# **A Privacy-Preserving Hybrid Federated Learning Framework for Multi-Modal Threat Intelligence**

## **Abstract**

This article proposes a state-of-the-art privacy-preserving hybrid federated learning framework for improving multi-modal threat intelligence in organizations. The architecture features a hierarchical neural network model consisting of modality-specific encoders— (Network Encoder, Log Encoder)—with convolution and recurrent components, an attention-based fusion mechanism, and a dedicated classifier for advanced persistent threat detection. These encode diverse sources of data: e.g., network traffic flows, system logs, and user behaviour analytics—with federated aggregation to form comprehensive threat models, while also ensuring data privacy. Gradient clipping and differential privacy using Gaussian noise injection (σ=1.0) during training provide security with respect to inference attacks. Including target noise in the perturbation of an adversarial training scheme enhances model robustness to poisoning attempts. From the experimental results demonstrating using CICIDS2017 dataset and synthetic behavioural logs, it can be concluded that detection accuracy has been improved significantly (89.7% vs. 78.3% base) while preserving privacy bounds (ε=3.6). The framework efficiently scales across heterogeneous organizational infrastructures, incurring minimal communication overhead (average 2.3MB per round) with convergence in three federated rounds. This framework signifies a major step forward in the mechanism of inter-organizational information sharing on threats, providing organizations with a principled way of weighing the improvement of joint security against confidentiality requirements. The contribution represents a dual benefit by laying the theoretical foundations and some practical implementation guidelines for privacy-preserving collaborative cyber defence systems against ever-changing advanced persistent threats.

**Keywords**

Federated learning, cybersecurity, multimodal data fusion, differential privacy, advanced persistent threats, threat intelligence sharing, privacy-preserving machine learning, adversarial training, collaborative security, cross-organizational threat detection