ABSTRACT

A comprehensive authentication and authorization system enables artificial intelligence (AI) agents to operate seamlessly across multiple security domains with varying trust models and credential requirements. The system generates environment-independent universal identifiers for AI agents using cryptographic keys and operational parameters, then translates these identifiers between heterogeneous authentication protocols including API keys, certificates, OAuth tokens, and hardware security modules through secure multiparty computation. Continuous behavioral authentication validates AI agents by analyzing operational patterns including API call sequences, resource utilization, decision-making patterns, and temporal behaviors using ensemble machine learning models. Privacy-preserving attribute verification employs zero-knowledge proofs to demonstrate capabilities without revealing sensitive information. Distributed session management with Byzantine fault tolerance ensures system reliability when up to f nodes fail in a network of 3f+1 nodes. A trust bridge protocol negotiates authentication requirements between domains with incompatible security models through multi-phase discovery, negotiation, establishment, and maintenance. The system achieves sub-second authentication latency across 100+ concurrent domains while maintaining cryptographic audit trails for regulatory compliance. Integration with Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP) enables comprehensive defensive cybersecurity operations. Applications include multi-cloud deployments, healthcare information exchange, financial services, and government federated systems requiring secure AI agent authentication.

Word Count: 196 words