🌐

Adversarial Defense for Federated Learning in IoT Malware Detection

Week 2

Task

- ☑ ~~Adversarial Defense for Federated Learning in IoT Malware Detection~~
- ☑ ~~Literature review~~
- ☑ ~~Problem statement~~
- ☑ ~~Objectives~~
- ☑ ~~Expected results~~
  - ☑ ~~Adversarial Defense Technique~~

Week 4

- ☑ ~~Literature review~~
  - ☑ ~~On Benchmark SOTA Attacks (White Box Attacks)~~
  - ☑ ~~On Benchmark SOTA Defense Technique~~
- ☑ ~~Brainstorm Adversarial Defense~~
  - ☑ ~~Unsupervised Approach~~
  - ☑ ~~Supervised Approach :~~ **~~Gradient-Based Filtering~~**
- ☑ ~~Sample Code~~