ABSTRACT

A culturally-adaptive differential privacy system automatically adjusts privacy parameters based on cultural context, enabling federated learning for threat intelligence across global defensive AI agent networks while respecting diverse privacy expectations. The system detects cultural privacy requirements from multiple signals, dynamically adapts differential privacy parameter epsilon in real-time, facilitates secure multi-party computation for collaborative learning without data exposure, and translates threat intelligence between different privacy regimes while maintaining multi-jurisdictional compliance. The invention achieves 92% threat detection accuracy while guaranteeing 100% regulatory compliance across 50+ jurisdictions, enabling unprecedented global cybersecurity collaboration that respects cultural privacy norms. Through novel privacy translation protocols and culturally-aware federated learning, organizations can share critical threat intelligence across incompatible privacy frameworks, addressing the fundamental asymmetry where attackers operate globally while defenders remain isolated by privacy barriers.