|  |  |
| --- | --- |
| ĐẠI HỌC ĐÀ NẴNG  **TRƯỜNG ĐẠI HỌC CNTT VÀ TRUYỀN THÔNG VIỆT - HÀN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – tự do – hạnh phúc**  *Đà Nẵng, ngày 25 tháng 03 năm 2021* |

**ĐỀ XUẤT ĐỀ TÀI**

**NGHIÊN CỨU KHOA HỌC SINH VIÊN NĂM 2021**

**1. Tên đề tài**: Nghiên cứu về virus máy tính và phát triển phần mềm phát hiện virus máy tính ứng dụng trí tuệ nhân tạo.

**2. Lĩnh vực nghiên cứu**:

Mạng máy tính và truyền thông (An ninh mạng)

**3. Tính cấp thiết**:

Ngày nay thời đại công nghệ thông tin, công việc thực hiện với máy tính cá nhân ngày càng nhiều, đặc biệt là việc trao đổi tệp tin với nhau ngày càng dễ dàng và phổ biến. Tuy nhiên sự thuận tiện ấy cũng tiềm ẩn nhiều nguy bị cơ tấn công từ các tổ chức bất chính. Theo số liệu thống kê của các tổ chức an ninh mạng như Kaspersky, Symantec, số lượng tấn công có chủ đích (APT) thông qua mã độc trong những năm gần đây ngày một gia tăng cả về số lượng lẫn mức độ nghiêm trọng. Vì vậy, việc phát hiện các mã độc để hạn chế tối đa tác hại của chúng lên hệ thống máy tính là rất cần thiết nhằm đảm bảo an toàn, an ninh mạng. Đặc biệt trong xu thế chuyển đổi số đang diễn ra mạnh mẽ ở nước ta trên nhiều lĩnh vực và cấp độ khác nhau, việc phát hiện và phòng ngừa các cuộc tấn công bằng mã độc có một vai trò hết sức quan trọng.

Vì lẽ đó, đề tài nhằm mục đích nghiên cứu các loại mã độc, các kỹ thuật dò tìm (phân loại) mã độc dựa vào các đặc trưng của mã độc, trên cơ sở đó huấn luyện các mô hình trí tuệ nhân tạo để phát hiện mã độc.

**4. Mục tiêu**:

Hiểu rõ về virus máy tính, các đặc trưng của virus máy tính.

Phát triển phần mềm cho phép phát hiện sự tồn tại của virus trên máy tính dựa vào các đặc trưng của virus.

**5. Nội dung chính**:

* Tìm hiểu, nghiên cứu đặc điểm của mã độc máy tính.
* Tìm hiểu, nghiên cứu các kỹ thuật phân tích mã độc: phân tích tĩnh, phân tích động.
* Xác định các đặc trưng của mã độc: host-based indicator, network-based indicator.
* Tìm hiểu, nghiên cứu các phương pháp phát hiện mã độc: signature-based và behavior-based.
* Tìm hiểu và nghiên cứu các mô hình học máy (trí tuệ nhân tạo) cho phép phát hiện mã độc hiệu quả.
* Phát triển phần mềm cho phép phát hiện các mã độc dựa trên các đặc tính của chúng ứng dụng trí tuệ nhân tạo.

**6. Sản phẩm và kết quả dự kiến**:

Phần mềm có 2 chức năng cơ bản:

* Quick Scan: Quét nhanh các ổ đĩa của máy tính hoặc các folder đã chọn, tìm kiếm các file có thể là mã độc với tập dữ liệu về các tệp mã độc đã có sẵn.
* Deep Scan: Quét sâu vào các folder và các tiến trình của máy tính để tìm kiếm các tệp mã độc biến thể hoặc các hoạt động không đúng của hệ điều hành.

**7. Thời gian nghiên cứu dự kiến**: 2 tháng.

**8. Kinh phí dự kiến**: Tự túc.

**Xác nhận của khoa Người hướng dẫn Sinh viên**

*(chữ ký, họ và tên)* *(chữ ký, họ và tên)* *(chữ ký, họ và tên)*