Face Processing in Video

Lê Văn Minh

Trường Đại học Công nghệ Thông tin - ĐHQG TP.HCM

What ?

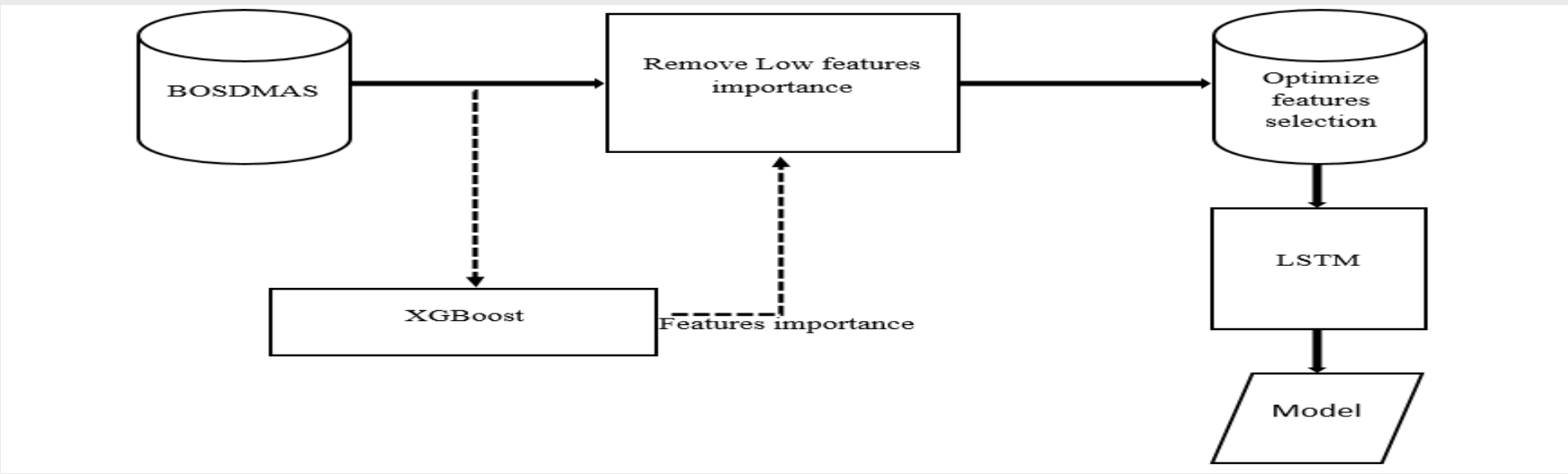
Trong bài nghiên cứu này, chúng tôi tìm hiểu:

- Máy tính trở thành không thể thiếu trong cuộc sống hàng ngày.
- Điều này mở ra nguy cơ tấn công mạng nguy hiểm.
- Malware là phổ biến và nguy hiểm nhất, xâm nhập hệ thống máy tính.
- Phát hiện malware bằng LSTM và XGBoost trở nên cực kỳ quan trọng.

Why ?

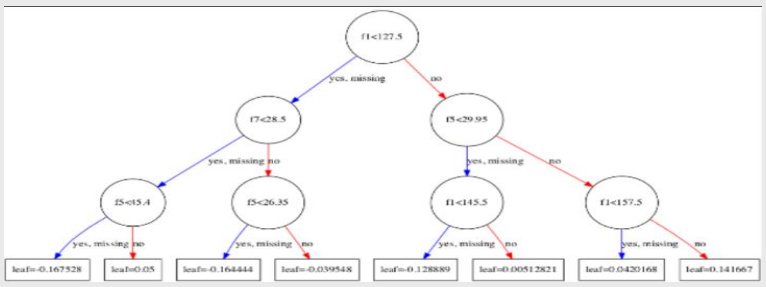
- XGBoost chọn lọc đặc trưng thông qua "feature importance", giúp xây dựng mô hình dự đoán hiệu quả, giảm chi phí và tăng tốc độ xử lý.
- LSTM học các mẫu dài hạn từ dữ liệu chuỗi, kết hợp đặc trưng tối ưu từ XGBoost, giúp phát hiện mã độc hiệu quả.
- Sự kết hợp LSTM và XGBoost tạo hệ thống phát hiện mã độc mạnh mẽ, tận dụng ưu điểm của cả hai phương pháp.

Overview



Description

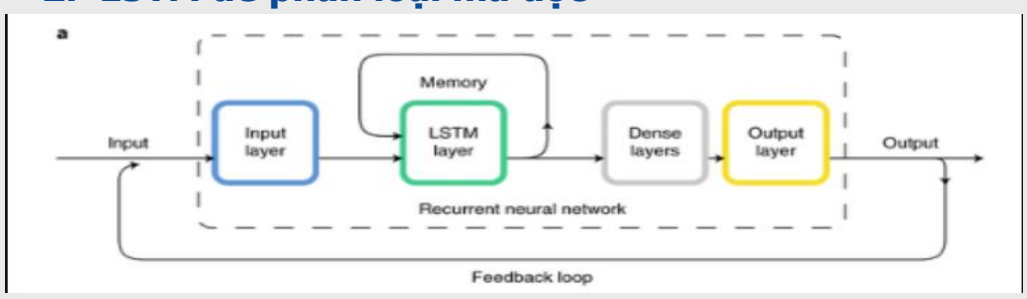
1. XGBoost để chọn lọc đặc trưng



Hình 1: XGBoost Plot of Single Decision Tree

XGBoost là một thuật toán học máy mạnh mẽ, có khả năng chọn lọc đặc trưng thông qua thông số "feature importance". Thông số này đo lường mức độ ảnh hưởng của từng đặc trưng đến kết quả dự đoán của mô hình bằng cách xem xét mức độ giảm giá trị của hàm mất mát khi đặc trưng đó được sử dụng để phân tách dữ liệu. Đặc trưng có mức độ giảm lớn hơn sẽ quan trọng hơn, giúp cải thiện hiệu suất mô hình.

2. LSTM để phân loại mã độc



LSTM là một loại mạng neural tái phát hiện được thiết kế để xử lý dữ liệu chuỗi, có khả năng nhớ và học các mẫu dài hạn từ dữ liệu đầu vào. LSTM được sử dụng để học các mẫu và mối quan hệ phức tạp giữa các chuỗi dữ liệu, giúp phát hiện các hành vi độc hại trong mã độc.

Các đặc trưng tối ưu từ XGBoost được sử dụng làm đầu vào để huấn luyện mô hình LSTM. Điều này giúp LSTM nhận biết các mẫu dựa trên chuỗi dữ liệu, cải thiện khả năng phát hiện các hành vi độc hại và các biến thể malware.

3. Kết hợp LSTM và XGBoost

Kết hợp sử dụng LSTM và các đặc trưng tối ưu từ XGBoost cung cấp một phương pháp mạnh mẽ và hiệu quả cho việc phát hiện mã độc trong môi trường an ninh mạng, tận dụng cả khả năng xử lý dữ liệu chuỗi của LSTM và khả năng chọn lọc đặc trưng của XGBoost để xây dựng hệ thống phát hiện malware linh hoạt và mạnh mẽ.

NII

Lê Văn Minh -Trường Đại học Công nghệ Thông tin - ĐHQG TP.HCM

TEL : 0399031463 **Email : minhlv.18@grad.uit.edu.vn**