rule, 2003

PROVISIONAL OR COMPLETE SPECIFICATION

(See Section 10 and rule 13)

TITLE OF THE INVENTION: SYSTEM AND METHOD FOR ASSIGNING, EMBEDDING, AND VERIFYING DIGITAL IDENTITY AND PROVENANCE OF AI ENTITIES

1. APPLICANT

Name	Nationality	Address
Srinivas Raju Chakravaram	Indian	Flat 101, Kakatiya Homes, Nallagandla HUDA Layout, Serilingampally, Hyderabad - 500019, Telangana State
Prathyusha Kasi	Indian	Flat 101, Kakatiya Homes, Nallagandla HUDA Layout, Serilingampally, Hyderabad - 500019, Telangana State

2. PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION

The following complete specification particularly describes the invention and the manner in which it is to be performed.

TECHNICAL FIELD

[001] The present disclosure relates to the field of artificial intelligence (AI) and digital identity systems. More particularly, the present disclosure relates to a system and method for assigning, embedding, and verifying digital identity and provenance of ai entities.

BACKGROUND

[002] As artificial intelligence (AI) systems increasingly generate digital content, make autonomous decisions, and power physical devices such as drones, robots, and smart IoT systems, serious concerns have emerged regarding the traceability, authenticity, and accountability of AI-generated outputs. Existing AI platforms do not natively embed persistent digital identities within their tools, agents, or outputs, leaving end-users, developers, and regulators with no reliable way to verify the origin, ownership, or trustworthiness of such content.

[003] Conventional methods for digital content verification are typically limited to file signatures, watermarks, or origin headers, which are format-specific, fragile, and easily tampered with. These techniques are insufficient in AI ecosystems where content is dynamically generated, transformed, or passed through multi-agent workflows. Most notably, current systems fail to account for the collaborative nature of AI agents, where multiple models or services contribute to a composite output, making attribution and provenance tracking difficult or impossible.

[004] Some digital rights management (DRM) and digital watermarking systems have attempted to address provenance in multimedia content. However, they are primarily focused on copyright protection and do not support identity tagging of autonomous decision-making, behavioral outputs, or real-time AI actions. Furthermore, they lack integration with AI model registries, provide no lineage tracing, and do not support dynamic trust scoring based on compliance or behavioral metrics.

[005] Similarly, device identity and management solutions, such as TPM-based authentication or serial number encoding, are fragmented and vendor-specific, with no unified framework for identifying AI-powered physical devices in a verifiable

and tamper-resistant manner. These systems also lack support for lifecycle logging or policy-based trust enforcement.

[006] There is also no standard or open framework enabling AI agents to verify each other's identities before collaboration, which poses a major security and interoperability risk in decentralized or agentic AI environments.

[007] In light of these limitations, there remains a critical unmet need for a unified, cross-modal identity infrastructure that assigns persistent, verifiable identifiers to AI tools, agents, and devices, supports chained provenance tracking, and provides publicly accessible verification interfaces for trust validation and regulatory compliance.

SUMMARY

[008] In one aspect of the present disclosure, A system and method for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices is provided.

[009] In some aspect of the present disclosure, a system for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, comprising a registration interface adapted to receive metadata corresponding to an AI tool, agent, or device submitted by a user; an AI identity and provenance engine communicatively coupled with the registration interface through a communication network; the AI identity and provenance engine including: a processor configured to process the received metadata and AI-generated outputs; wherein the processor is adapted to:

[010] assign a globally unique, cryptographically verifiable AI Registry Identifier (AIREG ID) to each registered AI tool, agent, or device; tag each output generated by the registered AI tool, agent, or device, comprising at least one of text, image, audio, video, or autonomous agent behaviour, with the corresponding AIREG ID and associated metadata by way of a metadata tagging engine; generate a chainable Provenance Identifier (PROV_ID) for each AI-generated output by way of a provenance tracking engine, wherein the PROV_ID records lineage, collaboration history, and generation context; verify the identity, trust score, and provenance history of the AI-generated output through a verification engine, the verification

engine comprising at least one of a browser extension, public web portal, or API endpoint; embed the AIREG ID and firmware-level metadata into AI-enabled physical devices using one or more of QR code, NFC tag, or cryptographic signature by way of a device identity engine; and restrict or allow execution of AI agent tasks or device operations based on policy-based trust evaluation using an execution control engine; wherein the system enables persistent digital identity management, end-to-end provenance traceability, and real-time verification for AI-generated outputs and devices.

[011] In some aspect of the present disclosure, the metadata tagging engine is configured to support both inline tagging, by embedding metadata directly into file headers or content wrappers, and detached tagging, using reference hashes or secure pointers for non-modifiable formats.

[012] In some aspect of the present disclosure, the metadata associated with the AIREG ID comprises at least one of: tool or model name, developer or organization, platform, version number, issuance timestamp, modality type, and trust status.

[013] In some aspect of the present disclosure, the provenance tracking engine is further configured to maintain a graph-based ancestry structure linking recursively chainable PROV_IDs to track collaborative and multi-agent output generation.

[014] In some aspect of the present disclosure, the verification engine is further adapted to display real-time provenance information, including the full chain of contributing AIREG IDs, associated trust scores, and registry metadata.

[015] In some aspect of the present disclosure, the device identity engine is further configured to log lifecycle events of physical AI devices, including manufacturing details, software or firmware updates, deployment locations, and operational tasks.

[016] In some aspect of the present disclosure, the execution control engine applies trust-based policies that permit task execution only if the associated AIREG ID and PROV_ID meet predefined thresholds for trust score, compliance level, or registry validation.

[017] In some aspect of the present disclosure, AI agents participating in multi-agent workflows exchange identity credentials using a peer-to-peer identity

negotiation protocol, including cryptographic challenge-response and optional zero-knowledge proof verification.

[018] In some aspect of the present disclosure, the processor is further configured to apply visual or invisible "Dignity Badges" to AI-generated outputs, embedding the AIREG ID and verification URL for public authentication and trust labeling.

[019] In some aspect of the present disclosure, A method for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, the method comprising the steps of receiving, by a registration interface, metadata associated with an AI tool, agent, or device; assigning, by a processor, a globally unique, cryptographically verifiable AI Registry Identifier (AIREG ID) to the AI tool, agent, or device based on the received metadata; tagging, by a metadata tagging engine, AI-generated outputs with the assigned AIREG ID and associated metadata, the outputs comprising at least one of text, image, audio, video, or agentic behavior; generating, by a provenance tracking engine, a chainable Provenance Identifier (PROV_ID) for each tagged output, the PROV_ID recording generation context and lineage; verifying, by a verification engine, the identity, trust score, and provenance chain of the AI-generated output using at least one of a browser extension, web portal, or API; embedding, by a device identity engine, the AIREG ID and metadata into AI-enabled physical devices using one or more of QR codes, NFC tags, or firmware-level cryptographic signatures; and enforcing, by an execution control engine, trust-based task execution policies based on validation of identity, provenance, and compliance status.

BRIEF DESCRIPTION OF DRAWINGS

[020] The accompanying drawings, which are incorporated in and constitute a part of this specification, show certain aspects of the subject matter disclosed herein and together with the description, help explain some of the principles associated with the disclosed implementations. In the drawing,

[021] Figure 1 illustrates a system (100) for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, in accordance with an aspect of the present disclosure; and

[022] Figure 2 illustrates a method for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, in accordance with an aspect of the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[023] The present disclosure elaborates on various embodiments in detail. While specific implementations are presented, they serve only as illustrative examples. Those skilled in the relevant field will recognize that other configurations and components may be utilized without deviating from the essence and scope of the disclosure. Consequently, the descriptions and drawings herein are to be understood as illustrative rather than restrictive.

[024] Specific details are included to provide a comprehensive understanding of the disclosure, but well-known elements may be omitted to maintain clarity and conciseness. References to 'one embodiment,' 'an embodiment,' 'one aspect,' or similar phrases signify that the described feature, structure, or characteristic is applicable to at least one embodiment. The repeated use of such terms does not necessarily refer to the same embodiment, nor are different embodiments mutually exclusive. Certain features may appear in some embodiments but not in others.

[025] Terms used in this document generally carry their ordinary meanings within the relevant field, contextualized to the disclosure. Synonyms and alternative terminology may also be employed without implying additional limitations. Examples provided herein are purely illustrative and do not define or constrain the scope of the disclosure. Similarly, the scope of the disclosure is not restricted to the embodiments explicitly described. For clarification, examples of instruments, methods, or results based on these embodiments are included, with headings and subtitles used for convenience rather than to impose limitations. Unless explicitly defined, technical and scientific terms are interpreted as understood by those skilled in the art. In cases of conflict, definitions within this document prevail.

[026] Additional features and advantages will be evident from the following description or can be learned through the application of the principles disclosed. These features and benefits may be achieved using the methods and combinations specifically outlined in the appended claims, as well as through the practice of the

described principles. The full scope of the disclosure will become clearer from the subsequent discussion and claims.

[027] As discussed before there remains a critical unmet need for a unified, cross-modal identity infrastructure that assigns persistent, verifiable identifiers to AI tools, agents, and devices, supports chained provenance tracking, and provides publicly accessible verification interfaces for trust validation and regulatory compliance. The present disclosure, therefore, addresses these shortcomings by introduces a universal system for assigning and embedding digital identities into AI tools, agents, and devices. It enables persistent tagging of AI-generated outputs with verifiable identity and provenance metadata. The system supports real-time verification, trust scoring, and collaborative lineage tracking across multi-agent workflows. It ensures transparency, accountability, and regulatory compliance in both digital and physical AI ecosystems.

[028] Figure 1 illustrates a system (100) for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, in accordance with an aspect of the present disclosure. Figure 1 illustrates a system (100) for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, in accordance with an aspect of the present disclosure. The system (100) is designed to provide a universal framework for digital identity assignment, metadata tagging, provenance tracking, trust validation, and execution control for AI-generated outputs and agentic behavior. The system (100) ensures end-to-end traceability, compliance, and lifecycle auditability of AI systems and their outputs across modalities such as text, image, video, audio, and autonomous behaviors.

[029] The system (100) includes a registration interface (102) configured to receive metadata associated with AI tools, agents, or physical devices submitted by a user or a developer. The registration interface (102) may be implemented as a web-based portal, an API gateway, or a developer dashboard through which information such as the AI model name, version, developer details, deployment platform, and intended modality are submitted for registration. The registration

interface (102) initiates the process of assigning a globally unique AI Registry Identifier (AIREG ID) to the submitted AI entity.

[030] The registration interface (102) communicates with the core processing architecture via a communication network (106), which may include a combination of public or private internet, virtual private networks (VPNs), or secure enterprise-grade connections. The communication network (106) facilitates bi-directional data exchange between user devices, developer platforms, and backend services, allowing seamless onboarding of AI entities and remote identity provisioning.

[031] An AI identity and provenance engine (104) forms the central processing module of the system (100) and is operatively connected to the communication network (106). The AI identity and provenance engine (104) is responsible for managing the core functions of digital identity assignment, output tagging, multi-agent provenance tracking, and real-time verification. This engine (104) houses several internal modules and sub-engines, orchestrated by a central processor (114) to carry out the invention's objectives.

[032] The AI identity and provenance engine (104) is communicatively coupled to a network interface (108) that enables communication with external systems and service endpoints over the communication network (106). The network interface (108) may support secure protocols such as HTTPS, TLS, or WebSocket communication for protected data transfer. In addition, an I/O interface (110) facilitates internal and external data routing and device control functions. This may include handling input/output requests, signal processing, and file transfer operations for registration and tagging workflows.

[033] A storage unit (112) is operatively connected to the AI identity and provenance engine (104) via a secure connection (116). The storage unit (112) may comprise a distributed or centralized database, including but not limited to SQL, NoSQL, graph, or ledger-based systems. It stores all registered metadata, issued AIREG IDs, embedded tagging data, PROV_ID logs, trust scores, lifecycle events of devices, and audit trails. In some embodiments, the storage unit (112) may include immutable storage, blockchain integrations, or WORM (write-once-read-many) compliant media for regulatory-grade recordkeeping.

[034] At the core of the AI identity and provenance engine (104) lies a processor (114) which executes various instructions stored in memory and coordinates the operation of subcomponents within the engine. The processor (114) may be implemented using a microcontroller, a digital signal processor, a multi-core CPU, or a custom ASIC/FPGA-based solution for high-performance identity operations. The processor (114) is configured to interact with several specialized engines, including a metadata tagging engine (118), a provenance tracking engine (120), a verification engine (122), a device identity engine (124), and an execution control engine (126), all collectively referenced as sub-module group (128).

[035] The metadata tagging engine (118) is configured to embed persistent digital identity information into all AI-generated outputs. These outputs may include text documents, images, audio files, videos, or encoded behaviors such as agent decision trees or task execution logs. The metadata tagging engine (118) may utilize various tagging methods such as EXIF metadata, JSON wrappers, binary headers, or embedded hash-linked footers. The AIREG ID and associated metadata are appended either inline (within the content) or as external hash-linked references for non-modifiable formats.

[036] The provenance tracking engine (120) is adapted to generate and manage recursively chainable Provenance Identifiers (PROV_IDs). Each PROV_ID captures the contextual metadata associated with content generation, such as the source agent, timestamp, contributing inputs, processing parameters, and versioning details. In collaborative environments, the provenance tracking engine (120) chains PROV_IDs from multiple contributing agents, building an ancestry graph that can be stored and queried for audit purposes. In certain implementations, a graph database such as Neo4j may be used to represent the lineage tree visually and structurally.

[037] The verification engine (122) is configured to authenticate the source, identity, and trustworthiness of AI-generated outputs in real time. This engine provides an interface for browser extensions, API consumers, or public web portals to inspect the metadata embedded in any content or device. Upon verification, it reveals the issuing AIREG ID, full provenance chain, associated registry metadata,

and trust score. The verification engine (122) may also support privacy-preserving techniques, such as zero-knowledge proofs, to allow verification without exposing sensitive metadata.

[038] The device identity engine (124) is responsible for managing digital identity provisioning and lifecycle tracking of physical AI-powered devices, such as robots, drones, and smart IoT systems. Each physical device is assigned an AIREG ID and tagged using visible or embedded identity mechanisms such as QR codes, NFC tags, or firmware-level cryptographic signatures. The device identity engine (124) logs deployment events, operational actions, firmware updates, and compliance checks to the storage unit (112), ensuring persistent traceability and security throughout the device's lifecycle.

[039] The execution control engine (126) governs task authorization and behavioral gating based on real-time evaluation of identity and trust. This module ensures that only verified and compliant AI tools or devices can execute sensitive operations, especially in agentic or safety-critical environments. The execution control engine (126) cross-checks the trust score, compliance status, and policy-based conditions before allowing an AI agent to proceed with a decision or task. In some embodiments, this engine may issue cryptographically signed execution tokens or revocation notices.

[040] All these modules (118, 120, 122, 124, 126) are orchestrated under the unified control of the processor (114) within the sub-module group (128). The interactions among these engines ensure a seamless flow from registration to output generation, metadata tagging, provenance logging, verification, and lifecycle control. The modular nature of this architecture allows each component to be scaled independently or integrated with third-party compliance, analytics, or AI orchestration platforms.

[041] In operation, when an AI model is first registered through the registration interface (102), the processor (114) invokes the metadata tagging engine (118) to generate a corresponding AIREG ID and persist it in the storage unit (112). Subsequently, when outputs are generated by this registered AI entity, the metadata tagging engine (118) embeds the AIREG ID and invokes the provenance tracking

engine (120) to issue a corresponding PROV_ID. If these outputs are consumed by another AI agent, the downstream outputs inherit and extend the PROV_ID chain, maintaining a full ancestral lineage.

[042] When a user or regulator wishes to verify the authenticity of an AI-generated output, the verification engine (122) is invoked. The user may use a browser extension, a web portal, or an API call to upload or reference the content. The engine (122) extracts the embedded AIREG ID and PROV_ID, fetches registry data from the storage unit (112), and displays a real-time verification report. In case of physical devices, the QR or NFC code may be scanned to access the associated digital passport.

[043] In applications involving collaborative AI agents or networks of intelligent devices, the system (100) enables peer-to-peer identity negotiation and cross-verification. Each agent exchanges identity proofs using the device identity engine (124) and verifies the counterpart using the verification engine (122). The outcome of such interaction influences trust-based execution decisions handled by the execution control engine (126), allowing or blocking task delegation or inter-agent data exchange.

[044] Through the integration of these components, the system (100) offers a robust and scalable identity infrastructure for artificial intelligence ecosystems. It supports transparency, security, and compliance across software-based AI systems and AI-enabled hardware. Figure 1 encapsulates the functional architecture of this system (100), demonstrating how individual modules work in tandem to deliver persistent identity assignment, verifiable provenance, and policy-enforced trust in AI outputs and operations.

[045] Figure 2 illustrates a method for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, in accordance with an aspect of the present disclosure.

[046] The method for assigning and embedding unique digital identities into AI tools, agents, and devices. The method includes registering metadata, tagging AI-generated outputs with identity and provenance, and enabling real-time verification.

It further tracks multi-agent lineage through chainable identifiers. Execution of AI actions is permitted only upon validated trust and compliance status.

[047] At step 202, the method 200 involves receiving (202), by a registration interface (102), metadata associated with an AI tool, agent, or device.

[048] At step 204, the method 200 involves assigning (204), by a processor (114), a globally unique, cryptographically verifiable AI Registry Identifier (AIREG ID) to the AI tool, agent, or device based on the received metadata.

[049] At step 206, the method 200 involves tagging (206), by a metadata tagging engine (118), AI-generated outputs with the assigned AIREG ID and associated metadata, the outputs comprising at least one of text, image, audio, video, or agentic behavior.

[050] At step 208, the method 200 involves generating (208), by a provenance tracking engine (120), a chainable Provenance Identifier (PROV_ID) for each tagged output, the PROV_ID recording generation context and lineage.

[051] At step 210, the method 200 involves verifying (210), by a verification engine (122), the identity, trust score, and provenance chain of the AI-generated output using at least one of a browser extension, web portal, or API.

[052] At step 212, the method 200 involves embedding (212), by a device identity engine (124), the AIREG ID and metadata into AI-enabled physical devices using one or more of QR codes, NFC tags, or firmware-level cryptographic signatures.

[053] At step 214, the method 200 involves enforcing (214), by an execution control engine (126), trust-based task execution policies based on validation of identity, provenance, and compliance status.

Advantages:

- The present disclosure provides a system that assigns persistent, verifiable digital identities to AI tools, agents, and devices.
- The present disclosure provides a system that embeds metadata across multi-modal AI outputs for traceable provenance.
- The present disclosure provides a system that enables real-time verification of AI-generated content through browser, API, or web interfaces.

- The present disclosure provides a system that logs collaborative workflows using recursively chainable provenance identifiers.
- The present disclosure provides a system that enforces trust-based execution control to prevent unauthorized AI behavior.

[054] The implementation set forth in the foregoing description does not represent all implementations consistent with the subject matter described herein. Instead, they are merely some examples consistent with aspects related to the described subject matter. Although a few variations have been described in detail above, other modifications or additions are possible. In particular, further features and/or variations can be provided in addition to those set forth herein. For example, the implementation described can be directed to various combinations and sub combinations of the disclosed features and/or combinations and sub combinations of the several further features disclosed above. In addition, the logic flows depicted in the accompanying figures and/or described herein do not necessarily require the particular order shown, or sequential order, to achieve desirable results. Other implementations may be within the scope of the following claims.

We claim(s)

1. A system (100) for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, comprising:

a registration interface (102) adapted to receive metadata corresponding to an AI tool, agent, or device submitted by a user;

an AI identity and provenance engine (104) communicatively coupled with the registration interface (102) through a communication network (106); the AI identity and provenance engine (104) including:

a processor (114) configured to process the received metadata and AI-generated outputs; wherein the processor (114) is adapted to:

(i) assign a globally unique, cryptographically verifiable AI Registry Identifier (AIREG ID) to each registered AI tool, agent, or device;

(ii) tag each output generated by the registered AI tool, agent, or device, comprising at least one of text, image, audio, video, or autonomous agent behaviour, with the corresponding AIREG ID and associated metadata by way of a metadata tagging engine (118);

(iii) generate a chainable Provenance Identifier (PROV_ID) for each AI-generated output by way of a provenance tracking engine (120), wherein the PROV_ID records lineage, collaboration history, and generation context;

(iv) verify the identity, trust score, and provenance history of the AI-generated output through a verification engine (122), the verification engine (122) comprising at least one of a browser extension, public web portal, or API endpoint;

(v) embed the AIREG ID and firmware-level metadata into AI-enabled physical devices using one or more of QR code, NFC tag, or cryptographic signature by way of a device identity engine (124); and

(vi) restrict or allow execution of AI agent tasks or device operations based on policy-based trust evaluation using an execution control engine (126);

wherein the system (100) enables persistent digital identity management, end-to-end provenance traceability, and real-time verification for AI-generated outputs and devices.

2. The system (100) as claimed in claim 1, wherein the metadata tagging engine (118) is configured to support both inline tagging, by embedding metadata directly into file headers or content wrappers, and detached tagging, using reference hashes or secure pointers for non-modifiable formats.
3. The system (100) as claimed in claim 1, wherein the metadata associated with the AIREG ID comprises at least one of: tool or model name, developer or organization, platform, version number, issuance timestamp, modality type, and trust status.
4. The system (100) as claimed in claim 1, wherein the provenance tracking engine (120) is further configured to maintain a graph-based ancestry structure linking recursively chainable PROV_IDs to track collaborative and multi-agent output generation.
5. The system (100) as claimed in claim 1, wherein the verification engine (122) is further adapted to display real-time provenance information, including the full chain of contributing AIREG IDs, associated trust scores, and registry metadata.
6. The system (100) as claimed in claim 1, wherein the device identity engine (124) is further configured to log lifecycle events of physical AI devices, including manufacturing details, software or firmware updates, deployment locations, and operational tasks.
7. The system (100) as claimed in claim 1, wherein the execution control engine (126) applies trust-based policies that permit task execution only if the associated AIREG ID and PROV_ID meet predefined thresholds for trust score, compliance level, or registry validation.
8. The system (100) as claimed in claim 1, wherein AI agents participating in multi-agent workflows exchange identity credentials using a peer-to-peer

identity negotiation protocol, including cryptographic challenge-response and optional zero-knowledge proof verification.

9. The system (100) as claimed in claim 1, wherein the processor (114) is further configured to apply visual or invisible "Dignity Badges" to AI-generated outputs, embedding the AIREG ID and verification URL for public authentication and trust labeling.

10. A method (200) for registering, tagging, and verifying the identity and provenance of artificial intelligence (AI) tools, agents, and AI-enabled physical devices, the method comprising the steps of:

(a) receiving (202), by a registration interface (102), metadata associated with an AI tool, agent, or device;

(b) assigning (204), by a processor (114), a globally unique, cryptographically verifiable AI Registry Identifier (AIREG ID) to the AI tool, agent, or device based on the received metadata;

(c) tagging (206), by a metadata tagging engine (118), AI-generated outputs with the assigned AIREG ID and associated metadata, the outputs comprising at least one of text, image, audio, video, or agentic behavior;

(d) generating (208), by a provenance tracking engine (120), a chainable Provenance Identifier (PROV_ID) for each tagged output, the PROV_ID recording generation context and lineage;

(e) verifying (210), by a verification engine (122), the identity, trust score, and provenance chain of the AI-generated output using at least one of a browser extension, web portal, or API;

(f) embedding (212), by a device identity engine (124), the AIREG ID and metadata into AI-enabled physical devices using one or more of QR codes, NFC tags, or firmware-level cryptographic signatures; and

(g) enforcing (214), by an execution control engine (126), trust-based task execution policies based on validation of identity, provenance, and compliance status.

Dated this 24th day of July 2025

Name: Meena
IN/PA – 4876
Agent for Applicant (s)

ABSTRACT

SYSTEM AND METHOD FOR ASSIGNING, EMBEDDING, AND VERIFYING DIGITAL IDENTITY AND PROVENANCE OF AI ENTITIES

A system (100) for registering, tagging, and verifying artificial intelligence (AI) tools, agents, and AI-enabled devices is disclosed. The system (100) includes a registration interface (102) to receive metadata and an AI identity and provenance engine (104) to process it. A processor (114) assigns a globally unique AI Registry Identifier (AIREG ID), tags AI-generated outputs (text, image, audio, video, or behavior) using a metadata tagging engine (118), and generates a chainable Provenance Identifier (PROV_ID) via a provenance tracking engine (120). A verification engine (122) enables identity and trust validation via browser, API, or portal. A device identity engine (124) embeds identifiers into physical devices, and an execution control engine (126) enforces trust-based operation policies. The system ensures digital identity, traceability, and real-time verification of AI outputs and devices.

Fig 1 is the reference.