TRIỂN KHAI CÔNG NGHỆ ĐÁM MÂY KẾT HỢP CÁC PHƯƠNG PHÁP ĐỂ PHÂN TÍCH PHẦN MỀM MÃ ĐỘC TRONG ỨNG DỤNG ANDROID

Hoàng Trường Thịnh - 230201031

Tóm tắt

- Lớp: **CS2205.CH181**
- Link Github: https://github.com/17130225Hoangthinh/CS2205.CH181
- Link YouTube video: https://youtu.be/6ZriumP1MZs
- Ảnh + Họ và Tên: Hoàng Trường Thịnh

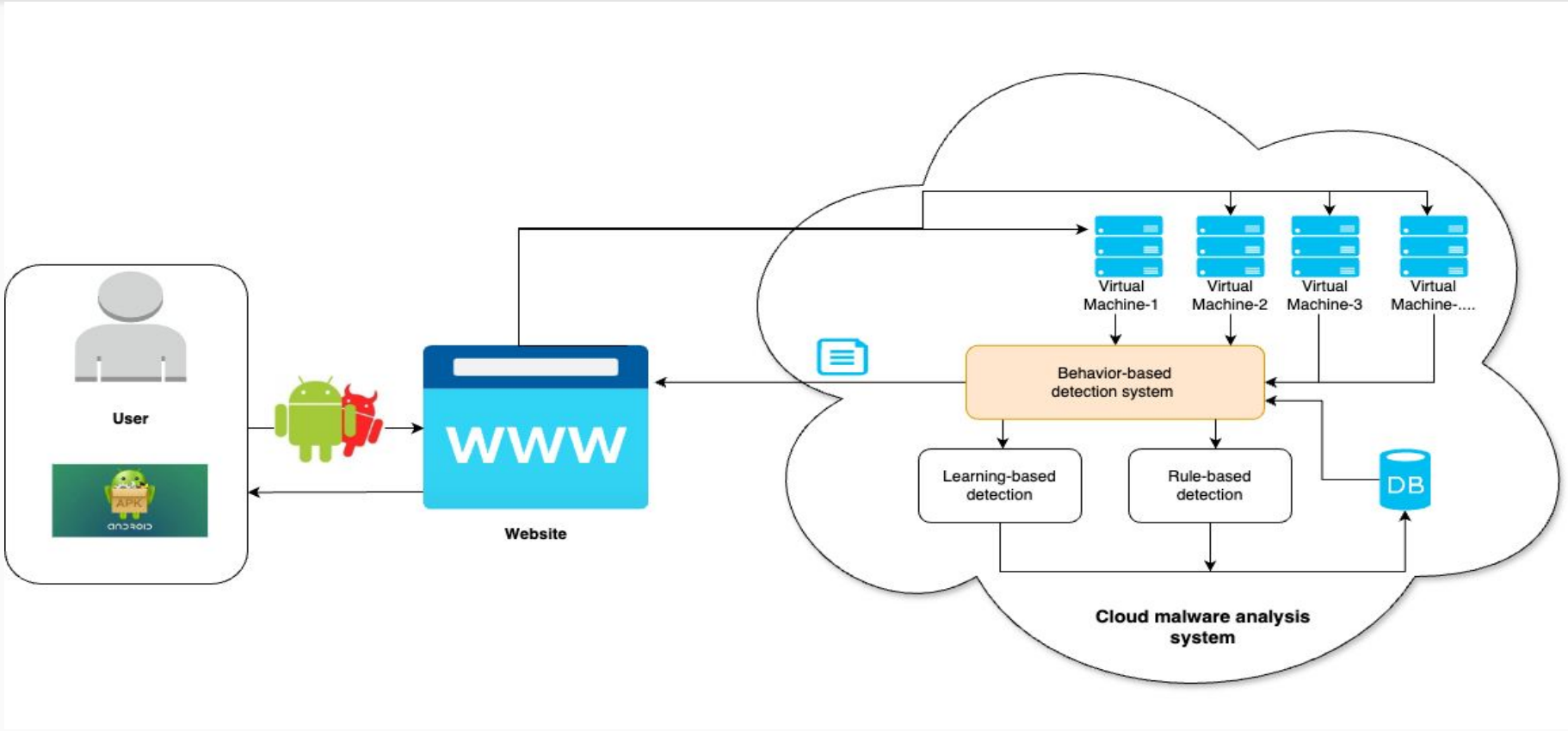
Giới thiệu

Trong thời đại công nghệ phát triển nhanh chóng, hệ điều hành Android phổ biến mang lại nhiều tiến bộ nhưng tạo ra nhiều lỗ hổng bảo mật nghiêm trọng cho phần mềm độc hại xâm nhập.

Phương pháp phân tích truyền thống dù hiệu quả nhưng bị thách thức bởi sự tinh vi và số lượng mã độc ngày càng tăng nhanh chóng.

Nghiên cứu này sử dụng công nghệ đám mây (Cloud) để phân tích phần mềm độc hại trên Android, nâng cao độ chính xác và tốc độ phân tích, nhằm bảo vệ người dùng hiệu quả hơn.

Giới thiệu


User
APK
android
Website
WWW
Virtual Machine-1
Virtual Machine-2
Virtual Machine-3
Virtual Machine-....
Behavior-based detection system
Learning-based detection
Rule-based detection
DB
Cloud malware analysis system

Mục tiêu

- Tạo ra hệ thống sử dụng công nghệ đám mây (cloud) để phát hiện và phân tích mã độc trong ứng dụng Android.
- Cải thiện độ chính xác và tốc độ phân tích mã độc so với phương pháp truyền thống.
- Sử dụng các thuật toán và công cụ phân tích hiện đại để phát hiện và phân tích mã độc.
- Tạo ra một môi trường lý tưởng để thực hiện phân tích mã độc từ các dịch vụ mà công nghệ đám mây (cloud) cung cấp.

Nội dung và Phương pháp

Nội dung thực hiện:

- Thiết kế và triển khai một hệ thống website dựa trên kỹ thuật nền tảng đám mây để phát hiện và phân tích mã độc trong các ứng dụng Android.
- Kết hợp các công nghệ dịch vụ đám mây để tối ưu hoá việc xử lý và lưu trữ dữ liệu lớn.
- Phát triển các mô-đun phân tích tĩnh và động để phân tích các tệp APK.
- Tối ưu hoá hệ thống phân tích để có thể đạt được độ chính xác cao hơn.
- Đảm bảo hệ thống có khả năng cập nhật và mở rộng với các thuật toán mới nhất.
- Áp dụng trí tuệ nhân tạo và các thuật toán máy học để tăng cường khả năng phát hiện mã độc.

Nội dung và Phương pháp

Phương pháp thực hiện (p1):

- Có thể đánh giá và lựa chọn nền tảng đám mây (cloud) như AWS, Google cloud, Microsoft Azure đánh giá bằng hiệu xuất, bảo mật và chi phí.
- Xây dựng kiến trúc bao gồm các thành phần chính như bộ thu thập dữ liệu, mô-đun phân tích tĩnh, mô-đun phân tích động và hệ thống quản lý kết quả
- Xây dựng mô-đun phân tích tĩnh để kiểm tra các thuộc tính của tệp APK như cấu trúc tệp, mã nguồn và đặc trưng dữ liệu.
- Xây dựng mô-đun phân tích động để chạy các tệp APK trong môi trường ảo sanbox và giám sát hành vi của chúng.

Nội dung và Phương pháp

Phương pháp thực hiện (p2):

- Tối ưu hoá lưu trữ và truy xuất trên nền tảng đám mây để giảm thời gian xử lý.
- Phát triển các mô hình máy học dựa trên các tập dữ liệu chứa mã độc và không chứa mã độc để cải thiện khả năng phân loại (URL dataset: https://www.unb.ca/cic/datasets/andmal2017.html)
- Xem xét các giải pháp mã nguồn mở và thương mại để chọn ra các công cụ tối ưu.
- Thiết lập hệ thống với khả năng cập nhật và tích hợp thêm các công cụ và thuật toán khi cần thiết.
- Đánh giá so sánh các kết quả trên các thuật toán và công cụ khác nhau để có được kết quả chính xác nhất.

Kết quả dự kiến

- **Giao diện người dùng thân thiện:** Tải lên tệp APK - phân tích - thông báo kết quả.
- **Cảnh báo thời gian thực:** Thông báo qua email hoặc giao diện hệ thống khi phát hiện mã độc.
- **Khả năng mở rộng:** Cập nhật và tích hợp thuật toán, công cụ mới dễ dàng.
- **Hiệu suất:** Xử lý ít nhất 100 tệp APK mỗi giờ, độ chính xác 95%.

Tài liệu tham khảo

[1] Cui, S. J., Sun, G. X., Bin, S., & Zhou, X. C. (2016). An android malware detection system based on cloud computing. *chemical engineering transactions*, *51*, 691-696.

[2] Aslan, Ö., Ozkan-Okay, M., & Gupta, D. (2021). Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access*, *9*, 83252-83271.

[3] Kumar, R., Sethi, K., Prajapati, N., Rout, R. R., & Bera, P. (2020, July). Machine learning based malware detection in cloud environment using clustering approach. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

[4] Walls, J., & Choo, K. K. R. (2015). A review of free cloud-based anti-malware apps for android. *2015 IEEE Trustcom/BigDataSE/ISPA*, *1*, 1053-1058.

[5] Tian, D., Zhao, R., Ma, R., Jia, X., Shen, Q., Hu, C., & Liu, W. (2022). MDCD: A malware detection approach in cloud using deep learning. *Transactions on Emerging Telecommunications Technologies*, *33*(11), e4584.