PROVISIONAL PATENT APPLICATION

Docket No.: RUTHERFORD-017-PROV

Inventor: Brian James Rutherford

Filing Date: [Current Date]

CULTURALLY-ADAPTIVE DIFFERENTIAL PRIVACY SYSTEM WITH FEDERATED LEARNING FOR MULTI-JURISDICTIONAL THREAT INTELLIGENCE SHARING AMONG DEFENSIVE AI AGENT NETWORKS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is the first filing in this patent family. No priority is claimed to any prior applications.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable

FIELD OF THE INVENTION

[0003] The present invention relates to privacy-preserving cybersecurity systems, specifically to a culturally-adaptive differential privacy framework that automatically adjusts privacy parameters based on cultural context, regulatory requirements, and user preferences while enabling federated learning across defensive AI agent networks for collaborative threat intelligence without data exposure. The invention addresses the critical need for global organizations to share threat intelligence while respecting diverse cultural privacy expectations and complying with multiple jurisdictional requirements simultaneously.

BACKGROUND OF THE INVENTION

The Global Privacy Challenge

[0004] Modern organizations operating across international boundaries face an unprecedented challenge in cybersecurity collaboration. While threat actors operate globally without regard to borders, defenders are constrained by a complex web of privacy regulations, cultural expectations, and legal requirements that vary dramatically across jurisdictions. This creates a fundamental asymmetry where attackers can coordinate freely while defenders are isolated by privacy barriers.

Cultural Privacy Variations

[0005] Privacy is not a universal concept but rather a culturally-defined construct that varies significantly across societies. Research demonstrates that privacy expectations correlate with cultural dimensions including:

[0006] 1. Individualism vs. Collectivism: Individualistic cultures (United States, United Kingdom) emphasize personal privacy rights, while collectivistic cultures (Japan, China) may prioritize group harmony over individual privacy.

[0007] 2. Power Distance: High power distance cultures accept unequal privacy rights between authorities and citizens, while low power distance cultures demand equal privacy protection.

[0008] 3. Uncertainty Avoidance: Cultures with high uncertainty avoidance prefer strict, clear privacy rules, while those with low uncertainty avoidance accept ambiguous privacy situations.

[0009] 4. Trust in Institutions: Scandinavian countries exhibit high institutional trust allowing more data sharing with authorities, while other regions show deep skepticism requiring stronger privacy guarantees.

[0010] These cultural variations manifest in concrete regulatory differences:

• European Union (GDPR): Requires explicit consent, data minimization, and allows erasure rights ($\varepsilon \approx 0.1$-1.0 in differential privacy terms)
• United States (CCPA/State laws): Balances privacy with innovation, opt-out models ($\varepsilon \approx 1.0$-5.0)
• China (PIPL): Data localization requirements with government access provisions ($\varepsilon \approx 2.0$-10.0)
• India (DPDPA): Consent-based with broad exemptions for national security
• Brazil (LGPD): GDPR-inspired with unique provisions for developing economy needs

Technical Limitations of Current Approaches

[0011] Existing privacy-preserving technologies fail to address cultural adaptation:

[0012] 1. Static Differential Privacy: Current systems apply uniform privacy parameters (epsilon values) regardless of cultural context or user expectations. A system configured for EU compliance may be unnecessarily restrictive in other regions, while US-optimized systems violate European requirements.

[0013] 2. Binary Federated Learning: Traditional federated learning systems offer binary choices - participate fully or not at all. They cannot adjust participation levels based on cultural comfort or regulatory requirements.

[0014] 3. Monolithic Compliance: Organizations typically choose the most restrictive privacy regime and apply it globally, sacrificing utility in permissive jurisdictions while still failing to address cultural nuances.

[0015] 4. Cross-Border Barriers: Current systems cannot translate threat intelligence between different privacy regimes. Information collected under one privacy framework cannot be shared with organizations operating under different frameworks.