|  |
| --- |
| **hiBỘ GIÁO DỤC VÀ ĐÀO TẠO**  HÀ NGỌC TUÂN ANH HỆ THỐNG XÂM NHẬP BẰNG AI 2025  **TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT HƯNG YÊN**  **HÀ NGỌC TUẤN ANH**  **HỆ THỐNG PHÁT HIỆN XÂM NHẬP BẰNG AI**  **ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC**  **HƯNG YÊN - 2025** |

|  |
| --- |
| **BỘ GIÁO DỤC VÀ ĐÀO TẠO**  **TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT HƯNG YÊN**  **HÀ NGỌC TUẤN ANH**  **HỆ THỐNG PHÁT HIỆN XÂM NHẬP BẰNG AI**  NGÀNH: CÔNG NGHỆ THÔNG TIN  CHUYÊN NGÀNH: PHÁT TRIỂN ỨNG DỤNG IOT  **ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC**  **NGƯỜI HƯỚNG DẪN**  **TS. CHU BÁ THÀNH**  **HƯNG YÊN - 2025** |

**NHẬN XÉT**

**Nhận xét của giảng viên hướng dẫn:**

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

.......................................................................................................................................

**GIẢNG VIÊN HƯỚNG DẪN**

*(Ký và ghi rõ họ tên)*

**LỜI CAM ĐOAN**

Em xin cam đoan đồ án tốt nghiệp “Hệ Thống Phát Hiện Xâm Nhập Bằng AI” là công trình nghiên cứu của bản thân. Những phần sử dụng tài liệu tham khảo trong đồ án đã được nêu rõ trong phần tài liệu tham khảo. Các số liệu, kết quả trình bày trong đồ án là hoàn toàn trung thực, nếu sai em xin chịu hoàn toàn trách nhiệm và chịu mọi kỷ luật của bộ môn và nhà trường đề ra.

*Hưng Yên, ngày … tháng … năm…..*

Sinh viên

…………………………………..

MỤC LỤC

[MỤC LỤC 5](#_Toc65180319)

[DANH SÁCH CÁC THUẬT NGỮ 7](#_Toc65180320)

[DANH SÁCH BẢNG BIỂU 8](#_Toc65180321)

[DANH SÁCH HÌNH VẼ 9](#_Toc65180322)

[CHƯƠNG 1: MỞ ĐẦU 10](#_Toc65180323)

[1.1 Lý do chọn đồ án 10](#_Toc65180324)

[1.2 Mục tiêu của đồ án 10](#_Toc65180325)

[1.2.1 Mục tiêu tổng quát 10](#_Toc65180326)

[1.2.2 Mục tiêu cụ thể 10](#_Toc65180327)

[1.3 Giới hạn và phạm vi của đồ án 10](#_Toc65180328)

[1.3.1 Đối tượng nghiên cứu 10](#_Toc65180329)

[1.3.2 Phạm vi nghiên cứu 11](#_Toc65180330)

[1.4 Nội dung thực hiện 11](#_Toc65180331)

[1.5 Phương pháp tiếp cận 11](#_Toc65180332)

[CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 12](#_Toc65180333)

[2.1 Phương pháp phát triển phần mềm hướng đối tượng 12](#_Toc65180334)

[2.2 Công nghệ áp dụng 12](#_Toc65180335)

[CHƯƠNG 3: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 13](#_Toc65180336)

[3.1 Đặc tả yêu cầu phần mềm 13](#_Toc65180337)

[3.1.1 Các yêu cầu chức năng 13](#_Toc65180338)

[3.1.2 Biểu đồ lớp thực thể 13](#_Toc65180339)

[3.1.3 Các yêu cầu phi chức năng 13](#_Toc65180340)

[3.2 Thiết kế hệ thống 13](#_Toc65180341)

[3.2.1 Thiết kế kiến trúc 13](#_Toc65180342)

[3.2.2 Thiết kê cơ sở dữ liệu 13](#_Toc65180343)

[3.2.3 Thiết kế lớp đối tượng 14](#_Toc65180344)

[3.2.4 Thiết kế giao diện 14](#_Toc65180345)

[CHƯƠNG 4: TRIỂN KHAI WEBSITE 15](#_Toc65180346)

[4.1 Xây dựng Web API 15](#_Toc65180347)

[4.2 Xây dựng các chức năng 15](#_Toc65180348)

[4.2.1 Các chức năng nghiệp vụ phân hệ người dùng 15](#_Toc65180349)

[4.2.2 Các chức hệ thống 15](#_Toc65180350)

[4.3 Kiểm thử và triển khai ứng dụng 15](#_Toc65180351)

[KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 16](#_Toc65180352)

[Kết quả đạt được 16](#_Toc65180353)

[Hạn chế của đề tài 16](#_Toc65180354)

[Hướng phát triển của đề tài 16](#_Toc65180355)

[TÀI LIỆU THAM KHẢO 17](#_Toc65180356)

[PHỤ LỤC 18](#_Toc65180357)

DANH SÁCH CÁC THUẬT NGỮ

|  |  |  |
| --- | --- | --- |
| Từ viết tắt | Từ đầy đủ | Giải thích |
|  |  |  |
| ………… | ……………………………… | ………………………………… |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

DANH SÁCH BẢNG BIỂU

[Bảng 1‑1 Danh mục ví dụ phạm vi nghiên cứu 11](#_Toc65180383)

DANH SÁCH HÌNH VẼ

[Hình 3‑1 Hình ví dụ 1 13](file:///E:\Bo%20mon\Bieu%20mau%20do%20an%20mon%20hoc\Bieu%20mau%20do%20an%20tot%20nghiep\ISO-IT13-M09.Mau%20Cuon%20do%20an%20tot%20nghiep%20Web24-2-2021.docx#_Toc65180467)

# MỞ ĐẦU

1.1 Lý do chọn đồ án

* Trong bối cảnh cuộc cách mạng công nghiệp 4.0 đang diễn ra mạnh mẽ, các công nghệ tiên tiến như trí tuệ nhân tạo (AI), Internet vạn vật (IoT), và học máy (Machine Learning) ngày càng đóng vai trò quan trọng trong nhiều lĩnh vực của đời sống. Một trong những ứng dụng nổi bật là mô hình “nhà thông minh” – nơi mà các thiết bị điện tử, cảm biến và hệ thống điều khiển được kết nối với nhau nhằm mang lại sự tiện nghi, tiết kiệm năng lượng và nâng cao chất lượng sống cho con người.
* Tuy nhiên, cùng với sự phát triển đó, các vấn đề về an ninh và bảo mật trong môi trường nhà thông minh cũng ngày càng trở nên nghiêm trọng. Việc các thiết bị IoT ngày càng phổ biến đồng nghĩa với việc có thêm nhiều điểm yếu tiềm tàng mà kẻ tấn công có thể khai thác. Ngoài ra, nguy cơ xâm nhập vật lý vào nhà ở, từ trộm cắp đến hành vi xâm phạm quyền riêng tư, cũng đặt ra yêu cầu cần có một hệ thống giám sát và cảnh báo thông minh, linh hoạt, và đáng tin cậy hơn các phương pháp truyền thống.
* Trong bối cảnh đó, việc ứng dụng trí tuệ nhân tạo vào hệ thống phát hiện xâm nhập trong nhà thông minh là một hướng đi đầy tiềm năng. Không chỉ giúp hệ thống an ninh hoạt động hiệu quả và chủ động hơn, AI còn có khả năng tự học, nhận diện hành vi bất thường, và phản ứng nhanh chóng trong thời gian thực.
* Xuất phát từ thực tiễn và nhu cầu bảo mật ngày càng cao trong các hệ thống nhà thông minh, nhóm/Em đã chọn đề tài:
* “Xây dựng hệ thống phát hiện xâm nhập sử dụng trí tuệ nhân tạo trong môi trường nhà thông minh”
* nhằm nghiên cứu, xây dựng và đánh giá một mô hình có khả năng hỗ trợ phát hiện và cảnh báo xâm nhập một cách thông minh, hiệu quả và phù hợp với xu hướng công nghệ hiện đại.

1.2 Mục tiêu của đồ án

1.2.1 Mục tiêu tổng quát

Mục tiêu tổng quát của đề tài là nghiên cứu và xây dựng một hệ thống phát hiện xâm nhập ứng dụng trí tuệ nhân tạo trong môi trường nhà thông minh, nhằm nâng cao hiệu quả giám sát, phát hiện sớm các hành vi xâm nhập trái phép, từ đó tăng cường mức độ an toàn và bảo mật cho người dùng trong không gian sống hiện đại. Việc ứng dụng công nghệ hiện đại, đề tài góp phần hiện đại hóa quy trình canh tác, tiết kiệm tài nguyên nước, giảm sức lao động và nâng cao năng suất cây trồng, phù hợp với xu hướng phát triển nông nghiệp thông minh.

1.2.2 Mục tiêu cụ thể

Tìm hiểu và phân tích các nguyên lý hoạt động của hệ thống nhà thông minh và các nguy cơ xâm nhập phổ biến, cả về mặt vật lý và trên nền tảng mạng.

Nghiên cứu các phương pháp phát hiện xâm nhập sử dụng trí tuệ nhân tạo, bao gồm học máy (Machine Learning), học sâu (Deep Learning), và các kỹ thuật phát hiện bất thường (Anomaly Detection).

Thu thập và xử lý dữ liệu từ các thiết bị đầu vào như cảm biến chuyển động, camera, hoặc bộ dữ liệu mô phỏng, nhằm phục vụ việc huấn luyện và kiểm thử mô hình AI.

Xây dựng mô hình phát hiện xâm nhập có khả năng nhận diện các hành vi bất thường trong môi trường nhà thông minh với độ chính xác cao.

Đánh giá hiệu quả của hệ thống thông qua các tiêu chí như độ chính xác, độ nhạy, tỉ lệ cảnh báo sai, và khả năng hoạt động thời gian thực.

Đề xuất các hướng phát triển và mở rộng hệ thống trong tương lai, bao gồm khả năng tích hợp với nền tảng nhà thông minh thực tế.

1.3 Giới hạn và phạm vi của đồ án

1.3.1 Đối tượng nghiên cứu

Đối tượng nghiên cứu của đề tài là hệ thống phát hiện xâm nhập sử dụng trí tuệ nhân tạo (AI) trong môi trường nhà thông minh (Smart Home). Cụ thể, đề tài tập trung vào việc nghiên cứu các hành vi xâm nhập trái phép vào không gian sống, bao gồm cả xâm nhập vật lý như đột nhập, chuyển động bất thường, và xâm nhập mạng thông qua các thiết bị IoT. Bên cạnh đó, đề tài còn nghiên cứu các loại dữ liệu đầu vào từ cảm biến chuyển động, camera giám sát, cảm biến cửa hoặc dữ liệu mạng của các thiết bị thông minh trong nhà. Trên cơ sở đó, các mô hình trí tuệ nhân tạo như học máy (Machine Learning), học sâu (Deep Learning), và kỹ thuật phát hiện bất thường (Anomaly Detection) được ứng dụng để phân tích, nhận dạng và phát hiện các tình huống xâm nhập. Đồng thời, hệ thống cũng hướng đến khả năng phản hồi nhanh chóng như gửi cảnh báo đến người dùng hoặc kích hoạt các biện pháp an ninh tự động khi phát hiện sự cố.

1.3.2 Phạm vi nghiên cứu

<Phạm vi không gian: tại đâu?

Phạm vi thời gian: Số liệu thứ cấp thu thập trong thời gian nào? Sơ cấp?

Ý nghĩa khoa học và thực tiễn của đề tài>

Bảng ‑ Danh mục ví dụ phạm vi nghiên cứu

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiêu đề 1** | **Tiêu đề 2** | **Tiêu đề 3** | **Tiêu đề 4** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1.4 Nội dung thực hiện

* Tìm hiểu yêu cầu người dùng.
* Thiết kế hệ thống đóng gói hoàn chỉnh.
* Nghiên cứu các chức năng: Giám sát môi trường, điều khiển tưới tiêu, cảnh báo, thống kê, AI.

1.5 Phương pháp tiếp cận

* Áp dụng kiến thức đã học vào lập trình.
* Sử dụng các tài liệu liên quan đến hỗ trợ việc thiết kế và lập trình.
* Tham khảo ý kiến đóng góp của giảng viên hướng dẫn.

# TÊN CHƯƠNG 2

*(Đặt tên Chương 2 theo nội dung lý thuyết mà sinh viên đã thực hiện, nghiên cứu. Ví dụ: " Công nghệ ảo hóa máy phục vụ", “Tổng quan về tường lửa PFSen”,...)*

2.1. Tổng quan về công nghệ mạng dự kiến triển khai

Tên đề mục này mang tính tổng quan về công nghệ sẽ triển khai. Ví dụ:   
“2.1. *Công nghệ ảo hóa máy phục vụ*”.

Nội dung phần này trình bày đơn giản, ngắn gọn đầy đủ theo ý hiểu của mình sau khi đã sử dụng tài liệu tham khảo: ***Không copy nguyên bản từ 1 tài liệu nào đó****.*

Dưới đây là một số gợi ý về nội dung trình bày:

* Giới thiệu tổng quan, thật ngắn gọn về mạng máy tính, thiết bị mạng và các vấn đề liên quan.;
* Giới thiệu ngắn gọn về hệ điều hành mạng, một số dịch vụ mạng;
* Giới thiệu một số công nghệ mạng mới: công nghệ ảo hóa máy phục vụ, công nghệ mạng WAN, mạng WLAN, MANET, kiểm thử xâm nhập mạng, bảo mật mạng;
* Nhận định, đánh giá chung về tình hình triển khai/áp dụng của công nghệ mạng mà đề tài thực hiện (trên thế giới, Việt Nam, doanh nghiệp,…).

2.2. Giới thiệu về công nghệ mạng mà đề tài sẽ triển khai

Tên đề mục này thể hiện rõ công nghệ mạng sẽ triển khai trong đề tài. Ví dụ: “2.2. Công nghệ ảo hóa máy phục vụ với Vmware Esx Server”;

Nội dung phần này trình bày chi tiết, đầy đủ về công nghệ mạng sẽ triển khai cho doanh nghiệp. Trong đó lưu ý:

* Giới thiệu, phân tích chi tiết về công nghệ mạng mà đề tài sẽ triển khai: khái niệm, nguyên lý hoạt động, mô hình kiến trúc tổng thể;
* Trình bày mô hình triển khai công nghệ mạng mới;
* Các vấn đề liên quan khi triển khai công nghệ này.

Một số chủ đề/nội dung (nhưng không giới hạn) về công nghệ mạng mới triển khai:

* Công nghệ ảo hóa với Vmware esx server, HyperV, Container Docker;
* Firewall, TMG, Pfsense, Fortigate, Cisco ASA;
* Bảo mật thiết bị IoT;
* Zero Trust;
* Network automation, Aws cloud computing, Penetration test;
* Sharepoint, VPN;
* Mạng Wifi 6, 5G, MANET.

# CHƯƠNG 3: TÊN CHƯƠNG 3

*(Đặt tên Chương 3 theo yêu cầu triển khai của đề tài.   
Ví dụ: “Triển khai công nghệ ảo hóa máy phục vụ cho công ty ABC”)*

*“Triển khai công nghệ hệ thống tường lửa PFsense cho công ty ABC”), ...*

# 3.1. Khảo sát hệ thống

3.1.1 Tổng quan về đơn vị /doanh nghiệp

* Thông tin cơ bản về doanh nghiệp (Tên công ty, địa chỉ, lĩnh vực hoạt động, quá trình phát triển cơ bản);
* Cơ cấu tổ chức của công ty (Các phòng /ban);
* Các phòng / ban và nhiệm vụ tương ứng (Trình bày ngắn gọn).

3.1.2 Khảo sát yêu cầu của doanh nghiệp

Sử dụng các câu hỏi, phương pháp phù hợp để thu thập những thông tin sau:

* Hiện trạng hệ thống mạng hiện tại đang có: Danh sách các thiết bị và cấu hình hiện tại, danh sách phần mềm, ứng dụng sử dụng, các dịch vụ mạng đang triển khai;
* Các yêu cầu tường minh của khách hàng đối với hệ thống khi triển khai công nghệ mạng mới mà đề tài đăng ký thực hiện:
  + Đối với người dùng bình thường: Khảo sát các phòng/ban về yêu cầu sử dụng hệ thống mạng như: Phần mềm sử dụng, các ứng dụng chuyên biệt, các yêu cầu khác đối với hệ thống (sử dụng Internet, bảo mật dữ liệu cá nhân);
  + Đối với người quản lý: Các nhu cầu về quản lý người dùng sử dụng hệ thống, yêu cầu kiểm soát việc truy cập Internet của người dùng;
  + Các yêu cầu của doanh nghiệp để dẫn tới sự cần thiết phải triển khai công nghệ đang tìm hiểu;
* Các yêu cầu không tường minh đối với hệ thống và công nghệ mạng mới:
* Chi phí cho dự án: Có thể đề cập luôn hoặc đề cập sau khi lên báo giá;
* Các công nghệ mạng phổ biến hiện nay: hiện nay các công nghệ nào đang phổ biến, các thiết bị/ hãng sản xuất nào được đánh giá cao;
* Tính sẵn sàng của hệ thống: hệ thống cần phải đáp ứng được nhu cầu sử dụng của người dùng như thế nào? (Đối với việc sử dụng bình thường, sử dụng các dịch vụ bên trong của công ty, các dịch vụ/kết nối Internet);
* Tính bảo mật của hệ thống: tính an toàn với dữ liệu người dùng, khả năng ngăn chặn và cảnh báo đối với các nguy cơ tấn công mạng, phần mềm mã độc;
* Nhu cầu mở rộng của hệ thống: Hệ thống sẽ đáp ứng được nhu cầu mở rộng trong thời gian là bao lâu với số lượng mở rộng như thế nào.

3.2. Phân tích yêu cầu và thiết kế giải pháp

* Phân tích yêu cầu của doanh nghiệp, của hệ thống mạng cần triển khai để xác định được những yêu cầu mà hệ thống cần phải đáp ứng hay các thiết lập của công nghệ sẽ triển khai;
* Thiết kế giải pháp triển khai cho hệ thống;
* Danh mục các thiết bị (nếu cần bổ sung – xem bảng dưới).

*Bảng 3.2:**Danh mục phần cứng của hệ thống mạng*

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên sản phẩm** | **Số lượng** | **Thông số kỹ thuật yêu cầu** |
| 1 | Switch Access | 02 | * 8 port 10/100/1000 Mbps * Support VLAN |
|  | … | … | … |

3.3. Triển khai, cài đặt và cấu hình hệ thống

3.3.1. Triển khai lắp đặt hệ thống phần cứng

- Mô tả các bước triển khai lắp đặt;

- Dựng video quá trình lắp đặt.

3.3.2. Cài đặt hệ điều hành /phần mềm mô phỏng

- Mô tả các bước cài đặt;

- Dựng video quá trình cài đặt hệ điều hành.

3.3.3. Cài đặt và cấu hình dịch vụ/công nghệ mạng mới

- Mô tả các bước cài đặt và cấu hình;

- Dựng video quá trình cài đặt và cấu hình dịch vụ.

3.4. Vận hành và xử lý sự cố hệ thống

* Vận hành hệ thống;
* Kiểm tra lại hoạt động của hệ thống xem đã phù hợp với các yêu cầu ở phần phân tích, hay khảo sát chưa;
* Phân tích, đánh giá một số sự cố có thể phát sinh và hướng xử lý sự cố.

# KẾT LUẬN

*(Tối thiểu một trang)*

Kết quả đạt được của đề tài

Trình bày các kết quả đạt được về lý thuyết và thực nghiệm (lưu ý trình bày ngắn gọn nhưng đủ ý, tránh viết lan man, chung chung).

Hạn chế của đề tài

Trình bày các mặt hạn chế của đề tài.

Hướng phát triển của đề tài

- Trình bày hướng phát triển tiếp theo của đề tài, khắc phục các hạn chế.

TÀI LIỆU THAM KHẢO

x

|  |  |
| --- | --- |
| [1] | Tên tác giả (năm XB), Tên sách, NXB, Nơi XB |
| [2] | ……….. |

PHỤ LỤC

1. <Tiêu đề phụ lục 1 (nếu có) >
2. <Tiêu đề phụ lục 1 (nếu có) >

…..