BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC THĂNG LONG

BÁO CÁO TỔNG KẾT ĐỀ TÀI NGHIÊN CỨU CẤP CƠ SỞ

ĐỀ TÀI: NGHIÊN CỨU KỸ THUẬT HỌC MÁY PHÁT HIỆN BẤT THƯỜNG TRONG LUỒNG THÔNG TIN TRÊN MẠNG

GIẢNG VIÊN HƯỚNG DẪN:	**PGS.TS Hoàng Trọng Minh**
	ThS. Trần Tuấn Toàn
CHỦ NHIỆM ĐỀ TÀI:	**A46225 – Phạm Anh Dũng**
THÀNH VIÊN:	**A46483 – Nguyễn Thị Thùy Trang**
	A46618 – Lê Xuân Dương

THỜI GIAN THỰC HIỆN:	**5 tháng (từ 10/2024 đến 3/2025)**

HÀ NỘI – 2025

LỜI CAM ĐOAN

Chúng tôi cam đoan rằng báo cáo: "Nghiên cứu kỹ thuật học máy phát hiện bất tường trong luồng thông tin trên mạng" là công trình nghiên cứu của chính nhóm chúng tôi.

Chúng tôi cam đoan các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Không có sản phẩm/nghiên cứu nào của người khác được sử dụng trong luận văn này mà không được trích dẫn theo đúng quy định.

Hà Nội, tháng 3 năm 2025

NHÓM NGHIÊN CỨU

LỜI CẢM ƠN

Trong quá trình học tập và nghiên cứu thực hiện luận văn, ngoài sự nỗ lực của cả nhóm, chúng tôi đã nhận được sự hướng dẫn nhiệt tình và quý báu của quý Thầy Cô, cùng với sự động viên và ủng hộ của gia đình, bạn bè và đồng nghiệp.

Với lòng kính trọng và biết ơn sâu sắc, chúng tôi xin gửi lời cảm ơn chân thành tới: Ban Giám hiệu trường Đại học Thăng Long và quý Thầy Cô đã tạo mọi điều kiện thuận lợi giúp chúng tôi hoàn thành luận văn.

Chúng tôi xin chân thành cảm ơn Thầy **PGS. TS Hoàng Trọng Minh**, và Thầy **ThS Trần Tuấn Toàn** đã hết lòng giúp đỡ, tạo điều kiện cho nhóm chúng tôi trong suốt quá trình thực hiện luận văn.

Chúng tôi xin chân thành cảm ơn gia đình, bạn bè thân thiết đã động viên, hỗ trợ chúng tôi để có thể học tập và hoàn thành luận văn.

Mặc dù đã có nhiều cố gắng, nỗ lực tìm tòi nghiên cứu, nhưng do thời gian có hạn và kinh nghiệm nghiên cứu khoa học còn hạn chế nên không thể tránh khỏi những thiếu sót. Chúng tôi rất mong muốn nhận được sự góp ý chân thành của quý Thầy Cô để kiến thức của nhóm chúng tôi ngày một hoàn thiện hơn.

Xin chân thành cảm ơn!

Hà Nội, tháng 3 năm 2025

NHÓM NGHIÊN CỨU

MỤC LỤC

DANH SÁCH BẢNG

DANH SÁCH HÌNH ẢNH

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Với sự phát triển nhanh chóng của chuyển đổi số, nhiều tổ chức, doanh nghiệp đang đối mặt với các mối đe dọa bảo mật không ngừng gia tăng, các cuộc tấn công cũng ngày càng trở nên phức tạp và khó phát hiện hơn. Việc ứng dụng học máy trong phát hiện luồng thông tin bất thường có thể giúp giảm thiểu sự can thiệp thủ công từ con người trong quản lý và vận hành mạng, từ đó giúp giảm chi phí. Hệ thống cũng có thể hoạt động liên tục và đưa ra các cảnh báo trong thời gian thực, giúp bảo vệ hệ thống mạng tốt hơn.

2. Tổng quan về vấn đề nghiên cứu

Thời đại công nghệ 4.0 đã thúc đẩy đột phá trong nhiều lĩnh vực như Trí tuệ nhân tạo (AI), Máy học (ML) cùng với sự phát triển bùng nổ của viễn thông, internet dẫn đến các mối đe dọa về bảo mật cũng gia tăng, làm xuất hiện các cuộc tấn công như DDoS (tấn công từ chối dịch vụ phân tán), tấn công bằng phần mềm độc hại, và xâm nhập hệ thống.

Luồng thông tin là cách thông tin được truyền tải từu một nguồn tới một đích. Việc phát hiện luồng thông tin bất thường đóng vai trò quan trọng trong việc ngăn chặn các cuộc tấn công mạng.

Trong những năm gần đây, việc áp dụng phương pháp học máy (ML) cho phân loại luồng thông tin đã đạt được những kết quả đáng chú ý. Với khả năng xử lý thông tin phức tạp từ nhiều đặc trưng khác nhau, mô hình học máy có thể phân loại các dữ liệu đầu vào với độ chính xác cao.

Đề tài Nghiên cứu kỹ thuật học máy phát hiện bất thường trong luồng thông tin trên mạng nhằm phát triển và thử nghiệm một hệ thống được thiết lập để học hoặc ghi nhận các luồng thông tin hợp pháp và bình thường trong mạng, sau đó phát hiện và thông báo các bất thường dựa trên hành vi hoặc thông số không phù hợp với mẫu đã học.

3. Mục đích nghiên cứu

Phát triển và thử nghiệm một module phần mềm sử dụng kỹ thuật học máy để phát hiện luồng thông tin bất thường. Cụ thể, thông qua các phần mềm giám sát để bắt các gói tin đi qua mạng, lọc ra gói nào bình thường, gói nào bất thường, dựa vào kỹ

thuật học máy tự động nhận diện, phân loại và dự đoán nhằm có thể chặn lại các nguồn phát gói tin bất thường, ngăn chặn các cuộc tấn công mạng.

4. Đối tượng và phạm vi nghiên cứu

- Đối tượng nghiên cứu:
  + Các gói tin được thu thập trên đường mạng
  + Nghiên cứu thuật toán học máy, phân loại và dự báo để phân loại gói tin.
- Phạm vi nghiên cứu:
  + Phát triển và thử nghiệm mô hình dữ liệu: lược đồ dữ liệu và mô tả dữ liệu của các gói tin
  + Cách xử lý dữ liệu dạng số, nhị phân, liệt kê, văn bản
  + Các phương pháp học máy và phân loại

5. Phương pháp nghiên cứu

- Phương pháp luận: Dựa trên cơ sở là các lý thuyết về các giao thức giám sát mạng, các thuật toán phân cụm trong các kỹ thuật học máy.
- Phương pháp đánh giá bằng mô hình thực nghiệm: Xây dựng mô hình mô phỏng, phát triển và thử nghiệm phần mềm giám sát các gói tin ứng dụng kỹ thuật học máy.

6. Bố cục báo cáo

Ngoài phần mở đầu, mục lục, kết luận và tài liệu tham khảo, nội dung chính của báo cáo được chia thành 4 chương, cụ thể như sau:

Chương 1 trình bày tổng quan về ứng dụng kỹ thuật học máy trong việc phân loại gói tin.

Chương 2 trình bày cơ sở lý thuyết và các công trình liên quan

Chương 3 trình bày đề xuất, nghieien cứu mô hình học máy cho dự án phân loại gói tin.

Chương 4 trình bày mô phỏng chương trình phân loại gói tin.

KẾT LUẬN

1. Kết quả nghiên cứu của đề tài

Thông qua đề tài "Nghiên cứu kỹ thuật học máy phát hiện bất tường trong luồng thông tin trên mạng", nhóm nghiên cứu đã thực hiện khảo sát, phân tích và xây dựng một chương trình phát hiện xâm nhập sử dụng các thuật toán học máy hiện đại. Cụ thể:

- Đã nghiên cứu tổng quan về các phương pháp học máy, đặc biệt là ứng dụng của chúng trong hệ thống phát hiện xâm nhập mạng (IDS).
- Sử dụng bộ dữ liệu CSE-CIC-IDS2018 – một trong những bộ dữ liệu cập nhật và đa dạng nhất – làm nền tảng huấn luyện và kiểm thử mô hình.
- Triển khai các thuật toán học máy như Logistic Regression, Random Forest, và Neural Network, qua đó đánh giá được hiệu suất của từng mô hình trong bài toán phân loại gói tin.
- Kết quả thực nghiệm cho thấy một số mô hình đạt độ chính xác và hiệu quả phân loại cao, đặc biệt trong việc nhận diện các luồng dữ liệu bất thường.

Hệ thống đã bước đầu chứng minh được khả năng phát hiện và phân loại các gói tin độc hại, góp phần nâng cao năng lực phòng thủ của hệ thống mạng trước các mối đe dọa an ninh.

2. Hạn chế của nghiên cứu

Mặc dù đạt được nhiều kết quả tích cực, đề tài vẫn tồn tại một số hạn chế:

- Việc xử lý dữ liệu lớn từ bộ CSE-CIC-IDS2018 gặp khó khăn do giới hạn về tài nguyên tính toán và thời gian xử lý.
- Một số mô hình học máy, đặc biệt là mạng nơ-ron, yêu cầu cấu hình máy mạnh và thời gian huấn luyện lâu, gây trở ngại trong việc thử nghiệm sâu hơn.
- Bộ dữ liệu mặc dù đa dạng nhưng vẫn là dữ liệu mô phỏng, chưa phản ánh toàn diện tính chất động và phức tạp của môi trường mạng thực tế.
- Việc tích hợp hệ thống vào một môi trường mạng thật để đánh giá hiệu năng thời gian thực chưa được thực hiện trong khuôn khổ đề tài.

3. Hướng phát triển

Trong giai đoạn tiếp theo, nhóm nghiên cứu định hướng mở rộng và nâng cao chất lượng hệ thống theo hai hướng chính:

a. Phát triển mô hình phân loại đa lớp (multi-class classification)

Hiện tại, mô hình chủ yếu thực hiện phân loại nhị phân (gói tin "bình thường" và "bất thường"). Tuy nhiên, trong thực tế, các cuộc tấn công mạng rất đa dạng về hình thức như: DDoS, Brute Force, Botnet, PortScan, SQL Injection, v.v. Do đó, việc xây dựng mô hình phân loại đa lớp sẽ giúp:

- Nhận diện cụ thể loại hình tấn công đang diễn ra thay vì chỉ phát hiện hành vi bất thường nói chung.
- Hỗ trợ đưa ra biện pháp ứng phó phù hợp hơn đối với từng loại đe dọa.
- Cải thiện độ chính xác và giá trị thực tiễn của hệ thống trong môi trường vận hành.

Việc huấn luyện mô hình phân loại đa lớp sẽ đòi hỏi kỹ thuật xử lý dữ liệu phức tạp hơn và cân nhắc kỹ lưỡng về mất cân bằng nhãn, nhưng là bước đi cần thiết để hệ thống có thể đáp ứng tốt các yêu cầu thực tiễn.

b. Tích hợp mô hình vào hệ thống giám sát mạng thời gian thực (real-time)

Một hướng phát triển quan trọng khác là đưa mô hình học máy vào ứng dụng thực tế theo thời gian thực. Việc này bao gồm:

- Xây dựng một pipeline cho phép thu thập, xử lý, và phân loại gói tin trực tiếp khi lưu lượng mạng diễn ra.
- Tối ưu hóa hiệu suất mô hình để đảm bảo tốc độ phản hồi nhanh, tránh tình trạng trễ trong phát hiện và cảnh báo.
- Thiết kế giao diện giám sát hoặc hệ thống cảnh báo tự động để thông báo ngay lập tức khi có dấu hiệu tấn công.

Khi tích hợp thành công vào hệ thống mạng doanh nghiệp hoặc tổ chức, mô hình không chỉ dừng lại ở mức độ nghiên cứu mà có thể trở thành một công cụ hỗ trợ an ninh mạng hiệu quả và ứng dụng thực tế cao.

PHỤ LỤC

1. Code xử lý dataset IDS 2018
   https://colab.research.google.com/drive/1bqkoL2I5K3GEnRD9CRr2T_VrjQJ5qYt2?usp=sharing
2. Code xây dựng mô hình
   https://colab.research.google.com/drive/1A_k8FfR0uFOumFC94VTzOZs8mNI7JEni?usp=sharing

TÀI LIỆU THAM KHẢO

[1] Badillo, Solveig, et al. "An introduction to machine learning." Clinical pharmacology & therapeutics 107.4 (2020): 871-885.

[2] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

[3] Khraisat, Ansam, et al. "Survey of intrusion detection systems: techniques, datasets and challenges." Cybersecurity 2.1 (2019): 1-22.

[4] University of New Burnswick, “CSE-CIC-IDS2018 on AWS” , https://www.unb.ca/cic/datasets/ids-2018.html

https://viblo.asia/p/optimizer-hieu-sau-ve-cac-thuat-toan-toi-uu-gdsgdadam-Qbq5QQ9E5D8

https://scikit-learn.org/stable/modules/linear_model.html#logistic-regression

[5] Nguyễn, Điệp Ngọc. "Nâng Cao Khả Năng Phát Hiện Xâm Nhập Mạng Sử Dụng Mạng CNN: Array." Journal of Science and Technology on Information and Communications 1.4B (2020): 61-68.

[6] Lê Hoàng Bảo, Phân loại lưu lượng mạng Internet dùng Machine Learning, Luận văn Thạc sĩ, Học viện Công nghệ Bưu chính Viễn thông, TP. Hồ Chí Minh, 2022.

[7] Nguyễn, V. C., Trần, N. T., & Đỗ, Đ. Q. (2023). Phát hiện xâm nhập website dựa trên cây quyết định và bộ dữ liệu huấn luyện IDS2021-WEB. An toàn thông tin.