AI4FIDS

An AI-based Federated Intrusion Detection System

AI4FIDS is a modular intrusion detection system designed to detect cyberattacks across network, host, and log data using federated learning. It enables multiple distributed clients to collaboratively train detection models without sharing raw data, preserving privacy. AI4FIDS supports the analysis of diverse data types, including system logs, operational metrics, network flows, and visual traffic representations, and detects threats against application-layer protocols such as KNX and OCPP.

AI4CYBER

Component

The AI4FIDS solution provides multiple benefits: Privacy-Preserving Threat Detection; Multimodal Intrusion Detection; Enhanced Detection Accuracy and Resilience; Support for Industrial Network Protocols; Robustness Against Adversarial and Model Poisoning Attacks; Scalability and Flexibility; Scalability and Flexibility; User-Friendly Federated Training Interface; Open and Extensible Design; Optimized for Heterogeneous Environments

AI4FIDS is a high-performance solution designed to detect a broad spectrum of attacks across network, host, and log data.

Its core feature is federated learning, allowing multiple clients to collaboratively train an intrusion detection model without sharing their raw data. The system also supports intrusion detection for application-level communication protocols, including, among others, KNX and OCPP. Furthermore, AI4FIDS integrates advanced mechanisms into the training process to address client data heterogeneity and defend against adversarial threats, ensuring the robustness of the resulting models in both data distribution and adversarial resilience.

YouTube Video Link

YouTube Video Link

AI4FIDS is partially available as open source. While the solution is still at the prototype stage, the final AI4FIDS tool is expected to adopt a dual licensing model.

Minds

Pavlos Bouzinis (pbouzinis@metamind.gr)
MetaMind Innovation (MINDS)

https://metamind.gr

- Makris, A. Karampasi, P. Radoglou-Grammatikis, N. Episkopos, E. Iturbe, E. Rios, N. Piperigkos, A. Lalos, C. Xenakis, T. Lagkas, V. Argyriou, and P. Sarigiannidis, “A comprehensive survey of federated intrusion detection systems: Techniques, challenges and solutions,” Computer Science Review, vol. 56, p. 100717, May 2025, doi: 10.1016/j.cosrev.2024.100717.
- P. Radoglou-Grammatikis, P. S. Bouzinis, I. Makris, T. Lagkas, V. ARgyriou, G. Th. Papadopoulos, P. Fouliras, G. Seritan and P. Sarigiannidis, “AI4FIDS: Multimodal Federated Intrusion Detection,” in IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2025.3562346.
- P. S. Bouzinis et al., "StatAvg: Mitigating Data Heterogeneity in Federated Learning for Intrusion Detection Systems," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2025.3564387

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450. Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.