**TRƯỜNG ĐẠI HỌC HỒNG ĐỨC**

**KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**THUYẾT MINH**

**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN NĂM HỌC 2022-2023**

**NGHIÊN CỨU XÂY DỰNG PHẦN MỀM SỬ DỤNG AI PHÁT HIỆN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ (DDOS)**

**Thuộc nhóm ngành khoa học: Khoa học máy tính**

**TRƯỜNG ĐẠI HỌC HỒNG ĐỨC**

**KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**THUYẾT MINH**

**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN NĂM HỌC 2022-2023**

**NGHIÊN CỨU XÂY DỰNG PHẦN MỀM SỬ DỤNG AI PHÁT HIỆN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ (DDOS)**

**Thuộc nhóm ngành khoa học: Khoa học máy tính**

# Nhóm sinh viên thực hiện(đại diện): Lê Xuân Quang Giới tính: Nam

Dân tộc: Kinh

Lớp, khoa: K23A, CNTT&TT Năm thứ: 3 /Số năm đào tạo: 4 Ngành học: Công nghệ thông tin

Người hướng dẫn: TS. Nguyễn Thế Cường

## TRƯỜNG ĐẠI HỌC HỒNG ĐỨC

**KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**THUYẾT MINH ĐỀ TÀI NGHIÊN CỨU KHOA HỌC SINH VIÊN**

**Năm học 2022 - 2023**

1. **Tên đề tài:** Nghiên cứu xây dựng phần mềm sử dụng AI phát hiện hình thức tấn công từ chối dịch vụ (DDoS).

## Cấp dự thi

Cấp trường.

## Nhóm sinh viên thực hiện

* 1. Họ và tên(người đại diện): Lê Xuân Quang

Lớp: K23A-CNTT Khoa: Công nghệ Thông tin

Điện thoại: 0852747537 Email: [lexuanquang1408@gmail.com](mailto:lexuanquang1408@gmail.com)

* 1. Họ và tên: Lê Đình Thắng

Lớp: K23A-CNTT Khoa: Công nghệ Thông tin

Điện thoại: 0925058118 Email: [ledinhthang.thvn@gmail.com](mailto:ledinhthang.thvn@gmail.com)

* 1. Họ và tên: Cao Sơn Đăng

Lớp: K23A-CNTT Khoa: Công nghệ Thông tin

Điện thoại: 0367756372 Email: [dangkudo230202@gmail.com](mailto:dangkudo230202@gmail.com)

3.2. Họ và tên: Hoàng Văn Huy

Lớp: K23A-CNTT Khoa: Công nghệ Thông tin

Điện thoại: 0859734136 Email: [Hoangvanhuy1709@gmail.com](mailto:Hoangvanhuy1709@gmail.com)

## Cơ quan chủ trì

Khoa Công nghệ thông tin và Truyền thông.

## Lĩnh vực nghiên cứu

Công nghệ thông tin.

## Loại hình nghiên cứu

Triển khai.

## Thời gian thực hiện

8 tháng, từ tháng 09/2022 đến 04/2023.

## Sự cần thiết của đề tài

Theo các báo cáo của securelist.com, trên toàn cầu, quý 1 năm 2022 đã phát hiện

91.052 cuộc tấn công DDoS. Hầu hết các cuộc tấn công (94,95%) kéo dài dưới 4 giờ, nhưng cuộc tấn công dài nhất tiếp tục trong 549 giờ (gần 23 ngày).Trong quý 2 năm 2022, các cuộc tấn công DDoS đã giảm 13,72% (xuống còn 78558) so với kỳ báo cáo trước đó. Hoạt động tăng đều đặn trong suốt quý: trung bình từ 731 cuộc tấn công mỗi ngày vào tháng 4 lên 845 vào tháng 5, lên 1195 vào tháng 6.

Đặc biệt, các thông báo được đăng ngày 21/8/2022 thì Google vừa chặn đứng cuộc tấn công DDoS lớn nhất từ trước tới nay, với đỉnh điểm lên tới 46 triệu yêu cầu mỗi giây

(rps), lớn hơn 76% so với đợt tấn công kỷ lục từng được ghi nhận trước đó. Theo bài đăng, quy mô của cuộc tấn công tương đương với việc hứng chịu toàn bộ lượng truy cập trong 1 ngày của Wikipedia - một trong những trang web có lưu lượng truy cập lớn nhất thế giới - chỉ trong vòng 10 giây.

Theo dữ liệu từ Cục An ninh mạng, Bộ công an, trong 6 tháng đầu năm 2021 đã phát hiện 2.551 vụ tấn công mạng, 5,4 triệu lượt địa chỉ IP của các cơ quan Nhà nước bị tấn công với 15 biến thể mã độc. Có gần 250 báo, tạp chí điện tử trong tổng số hơn 800 cơ quan báo chí. Đáng chú ý là các cơ quan truyền thông, báo chí luôn nằm trong top bị tấn công từ chối dịch vụ (DDoS). Việt Nam đứng thứ 6 về nguồn tấn công DDoS trên toàn cầu, sau Trung Quốc, Mỹ, Pháp, Nga và Brazil. Trong khi đó, tại khu vực châu Á - Thái Bình Dương, Việt Nam đứng thứ 2 về nguồn tấn công DDoS.

Theo nghiên cứu của Viện Ponemon(Hoa Kỳ), một cuộc tấn công DDoS sẽ tiêu tốn trung bình 22.000 đô la cho mỗi phút ngừng hoạt động mà nó gây ra.

Theo các số liệu thống kê cho thấy tổn thất về kinh tế, dữ liệu, tài nguyên… mà DDoS gây ra rất lớn. Cùng với sự phát triển của trí thông minh nhân tạo, nhóm em quyết định chọn đề tài: “Nghiên cứu xây dựng phần mềm sử dụng AI phát hiện hình thức tấn công từ chối dịch vụ (DDoS)” nhằm đóng góp một phần nhỏ vào công cuộc an ninh mạng.

## Sơ lược về tình hình nghiên cứu trong và ngoài nước về vấn đề chọn nghiên cứu

Cụm từ “Trí tuệ nhân tạo(AI)” ra đời vào những năm 1950 khi nghiên cứu ban đầu về khoa học tính toán khám phá các phương pháp tự động hóa đơn giản. Nhưng nó mới thật sự bùng nổ lan nhanh ra toàn thế giới trong vài năm gần đây. Đến nay đã có hơn 1,6 triệu bài báo khoa học liên quan đến trí tuệ nhân tạo được công bố, trong đó một lượng không nhỏ liên quan đến an ninh mạng. Một số thành tựu của trí thông minh nhân tạo đã đạy được trong an ninh mạng và các mặt của đời sống:

* Báo cáo Tin tức An ninh mạng thường niên năm 2018 của Cisco cho thấy, hơn 30% giám đốc về an ninh thông tin đã áp dụng AI như một cách để cải thiện hiệu quả tổng thể của chiến lược an ninh mạng.
* AlphaFold (DeepMind) dự đoán cấu trúc 3D của protein là một thành tựu nổi bật của AI trong lĩnh vực sinh học và y tế.
* AI đã giành giải cao nhất trong cuộc thi vẽ tranh có tên“Colorado State Fair fine art”.
* Năm 1997 đánh dấu một bước ngoặt lớn khi mà siêu máy tính DeepBlue của IBM (sau nhiều lần bị thua) đã đánh bại một siêu đại kiện tướng cờ vua Gary Kasparov.
* Hệ thống trí thông minh nhân tạo AlphaGo của Google giành chiến thắng trước nhà vô địch cờ vây thế giới Lee Se-dol vào năm 2016.

Ngành trí tuệ nhân tạo của Việt Nam tuy đang con rất non trẻ, nhưng tốc độ phát triển nhanh chóng và đã đạt được những thành tựu ngoài sức mong đợi:

* Ngày 17/4/2019, Tập đoàn Vingroup chính thức công bố thành lập Viện Nghiên cứu Trí tuệ Nhân tạo AI - VinAI Research.
* Hệ thống xe điện tự lái của VinAI.
* Ngày 20/4/2020, Viện Nghiên cứu Trí tuệ Nhân tạo VinAI Research công bố đã nghiên cứu thành công công nghệ nhận diện khuôn mặt chính xác và ổn định cả khi sử dụng khẩu trang.

Trong các thành tựu lớn đó thì an ninh mạng chưa được chú trong phát triển.

## Mục tiêu nghiên cứu

Trình bày về lý thuyết về hình thức tấn công từ chối dịch vụ DDoS, một số kĩ thuật trong trí tuệ nhân tạo dùng để dự đoán, nhận diện hình thức tấn công DDoS và xây dựng phần mềm phát hiện hình thức tấn công DDoS.

## Đối tượng và phạm vi nghiên cứu Đối tượng nghiên cứu

Các phương pháp tấn công DDoS và các giải pháp nhận dạng tấn công

DDoS.

## Phạm vi nghiên cứu

Dữ liệu về các tấn công dạng DDoS trong mạng các dịch vụ

## Nội dung nghiên cứu

* Tìm hiểu mô hình để nhận dạng đối tượng.
* Tìm hiểu các phương pháp tối ưu mô hình.
* Nghiên cứu xây dựng mô hình.
* Triển khai mô hình đã nghiên cứu.

## Phương pháp nghiên cứu

* Phương pháp chuyên gia.
* Phương pháp phân tích và tổng hợp lý thuyết.
* Phương pháp phân loại và hệ thống hóa lý thuyết.
* Phương pháp thực nghiệm.

1. **Hiệu quả và phạm vi sử dụng** (kinh tế, xã hội, giáo dục, khoa học, kỹ thuật**,..) và tính mới, đóng góp mới của đề tài**

Tạo mô hình tối ưu nhằm phát hiện tấn công DDoS, đóng góp ứng dụng cho cộng

đồng.

## Dự kiến kết quả

* Báo cáo tổng kết cơ sở lý thuyết về an ninh mạng và hình thức tấn công DDoS.
* Phân tích, đánh giá được dữ liệu về các cuộc tấn công DDoS đã có.
* Xây dựng được mô hình dự đoán, phát hiện được các tấn công DDoS.
* Đánh giá được mô hình phát hiện tấn công DDoS dựa vào thông tin liên quan.

## Nội dung và tiến độ thực hiện công việc

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TT** | **Nội dung công việc** | **Kết quả cần đạt được** | **Thời gian** | | **Người thực hiện** | **Ghi chú** |
| **Bắt đầu** | **Kết thúc** |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Xây dựng và bảo vệ thuyết minh đề tài | Thuyết minh đề tài | 09/2022 | 10/2022 | Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn  Huy |  |
| 2 | Tìm hiểu mô hình để nhận diện đối tượng, các phương pháp tối ưu mô hình | Tài liệu tìm hiểu | 10/2022 | 12/2022 | Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn  Huy |  |
| 3 | Nghiên cứu xây dựng mô hình | Các giải pháp đề xuất và chương trình thực nghiệm | 12/2022 | 04/2023 | Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn  Huy |  |
| 4 | Tổng hợp, viết báo cáo, viết bài báo khoa học, nghiệm thu đề tài | Đề tài được xếp loại Khá trở lên. | 04/2022 | 04/2023 | Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn  Huy |  |

1. **Sản phẩm**

Phần mềm phát hiện hình thức tấn công từ chối dịch vụ (DDoS).

## Nhu cầu kinh phí để thực hiện đề tài:

Theo quy chế chi tiêu nội bộ *(Ban hành theo Quyết định 2203/QĐ-ĐHHĐ ngày 28 tháng 11 năm 2014 của Hiệu trưởng trường Đại học Hồng Đức)* - Kinh phí đề tài dự thi cấp trường, cấp khoa: 1.000.000 đ/đề tài.

## Đề xuất các yêu cầu, điều kiện cho thực hiện đề tài

*Thanh Hóa, ngày 10 tháng 09 năm 2022*

## Hiệu trưởng Đơn vị chủ trì GV hướng dẫn

**Nguyễn Thế Cường**

**Trưởng nhóm**

**Lê Xuân Quang**