CLAIMS

MULTI-DOMAIN AUTHENTICATION AND AUTHORIZATION SYSTEM WITH CREDENTIAL PORTABILITY FOR AI AGENT NETWORKS

What is claimed is:

1. A system for authenticating artificial intelligence agents across multiple computing environments comprising:
   - a processor configured to execute instructions for generating environment-independent identifiers for artificial intelligence agents;
   - a credential translation engine for converting between heterogeneous authentication protocols; and
   - a behavioral authentication module for validating artificial intelligence agent authenticity using operational characteristics.
2. The system of claim 1, wherein said environment-independent identifiers are derived from a combination of cryptographic keys, operational parameters, and capability sets specific to each artificial intelligence agent.
3. The system of claim 1, wherein said credential translation engine converts between at least two credential types selected from the group consisting of: API keys, X.509 certificates, OAuth tokens, JWT tokens, SAML assertions, Kerberos tickets, hardware security module credentials, and behavioral authentication patterns.
4. The system of claim 1, wherein said operational characteristics comprise behavioral patterns including API call sequences, resource utilization patterns, decision-making patterns, interaction sequences, and temporal patterns.
5. The system of claim 1, further comprising a privacy-preserving attribute verification mechanism using zero-knowledge cryptographic proofs that demonstrate attribute possession without revealing attribute values.
6. The system of claim 1, wherein said system supports concurrent authentication across at least one hundred distinct computing environments with sub-second latency.
7. The system of claim 1, further comprising distributed session management with Byzantine fault tolerance supporting f faulty nodes with 3f+1 total nodes.
8. The system of claim 1, wherein said behavioral authentication module continuously validates artificial intelligence agents during operation using ensemble machine learning models.

9. The system of claim 8, wherein said ensemble machine learning models comprise at least two models selected from: Long Short-Term Memory networks, Isolation Forests, One-Class Support Vector Machines, and Autoencoders.
10. The system of claim 1, further comprising a trust bridge protocol module for establishing authentication requirements between environments with different security models through multi-phase negotiation.
11. The system of claim 1, wherein said credential translation engine employs secure multiparty computation wherein no single party has access to complete credential information.
12. The system of claim 1, further comprising a regulatory compliance engine that enforces authentication policies using formal logic reasoning and generates cryptographically protected audit trails.
13. The system of claim 1, wherein said system is integrated within a Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP) for defensive cybersecurity operations.
14. The system of claim 4, wherein said behavioral patterns are analyzed using statistical methods including Mahalanobis distance, Kullback-Leibler divergence, and Dynamic Time Warping.
15. The system of claim 1, further comprising predictive pre-authentication that analyzes agent behavior patterns to anticipate domain access requirements and pre-compute credential translations.
16. A method for cross-domain authentication of artificial intelligence agents comprising:
    - generating a universal identifier for an artificial intelligence agent based on cryptographic and operational characteristics;
    - translating said universal identifier to domain-specific credentials for a target domain while maintaining semantic equivalence of security properties; and
    - continuously validating said artificial intelligence agent through behavioral analysis during operation.
17. The method of claim 16, wherein generating said universal identifier comprises applying a privacy-preserving hash function to a combination of the agent's cryptographic keys, operational parameters, capability set, timestamp, and platform identifier.
18. The method of claim 16, wherein said behavioral analysis comprises:
    - establishing agent-specific baselines using machine learning during a training period;
    - comparing current operational patterns against established baselines;
    - calculating deviation metrics; and
    - triggering graduated security responses based on deviation thresholds.
19. The method of claim 16, further comprising establishing trust relationships between domains through a protocol comprising discovery, negotiation, establishment, and maintenance phases.

20. The method of claim 16, further comprising:
    - generating cryptographic commitments to agent attributes; and
    - providing zero-knowledge proofs that committed attributes satisfy domain requirements without revealing actual attribute values.
21. The method of claim 16, wherein translating comprises:
    - validating source credentials;
    - mapping security attributes between credential types;
    - generating target credentials according to target domain requirements; and
    - creating cryptographic bindings between source and target credentials for audit trail integrity.
22. The method of claim 16, wherein continuously validating comprises analyzing at least three of: API call patterns, resource consumption patterns, decision-making patterns, interaction sequences, or temporal patterns.
23. The method of claim 16, further comprising maintaining distributed session state across multiple domains using Byzantine fault tolerant consensus protocol.
24. The method of claim 23, wherein said Byzantine fault tolerant consensus protocol comprises request, pre-prepare, prepare, commit, and reply phases requiring agreement from at least 2f+1 nodes.
25. A non-transitory computer-readable medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:
    - creating an abstraction layer for artificial intelligence agent identities independent of specific authentication domains;
    - implementing credential translation between heterogeneous authentication systems using secure multiparty computation; and
    - performing continuous behavioral authentication of artificial intelligence agents based on operational patterns.
26. The computer-readable medium of claim 25, wherein the operations further comprise maintaining distributed session state with perfect forward secrecy through ephemeral key generation.
27. The computer-readable medium of claim 25, wherein the operations further comprise generating zero-knowledge proofs using bulletproofs for efficient range proofs on agent attributes.
28. The computer-readable medium of claim 25, wherein the operations further comprise enforcing regulatory compliance through description logic policy expression and automated conflict resolution.
29. The computer-readable medium of claim 25, wherein creating said abstraction layer comprises generating universal identifiers using SHA-3-512 hash function with forward security, unlinkability, non-invertibility, and collision resistance properties.

30. The computer-readable medium of claim 25, wherein performing behavioral authentication comprises:
    - training ensemble models including LSTM networks, Isolation Forests, One-Class SVMs, and Autoencoders;
    - continuously monitoring agent operations across multiple behavioral dimensions;
    - calculating weighted anomaly scores from multiple models; and
    - implementing graduated responses ranging from logging to agent suspension based on deviation levels.
31. The system of claim 1, wherein said system implements post-quantum cryptographic algorithms including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures.
32. The system of claim 1, further comprising homomorphic encryption capabilities enabling policy evaluation on encrypted credentials without decryption.
33. The system of claim 1, wherein said system dynamically adjusts security posture based on threat level by modifying authentication factors, session timeouts, and behavioral monitoring sensitivity.
34. The system of claim 1, further comprising federation interfaces for integration with external identity providers including Active Directory, LDAP, OAuth providers, and cloud IAM systems.
35. The system of claim 1, wherein said behavioral authentication module achieves at least 94% accuracy in detecting anomalous agent behavior with false positive rate below 5%.
36. The method of claim 16, further comprising caching frequently-used credential translations with TTL based on credential expiration and immediate invalidation upon revocation events.
37. The method of claim 16, wherein said method achieves average authentication latency below 200 milliseconds for full multi-domain authentication.
38. The method of claim 16, further comprising parallel processing of authentication requests using thread pools, asynchronous I/O operations, and lock-free data structures.
39. The computer-readable medium of claim 25, wherein the operations further comprise providing integration interfaces including REST API, gRPC, and native SDKs for Python, Java, Go, and JavaScript.
40. The computer-readable medium of claim 25, wherein the operations further comprise implementing rate limiting, DDoS protection via proof-of-work, replay prevention, and side-channel resistant cryptographic operations.

End of Claims