**1. Ngữ cảnh, mục tiêu của đề tài.**

**2. Phương pháp chính được sử dụng đề xuất trong tài liệu tham khảo** (hình ảnh mình họa của phương pháp, luồng hoạt động chính)

+ Tài liệu tham khảo: File‐level malware detection using byte streams

+ Đối tượng nghiên cứu chính: mã độc trong file microsoft office, (cụ thể hơn là file có định dạng OLE (Object Linking and Embedding) đuợc dùng cho microsoft office phiên bản từ 1997-2003)

+ Phương pháp chính được sử dụng đề xuất trong tài liệu tham khảo:

“Aggregates the stream-level results to get file-level results for malware detection”

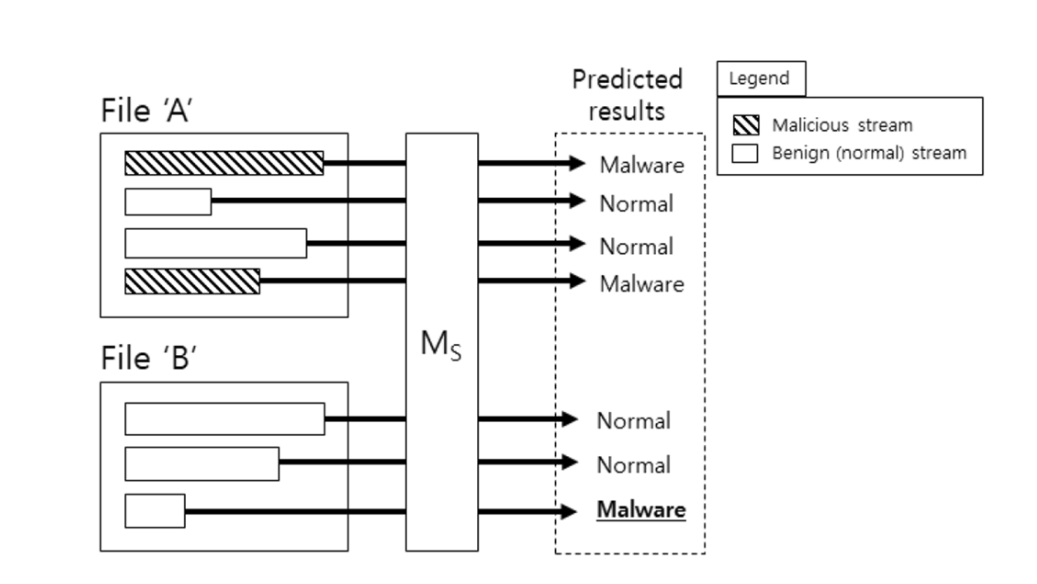
-> Tổng hợp các kết quả stream-level để tạo thành kết quả file-level trong việc phát hiện mã độc.

Các mô hình phát hiện mã độc trước đó:

-> MalConv and SPAP

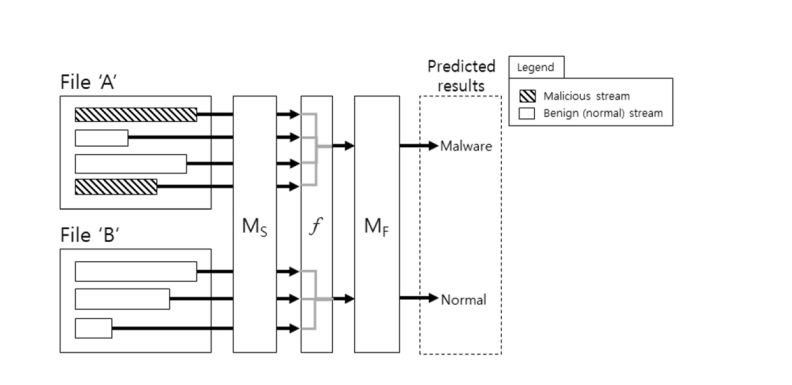
Có thể phát hiện mã độc theo từng stream riêng lẻ rất tốt

tuy nhiên không phát hiện được quan hệ giữa các stream trong cũng 1 file với nhau.

Mô hình phát hiện mã độc theo từng stream riêng lẻ

→ Tài liệu tham khảo đề xuất:

Sử dụng một hàm tổng hợp để tổng hợp kết quả riêng lẻ và cho qua một mô hình phát hiện mã độc file-level để đưa ra kết quả cuối cùng.



**3. Các công việc đã làm được.**

Đã build được mô hình Malconv, tìm được dataset bao gồm 1100 file

**4. Kế hoạch tiếp theo.**

Triển khai thêm hàm tổng hợp mà mô hình file-level để phát hiện mã độc.