**Title:** **Enhanced Security in RPL Based IoT Networks: Federated Learning for Blackhole Attack Prediction**

**Problem Statement:**

Design a Federated Learning model to predict and mitigate blackhole attacks in RPL-based IoT networks, addressing the limitations of traditional and deep learning models. Centralized methods fall short, and deep learning can be resource-intensive. This approach improves detection accuracy and network resilience through decentralized training.

**Proposed Methodology:**

In the realm of the Internet of Things (IoT), numerous applications rely on Low-Power and Lossy Networks (LLNs) to efficiently manage resources and ensure seamless communication among devices. The Routing Protocol for LLNs (RPL) is a widely adopted standard for these networks, crucial for establishing and maintaining reliable routes. However, RPL is susceptible to security threats such as Blackhole attacks, which can significantly disrupt network performance due to its routing mechanism's vulnerabilities. While existing solutions like ensemble learning models and deep learning approaches, including Recursive Neural Networks (RNN), have been employed to counteract these attacks, they often overburden the central server with high computational demands and require substantial bandwidth for data transfer, leading to potential bottlenecks and single points of failure. In contrast, federated learning offers a more efficient and secure alternative by allowing local training on data at each node, thereby reducing the load on the central server and minimizing data transmission. This study explores the implementation of federated learning to detect Blackhole attacks in RPL-based IoT networks. By leveraging distributed data and computational resources across multiple nodes, federated learning enhances detection capabilities while preserving data privacy. This continuous and recursive learning approach at the local nodes, combined with periodic aggregation at the central server, facilitates proactive detection and prevention of Blackhole attacks. If successful, this methodology can be extended to mitigate other attacks such as selective forwarding (Greyhole) attacks.