**CHƯƠNG 1. GIỚI THIỆU**

**1.1 Đặt vấn đề / Giới thiệu đề tài / Bối cảnh**

Trong kỷ nguyên chuyển đổi số hiện nay, Internet và các hệ thống mạng ngày càng thâm nhập sâu vào mọi lĩnh vực kinh tế - xã hội, từ tài chính, thương mại điện tử, y tế, giáo dục đến sản xuất công nghiệp. Tính đến đầu năm 2024, Việt Nam ghi nhận hơn 78,4 triệu người sử dụng Internet, chiếm 79,1% dân số, với tốc độ tăng trưởng đều đặn mỗi năm; dự kiến đến năm 2029 sẽ vượt mốc 100 triệu người dùng, đồng nghĩa với sự mở rộng không ngừng của hạ tầng số và nguy cơ tấn công mạng lan tỏa trên diện rộng.[1] [2] Song song với sự phát triển này, an ninh mạng trở thành đề xuất cấp thiết, đặc biệt trước thực trạng hình thức tấn công ngày càng tinh vi với quy mô lớn: Chỉ trong 6 tháng đầu năm 2024, hệ thống Viettel Threat Intelligence ghi nhận khoảng 500.000 cuộc tấn công DDoS, tăng 16% so với cùng kỳ năm 2023, tổng thiệt hại do mã hóa dữ liệu lên tới hơn 10 triệu USD [2]. Số vụ rò rỉ dữ liệu doanh nghiệp và tổ chức cũng tăng mạnh, trong đó phổ biến là lộ lọt dữ liệu khách hàng và thông tin danh tính điện tử. Một báo cáo khác cho thấy, trong năm 2024 có tổng cộng 659.000 vụ/cảnh báo tấn công mạng ghi nhận trên các tổ chức/đơn vị tại Việt Nam nhằm vào các ngành trọng yếu như tài chính, dịch vụ công, công nghiệp và giáo dục.

Trong bối cảnh đó, hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) đóng vai trò như một tuyến phòng thủ chủ động, giúp phát hiện sớm các hành vi bất thường và hỗ trợ phản ứng kịp thời trước các mối đe dọa an ninh. Tuy nhiên, các phương pháp IDS truyền thống chủ yếu dựa trên chữ ký (signature-based) hoặc luật định (rule-based) đang ngày càng bộc lộ những hạn chế rõ rệt, nhất là khi đối mặt với các hình thức tấn công phức tạp, chưa từng biết đến (zero-day) hoặc có khả năng ẩn mình cao.Nhằm khắc phục những điểm yếu này, các giải pháp dựa trên học máy – đặc biệt là học sâu (deep learning) – đã và đang được ứng dụng rộng rãi trong lĩnh vực phát hiện xâm nhập. Với khả năng tự động trích xuất đặc trưng, học biểu diễn và phát hiện các mẫu dữ liệu phức tạp, mô hình học sâu có thể phát hiện hiệu quả cả những hành vi bất thường tinh vi, nhờ đó cải thiện đáng kể khả năng bảo vệ hệ thống mạng trước các mối đe dọa mới.

Trong các môi trường mạng hiện đại, hệ thống phát hiện xâm nhập (IDS) đóng vai trò then chốt trong việc bảo vệ hạ tầng thông tin trước sự gia tăng về số lượng và mức độ tinh vi của các cuộc tấn công mạng. Tuy nhiên, khi các hệ thống ngày càng đa dạng về kiến trúc, thiết bị và lưu lượng – đặc biệt là trong các môi trường mạng không đồng nhất như mạng doanh nghiệp, mạng IoT và hệ thống điều khiển công nghiệp (ICS) thì các mô hình IDS truyền thống dần bộc lộ những hạn chế nhất định.

Hiện nay, nhiều nghiên cứu đã đề cập đến việc ứng dụng học sâu trong các hệ thống IDS, song phần lớn các nghiên cứu vẫn chỉ dừng lại ở việc đánh giá hiệu quả mô hình trên từng môi trường hoặc tập dữ liệu đơn lẻ, hoặc chỉ phản ánh những kết quả rời rạc trong những trường hợp thử nghiệm cụ thể. Cách tiếp cận này tuy giúp xác định tiềm năng của mô hình trong các bối cảnh nhất định, song lại hạn chế khả năng tổng quát hóa, đánh giá độ thích nghi thực tế cũng như tính ứng dụng rộng rãi của phương pháp khi triển khai trên nhiều loại môi trường mạng khác nhau.

Trước thách thức đó, việc đánh giá toàn diện hiệu năng và độ bền vững của các mô hình học sâu trong phát hiện xâm nhập là điều cần thiết. Bên cạnh chỉ số chính xác của mô hình, các mô hình này buộc phải thể hiện được khả năng thích ứng linh hoạt, đảm bảo độ ổn định trước sự biến động liên tục về kiến trúc, quy mô, lưu lượng dữ liệu cũng như đặc trưng an ninh của các môi trường mạng đa dạng ngày nay. Chỉ khi đáp ứng được những yêu cầu này, các giải pháp phát hiện xâm nhập dựa trên học sâu mới thực sự phát huy hiệu quả khi chuyển giao từ phòng thí nghiệm ra thực tế, góp phần nâng cao năng lực phòng thủ mạng trong kỷ nguyên kết nối liên tục. Vì vậy đề tài **"Đánh giá hiệu năng và độ bền vững của các giải pháp học sâu trong phát hiện xâm nhập trên các môi trường mạng không đồng nhất”** được thực hiện, nhằm cung cấp cái nhìn toàn diện về hiệu quả và tính ứng dụng thực tiễn của các phương pháp học sâu trong phát hiện xâm nhập, qua đó đóng góp cho việc xây dựng các hệ thống an ninh mạng thông minh, linh hoạt và bền vững.

**1.2 Những nghiên cứu liên quan**

**1.3 Mục tiêu đề tài**

**1.4 Đối tượng và phạm vi nghiên cứu**

**1.4.1 Đối tượng nghiên cứu**

**1.4.2 Phạm vi nghiên cứu**

**1.5 Phương pháp nghiên cứu**

**1.6 Bố cục quyển luận văn**

**CHƯƠNG 2 CƠ SỞ LÝ THUYẾT**

**2.1**

**2.2 DL**

**2.3 CNN**

**2.4 LSTM**

**2.5 GRU**

**2.6 DNN**

**2.7 CNN-DNN**

**2.8 CNN-LSTM**

**2.9 CNN-GRU**

**CHƯƠNG 3. PHƯƠNG PHÁP THỰC HIỆN**

**CHƯƠNG 4. KẾT QUẢ THỰC NGHIỆM**

**4.1. Thiết lập môi trường**

**4.2. Cơ sở đánh giá**

**4.3. Điều chỉnh siêu tham số và đào tạo mô hình**

**4.3.1. Mô hình CNN**

**4.3.2. Mô hình LSTM**

**4.3.3. Mô hình GRU**

**4.3.4. Mô hình RNN**

**4.3.5. Mô hình DNN**

**4.3.5. Mô hình CNN-LSTM**

**4.3.5. Mô hình GRU-LSTM**

**4.3.6. So sánh các mô hình**

**....**

**CHƯƠNG 5. KẾT LUẬN**

**5.1. Kết quả đạt được**

**5.2. Hạn chế**

**5.3. Hướng phát triển**