**Các thành viên của nhóm:**

* Hoàng Cường – N21DCAT007
* Đoàn Văn Minh Hoàng – N21DCAT022
* Tạ Minh Khoa- N21DCAT027
* Nguyễn Lâm Tất Thắng - N21DCAT049
* Nguyễn Tấn Tường – N21DCAT063

**1. Sự kiện khoa học**

**Sự kiện khoa học** liên quan đến chủ đề này là sự gia tăng tần suất và tinh vi của các cuộc tấn công từ chối dịch vụ (Denial of Service - DoS) và cách trí tuệ nhân tạo (AI) đang được áp dụng để cải thiện khả năng phát hiện và ngăn chặn các cuộc tấn công này. Một sự kiện nổi bật là việc các nghiên cứu gần đây đã chỉ ra rằng các hệ thống bảo mật dựa trên AI, sử dụng các thuật toán machine learning, đã cải thiện đáng kể khả năng phát hiện và phản ứng nhanh chóng với các cuộc tấn công DoS so với các phương pháp truyền thống. Ví dụ, nghiên cứu vào năm 2023 cho thấy việc áp dụng học sâu (deep learning) trong phân tích lưu lượng mạng có thể phát hiện các mẫu tấn công DoS với độ chính xác cao hơn.

**2. Nhiệm vụ nghiên cứu**

**Nhiệm vụ nghiên cứu** là phát triển và đánh giá các phương pháp sử dụng trí tuệ nhân tạo để phát hiện và ngăn chặn các cuộc tấn công DoS. Nghiên cứu sẽ tập trung vào việc cải thiện các thuật toán AI trong việc nhận diện lưu lượng mạng bất thường, phân loại các cuộc tấn công DoS, và thiết lập các cơ chế phản ứng tự động. Điều này bao gồm việc nghiên cứu các kỹ thuật machine learsning và deep learning để phát hiện sớm các cuộc tấn công DoS, đồng thời tối ưu hóa hiệu quả phòng chống để giảm thiểu ảnh hưởng đối với hệ thống và dịch vụ.

**3. Tên đề tài**

**Tên đề tài**: "Ứng dụng của trí tuệ nhân tạo trong phát hiện và ngăn chặn các mối đe dọa tấn công DoS"

**4. Từ tên đề tài, hãy cho biết: đối tượng nghiên cứu, khách thể nghiên cứu, phạm vi nghiên cứu**

* **Đối tượng nghiên cứu**:
  + Các thuật toán và kỹ thuật trí tuệ nhân tạo (AI) áp dụng trong việc phát hiện và ngăn chặn tấn công DoS. Điều này bao gồm các kỹ thuật như học sâu (deep learning), học máy (machine learning), và phân tích hành vi mạng.
* **Khách thể nghiên cứu**:
  + Các mối đe dọa cụ thể liên quan đến tấn công DoS, bao gồm các hình thức khác nhau của DoS như tấn công từ chối dịch vụ phân tán (DDoS), tấn công tắc nghẽn băng thông, và tấn công từ chối dịch vụ ứng dụng (application layer DoS).
* **Phạm vi nghiên cứu**:
  + **Phạm vi không gian**: Nghiên cứu có thể bao gồm các môi trường mạng khác nhau như doanh nghiệp, trung tâm dữ liệu, và hệ thống mạng trực tuyến.
  + **Phạm vi thời gian**: Nghiên cứu sẽ tập trung vào các giải pháp và công nghệ AI hiện tại trong vòng 5 năm qua, đồng thời phân tích các xu hướng và triển vọng phát triển trong tương lai gần.