AEGIS: A Secure Distributed Framework for Privacy-Preserving Multi-Institutional Data Analysis

Goel, Meetushi (School: Jayshree Periwal International School)
Umrao, Mradul (School: Shri Ram Public School)

Regulatory frameworks like GDPR, HIPAA, and CCPA prohibit raw data sharing across institutional boundaries, yet scientific progress increasingly depends on multi-party collaboration. Current systems treat privacy, Byzantine resilience, and auditability as separate concerns, leaving critical vulnerabilities when all three must hold simultaneously. This paper presents AEGIS (Adaptive, Encrypted, Guaranteed Integrity System), a distributed computing framework that resolves this trilemma by unifying cryptographic secure aggregation, adaptive differential privacy, and Byzantine fault tolerance into a single architecture. Raw data never leaves its source node, and organizations jointly compute aggregate statistics with mathematically provable security backed by tamper-evident Merkle-proof audit chains. A live 5-node benchmark validates AEGIS across 296 attack configurations spanning nine adversarial strategies and 10 rounds each. Byzantine consensus succeeded in 100% of rounds within the f < n/3 safety boundary, with secure aggregation errors below 2x10^-4 and a 40% message-complexity reduction over PBFT. Membership inference resistance was evaluated through 30 isolated probe queries across six epsilon values from 0.1 to 10.0, with adversary advantage strictly below the theoretical bound in all 30 cases. Production privacy budgets across all five nodes remained fully intact throughout, confirming zero privacy leakage from the audit process itself. AEGIS makes HIPAA-compliant multi-hospital research tractable, enables cross-bank fraud detection without exposing customer records, and supports multi-jurisdictional analytics on commodity hardware without trusted hardware dependencies.

Awards Won:
Association for the Advancement of Artificial Intelligence: AAAI Student Memberships for each finalist that is part of the 1st, 2nd, and 3rd Prize Winning projects and 5 Honorable Mention winning projects (up to 3 students per project) (in-kind award / part of the 1st-3rd prize)