PHÁT HIỆN MÃ ĐỘC ANDROID DÙNG FEDERATED LEARNING

Nguyễn Vương Thịnh

Trường Đại học Công nghệ Thông tin – ĐHQG TPHCM

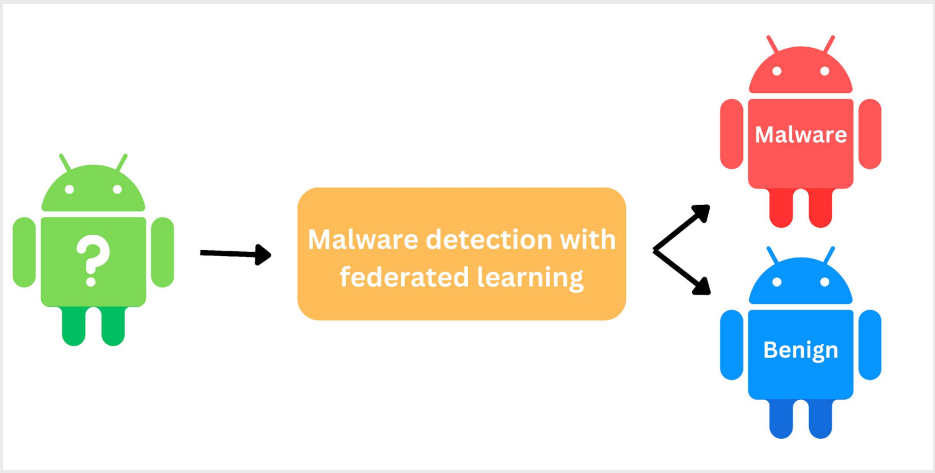
Mục tiêu

- Xây dựng mô hình phát hiện mã độc Android sử dụng Federated learning (FL).
- Giải quyết mối lo ngại liên quan vị phạm quyền riêng tư, bảo mật người dung trong việc phát hiện mã độc Android.

Lý do chọn đề tài

- Sự phát triển mạnh mẽ của các phần mềm độc hại trên các thiết bị điện tử Android đang ảnh hưởng nghiêm trọng đối với người dùng. Nên, việc phát hiện kịp thời mã độc là cần thiết.
- Nhưng, các phương pháp đang phụ thuộc vào việc gửi dữ liệu cá nhân vào máy chủ để xử lý tập trung, gây ra **vấn đề bảo mật thông tin**.

Tổng quan



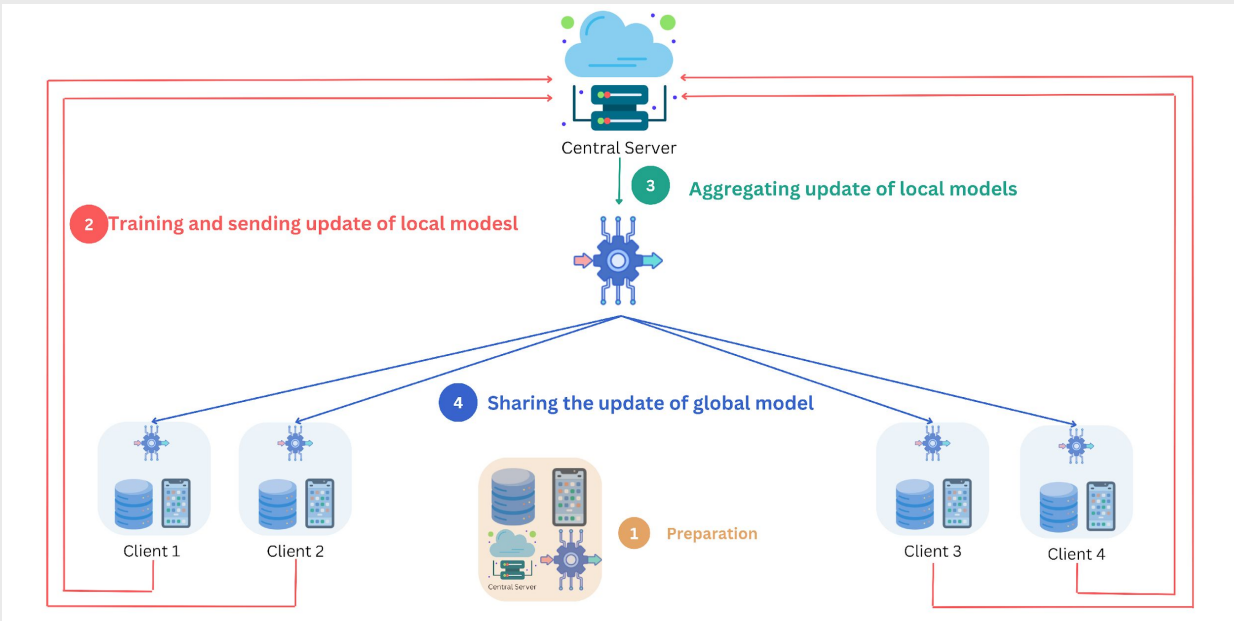
- Input: một phần mềm hệ điều hành Android
- Output: Kết quả xác nhận phần mềm có độc hại (Malware) hay không độc hại (Benign)

Hình 1. Input và Output của mô hình phát hiện mã độc Android

Chi tiết

1. Nội dung

- Khảo sát các công trình liên quan về phát hiện mã độc Android bằng học máy
- Tìm hiểu các bài toán vận dụng Federated learning để áp dụng vào phát hiện Malware



Hình 2. Federated learning framework

2. Phương pháp

- Xây dựng bộ dữ liệu gồm Malware và Benign
- Thiết lập các mô hình học máy (Random Forest, SVM và Naïve Bayes)
- Thiết lập Federated learning framework (Hình 2) gồm thiết bị Android (clients) và máy chủ (server) để trao đổi và cập nhật thông tin giữa model clients và server.
- Ứng dụng FL framework cho các mô hình học máy

3. Kết quả dự kiến

- Một mô hình phát hiện mã độc Android sử dụng Federated Learning
- Bảng số liệu so sánh kết quả giữa các mô hình máy học trên thang đo Accuracy, Precision, Recall và F1-score

NII

Nguyễn Vương Thịnh – Trường Đại học Công nghệ Thông tin – ĐHQG TPHCM

TEL : 0346324245 Email : thinhnv.17@grad.uit.edu.vn