A Distributed Continual Learning Framework for Intrusion Detection in Heterogeneous IoT Networks

The rapid proliferation of Internet of Things (IoT) devices in critical domains such as healthcare, industrial automation, and smart cities has significantly increased the attack surface for cyber threats, creating a dynamic and evolving threat landscape. Consequently, there is a growing need for advanced intrusion detection systems (IDS) that can effectively monitor, detect, and mitigate security breaches in real-time while meeting the constraints of IoT environments—such as limited computational resources, energy consumption, and data heterogeneity. In this work, the proposed distributed continual learning architecture employs task-incremental learning focuses on detecting and classifying a diverse range of cyberattacks that are particularly relevant to IoT networks, including Exploits, Reconnaissance, Malware, Fuzzer, Generic, Backdoor, Worm, and Denial of Service (DoS) attacks with the capability to dynamically incorporate new attack classes as they emerge in real-world deployments.

One of the major challenges in IDS is the high false positive rate, which can lead to alert fatigue and undermine the reliability of the system. To mitigate this a novel machine leaning model is to be integrated to reduce the false alarm rate while preserving detection sensitivity. Interpretability is another critical requirement for practical adoption of AI-driven security systems. To this end, the proposed work incorporates explainable AI (XAI) techniques to provide visual and quantitative insights into the model's decision-making process. Furthermore, the integration of a Large Language Model (LLM), Gemini, enhances interpretability by converting model outputs and feature contributions into contextual, actionable responses for security analysts.

To address these critical challenges including class imbalance, high false alarm rates, computational constraints and lack of interpretability, this research work propose a deep learning framework with metaheuristic optimization for intrusion detection in heterogeneous networks.