HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA VIỄN THÔNG I

ĐỒ ÁN
TỐT NGHIỆP ĐẠI HỌC

***Đề tài*:**

NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN ĐA TẤN CÔNG CHO HỆ THỐNG PHÁT HIỆN XÂM NHẬP TRONG MẠNG IOT SỬ DỤNG LOGIC MỜ

Giảng viên hướng dẫn	**:**	**TS. HOÀNG TRỌNG MINH**
Sinh viên thực hiện	**:**	**TRẦN NHẬT HOÀNG**
Lớp	**:**	**D18CQVT02-B**
Khoá	**:**	**2018-2023**
Hệ	**:**	**ĐH CHÍNH QUY**

Hà Nội, tháng 12 /2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA VIỄN THÔNG I

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

***Đề tài*:**

NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN ĐA TẤN CÔNG CHO HỆ THỐNG PHÁT HIỆN XÂM NHẬP TRONG MẠNG IOT SỬ DỤNG LOGIC MỜ

Giảng viên hướng dẫn	**:**	**TS. HOÀNG TRỌNG MINH**
Sinh viên thực hiện	**:**	**TRẦN NHẬT HOÀNG**
Lớp	**:**	**D18CQVT02-B**
Khoá	**:**	**2018-2023**
Hệ	**:**	**ĐH CHÍNH QUY**

Hà Nội, tháng 12 /202

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Điểm: …. (Bằng chữ:…….)

Ngày … tháng … năm 2022

Giảng viên hướng dẫn

NHẬN XÉT CỦA GIẢNG VIÊN PHẢN BIỆN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Điểm: … (Bằng chữ…….)

Ngày … tháng … năm 2022

Giảng viên phản biện

LỜI NÓI ĐẦU

Thế giới đang bước vào thời đại của Internet vạn vật (IoT). Các sản phẩm tiêu dùng, hàng hóa lâu bền, ô tô và xe tải, linh kiện công nghiệp và tiện ích, cảm biến và các vật dụng hàng ngày khác đang được kết hợp với kết nối Internet và khả năng phân tích dữ liệu mạnh mẽ, hứa hẹn sẽ thay đổi cách chúng ta làm việc, sống và giải trí. Các dự báo về tác động của IoT đối với Internet và nền kinh tế là rất ấn tượng, với một số dự đoán có tới 100 tỷ thiết bị IoT sẽ được kết nối vào năm 2025. Tuy nhiên, do tính động và tính không đồng nhất, các mạng IoT phải đối mặt với rất nhiều các cuộc tấn công an ninh mạng. Do đó, việc bảo vệ mạng IoT khỏi các cuộc tấn công là một nhiệm vụ cấp thiết hiện nay. Một trong các giải pháp phổ biến được sử dụng đó là hệ thống phát hiện xâm nhập (IDS).

Một IDS có khả năng giám sát các hoạt động mạng giữa các thiết bị được kết nối và tạo ra cảnh báo ngay khi nào phát hiện thấy bất kỳ vi phạm nào. Tuy nhiên, việc phát triển IDS cho mạng IoT vẫn là một nhiệm vụ đầy thách thức do các đặc điểm của mạng IoT như khả năng xử lý và lưu trữ hạn chế. Rất nhiều các kỹ thuật đã được sử dụng với mục đích phát triển IDS cho mạng Iot như học máy, học sâu, logic mờ. Trong các kỹ thuật đó, Logic Mờ (Fuzzy Logic) được đánh giá là một kỹ thuật đơn giản và hiệu quả, rất phù hợp với các yêu cầu của mạng IoT. Trong đồ án này, em sẽ trình bày mô hình giải pháp sử dụng Logic Mờ cho IDS để phát hiện đa tấn công trong hệ thống IoT. Mô hình sẽ được mô phỏng trên Matlab và đánh giá độ chính xác bằng tập dữ liệu IoT-23.

Bố cục của đồ án bao gồm 3 chương:

Chương 1: Tổng quan về hệ thống IoT

Chương 2: Các giải pháp hiện tại cho hệ thống phát hiện xâm nhập IDS

Chương 3: Giải pháp sử dụng logic mờ cho hệ thống phát hiện xâm nhập IDS

Bằng sự cố gắng và nỗ lực em đã hoàn thành xong đồ án tốt nghiệp của mình. Do có sự hạn chế về mặt thời gian và mức độ hiểu biết của bản thân nên không thể tránh khỏi những thiếu sót trong quá trình nghiên cứu. Vì thế, em rất mong nhận được những lời góp ý và sự chỉ bảo thêm của các thầy cô và các bạn để em có thêm những kiến thức phục vụ cho học tập cũng như công việc sau này.

LỜI CẢM ƠN

Kết quả của đồ án tốt nghiệp đại học là quá trình tích lũy kiến thức sau hơn 4 năm học tại Học Viện Công Nghệ Bưu Chính Viễn Thông. Để có được những kiến thức quý giá thì em xin gửi lời cảm ơn chân thành và sâu sắc nhất tới tất cả các thầy cô giáo, các cán bộ giảng viên đã và đang dạy tại trường Học viện Công nghệ Bưu chính Viễn Thông, đặc biệt là các thầy, các cô trong khoa Viễn Thông 1, cảm ơn tất cả các thầy cô trong những năm qua đã dìu dắt, dạy dỗ để em có được ngày báo cáo tốt nghiệp hôm nay.

Em cũng xin được gửi lời cảm ơn chân thành và sâu sắc tới Thầy giáo, ***TS. Hoàng Trọng Minh*** – giảng viên trực tiếp hướng dẫn em hoàn thành đồ án tốt nghiệp. Thầy rất nhiệt tình và chỉ bảo em một cách tỉ mỉ cẩn thận.

Xin được cám ơn gia đình, bạn bè đã thường xuyên quan tâm, giúp đỡ, chia sẻ kinh nghiệm, trong thời gian học tập, nghiên cứu cũng như trong suốt quá trình em thực hiện làm đồ án tốt nghiệp.

Hà Nội, ngày 16 tháng 10 năm 2022

Sinh viên thực hiện

Trần Nhật Hoàng

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

THUẬT NGỮ VIẾT TẮT

6LoWPAN	IETF Low Power Wireless Personal Area Networks	Mạng khu vực cá nhân không dây công suất thấp IETF
AES	Advance Encryption Standard	Chuẩn mã hóa nâng cao
AHNs	Ad Hoc Networks	Mạng Ad-hoc
ANN	Artificial Neural Network	Mạng nơ-ron nhân tạo
ANSI	The American National Standards Institute	Viện tiêu chuẩn quốc gia Mỹ
APIs	Application Programming Interfaces	Giao diện ứng dụng
CEN/CENELEC	European Committee For Electro-Technical Standardization	Ủy ban châu Âu về tiêu chuẩn hóa kỹ thuật điện
CESI	China Electronics Standardization Institute	Viện tiêu chuẩn hóa điện tử Trung Quốc
CNN	Convolutional Neural Network	Mạng nơ-ron tích chập
CoAP	The Constrained Application Protocol	Giao thức ứng dụng bị hạn chế
CPS	Cyber-Physical Systems	Hệ thống vật lý mạng
DAG	Directed Acyclic Graph	Đồ thị tuần hoàn có hướng
DDoS	Distributed DoS	Tấn công từ chối dịch vụ phân tán
DIO	Information Object	Đối tượng thông tin
DoS	Denial Of Service	Tấn công từ chối dịch vụ
ECC	Elliptic Curve Cryptography	Mã hóa đường cong elip
EPCglobal	Electronic Product Code Global	Mã sản phẩm điện tử toàn cầu
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
FCNN	Fully Connected Neural Networks	Mạng nơ-ron kết nối đầy đủ
FIS	Fuzzy Inference System	Hệ thống suy luận mờ
GA	Genetic Algorithm	Thuật toán di truyền
GLN	Global Location Number	Mã vị trí toàn cầu
GTIN	Global Trade Identification Number	Mã nhận dạng thương mại toàn cầu
HIoT	Health Internet Of Things	IoT cho chăm sóc sức khỏe
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IEC	International Electro-Technical Commision	Ủy ban kỹ thuật điện quốc tế
IFP	Interface Profile	Hồ sơ giao diện
IoT	Internet Of Things	Vạn vật kết nối Internet
ISO	International Organization For Standardization	Tổ chức Quốc tế về Tiêu chuẩn hóa
ITU	International Telecommunication Union	Liên minh Viễn thông Quốc tế
M2M	Machine To Machine	Thiết bị đến thiết bị

MEMS	Micro-Lectronic-Mechanical System	Hệ thống vi điện tử-cơ khí
ONS	Global Object Naming Service	Dịch vụ đặt tên đối tượng toàn cầu
OSGi	Open Services Gateway Initiative	Sáng kiến Cổng Dịch vụ Mở
QoS	Quality of Service	Chất lượng dịch vụ
RBF	Radial Basis Function	Chức năng trung tâm chính
REST	Representation State Transfer	Chuyển giao trạng thái đại diện
RFID	Radio Frequency Identification	Nhận dạng tần số vô tuyến điện
RNN	Recurrent Neural Network	Mạng nơ-ron hồi quy
RPL	Routing Protocol For Low-Power And Lossy Networks	Giao thức định tuyến cho các mạng có tổn thất và công suất thấp
SIA	SOCRADES Integration Architecture	Kiến trúc tích hợp SOCRADES
SIoT	Social Iot	Mạng xã hội IoT
SoA	Service-Oriented Architecture	Kiến trúc hướng dịch vụ
SPP	Service Provisioning Process	Quy trình cung cấp dịch vụ
SSCC	Serial Shipping Container Code	Mã công-te-nơ vận chuyển nối tiếp
SVM	Support Vector Machines	Thuật toán ML
TEA	Tiny Encryption Algorithm	Thuật toán mã hóa nhỏ
TLBO	Teaching-learning-based optimization	Thuật toán tối ưu dựa trên dạy và học
UHF	Ultra High Frequency	Siêu cao tần
UUID	Universal Unique Identifier	Mã định danh duy nhất toàn cầu
VE	Virtual Entity	Thực thể ảo
WBSNs	Wearable Body Sensor Networks	Mạng cảm biến cơ thể đeo được
WLAN	wireless local area network	Mạng lưới không dây khu vực địa phương
WMNs	Wireless Mesh Networks	Mạng lưới không dây
WSC	World Standards Cooperation	Hợp tác tiêu chuẩn thế giới
WSDL	Web Services Description Language	Ngôn ngữ mô tả dịch vụ web
WSN	Wireless Sensor Network	Mạng cảm biến không dây

CHƯƠNG 1: TỔNG QUAN VỀ HỆ THỐNG IOT

1.1. Giới thiệu về hệ thống IoT

1.1.1. Khái niệm về mạng IoT

Internet of Things (IoT) đang trở thành một bước tiến cách mạng trong thế giới hiện đại và là một cột mốc quan trọng đạt được trong lĩnh vực công nghệ thông tin và truyền thông. Với IoT chúng ta có thể điều khiển từ xa hầu hết mọi thiết bị điện xung quanh chúng ta. IoT là một công nghệ tuyệt trong cuộc sống của chúng ta, đánh giá từ cách chúng ta phản ứng với hành vi của bản thân trong cuộc sống hàng ngày. Từ các thiết bị điện gia dụng (như tủ lạnh AC) và các thiết bị điều khiển từ xa (như TV) đến các phương tiện cung cấp tuyến đường ngắn nhất và an toàn nhất cho chúng ta. Tất cả đều có thể được kiểm soát bằng cách sử dụng điện thoại thông minh bao gồm cả đồng hồ thông minh của chúng ta.

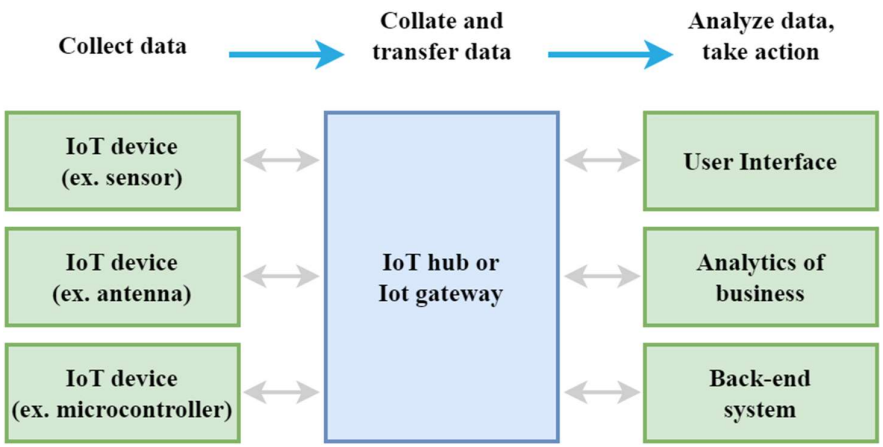
IoT là một mạng lớn bao gồm các thiết bị được kết nối với nó như được cho trong Hình 1.1. Các thiết bị được kết nối thu thập dữ liệu và chia sẻ cách chúng đang được vận hành và thực hiện các nhiệm vụ được giao. Tất cả là nhờ cảm biến. Chúng được nhúng vào điện thoại di động của chúng ta và nhiều thiết bị điện khác và các thiết bị dựa trên tín hiệu sẽ được kết nối với mạng IoT.

Hình 1.1. Các thiết bị được kết nối với mạng IoT

Hệ sinh thái IoT liên quan đến các thiết bị thông minh hỗ trợ web sử dụng các hệ thống tích hợp, chẳng hạn như bộ xử lý, cảm biến và phần cứng truyền thông, để lắp ráp,

gửi và hoạt động trên dữ liệu mà chúng thu được. Các thiết bị IoT chia sẻ dữ liệu cảm biến mà chúng thu thập bằng cách truyền tải đến máy chủ lưu trữ IoT hoặc thiết bị biên khác nơi dữ liệu được gửi đến đám mây để phân tích hoặc phân tích tại chỗ. Sau đó, các thiết bị này giao tiếp với các thiết bị được kết nối khác và hoạt động dựa trên thông tin mà chúng thu được từ nhau. Các thiết bị thực hiện hầu hết công việc mà không có sự can thiệp của con người, mặc dù mọi người có thể tương tác với các thiết bị, chẳng hạn, để cấu hình, hướng dẫn hoặc truy cập dữ liệu. Các giao thức kết nối, giao thức mạng và các giao thức thông tin được sử dụng với các thiết bị hỗ trợ web này phụ thuộc nhiều vào các ứng dụng IoT (internet vạn vật) cụ thể được triển khai. IoT là một hệ thống có thể sử dụng học máy, hay còn được gọi là trí tuệ nhân tạo có thể giúp tạo ra các quy trình dữ liệu thuận tiện hơn và năng động hơn nhiều.

IoT bao gồm các hệ thống được kết nối, cảm biến, ăng ten ô tô, và nhiều hơn nữa. Vì IoT tạo ra và phân tích một lượng lớn dữ liệu, nó là một động cơ chính của các dự án phân tích dữ liệu lớn. Đặc biệt, nó có thể tạo ra một lượng lớn dữ liệu trong thời gian thực. Thông qua các thiết bị IoT khác nhau, có thể theo dõi được hiệu suất của tất cả nhân viên, cũng như các hoạt động nâng cao ở tất cả các địa điểm. Ví dụ về thu thập dữ liệu IoT để xử lý dữ liệu được đưa ra trong Hình 1.2.



Hình 1.2. Sự kết nối dữ liệu IoT và xử lý dữ liệu

1.1.2. Những tiêu chuẩn trong mạng IoT

Có ý kiến cho rằng việc thiếu các tiêu chuẩn có thể làm giảm khả năng cạnh tranh của các sản phẩm IoT. Trong thập kỷ qua, một số tiêu chuẩn kỹ thuật đã được phát triển bởi các tổ chức khác nhau; các tiêu chuẩn này ngày càng đóng vai trò quan trọng hơn đối

với sự thành công của IoT. Đặc biệt, các tiêu chuẩn về phần mềm trung gian và giao diện là vô cùng quan trọng. Các nỗ lực nghiên cứu bao gồm: (1) thiết kế các chính sách và kiến trúc phân tán; (2) đảm bảo quyền riêng tư và bảo vệ người dùng; (3) nhận ra độ tin cậy, khả năng chấp nhận và bảo mật của mạng; (4) phát triển các tiêu chuẩn; (5) khám phá các công nghệ cho phép mới như các thiết bị hệ thống cơ điện tử vi mô (MEMS) và bản địa hóa phổ biến.

Các tiêu chuẩn về IoT đã thu hút rất nhiều sự quan tâm ở nhiều quốc gia. Trên bình diện quốc tế ITU, Electronic Mã sản phẩm toàn cầu (EPCglobal), Ủy ban kỹ thuật điện quốc tế (IEC), Tổ chức tiêu chuẩn hóa quốc tế (ISO) và IEEE đã cung cấp một bộ tiêu chuẩn để xác định, thu thập và chia sẻ dữ liệu bằng cách sử dụng công nghệ RFID. Trong khu vực, Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI) và Ủy ban Tiêu chuẩn Kỹ thuật Điện tử Châu Âu (CEN / CENELEC) đã phát hành một bộ tiêu chuẩn về các công nghệ cơ bản trong IoT, chẳng hạn như RFID, WSN, v.v. Viện Tiêu chuẩn Quốc gia Hoa Kỳ (ANSI) ở Hoa Kỳ đang nghiên cứu các tiêu chuẩn quản lý của IoT. Nghiên cứu về IoT ở Hoa Kỳ đã trở thành một ưu tiên nghiên cứu quốc gia; IoT dự kiến sẽ được áp dụng trong quân sự, hậu cần, tự động hóa công nghiệp, ngành bán lẻ, sân bay, trung tâm giao thông công cộng và bệnh viện. Tại Nhật Bản, "uID" được phát triển như một cơ sở hạ tầng để kết nối các nghiên cứu cơ bản với nghiên cứu ứng dụng và phát triển. Hiệp hội Tiêu chuẩn Truyền thông Trung Quốc và Viện Tiêu chuẩn hóa Điện tử Trung Quốc (CESI) đang nghiên cứu các tiêu chuẩn của RFID bán thụ động và RFID băng tần siêu cao (UHF). 973 Dự án đã được phát triển ở Trung Quốc dựa trên tiêu chuẩn hóa và các kỹ thuật cơ bản của IoT. Bảng 1.1 tóm tắt các tiêu chuẩn liên quan đến IoT.

Công nghệ	**Tiêu chuẩn**
Truyền thông	IEEE 802.15.4(ZigBee)
	IEEE 802.11 (WLAN)
	IEEE 802.15.1(Bluetooth, Low energy Bluetooth)
	IEEE 802.15.6 (Wireless Body Area Networks)
	IEEE 1888
	IPv6
	3G/4G

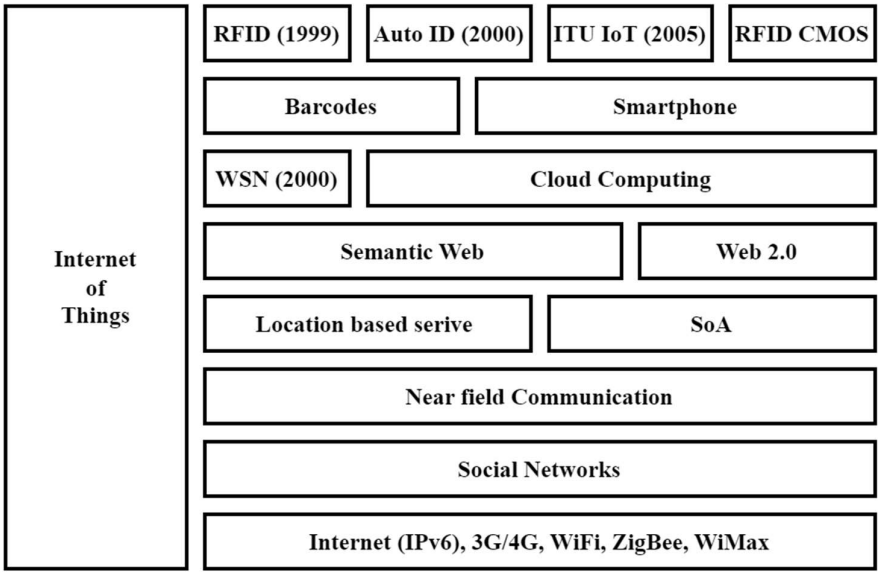
	UWB
RFID	RFID tag ISO 11784
	RFID air interface Protocol: ISO 11785
	RFID payment system and contactless smart card: ISO 14443/15693
	Mobile RFID: , ISO/IEC 18092 ISO/IEC 29143
	ISO 18000-1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies
	ISO 18000-2 – for frequencies below 135 kHz
	ISO 18000-3 – for 13.56 MHz
	ISO 18000-4 – for 2.45 GHz
	ISO 18000-6 – for 860 to 960 MHz
	ISO 18000-7 – for 433 MHz
Mã hóa và nội dung dữ liệu	EPC Global Electronic Product Code, or EPCTM
	EPC Global Physical Mark Up Language
	EPC Global Object Naming Service (ONS)
Mã sản phẩm điện tử	Auto-ID: Global Trade Identification Number (GTIN), Serial Shipping Container Code (SSCC), and the Global Location Number (GLN)
Cảm biến	ISO/IEC JTC1 SC31 and ISO/IEC
	JTC1 WG7
	Sensor Interfaces: IEEE 1451.x, IEC SC 17B, EPC global, ISO TC 211, ISO TC 205
Quản lý mạng	ZigBee Alliance, IETF SNMP WG, ITU-T SG 2, ITU-T SG 16, IEEE 1588
Trung gian	ISO TC 205, ITU-T SG 16
QoS	ITU-T, IETF

Bảng 1.1. Tóm tắt các tiêu chuẩn trong IoT

Tiêu chuẩn hóa IoT tính đến hiệu quả và tính khả dụng của các thông số kỹ thuật. Trong khi nhiều tổ chức đang làm việc trên các tiêu chuẩn cơ bản cho IoT, sự hợp tác toàn

cầu giữa các cơ quan tiêu chuẩn là cần thiết để đối phó với sự thiếu nhất quán giữa các cơ quan tiêu chuẩn và các tiêu chuẩn; Tổ chức Hợp tác Tiêu chuẩn Thế giới (WSC) phải có thể quản lý các mối quan hệ giữa các cơ quan tiêu chuẩn quốc tế và các cơ quan tiêu chuẩn khu vực.

Bên cạnh đó, cần nhấn mạnh tầm quan trọng của các tiêu chuẩn đối với sự phát triển công nghệ của IoT. Một mặt, các tiêu chuẩn giúp các nhà phát triển và người dùng xác định các giao thức kỹ thuật tốt nhất cho các ứng dụng và dịch vụ động trong IoT. Mặt khác, việc tiêu chuẩn hóa các công nghệ trong IoT là quan trọng và cấp bách, có thể và sẽ đẩy nhanh sự lan rộng của công nghệ IoT. Hình 1.3 tóm tắt các công nghệ cho phép IoT.



Hình 1.3. Tóm tắt các công nghệ cho phép trong IoT

1.2. Kiến trúc hướng dịch vụ của mạng IoT

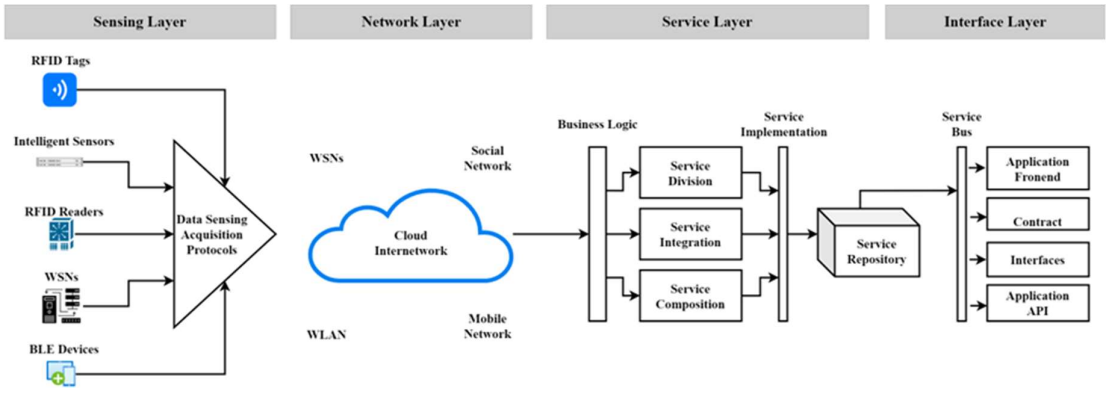
Yêu cầu quan trọng của IoT là các thiết bị trong mạng phải được kết nối với nhau. Kiến trúc hệ thống IoT phải đảm bảo các hoạt động của IoT, giúp thu hẹp khoảng cách giữa thế giới vật lý và thế giới ảo. Thiết kế kiến trúc IoT liên quan đến nhiều yếu tố như mạng, truyền thông, mô hình và quy trình kinh doanh và bảo mật. Khi thiết kế kiến trúc của IoT, khả năng mở rộng và khả năng tương tác giữa các thiết bị không đồng nhất và mô hình kinh doanh của chúng cần được xem xét. Do thực tế là mọi thứ có thể di chuyển theo địa lý và cần tương tác với những người khác trong chế độ thời gian thực, kiến trúc IoT phải thích ứng để làm cho các thiết bị tương tác với những thiết bị khác một cách linh hoạt

và hỗ trợ giao tiếp rõ ràng các sự kiện. Ngoài ra, IoT nên có bản chất phi tập trung và không đồng nhất.

Trong IoT, kiến trúc hướng dịch vụ (SoA) có thể là bắt buộc đối với các nhà cung cấp dịch vụ và người dùng. SoA đảm bảo khả năng tương tác giữa các thiết bị không đồng nhất theo nhiều cách. Hình 1.2 cung cấp một SoA tổng quát, bao gồm bốn lớp với các chức năng phân biệt như sau:

- **Lớp cảm biến** được tích hợp với các đối tượng phần cứng có sẵn để cảm nhận trạng thái của môi trường xung quanh;
- **Lớp mạng** là cơ sở hạ tầng để hỗ trợ qua các kết nối không dây hoặc có dây giữa các thiết bị;
- **Lớp dịch vụ** là tạo và quản lý các dịch vụ theo yêu cầu của người dùng hoặc ứng dụng;
- **Lớp giao diện** bao gồm các phương thức tương tác với người dùng hoặc ứng dụng.

SoA coi một hệ thống phức tạp như một tập hợp các đối tượng đơn giản hoặc hệ thống con được xác định rõ ràng. Các đối tượng hoặc hệ thống con đó có thể được tái sử dụng và duy trì riêng lẻ; do đó, các thành phần phần mềm và phần cứng trong IoT có thể được tái sử dụng và nâng cấp một cách hiệu quả. Do những ưu điểm này, SoA đã được ứng dụng rộng rãi như một kiến trúc chủ đạo cho mạng cảm biến không dây. Khi SoA được áp dụng trong IoT, nó được thiết kế để cung cấp khả năng mở rộng, tính mô-đun và khả năng tương tác giữa những đối tượng không đồng nhất. Ngoài ra, các chức năng và khả năng được trừu tượng hóa thành một tập hợp dịch vụ chung. Hình 1.4 cung cấp một ví dụ về SoA được đề xuất cho IoT và chi tiết về các thành phần của nó được thảo luận bên dưới.



Hình 1.4. Kiến trúc hướng dịch vụ của IoT

1.2.1. Lớp cảm biến

IoT được kỳ vọng là một mạng kết nối các thiết bị vật lý trên toàn thế giới, trong đó mọi thứ được kết nối liền mạch và có thể được điều khiển từ xa. Trong lớp cảm biến, các hệ thống thông minh trên thẻ hoặc cảm biến có thể tự động cảm nhận môi trường và trao đổi dữ liệu giữa các thiết bị.

Trong vài năm qua, công nghệ cảm biến và giao tiếp tiên tiến đã làm cho mọi thứ với RFID hoặc cảm biến trở nên linh hoạt và dễ tiếp cận hơn, điều này mở rộng đáng kể khả năng của IoT theo nghĩa mọi thứ có thể được nhận dạng duy nhất và môi trường xung quanh có thể được giám sát cho các mục đích và ứng dụng khác nhau. Mọi đối tượng trong IoT đều có danh tính kỹ thuật số và có thể dễ dàng theo dõi trong miền kỹ thuật số. Kỹ thuật gán danh tính duy nhất cho một đối tượng được gọi là định danh duy nhất phổ quát (UUID). Đặc biệt, UUID rất quan trọng để triển khai thành công các dịch vụ trong một mạng lưới khổng lồ như IoT. Các số nhận dạng có thể đề cập đến tên và địa chỉ.

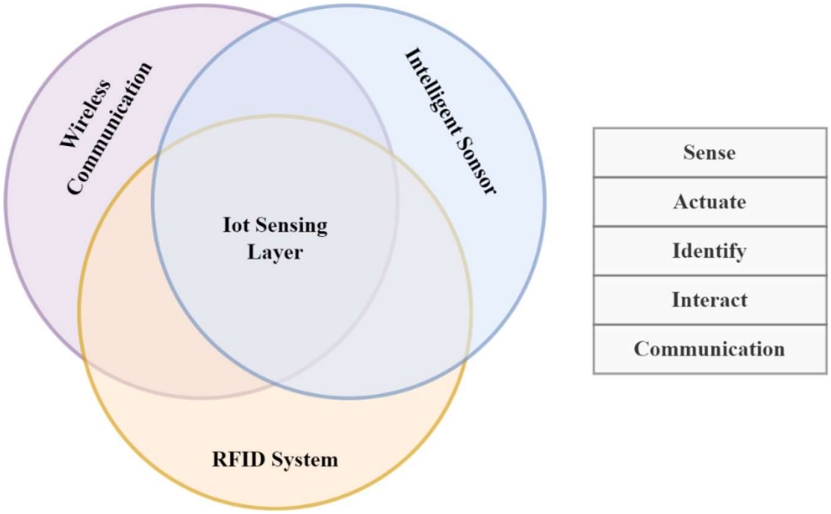
Khi xác định lớp cảm biến của IoT, cần xem xét các khía cạnh sau:

- **Chi phí, kích thước, tài nguyên và tiêu thụ năng lượng**: Những thứ có thể được trang bị các thiết bị cảm biến như thẻ RFID, nút cảm biến. Do có một số lượng lớn các cảm biến trong các ứng dụng hệ thống phức tạp, các thiết bị thông minh nên được thiết kế để giảm thiểu tài nguyên cần thiết cũng như chi phí.
- **Triển khai**: Những thứ cảm biến (thẻ RFID, cảm biến, v.v.) có thể được triển khai một lần, hoặc tăng dần, hoặc ngẫu nhiên tùy thuộc vào yêu cầu của ứng dụng.
- **Tính không đồng nhất**: Sự đa dạng của những đối tượng có các thuộc tính khác nhau có thể làm cho IoT trở nên rất không đồng nhất.
- **Liên lạc**: Cảm biến phải có thể truyền được để làm cho mọi thứ có thể truy cập và lấy được.
- **Mạng**: Những đối tượng có thể được tổ chức dưới dạng mạng multi-hop, mesh hoặc ad hoc.

Khi quy mô của IoT tăng lên, một số lượng lớn các thành phần phần cứng và phần mềm có thể được tham gia; do đó, IoT cũng nên bổ xung các tính năng sau:

- **Hiệu suất năng lượng**: Các cảm biến phải hoạt động mọi lúc để thu thập dữ liệu thời gian thực. Điều này mang lại thách thức trong việc cung cấp năng lượng cho các cảm biến; hiệu suất năng lượng cao cho phép các cảm biến hoạt động trong thời gian dài hơn mà không bị gián đoạn dịch vụ.
- **Giao thức:** Những thứ khác nhau hiện có trong IoT cung cấp nhiều chức năng của hệ thống. IoT phải hỗ trợ sự cùng tồn tại của các giao tiếp khác nhau như WLAN, ZigBee và Bluetooth.

Từ quan điểm của thiết kế phần cứng, các vấn đề chính của thiết kế phần cứng là hệ thống nhận dạng không dây, thẻ chi phí cực thấp và cảm biến di động thông minh (Hình 1.5).



Hình 1.5. Chức năng của lớp cảm biến trong IoT

1.2.2. Lớp mạng

Lớp mạng trong IoT, kết nối tất cả mọi thứ và cho phép chúng nhận thức được môi trường xung quanh. Thông qua lớp mạng, mọi thứ có thể chia sẻ dữ liệu với những thiết bị được kết nối, điều này rất quan trọng đối với việc quản lý và xử lý sự kiện thông minh trong IoT. Hơn nữa, lớp mạng có khả năng tổng hợp dữ liệu từ các cơ sở hạ tầng CNTT hiện có; dữ liệu sau đó có thể được truyền tới các đơn vị ra quyết định đối với các dịch vụ phức hợp cấp cao. Trong một SoA, các dịch vụ luôn được thực hiện bởi những thiết bị được triển khai trong một mạng không đồng nhất. Những thiết bị liên quan cũng có thể được tích hợp thông qua dịch vụ Internet. Giao tiếp trong mạng có thể liên quan đến Chất

lượng Dịch vụ (QoS) để đảm bảo các dịch vụ đáng tin cậy cho những người dùng hoặc ứng dụng khác nhau.

Mặt khác, điều cần thiết là mạng phải tự động khám phá và lập bản đồ mọi thực thể trong mạng. Mọi thiết bị cần được gán vai trò tự động để triển khai, quản lý và lập lịch trình cho các hành vi của mọi thiết bị và có thể chuyển sang bất kỳ vai trò nào bất kỳ lúc nào theo yêu cầu. Điều này cho phép các thiết bị thực hiện các tác vụ một cách cộng tác. Trong lớp mạng, các vấn đề sau cần được giải quyết:

- Công nghệ quản lý mạng bao gồm quản lý mạng cố định, không dây, di động
- Hiệu quả năng lượng mạng
- Yêu cầu của QoS
- Công nghệ khai thác và tìm kiếm
- Xử lý dữ liệu và tín hiệu
- An ninh và sự riêng tư

Trong số các vấn đề này, bảo mật thông tin và bảo mật quyền riêng tư của con người là rất quan trọng vì khả năng triển khai, tính di động và tính phức tạp của nó. Để bảo mật thông tin, công nghệ mã hóa hiện có được sử dụng trong WSN có thể được mở rộng và triển khai trong IoT. Tuy nhiên, nó có thể làm tăng độ phức tạp của IoT. Các công nghệ an ninh mạng hiện có có thể cung cấp cơ sở cho quyền riêng tư và bảo mật trong IoT, nhưng vẫn cần phải làm nhiều việc hơn.

1.2.3. Lớp dịch vụ

Lớp dịch vụ dựa trên công nghệ phần mềm trung gian, là nhân tố chính của các dịch vụ và ứng dụng trong IoT. Công nghệ phần mềm trung gian cung cấp một nền tảng hiệu quả về chi phí, nơi các nền tảng phần cứng và phần mềm có thể được sử dụng lại.

Lớp dịch vụ liên quan đến các hoạt động được yêu cầu bởi các đặc tả dịch vụ trung gian. Các dịch vụ trong lớp dịch vụ chạy trực tiếp trên mạng để định vị hiệu quả các dịch vụ mới cho một ứng dụng và truy xuất siêu dữ liệu động về các dịch vụ. Hầu hết các thông số kỹ thuật được thực hiện bởi các tiêu chuẩn khác nhau do các tổ chức khác nhau phát triển. Tuy nhiên, một lớp dịch vụ được chấp nhận rộng rãi là rất quan trọng đối với IoT.

Lớp dịch vụ thực tế bao gồm một tập hợp tối thiểu các yêu cầu chung của ứng dụng, giao diện lập trình ứng dụng (API) và các giao thức hỗ trợ các ứng dụng và dịch vụ được yêu cầu.

Tất cả các hoạt động hướng đến dịch vụ, chẳng hạn như trao đổi và lưu trữ thông tin, quản lý dữ liệu, công cụ tìm kiếm và giao tiếp, đều được thực hiện ở lớp dịch vụ. Các hoạt động được tiến hành bởi các thành phần sau:

- Khám phá dịch vụ tìm các đối tượng có thể cung cấp dịch vụ và thông tin được yêu cầu một cách hiệu quả.
- Thành phần dịch vụ cho phép tương tác giữa những thứ được kết nối. Khám phá khai thác các mối quan hệ của mọi thứ để tìm ra dịch vụ mong muốn, và lịch trình cấu thành dịch vụ hoặc tái tạo lại dịch vụ phù hợp hơn để có được những dịch vụ đáng tin cậy nhất.
- Quản lý độ tin cậy nhằm mục đích hiểu cách xử lý thông tin do các dịch vụ khác cung cấp.
- API dịch vụ cung cấp sự tương tác giữa các dịch vụ theo yêu cầu của người dùng.

Kiến trúc tích hợp SOCRADES (SIA) đã được đề xuất có thể được sử dụng để tương tác giữa các ứng dụng và các lớp dịch vụ một cách hiệu quả. Với kiến trúc này, những thực thể được đưa vào các thiết bị cung cấp dịch vụ ở cấp độ thấp như dịch vụ khám phá mạng, dịch vụ trao đổi siêu dữ liệu và các sự kiện đăng ký và xuất bản không đồng bộ. Chuyển trạng thái biểu diễn (REST) được định nghĩa để tăng khả năng tương tác cho việc kết hợp lỏng lẻo giữa các dịch vụ và các ứng dụng phân tán. Theo truyền thống, lớp dịch vụ cung cấp API chung cho các ứng dụng, nhưng kết quả nghiên cứu gần đây đã chỉ ra rằng quá trình cung cấp dịch vụ (SPP) có thể cung cấp hiệu quả sự tương tác giữa các ứng dụng và dịch vụ. SPP trước tiên thực hiện một "truy vấn loại", gửi một yêu cầu cho các dịch vụ có định dạng WSDL chung, sau đó "tìm kiếm ứng viên" được gọi để tìm các dịch vụ tiềm năng. Dựa trên "Bối cảnh ứng dụng" và "Thông tin QoS", phiên bản dịch vụ được xếp hạng và "Cung cấp dịch vụ theo yêu cầu" sẽ cố gắng khám phá phiên bản dịch vụ phù hợp với yêu cầu của ứng dụng. Cuối cùng, "Đánh giá quá trình" được sử dụng để đánh giá quá trình.

1.2.4. Lớp giao diện

Trong IoT, một số lượng lớn các thiết bị tham gia; những thiết bị đó có thể được cung cấp bởi các nhà cung cấp khác nhau và do đó không phải lúc nào cũng tuân thủ các tiêu chuẩn giống nhau. Vấn đề tương thích giữa các thiết bị không đồng nhất phải được giải quyết để các thiết bị có thể tương tác với nhau. Khả năng tương thích liên quan đến việc trao đổi thông tin, giao tiếp và xử lý sự kiện. Rất cần một cơ chế giao diện hiệu quả để đơn giản hóa việc quản lý và kết nối mọi thứ.

Hồ sơ giao diện (IFP) có thể được xem như một tập hợp con của các tiêu chuẩn dịch vụ cho phép tương tác tối thiểu với các ứng dụng đang chạy trên các lớp ứng dụng. Các cấu hình giao diện được sử dụng để mô tả các thông số kỹ thuật giữa các ứng dụng và dịch vụ. Một minh họa về lớp giao diện là việc triển khai Universal Plug and Play (UPnP), cơ chế này sẽ chỉ định một giao thức cho các tương tác liền mạch giữa những thiết bị không đồng nhất.

1.3. Các công nghệ được sử dụng trong mạng IoT

1.3.1. Công nghệ theo dõi và nhận dạng

Khái niệm IoT được đặt ra dựa trên các công nghệ nhận dạng và theo dõi hỗ trợ RFID. Một hệ thống RFID cơ bản bao gồm một đầu đọc RFID và một thẻ RFID. Do khả năng xác định và theo dõi, hệ thống RFID đã được ứng dụng rộng rãi trong lĩnh vực hậu cần, chẳng hạn như theo dõi gói hàng, quản lý chuỗi cung ứng, các ứng dụng chăm sóc sức khỏe, v.v. Hệ thống RFID có thể cung cấp đầy đủ thông tin thời gian thực về những thứ trong IoT, rất hữu ích cho các nhà sản xuất, nhà phân phối và nhà bán lẻ. Ví dụ, ứng dụng RFID trong quản lý chuỗi cung ứng có thể cải thiện việc quản lý hàng tồn kho. Một số lợi thế được xác định bao gồm giảm chi phí lao động, đơn giản hóa quy trình kinh doanh và cải thiện hiệu quả.

Gần đây, có báo cáo rằng 3% công ty EU đang sử dụng RFID. Trong các ứng dụng dựa trên RFID, 56% cho kiểm soát ra vào, 29% cho chuỗi cung ứng, 25% cho phí cầu đường cao tốc, 24% cho kiểm soát an ninh, 21% kiểm soát sản phẩm và 15% cho quản lý tài sản. Thế hệ tiếp theo của công nghệ RFID sẽ tập trung vào việc sử dụng RFID ở cấp độ mặt hàng và các vấn đề quản lý nhận biết RFID. Mặc dù công nghệ RFID được sử dụng

thành công trong nhiều lĩnh vực, nó vẫn đang phát triển trong việc phát triển các hệ thống hoạt động. Các vấn đề đã xác định khác cần được giải quyết để sử dụng trong IoT, bao gồm:

- **Sự va chạm của các bản đọc RFID**: Nó bao gồm các va chạm giữa các đầu đọc RFID hoặc thẻ RFID và nhiều lần đọc của cùng một thẻ RFID.
- **Giao thoa tín hiệu:** Nhiễu xảy ra trong hệ thống RFID hoặc với các thiết bị dựa trên sóng vô tuyến khác.
- **Bảo vệ quyền riêng tư**: Nó bao gồm quyền riêng tư của khách hàng và tính bảo mật của các thẻ RFID có thể được quét bởi các máy quét RFID được ủy quyền.
- **Tiêu chuẩn**: Các tiêu chuẩn áp dụng phổ biến vẫn còn thiếu đối với RFID.
- **Sự tích hợp**: Sự tích hợp của RFID và cảm biến thông minh.

1.3.2. Sự tích hợp WSN và RFID

Nhiều loại cảm biến thông minh đã được phát triển dựa trên các nguyên tắc vật lý của tia hồng ngoại, tia γ, áp suất, độ rung, điện từ, cảm biến sinh học và tia X. Dữ liệu từ các cảm biến đó trong IoT có thể được thu thập và tích hợp để phân tích, ra quyết định và lưu trữ. Ví dụ về cảm biến tích hợp RFID là cảm biến định vị On / Off-board, thẻ cảm biến, thiết bị cảm biến và thẻ độc lập và hệ thống đọc RFID.

Việc tích hợp các cảm biến và RFID tạo lợi thế cho IoT trong việc triển khai các dịch vụ công nghiệp và triển khai thêm các dịch vụ trong các ứng dụng mở rộng. Tích hợp IoT với RFID và WSN giúp có thể phát triển các ứng dụng IoT trong chăm sóc sức khỏe, ra quyết định đối với các hệ thống phức tạp và các hệ thống thông minh như giao thông thông minh, thành phố thông minh hoặc hệ thống phục hồi thông minh.

1.3.3. Truyền thông

Các thiết bị phần cứng liên quan đến các thông số kỹ thuật rất đa dạng về khả năng giao tiếp, tính toán, bộ nhớ và lưu trữ dữ liệu hoặc khả năng truyền tải. Một ứng dụng IoT bao gồm nhiều loại thiết bị. Tất cả các loại thiết bị phần cứng phải được tổ chức tốt thông qua mạng và có thể truy cập được thông qua giao tiếp có sẵn. Thông thường, các thiết bị có thể được tổ chức theo các cổng cho mục đích giao tiếp qua Internet.

IoT có thể là tập hợp các mạng không đồng nhất, chẳng hạn như WSN, mạng lưới không dây, mạng di động và WLAN. Các mạng này giúp thực hiện các hoạt động phức tạp như ra quyết định, tính toán và trao đổi dữ liệu. Ngoài ra, truyền thông đáng tin cậy giữa cổng và mọi thứ là điều cần thiết để đưa ra quyết định tập trung đối với IoT. Cổng có khả năng chạy cục bộ thuật toán tối ưu hóa phức tạp bằng cách khai thác kiến thức mạng của nó. Sự phức tạp tính toán được chuyển từ những thiết bị sang cổng vào; có thể thu được tuyến đường tối ưu toàn cục và các giá trị tham số cho cổng vào.

Khả năng phần cứng và các yêu cầu giao tiếp khác nhau giữa các loại thiết bị. Những thiết bị trong IoT có thể có các khả năng rất khác nhau về tính toán, bộ nhớ, sức mạnh hoặc giao tiếp. Ví dụ, điện thoại di động hoặc máy tính bảng có khả năng giao tiếp và tính toán tốt hơn nhiều so với một sản phẩm điện tử đơn năng như đồng hồ theo dõi nhịp tim. Tương tự như vậy, mọi thứ có thể có các yêu cầu rất khác nhau về Chất lượng Dịch vụ (QoS), đặc biệt là ở các khía cạnh về độ trễ, mức tiêu thụ năng lượng và độ tin cậy. Ví dụ, giảm thiểu việc sử dụng năng lượng cho các mục đích truyền thông hoặc tính toán là một hạn chế lớn đối với các thiết bị chạy bằng pin không có kỹ thuật thu năng lượng hiệu quả; hạn chế năng lượng này không quan trọng đối với các thiết bị có kết nối nguồn điện.

IoT cũng sẽ được hưởng lợi rất nhiều từ các giao thức hiện có trên Internet như IPv6. Các tiêu chuẩn và giao thức truyền thông thường được sử dụng bao gồm:

- RFID (ví dụ: ISO 18000 6c EPC lớp 1 Gen2),
- NFC, IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee), IEEE 802.15.1 (Bluetooth)
- Cảm biến không dây Multihop / Mạng lưới
- IETF Mạng cá nhân không dây công suất thấp (6LoWPAN)
- Máy đến Máy (M2M)
- Các công nghệ IP truyền thống, chẳng hạn như IP, IPv6, v.v.

Chi tiết về các công nghệ truyền thông có thể được tìm thấy trong Bảng 1.2.

Giao thức truyền thông	**Tốc độ truyền tải**	**Dải tần**	**Phạm vi truyền**
RFID	424 kbps	135 Khz	>50 cm
		13.56 MHz	>50 cm

		866–960 MHz	>3 m
		2.4 Ghz	>1.5 m
NFC	100 kbps –10 Mbps	2.45 GHz	
ZigBee	256 kbps/20 kbps	2.4 GHz/ 900 MHz	10 m
Bluetooth	1 Mbps	2.4 GHz	10 m
BLE	10 kbps	2.4 GHz	10 m
UWB	50 Mbps	Wide range	30 m
WiFi	50–320 Mbps	2.4/5.8 GHz	100 m
Wi-Max	70 Mbps	2–11 GHz	50 km
UMTS/CDMA/EDGE/MBWA	2 Mbps	896 MHz	~

Bảng 1.2. Các công nghệ truyền thông trong IoT

1.3.4. Mạng thông tin

Có rất nhiều giao thức đa lớp dành cho Mạng không dây như Mạng lưới không dây (WMN) hoặc Mạng quảng cáo (AHN). Tuy nhiên, chúng không thể được áp dụng cho IoT do một số lý do. Thứ nhất, sự không đồng nhất của IoT do thực tế là mọi thứ đã đa dạng hóa cấu hình phần cứng, yêu cầu QoS, chức năng và mục tiêu. Mặt khác, các nút trong WSN thường có các thông số kỹ thuật phần cứng tương tự, các yêu cầu giao tiếp tương tự và mục tiêu được chia sẻ. Thứ hai, Internet tham gia vào IoT, từ đó nó kế thừa một kiến trúc phân cấp và tập trung. So sánh, WSN, WMN và AHN có kiến trúc mạng tương đối phẳng: các nút trong các mạng này giao tiếp theo kiểu đa bước và không liên quan đến Internet.

1.3.5. Quản lý dịch vụ

Quản lý dịch vụ đề cập đến việc thực hiện và quản lý các dịch vụ đáp ứng nhu cầu của người dùng hoặc ứng dụng. SoA có thể thúc đẩy việc đóng gói các dịch vụ. Việc đóng gói cho phép các chi tiết của các dịch vụ, chẳng hạn như việc triển khai và các giao thức, được ẩn đằng sau các phiên bản của dịch vụ. SoA cho phép các ứng dụng sử dụng các đối tượng dịch vụ tương thích. Mặt khác, bản chất năng động của các ứng dụng IoT đòi hỏi

IoT phải cung cấp dịch vụ đáng tin cậy và nhất quán; nó có thể được hưởng lợi từ một kiến trúc hướng dịch vụ hiệu quả để tránh những hỏng hóc do lệch thiết bị hoặc hết pin.

1.3.5.1. Thành phần dịch vụ động

Như đã báo cáo nền tảng Open Services Gateway (OSGi) cung cấp kiến trúc SoA động, có khả năng hỗ trợ các dịch vụ thông minh. Các ứng dụng thành công trong ngành công nghiệp phần mềm đã cho thấy tính hiệu quả và mô-đun hóa của OSGi trong các lĩnh vực đa dạng như ứng dụng di động, trình plug-in và máy chủ ứng dụng. Đối với IoT, cấu phần dịch vụ dựa trên nền tảng OSGi có thể được Apache Felix iPoJo triển khai.

1.3.5.2. Nhận biết và thực hiện các dịch vụ

IoT hướng đến dịch vụ và là tập hợp con bắt buộc của Internet tương lai - mọi đối tượng vật lý và ảo đều có thể giao tiếp với các đối tượng khác cung cấp dịch vụ liền mạch cho các đối tượng khác. Hàng triệu thiết bị trong IoT cần có khả năng tương tác lẫn nhau. SoA giúp mọi đối tượng có thể cung cấp các chức năng của nó như các dịch vụ tiêu chuẩn. Để tổ chức các dịch vụ mà các đối tượng thực cung cấp, mỗi dịch vụ có thể được xác định duy nhất bởi một phần tử ảo trong IoT.

Trong IoT, các dịch vụ có thể được tạo và triển khai thông qua các bước sau: (1) phát triển các nền tảng cấu thành dịch vụ; (2) trừu tượng hóa các chức năng và khả năng giao tiếp của thiết bị; (3) cung cấp một tập hợp các dịch vụ chung. Các dịch vụ xác định việc quản lý, liên quan đến việc quản lý bối cảnh và phân loại đối tượng. IoT tạo ra một phản chiếu cho từng đối tượng thực theo cách để tạo ra sự đồng bộ hóa lại khả dụng.

Dịch vụ trong IoT có thể được coi là tập hợp dữ liệu và các hành vi liên quan để thực hiện một chức năng hoặc tính năng cụ thể của thiết bị hoặc các phần của thiết bị. Nhìn chung, các dịch vụ có thể được phân thành hai loại: dịch vụ chính và dịch vụ thứ cấp. Cái trước biểu thị các dịch vụ thể hiện các chức năng chính tại một nút, có thể được coi là thành phần cơ bản của các dịch vụ và có thể được bao gồm bởi một dịch vụ khác. Dịch vụ thứ cấp có thể cung cấp chức năng phụ trợ cho dịch vụ chính hoặc các dịch vụ thứ cấp khác. Một dịch vụ có thể sử dụng các dịch vụ chính hoặc phụ khác và hoặc một tập hợp các đặc điểm tạo nên dịch vụ. Trong IoT, mỗi dịch vụ có thể bao gồm một hoặc nhiều đặc điểm, xác định các thuộc tính của dịch vụ, chẳng hạn như cấu trúc dữ liệu, quyền, bộ mô tả, v.v.

Trong đặc tả Bluetooth SIG mới được phát hành, một dịch vụ có thể được mô tả tốt bằng ngôn ngữ XML để dễ dàng trao đổi với các phần mềm trung gian khác. Ví dụ về "Dịch vụ Nhiệt kế Sức khỏe". Dịch vụ này cung cấp các phép đo của nhiệt kế sức khỏe bằng UUID (0x1809) như trong Hình 1.6 và người dùng không cần biết cách thu thập dữ liệu đo lường.

```
<?xml version="1.0" encoding="utf-8"?>
<service uuid = "1809">
    <uri>org.bluetooth.service.health_thermometer</uri>
    <description>Health Thermometer Service</description>
    <characteristic> uuid = "2a1c", id = "xgatt_temperature_celsius">
        <description> Celsius temperature </description>
        <properties indicate = "true" />
        <value type = "hex"> 0000000000 </value>
    </characteristic>
</service>
```

Hình 1.6. Ví dụ minh họa của dịch vụ trong IoT

Các đặc điểm của dịch vụ bao gồm ba thành phần:

- Khai báo mô tả các thuộc tính của giá trị đặc trưng như đọc, ghi, chỉ báo, cũng như các xử lý và kiểu giá trị.
- Giá trị được chỉ định cho thuộc tính
- Bộ mô tả cung cấp thông tin phụ trợ về các đặc điểm.

Bảng 1.3 cho thấy một ví dụ về các đặc điểm của một dịch vụ.

Kiểu	**Quyền**	**Giá trị**
0X2800 (Service UUID)	Read	E0:FF
0X2803 (Characteristic UUID)	Read	10:29:00:E1:FF

Bảng 1.3. Các đặc trưng của dịch vụ

1.3.5.3. Tích hợp các công nghệ dịch vụ

Như đã đề cập ở trên, Hình 1.4 đã chỉ ra kiến trúc của IoT, bao gồm bốn lớp: lớp giao diện, lớp ứng dụng, lớp mạng và lớp cảm biến. (1) Lớp giao diện cung cấp giao diện cho các ứng dụng, dịch vụ bên ngoài, v.v.; (2) Lớp ứng dụng cung cấp các chức năng được xây dựng dựa trên việc triển khai IoT. Lớp ứng dụng được kết nối với các thành phần mô hình hóa quy trình cho các quy trình kinh doanh nhận biết IoT; các quy trình có thể được thực thi trong các thành phần thực thi quy trình; (3) Lớp mạng chứa ba thành phần cơ bản:

sắp xếp thực thể dịch vụ, thực thể ảo và thông tin, và tài nguyên. Việc sắp xếp và tiếp cận các dịch vụ cho các thực thể và dịch vụ bên ngoài được tổ chức bởi thành phần sắp xếp thực thể dịch vụ. Thành phần thực thể ảo (VE) đang hoạt động để liên kết VE với các dịch vụ có liên quan; nó cũng là một phương tiện để tìm kiếm các dịch vụ như vậy. Mô-đun tài nguyên cung cấp các chức năng theo yêu cầu của dịch vụ để xử lý thông tin và thông báo cho phần mềm ứng dụng và dịch vụ về các sự kiện liên quan đến tài nguyên và thực thể ảo; (4) Lớp cảm biến liên quan đến các thiết bị cảm biến, chẳng hạn như thẻ RFID, nút cảm biến, v.v., có thể ghi lại, thu thập và xử lý các quan sát và đo lường. Lớp mạng có thể truy cập lớp cảm biến với API cấp thiết bị, cung cấp trao đổi dữ liệu giữa các ứng dụng trong thế giới thực.

1.3.6. Bảo mật và quyền riêng tư

Đối với IoT, bảo mật và quyền riêng tư là hai thách thức quan trọng. Để tích hợp các thiết bị của lớp cảm biến như các bộ phận bên trong của IoT, công nghệ bảo mật hiệu quả là điều cần thiết để đảm bảo an ninh và bảo vệ quyền riêng tư trong các hoạt động khác nhau như hoạt động cá nhân, quy trình kinh doanh, vận chuyển và bảo vệ thông tin. Các ứng dụng của IoT có thể bị ảnh hưởng bởi các mối đe dọa phổ biến như các cuộc tấn công thẻ RFID và rò rỉ dữ liệu. Trong hệ thống RFID, một số phương án bảo mật và giao thức xác thực đã được đề xuất để đối phó với các mối đe dọa bảo mật. Ví dụ: Juels đề xuất phương pháp "thẻ chặn" để ngăn chặn việc theo dõi trái phép. Mặt khác, các thuật toán mật mã khóa đối xứng chi phí thấp, chẳng hạn như Thuật toán mã hóa nhỏ (TEA) và Tiêu chuẩn mã hóa nâng cao (AES), đã được đề xuất để bảo vệ việc trao đổi dữ liệu. Bên cạnh đó, thẻ RFID chi phí thấp đã triển khai một số thuật toán mật mã khóa bất đối xứng như mật mã đường cong Elliptic (ECC) để bảo mật. Mặt khác, các giao thức bảo mật được phát triển cho WSN có thể được tích hợp như một phần nội tại của IoT. Những thách thức trong bảo mật và bảo vệ quyền riêng tư được tóm tắt là khả năng phục hồi trước các cuộc tấn công, xác thực dữ liệu, kiểm soát truy cập và quyền riêng tư của khách hàng.

1.4. Ứng dụng mạng IoT trong thực tế

IoT cho phép thu thập, lưu trữ và truyền thông tin cho những thiết bị được trang bị thẻ hoặc cảm biến. Các thẻ đã được sử dụng rộng rãi trong quản lý chuỗi cung ứng, sản xuất, giám sát môi trường, bán lẻ, vận hành kệ thông minh, chăm sóc sức khỏe, ngành thực

phẩm và nhà hàng, ngành hậu cần, ngành du lịch và lữ hành, dịch vụ thư viện và nhiều lĩnh vực khác.

IoT có tầm quan trọng cao đối với nền kinh tế và xã hội. Để tăng tốc các ứng dụng của IoT, sự phát triển của cơ sở hạ tầng CNTT đóng một vai trò quan trọng. Có thể thấy trước rằng IoT sẽ góp phần to lớn trong việc giải quyết các vấn đề xã hội như giám sát chăm sóc sức khỏe, giám sát cuộc sống hàng ngày và kiểm soát tắc nghẽn giao thông. IoT làm cho sự kết nối của mọi thứ khuếch đại những tác động sâu sắc.

Hiện tại, IoT đã được triển khai thành công trên nhiều lĩnh vực:

- Đối với người dùng, một số lượng lớn các thành phần phần cứng và phần mềm (thẻ RFID, điện thoại di động, mạng xã hội và ứng dụng di động) đã được phát triển cho người tiêu dùng cho phép người dùng truy cập thông tin bổ sung về sản phẩm.
- Đối với các nhà sản xuất, ngày càng có nhiều sản phẩm được tạo ra với các công nghệ nhận dạng độc đáo, chẳng hạn như mã vạch, thẻ RFID, cảm biến thông minh trên thiết bị điện tử cá nhân và thiết bị gia dụng. Các công nghệ nhận dạng này làm cho sản phẩm được giám sát và theo dõi trong vòng đời của chúng.
- Nó có thể tăng hiệu quả của các ngành công nghiệp truyền thống bằng cách giới thiệu các kỹ thuật xử lý và trao đổi dữ liệu mới.

1.4.1. Ứng dụng trong ngành công nghiệp

IoT có thể cải thiện các giao dịch kinh doanh với các mạng dịch vụ thông minh hơn, điều này sẽ cải thiện đáng kể hiệu quả xử lý thông tin thời gian thực và quản lý các ứng dụng tinh vi, chẳng hạn như thanh toán trực tuyến, lưu trữ dữ liệu quan trọng, QoS tổng hợp và các chỉ số hiệu suất liên quan.

IoT có thể giảm khoảng cách giữa các thành phần trong nền kinh tế kỹ thuật số hiện tại, nơi nền kinh tế lấy dịch vụ làm trung tâm được thực hiện thông qua các giao dịch mạng. Trong khi đó, mô hình kinh doanh có thể được hưởng lợi từ IoT ở cấp độ nội bộ và giữa các tổ chức. Các doanh nghiệp sử dụng IoT có thể được hưởng lợi từ các sản phẩm cạnh tranh, mô hình kinh doanh xanh hơn và có lợi hơn, tài nguyên được tối ưu hóa và xử lý thông tin theo thời gian thực. IoT được kết nối toàn cầu có thể cung cấp cho các doanh nghiệp các mạng dịch vụ tích hợp như ví dụ trong Hình 1.4. Các nhà sản xuất có thể được

hưởng lợi, IoT cho phép các đối tác kinh doanh tích hợp liền mạch các nguồn lực của doanh nghiệp (Bảng 1.4).

Sự triển khai trong doanh nghiệp	**Ứng dụng**
Logistics và SCM (Supply Chain Management)	Quản lý vị trí hàng hóa
	Ngăn ngừa bị đánh cắp
	Quản lý Container trong SC
	Quản lý các sự kiện SC
Quản lý truy cập	Hệ thống điều khiển truy cập NCF
	E-home
	Bảo mật cơ sở hạ tầng
Kiểm soát quy trình công nghiệp	Hệ thống điều khiển chất lượng thông minh

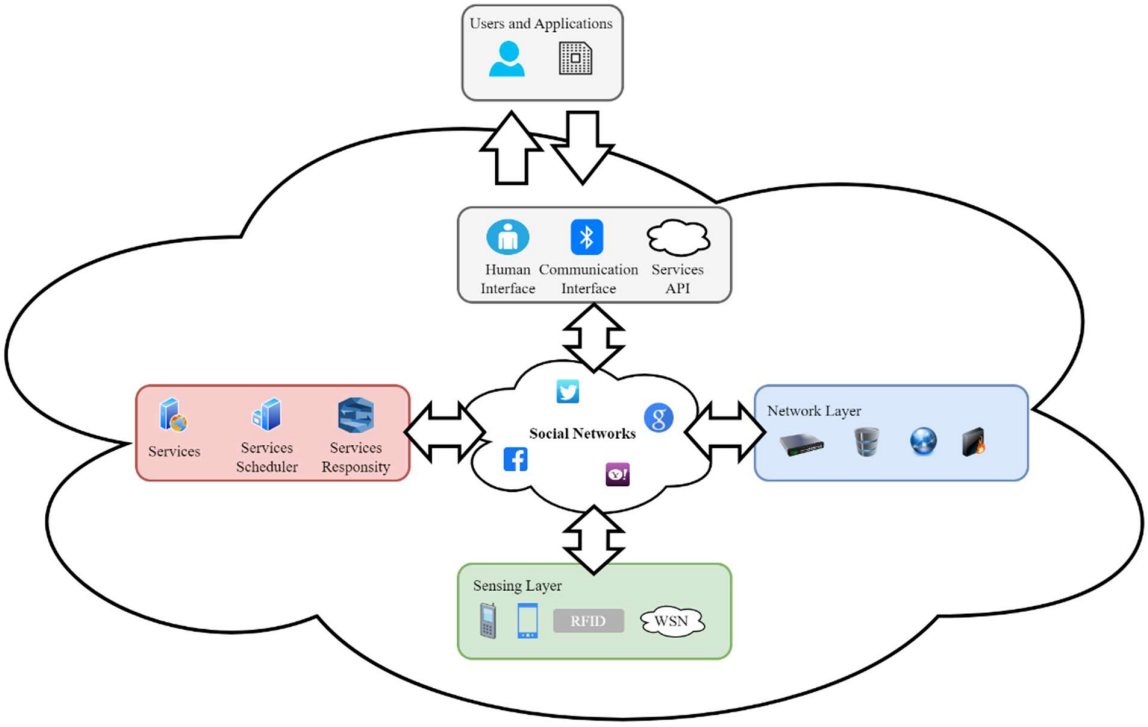
Bảng 1.4. Các ứng dụng trong doanh nghiệp của IoT

1.4.2. Mạng xã hội IoT

Gần đây, ý tưởng tích hợp IoT với các mạng xã hội đã được đề xuất và một mô hình mới "Mạng xã hội vạn vật (SIoT)" được đề xuất để mô tả một thế giới nơi mọi thứ xung quanh con người có thể được cảm nhận và nối mạng một cách thông minh. SIoT có thể thực hiện khám phá mọi thứ và dịch vụ một cách hiệu quả và cải thiện khả năng mở rộng của IoT tương tự như các mạng xã hội của con người. Các công nghệ bảo vệ và quyền riêng tư được sử dụng trong mạng xã hội có thể được cấy ghép vào IoT để cải thiện tính bảo mật của IoT.

Khái niệm SIoT được thúc đẩy bởi các mạng xã hội phổ biến trên Internet: Facebook, Twitter, và blog vi mô; những mạng lưới này đang thâm nhập vào cuộc sống hàng ngày của mọi người. Vì vậy, SIoT đã thu hút được rất nhiều sự quan tâm của các nhà khoa học và nhà nghiên cứu về kinh doanh điện tử, học tập điện tử, xã hội học, tâm lý học và mạng. Phương pháp *homophily* được đề xuất để thiết lập mức độ tin cậy cao hơn; nó có thể hữu ích để tối ưu hóa mối quan hệ giữa mọi thiết bị và người dùng.

Đã có những nghiên cứu về việc tích hợp IoT và các mạng xã hội hiện có (như Facebook, Twitter, v.v.). Fielding và Taylor đã nghiên cứu tiềm năng của SIoT trong việc hỗ trợ các ứng dụng mới và các dịch vụ mạng. Trong Hình 1.7, một sơ đồ tích hợp của mạng xã hội vào IoT được mô tả và kiến trúc hệ thống để triển khai SIoT được đưa ra



Hình 1.7. Kiến trúc của Social IoT

1.4.3. Ứng dụng trong chăm sóc sức khỏe

Chăm sóc sức khỏe là một lĩnh vực ứng dụng quan trọng của IoT. IoT được áp dụng để nâng cao chất lượng dịch vụ và giảm chi phí. Một số cảm biến hoặc thiết bị y tế được sử dụng để theo dõi các thông số y tế như nhiệt độ cơ thể, mức đường huyết và huyết áp. Những tiến bộ trong công nghệ cảm biến, truyền thông không dây và xử lý dữ liệu là động lực để triển khai IoT trong các hệ thống chăm sóc sức khỏe. Mạng cảm biến cơ thể có thể đeo được (WBSN) mới nổi được phát triển để theo dõi các hoạt động hoặc thông số y tế của bệnh nhân một cách liên tục. IoT có thể cung cấp cho các hệ thống chăm sóc sức khỏe sự kết nối với nhau của các thiết bị không đồng nhất như vậy để có được bức tranh toàn cảnh về các thông số sức khỏe.

IoT có thể được sử dụng để cải thiện các giải pháp sống được hỗ trợ hiện tại. Các thiết bị y tế được kết nối với IoT bao gồm cảm biến y tế và cảm biến đeo được. Các cảm biến này có thể được sử dụng để thu thập thông tin chăm sóc sức khỏe và truyền đến các trung tâm y tế từ xa. IoT với cảm biến sinh học đeo được đã được ứng dụng trong việc theo dõi bệnh nhân, theo dõi các hoạt động hàng ngày và chăm sóc người già. Có thể thấy trước rằng IoT với các cảm biến y tế thông minh sẽ nâng cao chất lượng cuộc sống một cách

đáng kể và ngăn ngừa sự xuất hiện của các vấn đề sức khỏe. Trên thực tế, các cảm biến y tế chi phí thấp có thể được kết nối không dây với những thứ khác trong IoT; việc phát triển các cảm biến cấy ghép để theo dõi tình trạng sức khỏe của bệnh nhân trở nên khả thi. Ví dụ: các công nghệ dựa trên BLE được áp dụng để kết nối mọi thứ trong cuộc sống hàng ngày của chúng ta như điện thoại thông minh, cảm biến cơ thể, thiết bị gia dụng và máy tính cá nhân cho các ứng dụng trong chăm sóc sức khỏe, thể dục, bảo mật và giải trí gia đình.

Mặt khác, sự phát triển nhanh chóng của các thiết bị di động và các ứng dụng y tế tạo ra một thị trường rộng lớn cho việc ứng dụng IoT. Các ứng dụng sức khỏe di động cá nhân đã được phát triển để phục vụ các công việc chăm sóc sức khỏe như đo huyết áp hoặc ghi lại lượng đường trong máu. Một khái niệm mới có tên là Internet vạn vật sức khỏe (HIoT) đã được đề xuất để khai thác các công nghệ cảm biến và mạng không dây trong việc theo dõi các tình trạng y tế.

1.4.4. Cơ sở hạ tầng

IoT cũng đã được phát triển trong nhiều lĩnh vực cơ sở hạ tầng: thành phố thông minh, giám sát môi trường, nhà thông minh và tòa nhà. Trong các tòa nhà thông minh, IoT được sử dụng để cải thiện chất lượng tòa nhà và giảm thiểu chất thải. Thuật ngữ 'Thành phố thông minh' đã được đề xuất như một hệ sinh thái vật lý mạng với các cảm biến thông minh và các dịch vụ mới trên toàn thành phố. Ví dụ, dự án ‘Sensing China’ được khởi động tại Trung Quốc vào tháng 6 năm 2010. Sau khi hoàn thành dự án, người ta đoán trước rằng mọi thứ sẽ có thẻ nhận dạng có thể phát thông tin lên Internet. Mọi người có thể theo dõi việc sử dụng các thiết bị và giám sát bất kỳ chỉ số hoặc đối tượng nào; dữ liệu thu thập được có thể được sử dụng để giảm lãng phí và chi phí. Có thể thấy trước việc triển khai thành công IoT trong một cộng đồng hoặc thậm chí một thành phố.

1.4.5. An ninh và giám sát

Trong một mô hình ảo của IoT, mọi đối tượng vật lý đều có thể tìm thấy một đối tác phản hồi có thể cung cấp dịch vụ cho người dùng. Mỗi đối tượng nên được giải quyết tốt và được gắn nhãn trong IoT. Tuy nhiên, sự kết nối giữa các đối tượng có thể mang lại các vấn đề an ninh chưa từng có; bảo vệ an ninh mạnh mẽ là cần thiết để tránh các cuộc tấn công và trục trặc. Trong các mạng truyền thống, chẳng hạn như Internet, các giao thức bảo

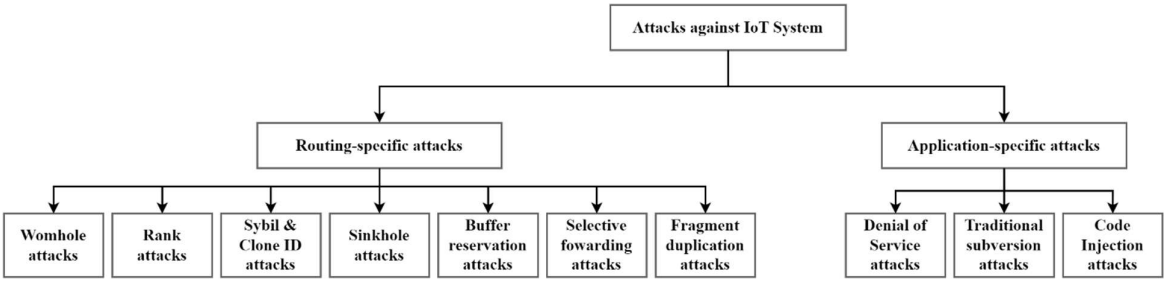
mật và đảm bảo quyền riêng tư được sử dụng rộng rãi để bảo vệ quyền riêng tư và truyền thông. Tuy nhiên, các kỹ thuật bảo mật được áp dụng trong các mạng thông thường không đủ cho IoT. Các giao thức và cơ chế bảo mật hiện tại cần được cải thiện trước khi chúng có thể dễ dàng được áp dụng trong IoT.

Mặt khác, khung pháp lý và kỹ thuật cũng rất cần thiết. Do tính năng động, không chắc chắn và phức tạp của IoT, việc bảo vệ hàng nghìn thậm chí hàng triệu thiết bị thông minh là một nhiệm vụ rất thách thức. Bên cạnh đó, sự không đồng nhất ảnh hưởng lớn đến việc bảo vệ an ninh của các mạng có thể bị xử lý. Mọi thiết bị có thể bị nhiều mối đe dọa như rò rỉ dữ liệu và các mối đe dọa từ các mạng bên ngoài. Do đó, các công nghệ bảo mật phải cung cấp sự bảo vệ mạnh mẽ cho tất cả các cấp độ của các thành phần hệ thống ở tất cả các giai đoạn: từ lớp cảm biến đến lớp giao diện, từ nhận dạng đến cung cấp dịch vụ và từ thẻ RFID đến cơ sở hạ tầng CNTT. Nói cách khác, thông tin cần được bảo mật từ khi bắt đầu tồn tại cho đến khi kết thúc vòng đời của nó.

Quyền riêng tư thông tin là một trong những chủ đề nhạy cảm nhất đối với IoT. Nhu cầu về khả năng truy cập dữ liệu dễ dàng mang lại thách thức để bảo vệ thông tin trong các dịch vụ được cá nhân hóa. Để thiết kế cơ chế bảo vệ quyền riêng tư, một số yếu tố cần được xem xét. Ví dụ, giai đoạn xác thực sử dụng liên quan đến sự phát triển của kiểm soát truy cập và quản lý tin cậy.

1.5. Các rủi ro về an ninh mạng trong mạng IoT

Mặc dù IoT là một mô hình mới nổi, nhưng một phần quan trọng của tầng ứng dụng trong IoT được tiếp nhận từ các mô hình phần mềm hiện có. Điều này có ý nghĩa quan trọng cơ sở hạ tầng IoT vì khi này những mối đe dọa không chỉ giới hạn ở các giao thức định tuyến mới, chẳng hạn như 6LoWPAN và RPL, mà còn bao gồm các mối đe dọa đối với cơ sở hạ tầng hiện có, chẳng hạn như IPv6, các cuộc tấn công dành riêng cho ứng dụng và các cuộc tấn công cụ thể vào phương tiện vật lý, chẳng hạn như phổ vô tuyến. Các cuộc tấn công khác nhau cho một hệ thống IoT điển hình được tóm tắt trong Hình 1.8.



Hình 1.8. Các kiểu tấn công trong IoT

1.5.1. Những rủi ro về định tuyến

Thông tin định tuyến trong hệ thống IoT có thể được sửa đổi hoặc giả mạo để định tuyến lưu lượng theo cách độc hại hoặc để khởi động một cuộc tấn công tiếp theo vào mạng IoT. Các cuộc tấn công này là phổ biến nhất trong các mạng IoT bị hạn chế về tài nguyên. Các cuộc tấn công định tuyến có liên quan nhất trong IoT bao gồm:

- **Rank attack**: Một đặc điểm của mạng 6LoWPAN là sử dụng xếp hạng để thiết lập đường dẫn định tuyến tối ưu. Trong tình huống này, xếp hạng nút (Node Ranking) cho biết chất lượng của đường dẫn từ một nút đến một nút khác. Mỗi khi một nút cập nhật thứ hạng hoặc cấp độ gốc ưu tiên của nó, nó phải thông báo cho các nút khác bằng cách gửi thông tin cập nhật trong Đối tượng thông tin đồ thị chu kỳ có hướng (DAG) tiếp theo (DIO). RPL sử dụng quy tắc xếp hạng, tức là một nút trong nút cha phải luôn có thứ hạng thấp hơn các nút con của nó để ngăn việc tạo vòng lặp. Theo cách này, thứ hạng cho phép tạo cấu trúc liên kết tối ưu, ngăn chặn việc tạo vòng lặp và quản lý chi phí điều khiển. Và trong thực tế thông tin xếp hạng có thể bị kẻ tấn công giả mạo sao cho nó chọn nút có xếp hạng kém nhất làm nút gốc. Do đó, điều này sẽ dẫn đến việc làm xáo trộn cấu trúc liên kết của mạng, từ đó gây ra sự chậm trễ trong quá trình truyền thông thường.
- **Wormhole attack**: Lỗ sâu có thể được coi là một đường hầm giữa hai nút sử dụng liên kết có dây hoặc không dây và có thể được sử dụng để đạt được tốc độ truyền nhanh hơn hoặc kết nối chuyên dụng giữa các nút đó. Tuy nhiên, lỗ sâu có thể được kẻ tấn công sử dụng để tạo một đường hầm chuyên dụng với một nút trên Internet. Tấn công lỗ sâu không phải là mới đối với các hệ thống IoT và đã được xác định trong lịch sử là mối đe dọa tiềm ẩn đối với các mạng cảm biến không dây.

- **Sinkhole attack**: Mục tiêu của một cuộc tấn công hố sụt là thu hút lưu lượng truy cập thông qua một nút được chỉ định bằng cách sử dụng thông tin bất hợp pháp làm cho nút đó trở thành một điểm định tuyến sinh lợi (trạm cơ sở trong mạng không dây). Tuy nhiên, việc tạo một lỗ hổng không nhất thiết làm gián đoạn quá trình truyền trong 6LoWPAN, bằng cách chuyển hướng lưu lượng truy cập qua một tuyến đường cụ thể sẽ tạo cơ hội để khởi chạy các cuộc tấn công khác, chẳng hạn như lỗ sâu và tấn công chuyển tiếp chọn lọc được mô tả bên dưới.

- **Selective forwarding attack**: Với một cuộc tấn công chuyển tiếp có chọn lọc, một nút độc hại cố gắng phá vỡ đường truyền và định tuyến hợp pháp. Nút độc hại trong trường hợp này cố gắng chặn một số gói nhất định và chuyển tiếp các gói đã chọn, do đó ảnh hưởng đến việc định tuyến để thực hiện các mục tiêu độc hại. Chẳng hạn, kẻ tấn công có thể chuyển tiếp tất cả các thông báo điều khiển RPL nhưng chặn các thông báo còn lại. Có thể nhận thấy, kiểu tấn công này có thể gây ra nhiều thiệt hại hơn khi được sử dụng kết hợp với đòn tấn công hố sụt.

- **Fragment duplication attack**: Tấn công sao chép phân đoạn tận dụng một điểm yếu trong lớp 6LoWPAN liên quan đến cách các gói bị phân mảnh được nhận và lắp ráp bởi một nút IoT. Do sự tích hợp của 6LoWPAN với mạng IPv6, các gói lớn hơn được hỗ trợ bởi IPv6 phải được phân chia thành các gói nhỏ hơn để được xử lý bởi các nút bị hạn chế tài nguyên trong hệ thống IoT. Tuy nhiên, nút người nhận không thể xác minh xem hai đoạn của gói có được gửi bởi cùng một nguồn hay không, do đó nút người nhận không thể phân biệt giữa các đoạn hợp pháp và giả mạo. Một nút độc hại có thể khai thác lỗ hổng này để chặn việc lắp ráp lại các gói được nhắm mục tiêu, chẳng hạn như các gói thiết lập kết nối. Điều này có thể dẫn đến việc làm gián đoạn lưu lượng truy cập hợp pháp cũng như tiêu tốn tài nguyên có sẵn cho nút nạn nhân.

- **Buffer reservation attack**: Cuộc tấn công dự trữ bộ đệm được liên kết chặt chẽ với cuộc tấn công sao chép đoạn và có thể được gây ra do hậu quả của một cuộc tấn công sao chép đoạn thành công. Cuộc tấn công dự trữ bộ đệm cũng nhắm vào lỗ hổng trong cơ chế phân mảnh được sử dụng bởi các mạng 6LoWPAN. Nó tận dụng thực tế là người nhận gói bị phân mảnh không thể xác định xem tất cả các mảnh có

được nhận chính xác hay không. Do đó, một nút người nhận dự trữ một không gian bộ đệm dựa trên thông tin được cung cấp trong tiêu đề 6LoWPAN với bất kỳ phân đoạn bổ sung nào bị loại bỏ. Lợi dụng cấu hình này, một nút độc hại có thể gửi cho nạn nhân một FRAG1 duy nhất để dự trữ không gian bộ đệm tùy ý, do đó tiêu tốn bộ nhớ khan hiếm của nút bị hạn chế tài nguyên.

- **Sybil and clone ID attack**: Các cuộc tấn công Sybil và Clone ID giống nhau ở chỗ mục tiêu của kẻ tấn công là sử dụng danh tính logic giả mạo trong mạng mà không triển khai các thiết bị vật lý. Cụ thể, đối với cuộc tấn công Clone ID, kẻ tấn công sử dụng danh tính logic của nạn nhân trong mạng trong khi trong cuộc tấn công Sybil, kẻ tấn công giả định nhiều danh tính logic trong mạng mà không triển khai các nút vật lý. Những danh tính logic này có thể hiện không có trong mạng.

1.5.2. Những rủi ro về ứng dụng

Mặc dù định tuyến là một thành phần thiết yếu của hệ thống IoT, nhưng các thiết bị IoT dự kiến sẽ lưu trữ phần mềm ứng dụng theo yêu cầu của chức năng dự kiến sẽ được thực hiện, chẳng hạn như giám sát nhiệt độ và quản lý chuỗi cung ứng. Là các ứng dụng phần mềm, chúng có thể tạo ra các lỗ hổng bổ sung cho bề mặt tấn công tổng thể của hệ thống IoT. Các rủi ro về ứng dụng điển hình như:

- **Tấn công từ chối dịch vụ**: Trước đây, các cuộc tấn công từ chối dịch vụ (DoS) được nhắm mục tiêu làm cho nạn nhân không thể sử dụng dịch vụ hợp pháp. Điều này có thể đạt được bằng cách làm quá tải nạn nhân với khối lượng yêu cầu cực lớn hoặc bằng cách làm cạn kiệt tài nguyên, chẳng hạn như bộ nhớ và sức mạnh tính toán có sẵn cho nạn nhân. Trong IoT, mối đe dọa của một cuộc tấn công DoS là gấp đôi; nạn nhân có thể là một phần của mạng đang bị đe dọa mà kẻ tấn công muốn làm cho không khả dụng hoặc nạn nhân có thể được sử dụng làm các bot để khởi chạy DoS phân tán (DDoS) trên mạng IoT mục tiêu.

- **Tiêm mã độc**: Tiêm mã độc là một mối đe dọa dành riêng cho ứng dụng khác đối với các hệ thống IoT. Trong trường hợp này, kẻ tấn công cố gắng tiêm mã độc để có quyền truy cập vào nạn nhân. Do đó, kẻ tấn công có thể làm hỏng hoạt động bình thường bằng cách gây ra mối đe dọa đối với dữ liệu hoặc mạng bằng cách sử dụng một trong các cuộc tấn công định tuyến cụ thể được mô tả trong phần trước.

1.5.3. Các kiểu tấn công truyền thống

Ngoài các cuộc tấn công đã đề cập ở trên, các hệ thống IoT dễ bị tấn công trước các cuộc tấn công hiện có nhắm vào hệ thống máy tính, chẳng hạn như chặn tin nhắn, ngụy tạo, sửa đổi, và lừa đảo. Cũng giống như các cuộc tấn công dành riêng cho định tuyến, các cuộc tấn công này cũng có thể là một phần của cuộc tấn công phức tạp và tinh vi hơn. Do đó cần nhiều hơn những nỗ lực để giúp hệ thống IoT chống lại được các rủi ro này.

1.6. Kết luận chương

Trong chương này của đồ án đã trình tổng quan về hệ thống IoT, các khái niệm, các tiêu chuẩn, các công nghệ được sử dụng cũng như là các ứng dụng và rủi ro về an ninh mạng đối với hệ thống IoT. Trong vài năm qua, IoT đã được phát triển nhanh chóng và một số lượng lớn các công nghệ hỗ trợ đã được đề xuất. IoT đã là xu hướng của Internet tiếp theo. Điều này đem lại rất nhiều lợi ích cho cuộc sống trong rất nhiều lĩnh vực từ doanh nghiệp, mạng xã hội, chăm sóc sức khỏe cũng như là cơ sở hạ tầng, an ninh và giám sát. Đi cùng với sự phát triển đó, các hệ thống IoT cũng phải đối mặt với những rủi ro và thách thức về an toàn và quyền riêng tư. Một phần quan trọng của tầng ứng dụng trong IoT được tiếp nhận từ các mô hình phần mềm hiện có nên những mối đe dọa không chỉ giới hạn ở các giao thức mới, mà còn bao gồm cả các mối đe dọa đối với cơ sở hạ tầng hiện có. Đồng thời do đăng tính không đồng nhất và động nên việc triển khai các giải pháp an toàn cũng gặp phải những thách thức lớn. Do đó, các hệ thống IoT yêu cần cần có những giải pháp an toàn mới như hệ thống phát hiện xâm nhập được thiết kế riêng để phù hợp với những đặc trưng của IoT.

CHƯƠNG 2: CÁC GIẢI PHÁP HIỆN TẠI CHO HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS

2.1. Khái niệm về IDS trong mạng IoT

Sự tiến bộ trong các công nghệ như cảm biến, tự động hóa trong nhận dạng và theo dõi đối tượng, giao tiếp giữa các thiết bị được kết nối với nhau, các dịch vụ Internet tích hợp và phân tán dẫn đến việc sử dụng các thiết bị thông minh và mạng lưới IoT ngày càng tăng trong các hoạt động hàng ngày. Tuy nhiên, nhu cầu của các thiết bị IoT với các ứng dụng trong thế giới thực đã làm tăng rủi ro cho các dịch vụ Internet cũng như các thiết bị. Các CPS (Cyber-Physical Systems) được xây dựng với cơ sở hạ tầng quan trọng dễ bị đe dọa về an ninh như báo động giả trong các thiết bị gia dụng làm ảnh hưởng đến an ninh và quyền riêng tư của các cá nhân, lỗi trong các nhà máy điện và giao thông ảnh hưởng đến các hoạt động hàng ngày của các thành phố và quốc gia. Do đó, việc tiếp xúc với các lỗ hổng trong tài nguyên hệ thống có xu hướng vi phạm các yêu cầu bảo mật của người dùng cũng như hệ thống. Các thử nghiệm cho thấy rằng bảo mật và quyền riêng tư của thiết bị có thể bị vi phạm dễ dàng do năng lượng thấp và khả năng tính toán của các thiết bị được kết nối được kết nối với số lượng lớn. Do đó, việc thiết kế các giải pháp bảo mật phù hợp cho mạng IoT là một nhiệm vụ đầy thách thức để cho phép người dùng tận dụng các cơ hội do thiết bị IoT mang lại trong khi vẫn đáp ứng các yêu cầu bảo mật.

Các phương pháp được triển khai để đảm bảo tính bảo mật của các thiết bị IoT như tường lửa và cơ chế kiểm soát truy cập tập trung vào việc cung cấp tính bảo mật và tính xác thực của dữ liệu, kiểm soát truy cập trong mạng của các thiết bị IoT và phát triển các chính sách bảo mật và quyền riêng tư để tạo niềm tin giữa các cá nhân. Mặc dù kết hợp các cơ chế bảo mật này, các mạng IoT vẫn phải đối mặt với các mối đe dọa bảo mật. Do đó, các mạng IoT cần một cơ chế bảo mật có thể hoạt động như một tuyến phòng thủ để phát hiện những kẻ xâm nhập. Do đó, Hệ thống phát hiện xâm nhập (IDS) được sử dụng làm công cụ bảo vệ cho các hệ thống thông tin và truyền thông.

Một IDS có khả năng kiểm tra các hoạt động mạng giữa các thiết bị được kết nối và đưa ra cảnh báo bất cứ khi nào phát hiện thấy bất kỳ vi phạm nào. IDS được coi là một cơ chế bảo vệ thiết yếu cho các mạng IP truyền thống do khả năng giám sát và cảnh báo của nó. Mặc dù, IDS hoạt động tốt cho các mạng truyền thống, nhưng việc phát triển IDS cho

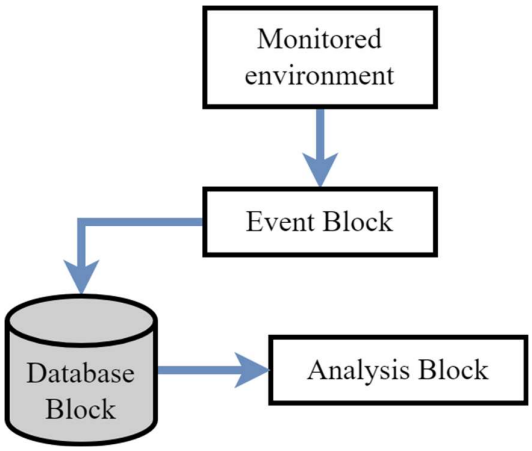
mạng IoT vẫn là một nhiệm vụ đầy thách thức. Điều này là do các đặc điểm của mạng IoT như khả năng xử lý và lưu trữ hạn chế của các nút tác nhân IDS của mạng.

Trong các mạng IP truyền thống, nhà phân tích bảo mật chỉ định các IDS agent có khả năng hoạt động trong môi trường thay đổi linh hoạt, trong khi đó, trong các nút mạng IoT được tăng cường kỹ thuật số với các cảm biến, bộ truyền động, logic lập trình và giao diện truyền thông. Do đó, để phát triển các nút có khả năng như vậy và đảm bảo an ninh là một thách thức trong các mạng IoT. Trong các mạng IP thông thường, các nút thể hiện khả năng kết nối đáng tin cậy và chuyển tiếp các gói từ nguồn đến đích. Trong khi, trong các mạng IoT, các thiết bị không phải lúc nào cũng được kết nối. Các thiết bị thể hiện kết nối không liên tục sẽ kết nối định kỳ để tiết kiệm mức tiêu thụ năng lượng và băng thông. Chẳng hạn, các hệ thống báo động gia đình dựa trên IoT có các nút cảm biến với khả năng kết nối không liên tục và khả năng giao tiếp tầm ngắn. Do đó, cần có nhiều nút để chuyển tiếp thông tin trong mạng. Dữ liệu được thu thập từ nút di chuyển qua đường dẫn được chỉ định bởi các cảm biến và cung cấp thông tin đi qua cổng đến đích. Loại cơ sở hạ tầng này đặt ra những thách thức cho IDS trong việc xác định sự xâm nhập. Một thách thức bảo mật khác liên quan đến các giao thức mạng được sử dụng bởi các mạng IoT, chẳng hạn như IEEE 802.15.4, IPv6 qua Mạng khu vực cá nhân không dây công suất thấp (6LoWPAN), Giao thức định tuyến IPv6 cho mạng công suất thấp và tổn thất (RPL) và Bị ràng buộc Giao thức ứng dụng (CoAP). Do đó, các giao thức IoT khác nhau khiến IDS gặp phải các lỗ hổng và yêu cầu khác nhau. Do đó, những thách thức như vậy cần được giải quyết và giảm thiểu bằng IDS được thiết kế cho IoT, một mô hình được phát triển có khả năng quản lý, phân loại và tương quan với các cảnh báo được tạo.

2.2. Các phương pháp hiện tại được sử dụng cho IDS

Có nhiều phương pháp khác nhau được IDS sử dụng để phát hiện các thay đổi trên hệ thống. Những thay đổi này có thể là các cuộc tấn công bên ngoài hoặc lạm dụng bởi nhân viên nội bộ. Trong số nhiều phương pháp, có bốn phương pháp nổi bật và được sử dụng rộng rãi là dựa trên đặc trưng, dựa trên bất thường, dựa trên phân tích giao thức Stateful và dựa trên sự kết hợp. Hầu hết các hệ thống IDS hiện tại đều sử dụng phương pháp kết hợp là sự kết hợp của các phương pháp khác để mang lại khả năng phát hiện và ngăn chặn tốt hơn. Tất cả các phương pháp sử dụng cùng một mô hình chung và sự khác

biệt giữa chúng chủ yếu là cách chúng xử lý thông tin thu thập được từ môi trường được giám sát để xác định xem có xảy ra vi phạm chính sách đã đặt hay không. Hình 2.1 thể hiện một kiến trúc chung mà các hệ thống này dựa trên. Kiến trúc này được phát triển bởi Nhóm công tác phát hiện xâm nhập và có bốn khối chức năng, khối Sự kiện (Event Block) là tập hợp các sự kiện đến từ hệ thống được giám sát và sẽ được phân tích bởi các khối khác, sau đó là khối Cơ sở dữ liệu (Database Block) là cơ sở dữ liệu lưu trữ các sự kiện từ các khối Sự kiện, sau đó là các khối Phân tích (Analysis Block) xử lý các sự kiện và gửi cảnh báo.



Hình 2.1. Kiến trúc chung của hệ thống phát hiện xâm nhập

2.2.1. Phương pháp dựa trên bất thường

Phương pháp dựa trên sự bất thường hoạt động bằng cách so sánh hoạt động được quan sát với hồ sơ cơ sở. Hồ sơ cơ sở là hành vi an toàn đã học được của hệ thống, được giám sát và được phát triển trong giai đoạn đào tạo khi IDS tìm hiểu môi trường và phát triển hồ sơ an toàn của hệ thống được giám sát. Môi trường này có thể là mạng, người dùng, hệ thống, v.v.

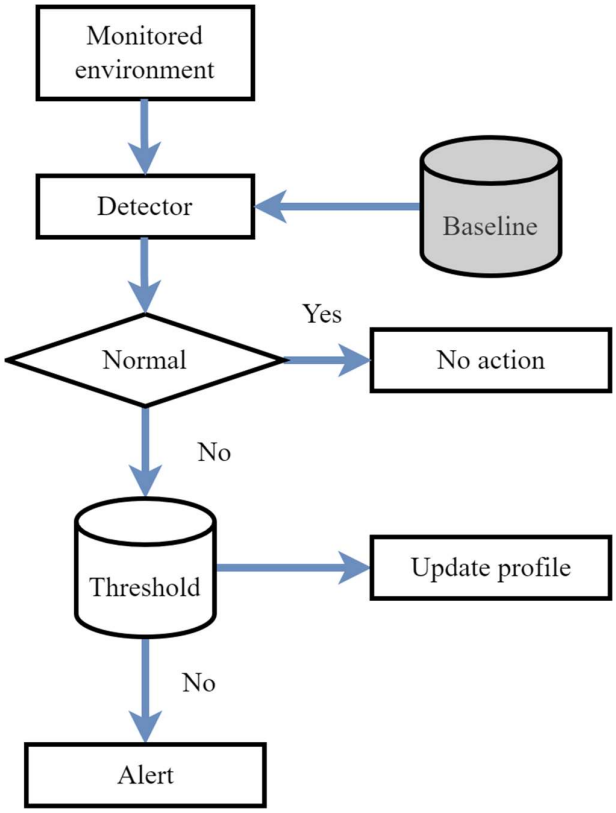
Hồ sơ có thể cố định hoặc động. Cấu hình cố định không thay đổi sau khi được thiết lập trong khi cấu hình động thay đổi khi hệ thống được giám sát phát triển. Một cấu hình động bổ sung thêm vào hệ thống khi IDS tiếp tục cập nhật cấu hình, điều này cũng mở ra khả năng trốn tránh. Kẻ tấn công có thể trốn tránh IDS sử dụng cấu hình động bằng cách lan truyền cuộc tấn công trong một khoảng thời gian dài. Khi làm như vậy, các hành vi của cuộc tấn công của trở thành một phần của hồ sơ vì IDS kết hợp các thay đổi vào hồ sơ khi hệ thống bình thường thay đổi. Sử dụng ngưỡng được xác định trước, bất kỳ sai lệch nào nằm ngoài ngưỡng đều được báo cáo là vi phạm. Một hồ sơ cố định rất hiệu quả trong việc

phát hiện các cuộc tấn công mới vì bất kỳ thay đổi nào so với hành vi bình thường đều được phân loại là bất thường. Các phương pháp dựa trên sự bất thường có thể phát hiện các cuộc tấn công zero-day vào môi trường mà không cần bất kỳ bản cập nhật nào cho hệ thống. Phương pháp phát hiện xâm nhập bất thường sử dụng ba kỹ thuật chung để phát hiện bất thường đó là phát hiện bất thường thống kê, Khai thác tri thức/dữ liệu và dựa trên học máy.

Các kỹ thuật bất thường thống kê được sử dụng để xây dựng hai cấu hình bắt buộc, một trong giai đoạn học tập, sau đó được sử dụng làm cấu hình cơ sở và cấu hình hiện tại được so sánh với cấu hình cơ sở và bất kỳ sự khác biệt nào được đánh dấu là bất thường tùy thuộc vào ngưỡng cài đặt của môi trường được giám sát . Ngưỡng phải được điều chỉnh theo các yêu cầu và hành vi của môi trường được giám sát để hệ thống có hiệu quả.

Kỹ thuật khai thác kiến thức/dữ liệu được sử dụng để tự động hóa các trình giám sát kỹ thuật tìm kiếm các điểm bất thường. Kỹ thuật này tạo ra nhiều kết quả cảnh giả nhất do nhiệm vụ phức tạp là xác định và phân loại chính xác các sự kiện được quan sát trên hệ thống. Kỹ thuật học máy hoạt động bằng cách phân tích các luồng dữ liệu và nó là kỹ thuật được sử dụng rộng rãi.

Kiến trúc chung của một hệ thống IDS dựa trên sự bất thường được thể hiện trong hình 2.2. Môi trường được giám sát được giám sát bởi bộ phát hiện kiểm tra các sự kiện được quan sát dựa trên hồ sơ cơ sở. Nếu các sự kiện được quan sát khớp với đường cơ sở thì không có hành động nào được thực hiện, nhưng nếu nó không khớp với cấu hình đường cơ sở và nằm trong phạm vi ngưỡng chấp nhận được thì cấu hình sẽ được cập nhật. Nếu các sự kiện được quan sát không khớp với hồ sơ cơ sở và nằm ngoài phạm vi ngưỡng thì chúng được đánh dấu là bất thường và cảnh báo sẽ được đưa ra.



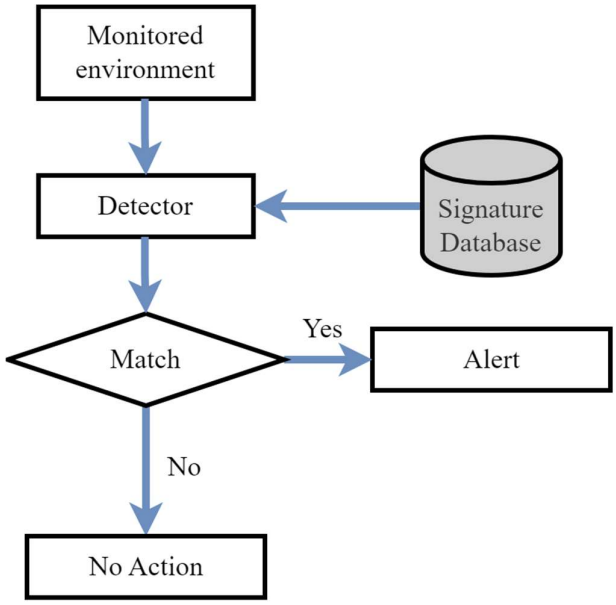
Hình 2.2. Kiến trúc IDS dựa trên bất thường

2.2.2. Phương pháp dựa trên đặc trưng

Phương pháp dựa trên chữ ký hoạt động bằng cách so sánh đặc trưng được quan sát với đặc trưng trong hồ sơ. Tệp này có thể là cơ sở dữ liệu hoặc danh sách các dấu hiệu tấn công đã biết. Bất kỳ đặc trưng nào được quan sát trên môi trường được giám sát khớp với đặc trưng trong tệp đều bị gắn cờ là vi phạm chính sách bảo mật hoặc là một cuộc tấn công. IDS dựa trên đặc trưng có ít chi phí hoạt động vì nó không kiểm tra mọi hoạt động hoặc lưu lượng mạng trên môi trường được giám sát. Thay vào đó, cơ chế sẽ chỉ tìm kiếm các đặc trưng đã biết trong cơ sở dữ liệu hoặc tệp. Không giống như phương pháp dựa trên sự bất thường, hệ thống phương pháp dựa trên đặc trưng rất dễ triển khai vì nó không cần tìm hiểu môi trường. Phương pháp này hoạt động bằng cách đơn giản là tìm kiếm, kiểm tra và so sánh nội dung của các gói mạng để tìm các đặc trưng của các mối đe dọa đã biết. Phương pháp dựa trên đặc trưng rất hiệu quả đối với các cuộc tấn công/vi phạm đã biết nhưng nó không thể phát hiện các cuộc tấn công mới cho đến khi nó được cập nhật với các đặc trưng mới. IDS dựa trên đặc trưng rất dễ trốn tránh vì chúng dựa trên các cuộc tấn công đã biết và phụ thuộc vào các đặc trưng mới được áp dụng trước khi chúng có thể phát hiện các

cuộc tấn công mới. Các hệ thống phát hiện dựa trên đặc trưng có thể dễ dàng bị vượt qua bởi những kẻ tấn công sửa đổi các cuộc tấn công đã biết và các hệ thống đích chưa được cập nhật bằng đặc trưng mới. Phương pháp dựa trên đặc trưng yêu cầu các nguồn lực đáng kể để theo kịp số lượng sửa đổi tiềm ẩn đối với các mối đe dọa đã biết. Phương pháp dựa trên đặc trưng đơn giản hơn để sửa đổi và cải thiện vì hiệu suất của nó chủ yếu dựa trên các đặc trưng hoặc quy tắc được triển khai.

Kiến trúc chung của một phương pháp dựa trên đặc trưng được thể hiện trong Hình 2.3. Kiến trúc này sử dụng bộ phát hiện để tìm và so sánh các chữ ký hoạt động được tìm thấy trong môi trường được giám sát với các chữ ký đã biết trong cơ sở dữ liệu chữ ký. Nếu tìm thấy sự trùng khớp, một cảnh báo sẽ được đưa ra và không có sự trùng khớp nào thì sẽ không có cảnh báo.



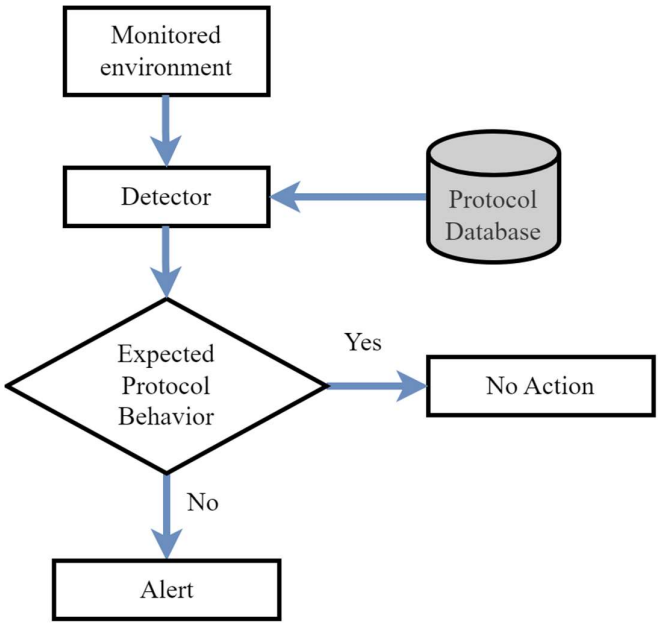
Hình 2.3. Kiến trúc IDS dựa trên đặc trưng

2.2.3. Phương pháp dựa trên phân tích giao thức

Phương pháp phân tích giao thức Stateful hoạt động bằng cách so sánh các cấu hình đã được thiết lập về cách các giao thức nên hoạt động đối với hành vi được quan sát. Các hồ sơ giao thức đã thiết lập được thiết kế và thiết lập bởi các nhà cung cấp. Không giống như phương pháp dựa trên đặc trưng chỉ so sánh hành vi được quan sát với một danh sách, phân tích giao thức Stateful có hiểu biết sâu sắc về cách các giao thức và ứng dụng tương tác và hoạt động. Sự hiểu biết và phân tích sâu này đặt ra một chi phí rất cao cho các hệ

thống. Phân tích giao thức statefull có thể kết hợp và bổ sung tốt cho các phương pháp IDS khác, điều này đã dẫn đến sự phát triển của các phương pháp Hybrid. Sự hiểu biết sâu sắc của phân tích giao thức statefull về cách giao thức hoạt động được sử dụng làm cơ sở để phát triển IDS hiểu hành vi lưu lượng truy cập web và có hiệu quả trong việc bảo vệ các trang web. Mặc dù phân tích giao thức Stateful có hiểu biết sâu sắc về các giao thức được giám sát, nhưng nó có thể dễ dàng tránh được bởi các cuộc tấn công tuân theo và nằm trong hành vi chấp nhận được của các giao thức. Các phương pháp và kỹ thuật phân tích giao thức statefull đã dần được điều chỉnh và tích hợp vào các phương pháp khác trong thập kỷ qua. Điều này đã dẫn đến sự suy giảm của IDS chỉ sử dụng phương pháp phân tích giao thức Stateful.

Kiến trúc chung của phân tích giao thức Stateful được thể hiện trong Hình 2.4. Kiến trúc này giống với kiến trúc của phương pháp dựa trên chữ ký với một ngoại lệ, thay vì cơ sở dữ liệu chữ ký, phân tích giao thức statefull có cơ sở dữ liệu về hành vi giao thức được chấp nhận.

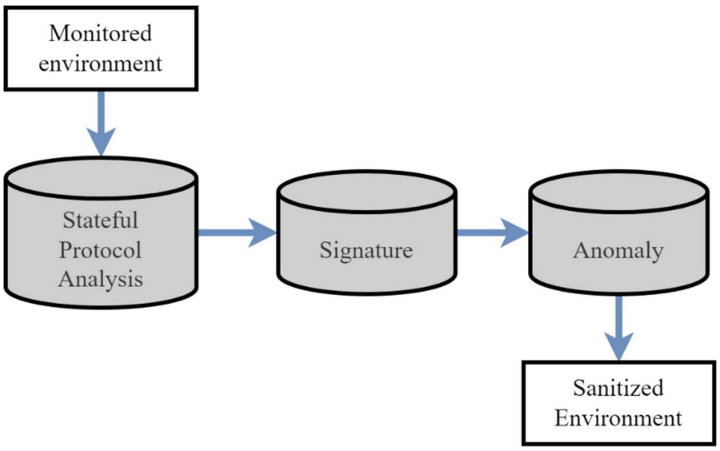


Hình 2.4. Kiến trúc IDS dựa trên phân tích giao thức

2.2.4. Phương pháp kết hợp

Phương pháp dựa trên sự kết hợp hoạt động bằng cách kết hợp hai hoặc nhiều phương pháp khác. Kết quả là một phương pháp tốt hơn tận dụng được thế mạnh của các phương pháp được kết hợp. Prelude là một trong những IDS kết hợp đầu tiên cung cấp

khung dựa trên Định dạng trao đổi thông báo phát hiện xâm nhập (IDMEF), một tiêu chuẩn IETF cho phép các cảm biến khác nhau giao tiếp với nhau. Trong Snort được sửa đổi bằng cách thêm một công cụ dựa trên sự bất thường vào công cụ dựa trên đặc trưng và sau đó hệ thống kết hợp mới được thử nghiệm với Snort thông thường bằng cách sử dụng cùng một dữ liệu thử nghiệm. Hệ thống kết hợp đã phát hiện nhiều xâm nhập hơn so với hệ thống thông thường. Một hệ thống phát hiện xâm nhập kết hợp của các mạng cảm biến không dây dựa trên cụm đã được đề xuất hoạt động bằng cách chia phát hiện thành hai, đầu tiên sử dụng mô hình dựa trên sự bất thường để lọc dữ liệu và sau đó sử dụng mô hình dựa trên đặc trưng để phát hiện các nỗ lực xâm nhập. Tổng quan về một phương pháp dựa trên sự kết hợp được thể hiện trong Hình 2.5, ba phương pháp khác được kết hợp. Môi trường được giám sát được phân tích bằng phương pháp đầu tiên và được chuyển sang phương pháp tiếp theo và sau đó là phương pháp cuối cùng. Điều này tạo ra một hệ thống tốt hơn.



Hình 2.5. Kiến trúc IDS kết hợp

2.3. Các kỹ thuật được sử dụng trong IDS

Trong những năm gần đây, đã có rất nhiều các kỹ thuật được sử dụng để cải thiện sự chính xác của các hệ thống phát hiện xâm nhập. Tuy nhiên các kỹ thuật này có thể được chia thành 4 nhóm chính: học có giám sát (supervised learning), học không giám sát (unsupervised learning), học tăng cường (reinforcement learning), và học sâu (deep learning).

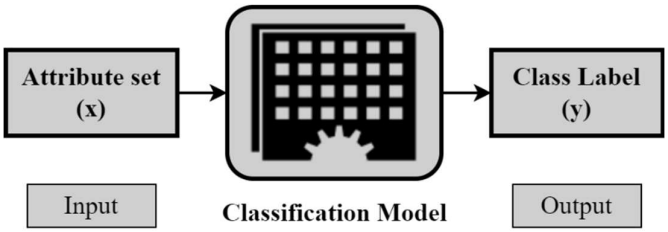
Học có giám sát liên quan đến việc thu thập và kiểm tra mọi biến đầu vào và biến đầu ra, đồng thời sử dụng thuật toán để tìm hiểu hành vi bình thường của người dùng từ đầu vào đến đầu ra. Mục tiêu là ước tính hàm ánh xạ tối ưu để khi một bản ghi đầu vào mới

được thu thập sẽ dự đoán các biến đầu ra cho bản ghi đó. Mặt khác, Học không giám sát cố gắng xác định các hành động được yêu cầu từ dữ liệu hệ thống hiện có, chẳng hạn như thông số kỹ thuật của giao thức và các trường hợp lưu lượng mạng mà bạn chỉ có dữ liệu đầu vào và không có biến đầu ra tương ứng, trong khi các phương pháp học tăng cường cho phép một agent học trong môi trường tương tác bằng cách thử và lỗi bằng cách sử dụng thông tin phản hồi từ các hành động và kinh nghiệm của chính nó. Trong học tăng cường, mục đích là để có được một mô hình hành động phù hợp có thể tối đa hóa tổng phần thưởng tích lũy của agent. Các mô hình học sâu dựa trên mạng nơ-ron nhân tạo, cụ thể là mạng nơ-ron tích chập (CNN). Học máy là quá trình trích xuất kiến thức từ lượng lớn dữ liệu. Các mô hình học máy bao gồm một tập hợp các quy tắc, phương pháp hoặc "các hàm truyền" phức tạp có thể được áp dụng để tìm các mẫu dữ liệu thú vị hoặc để nhận biết hoặc dự đoán hành vi. Các kỹ thuật học máy đã được áp dụng rộng rãi trong lĩnh vực IDS để trích xuất kiến thức từ bộ dữ liệu xâm nhập, các thuật toán và kỹ thuật khác nhau như phân cụm, mạng nơ-ron, quy tắc kết hợp (association rules), cây quyết định (decision tree), thuật toán di truyền (genetic algorithm) và phương pháp lân cận gần nhất (nearest neighbour methods) được sử dụng. Mục đích chính của việc sử dụng các phương pháp học máy là tạo ra các IDS đòi hỏi ít kiến thức của con người hơn và cải thiện độ chính xác. Số lượng IDS sử dụng các kỹ thuật học máy đã tăng lên trong vài năm qua. Mục tiêu chính của IDS dựa trên nghiên cứu máy học là phát hiện các mẫu và xây dựng hệ thống phát hiện xâm nhập dựa trên tập dữ liệu.

2.3.1. Học có giám sát trong hệ thống phát hiện xâm nhập

Kỹ thuật IDS dựa trên học có giám sát phát hiện xâm nhập bằng cách sử dụng dữ liệu đào tạo được dán nhãn. Một cách tiếp cận học tập có giám sát thường bao gồm hai giai đoạn, đó là đào tạo và kiểm tra. Trong giai đoạn đào tạo, các tính năng và lớp có liên quan được xác định và sau đó thuật toán sẽ học từ các mẫu dữ liệu này. Trong IDS học có giám sát, mỗi bản ghi là một cặp, chứa nguồn dữ liệu mạng hoặc máy chủ và giá trị đầu ra tương ứng (tức là nhãn), cụ thể là xâm nhập hoặc bình thường. Tiếp theo, lựa chọn tính năng có thể được áp dụng để loại bỏ các tính năng không cần thiết. Sử dụng dữ liệu đào tạo cho các tính năng đã chọn, kỹ thuật học có giám sát sau đó được sử dụng để đào tạo bộ phân loại để tìm hiểu mối quan hệ cố hữu tồn tại giữa dữ liệu đầu vào và giá trị đầu ra được dán nhãn. Trong giai đoạn thử nghiệm, mô hình được đào tạo được sử dụng để phân loại dữ

liệu chưa biết thành lớp xâm nhập hoặc lớp bình thường. Sau đó, trình phân loại kết quả trở thành một mô hình, được cung cấp một tập hợp các giá trị tính năng, dự đoán lớp mà dữ liệu đầu vào có thể thuộc về. Hình 2.6 cho thấy một cách tiếp cận chung để áp dụng các kỹ thuật phân loại. Hầu hết các IDS hiện có được đề xuất đều được đào tạo theo cách có giám sát. Điều đó có nghĩa rằng các chuyên gia an ninh mạng cần gắn nhãn lưu lượng mạng và thỉnh thoảng sửa đổi mô hình theo cách thủ công.



Hình 2.6. Phân loại theo nhiệm vụ

Có nhiều phương pháp phân loại như decision trees, genetic algorithm, mạng nơ-ron, support vector machines (SVM). Mỗi kỹ thuật sử dụng một phương pháp học để xây dựng một mô hình phân loại. Tuy nhiên, một cách tiếp cận phân loại phù hợp không chỉ xử lý dữ liệu đào tạo mà còn xác định chính xác loại bản ghi mà nó chưa từng thấy trước đây. Tạo ra các mô hình phân lớp có khả năng khái quát hóa đáng tin cậy là nhiệm vụ quan trọng của thuật toán học.

Decision trees có ba thành phần cơ bản. Thành phần đầu tiên là nút quyết định, được sử dụng để xác định thuộc tính kiểm tra. Thứ hai là một nhánh, trong đó mỗi nhánh đại diện cho một quyết định có thể dựa trên giá trị của thuộc tính thử nghiệm. Thứ ba là một lá bao gồm lớp mà mẫu đang xét thuộc về. Có nhiều thuật toán cây quyết định khác nhau, bao gồm ID3, C4.5 và CART.

Giải thuật di truyền (GA) Giải thuật di truyền là một cách tiếp cận heuristic để tối ưu hóa, dựa trên các nguyên tắc tiến hóa. Mỗi giải pháp khả thi được biểu diễn dưới dạng một chuỗi bit (gen) hoặc nhiễm sắc thể và chất lượng của các giải pháp được cải thiện theo thời gian bằng cách áp dụng các toán tử chọn lọc và tái tạo. Khi áp dụng thuật toán di truyền vào bài toán phân loại xâm nhập, thường có hai kiểu mã hóa nhiễm sắc thể: một là theo phân cụm để tạo ra phương pháp mã hóa nhiễm sắc thể nhị phân; một cách khác là chỉ định trung tâm cụm (ma trận nguyên mẫu cụm) bằng một nhiễm sắc thể mã hóa số nguyên. Mọi quy tắc được đại diện bởi một bộ gen và quần thể chính của bộ gen là một số quy tắc

ngẫu nhiên. Mỗi bộ gen bao gồm các gen khác nhau tương ứng với các đặc điểm như nguồn IP, đích IP, cổng nguồn, cổng đích và 1 loại giao thức.

Mạng nơ-ron nhân tạo (ANN) ANN là một trong những phương pháp học máy được áp dụng rộng rãi nhất và đã được chứng minh là thành công trong việc phát hiện các phần mềm độc hại khác nhau. Kỹ thuật học thường xuyên nhất được sử dụng cho học có giám sát là thuật toán lan truyền ngược (BP). Thuật toán BP đánh giá độ dốc của lỗi mạng đối với các trọng số có thể sửa đổi của nó. Tuy nhiên, đối với IDS dựa trên ANN, độ chính xác của việc phát hiện, đặc biệt đối với các cuộc tấn công ít thường xuyên hơn và độ chính xác của việc phát hiện vẫn cần phải được cải thiện. Tập dữ liệu huấn luyện cho các cuộc tấn công ít thường xuyên hơn là nhỏ so với tập dữ liệu của các cuộc tấn công thường xuyên hơn và điều này khiến ANN khó tìm hiểu chính xác các thuộc tính của các cuộc tấn công này. Do đó, độ chính xác phát hiện thấp hơn đối với các cuộc tấn công ít thường xuyên hơn. Trong lĩnh vực bảo mật thông tin, thiệt hại rất lớn có thể xảy ra nếu các cuộc tấn công tần suất thấp không được phát hiện. Chẳng hạn, nếu cuộc tấn công User to Root (U2R) trốn tránh bị phát hiện, tội phạm mạng có thể giành được các đặc quyền của người dùng root và do đó thực hiện các hoạt động độc hại trên hệ thống máy tính của nạn nhân. ANN thường bị cực tiểu cục bộ và do đó việc học có thể trở nên rất tốn thời gian. Điểm mạnh của ANN là với một hoặc nhiều lớp ẩn, nó có thể tạo ra các mô hình phi tuyến tính cao nắm bắt các mối quan hệ phức tạp giữa các thuộc tính đầu vào và nhãn phân loại. Với sự phát triển của nhiều biến thể như NN hồi quy và NN tích chập, ANN là công cụ mạnh mẽ trong nhiều nhiệm vụ phân loại bao gồm cả IDS.

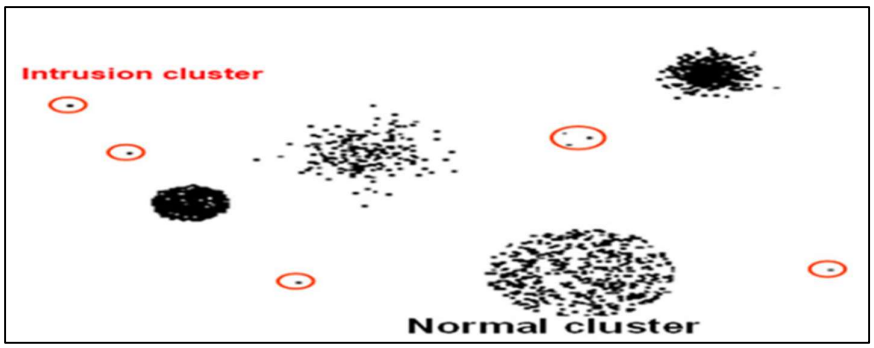
Logic mờ Kỹ thuật này dựa trên mức độ không chắc chắn hơn là logic Boolean đúng hoặc sai. Do đó, kỹ thuật này trình bày một cách đơn giản để đi đến kết luận dựa trên dữ liệu đầu vào không rõ ràng, mơ hồ, không chính xác hoặc bị thiếu. Với một miền mờ, logic mờ cho phép một mẫu dữ liệu có thể thuộc về, có thể một phần, vào nhiều lớp cùng một lúc. Do đó, logic mờ là một công cụ phân loại tốt cho các vấn đề IDS vì bản thân tính bảo mật bao gồm sự mơ hồ và ranh giới giữa trạng thái bình thường và bất thường không được xác định rõ. Ngoài ra, vấn đề phát hiện xâm nhập chứa các tính năng số khác nhau trong dữ liệu được thu thập và một số số liệu thống kê có nguồn gốc. Xây dựng IDS dựa trên dữ liệu số với ngưỡng cứng sẽ tạo ra báo động sai cao. Không thể nhận ra một hoạt động chỉ khác một chút so với mô hình hoặc một thay đổi nhỏ trong hoạt động bình thường

có thể tạo ra báo động sai. Với logic mờ, có thể lập mô hình bất thường nhỏ này để giữ tỷ lệ sai thấp.

Support vector machines (SVM) SVM là bộ phân loại phân biệt được xác định bởi một siêu phẳng phân tách. Các SVM sử dụng chức năng kernel để ánh xạ dữ liệu đào tạo vào một không gian có kích thước cao hơn để sự xâm nhập được phân loại tuyến tính. SVM nổi tiếng với khả năng tổng quát hóa và chủ yếu có giá trị khi số lượng thuộc tính lớn và số lượng điểm dữ liệu nhỏ. Các loại siêu phẳng phân tách khác nhau có thể đạt được bằng cách áp dụng một kernel, chẳng hạn như tuyến tính, đa thức, Hàm cơ sở xuyên tâm Gaussian (RBF) hoặc tiếp tuyến hyperbol. Trong bộ dữ liệu IDS, nhiều tính năng dư thừa hoặc ít ảnh hưởng đến việc phân tách các điểm dữ liệu thành các lớp chính xác. Do đó, việc lựa chọn thuộc tính nên được xem xét trong quá trình đào tạo SVM. SVM cũng có thể được sử dụng để phân loại thành nhiều lớp.

2.3.2. Học không giám sát trong hệ thống phát hiện xâm nhập

Học không giám sát là một loại học máy sử dụng các bộ dữ liệu đầu vào không có nhãn để trích xuất thông tin. Các điểm dữ liệu đầu vào thường được coi là một tập hợp các biến ngẫu nhiên. Sau đó, một mô hình mật độ chung được tạo cho tập dữ liệu. Trong học có giám sát, các nhãn đầu ra được cung cấp và sử dụng để huấn luyện máy nhận được kết quả cần thiết cho một điểm dữ liệu. Ngược lại, trong học tập không giám sát, không có nhãn nào được đưa ra và thay vào đó, dữ liệu được nhóm tự động thành các lớp khác nhau thông qua quá trình học tập. Trong bối cảnh phát triển IDS, phương tiện học tập không giám sát, sử dụng cơ chế xác định xâm nhập bằng cách sử dụng dữ liệu chưa được gắn nhãn để huấn luyện mô hình. Lưu lượng truy cập mạng IoT được nhóm thành các nhóm, dựa trên sự giống nhau của lưu lượng truy cập mà không cần xác định trước các nhóm này.



Hình 2.7. Xử dụng phân cụm để phát hiện xâm nhập

Như được hiển thị trong Hình 2.7, sau khi các điểm dữ liệu được nhóm lại, tất cả các trường hợp xuất hiện trong các cụm nhỏ đều được gắn nhãn là xâm nhập vì các lần xuất hiện bình thường sẽ tạo ra các cụm lớn so với các trường hợp bất thường. Ngoài ra, các cuộc xâm nhập độc hại và các trường hợp bình thường là không giống nhau, do đó chúng không rơi vào một cụm giống hệt nhau.

K-means Kỹ thuật K-means là một trong những kỹ thuật phân tích phân cụm phổ biến nhất nhằm mục đích tách các đối tượng dữ liệu 'n' thành các cụm 'k' trong đó mỗi đối tượng dữ liệu được chọn trong cụm có giá trị trung bình gần nhất. K có nghĩa là nó là một thuật toán phân cụm được thực hiện theo vòng lặp sao cho đạt được giá trị cao nhất sau mỗi lần lặp lại. Đây là một kỹ thuật phân cụm dựa trên khoảng cách và thuật toán này không cần tính toán khoảng cách giữa tất cả các tổ hợp bản ghi. Mà thuật toán này áp dụng một số liệu Euclide như một thước đo tương tự. Số lượng cụm được xác định trước bởi người dùng. Như vậy, thuật toán phân cụm này có thể được sử dụng trong IDS để giảm đặc trưng xâm nhập, tạo đặc trưng chất lượng cao hoặc các nhóm xâm nhập tương tự.

Phân tách giá trị số ít (Singular value decomposition) Đó là một phương pháp phân tách một ma trận thành các ma trận khác dưới dạng một loạt các xấp xỉ tuyến tính biểu diễn cấu trúc ý nghĩa cơ bản của ma trận. Mục tiêu của Phân tách giá trị đơn lẻ là khám phá bộ thuộc tính tối ưu giúp dự đoán tốt nhất việc phát hiện.

Phân tích thành phần độc lập Nó được sử dụng để thể hiện các yếu tố ẩn là nền tảng cho các tập các thuộc tính ngẫu nhiên.

2.3.3. Học tăng cường trong hệ thống phát hiện xâm nhập

Học tăng cường sâu sử dụng các nguyên tắc học sâu và học tăng cường để xây dựng IDS. Học tăng cường liên quan đến một agent tương tác với một môi trường. Agent cố gắng đạt được một mục tiêu nào đó trong môi trường. Mục đích của agent là học cách tương tác với môi trường của nó theo cách cho phép nó đạt được mục tiêu của mình.

Học tăng cường sâu là ứng dụng của học tăng cường để đào tạo mạng lưới nơ-ron sâu. Nó có một lớp đầu vào, một lớp đầu ra và nhiều lớp ẩn giống như các mạng thần kinh sâu trước đây. Tuy nhiên, đầu vào của khi này là trạng thái của môi trường. Ngoài ra, thuật

toán cung cấp tín hiệu phần thưởng của mình vào mạng để có thể học cách liên kết những hành động nào tạo ra kết quả với một trạng thái cụ thể của môi trường.

Mạng Q sâu Đó là sự kết hợp giữa học tăng cường và mạng lưới nơ-ron sâu trên quy mô lớn. Thuật toán được phát triển bằng cách tăng cường thuật toán RL cổ điển có tên là Q-Learning với các mạng nơ-ron sâu.

Double Q-learning Đó là một thuật toán học tăng cường ngoài chính sách, sử dụng ước tính kép để chống lại các vấn đề với Q-learning truyền thống.

2.3.4. Học sâu trong hệ thống phát hiện xâm nhập

Học sâu là một hình thức học máy trong đó máy tính sử dụng hệ thống phân cấp dữ liệu dựa trên kinh nghiệm và tạo thành nhiều lớp làm đầu ra. Học sâu có thể được giám sát cũng như không được giám sát. Trong trường hợp học sâu có giám sát, dữ liệu có thể được phân loại trong khi trong trường hợp học sâu không giám sát, các mẫu dữ liệu được phân tích. Học sâu có liên quan trực tiếp đến trí tuệ nhân tạo, nơi máy móc sẽ tiếp thu kiến thức bằng cách học hỏi kinh nghiệm và sẽ thay thế trí thông minh của con người. Học sâu hoạt động trên nền tảng mạng nơ-ron nhân tạo bằng cách nghiên cứu lượng dữ liệu khổng lồ với sự trợ giúp của các thuật toán được chuẩn bị bởi con người. Nó được gọi là "học sâu" vì các mạng lưới nơ-ron nhân tạo sở hữu các lớp sâu khác nhau cho phép chúng học hỏi.

Trong các mạng nơ-ron, mỗi nút của mỗi lớp ẩn đơn sẽ tính toán các giá trị có trọng số nhận được từ lớp trước và chuyển các giá trị đầu ra cho lớp tiếp theo. Giá trị kết quả của lớp cuối cùng có thể được coi là kết quả cuối cùng mà mạng thần kinh đạt được từ dữ liệu thô.

Mạng nơ ron được kết nối đầy đủ (FCNN) Mạng nơ ron chuyển tiếp được kết nối đầy đủ là kiến trúc mạng tiêu chuẩn được áp dụng chủ yếu trong các ứng dụng mạng nơ-ron cơ bản. Được kết nối đầy đủ biểu thị rằng một nơ-ron riêng lẻ trong lớp trước đó được liên kết với mọi nơ-ron trong lớp tiếp theo. Feedforward chỉ ra rằng các nơ-ron trong bất kỳ lớp trước nào chỉ được kết nối với các nơ-ron trong lớp tiếp theo. Mạng nơ-ron được kết nối đầy đủ có thể được sử dụng để trích xuất thuộc tính.

Mạng thần kinh hồi quy (RNN) Mạng thần kinh hồi quy có thể hoạt động hiệu quả trên một chuỗi dữ liệu có độ dài đầu vào thay đổi. Điều này có nghĩa là các RNN sử

dụng thông tin về trạng thái trước đó của nó làm đầu vào cho dự đoán hiện tại của chúng và chúng ta có thể lặp lại quy trình này cho một số bước tùy ý cho phép mạng truyền thông tin qua trạng thái ẩn của nó theo thời gian. Về cơ bản, điều này giống như cung cấp cho mạng lưới thần kinh một bộ nhớ ngắn hạn. Tính năng này làm cho RNN rất hiệu quả để làm việc với các chuỗi dữ liệu xảy ra theo thời gian.

Mạng nơ-ron tích chập (CNN) Mạng nơ ron tích chập bao gồm một hoặc nhiều lớp tích chập và sau đó được liên kết bởi một hoặc nhiều lớp được kết nối đầy đủ như trong mạng nơ-ron đa lớp tiêu chuẩn. Mạng nơ-ron tích chập chứa một lớp đầu vào và một lớp đầu ra, cũng như nhiều lớp ẩn. Các lớp ẩn của CNN thường chứa một chuỗi các lớp tích chập. CNN nhận đầu vào 2-D và trừu tượng hóa các thuộc tính thông qua một chuỗi các lớp ẩn. CNN hoạt động tốt hơn khi dựa trên kiến trúc của các mạng nơ-ron thông do được hưởng lợi từ các đặc điểm không gian. Thuộc tính không gian thường được áp dụng cho có thuộc tính lưu lượng lĩnh vực IDS. Khi áp dụng các thuộc tính không gian, lưu lượng mạng được cải tạo thành các ảnh lưu lượng; Theo đó, kỹ thuật phân loại hình ảnh được sử dụng để phân loại các ảnh lưu lượng, từ đó có thể phát hiện lưu lượng xâm nhập.

2.4. Các hướng nghiên cứu trong tương lai

Với sự phức tạp và các đòi hỏi đặc biệt của mạng IoT đối với những hệ thống phát hiện xâm nhập (IDS), sau đây là các hướng cần tiếp tục được nhiên cứu để hoàn thiện khả năng bảo mật tổng thể cho các IDS trong mạng Iot:

- **Tài nguyên hạn chế**: Một thiết bị IoT điển hình có tài nguyên hạn chế như sức mạnh xử lý hạn chế, dung lượng lưu trữ thấp và nguồn pin hạn chế. Trong bối cảnh này, hệ thống phát hiện xâm nhập tiêu tốn tài nguyên sẽ làm cạn kiệt tài nguyên của hệ thống IoT. Do đó, điều quan trọng là phải có một hệ thống phát hiện xâm nhập đáp ứng hai đặc điểm quan trọng: (1) bất kỳ IDS nào không phải chịu chi phí thông tin và tính toán đáng kể, và (2) IDS phải đạt được độ chính xác phát hiện cao. Đặc biệt, việc sử dụng các hệ thống phát hiện dựa trên sự bất thường yêu cầu tài nguyên cao hơn đáng kể so với các hệ thống phát hiện dựa trên đặc trưng, trong khi phải đánh đổi giữa độ chính xác của phát hiện và chi phí chung. Chẳng hạn, phát hiện bất thường đặc biệt hiệu quả đối với các cuộc tấn công chưa biết trước đây, nhưng sẽ gây ra chi phí hoạt động đáng kể. Như vậy cần có sự đánh đổi giữa ba yếu tố quan

trọng (1) độ chính xác phát hiện cao, (2) chi phí hoạt động và (3) bảo vệ quyền riêng tư. Hơn nữa, cần có những nỗ lực chuyên dụng để đưa ra các phương pháp xem xét các hạn chế về tài nguyên chủ yếu tập trung vào mức tiêu thụ năng lượng bất khả tri của tài nguyên và mức tiêu thụ bộ nhớ.

- **Tấn công nhiều giai đoạn**: Một cuộc xâm nhập điển hình thường được thực hiện qua nhiều giai đoạn, mỗi giai đoạn cố gắng khai thác một lỗ hổng cụ thể. Các cuộc tấn công tinh vi như vậy được gọi là tấn công nhiều giai đoạn và là cơ chế phổ biến cho các hệ thống máy tính truyền thống và mới nổi như IoT. Mặc dù các mối đe dọa như vậy đã được điều tra trong các lĩnh vực khác, chẳng hạn như di động, các hệ thống phát hiện hiện có cho IoT chỉ tập trung vào việc phát hiện các mối đe dọa riêng lẻ, không liên quan đến mối quan hệ tiềm ẩn giữa chúng. Tuy nhiên bản chất năng động của các hệ thống IoT cũng là thách thức làm cho việc phát hiện cuộc tấn công nhiều giai đoạn trở nên không đơn giản và đòi hỏi những nỗ lực rõ ràng để giải quyết.

- **Bảo vệ thiết bị**: Một trong những vấn đề cốt lõi liên quan đến bảo mật của hệ thống IoT là bảo mật của thiết bị vì nó thường bị nhà sản xuất bỏ qua. Thiếu sự bảo về ở cấp thiết bị trong các hệ thống như vậy đã dẫn đến các cuộc tấn công bảo mật nghiêm trọng như Mirai botnet vào năm 2016 và các phiên bản mới hơn của nó, chẳng hạn như Brickerbot và Reaper. Để bảo vệ chống lại các mối đe dọa như vậy, các biện pháp bảo mật cấp thiết bị là điều tối quan trọng để có thể bảo vệ các hệ thống IoT.

- **Các cuộc tấn công quy mô lớn**: Với việc áp dụng rộng rãi các hệ thống IoT, số lượng thiết bị IoT đang tăng theo cấp số nhân với một số ước tính dự đoán hơn 50 tỷ thiết bị IoT vào năm 2020. Tác động của sự tăng trưởng này đối với việc bảo mật hệ thống IoT là hai vấn đề lớn; thứ nhất, quy mô khổng lồ khiến các hệ thống IoT trở thành mục tiêu béo bở cho các tác nhân độc hại và thứ hai, nó cũng thể hiện các hệ thống IoT như một nguồn tài nguyên có thể được sử dụng để khởi động một cuộc tấn công quy mô lớn. Một ví dụ về các cuộc tấn công như vậy là các botnet, tức là Mirai botnet và Brickerbot đã khởi chạy Dịch vụ từ chối phân tán (DDoS) làm tổn hại dịch vụ Hệ thống tên miền (DNS). Ngoài ra, do bản chất của các hệ thống IoT, các cuộc tấn công định tuyến thường dễ lây lan, tức là ảnh hưởng đến tất cả các thiết

bị trong LoWPAN. Các cuộc tấn công này đòi hỏi một cách tiếp cận toàn diện để phát hiện xâm nhập có thể giám sát và phát hiện trạng thái của toàn bộ mạng cũng như các thiết bị riêng lẻ.

- **Thử nghiệm và đánh giá hạn chế**: Để đánh giá hiệu quả của các nỗ lực phát hiện xâm nhập, cần có thử nghiệm nghiêm ngặt để tích hợp nhiều khía cạnh của đánh giá. Mặc dù, các thử nghiệm đã được tiến hành để chứng minh tính hiệu quả đối với độ chính xác phát hiện và tỷ lệ dương tính giả, nhưng đánh giá này được thực hiện mà không sử dụng phần mềm hoặc phần cứng mô phỏng thích hợp để sao chép cài đặt IoT ngoài đời thực. Chẳng hạn, một số nỗ lực đã sử dụng bộ dữ liệu KDD 99 trong một môi trường biệt lập để tiến hành thử nghiệm, tuy nhiên, nó có nhiều hạn chế là: (1) bộ dữ liệu KDD 99 không phản ánh chính xác các loại mối đe dọa hiện tại phổ biến đối với IoT các hệ thống và (2) tiến hành đánh giá trong một môi trường biệt lập không tính đến các yếu tố quan trọng như hạn chế về tài nguyên của một thiết bị IoT điển hình. Những thách thức này đòi hỏi những nỗ lực rõ ràng để cải thiện công nghệ tiên tiến nhất liên quan đến việc đánh giá các kế hoạch phát hiện xâm nhập trong các hệ thống IoT.

2.5. Kết luận chương

Trong chương 2, các phương pháp đang được sử dụng cho hệ thống phát hiện xâm nhập IDS để phát hiện ra các cuộc tấn công trong mạng IoT đã được phân loại và phân tích. Các nghiên cứu gần đây chỉ ra có rất nhiều các phương pháp để phát hiện những thay đổi trên hệ thống, tuy nhiên có bốn phương pháp nổi bật được sử dụng nhiều trong việc thiết kế các hệ thống phát hiện xâm nhập trong IoT là phương pháp dựa trên đặc trưng, phương pháp dựa trên sự bất thường, phương pháp dựa trên phân tích giao thức và phương pháp cuối cùng là phương pháp kết hợp. Phương pháp cuối cùng là sự tổng hòa của các phương pháp trên giúp tăng khả năng phát hiện các cuộc tấn công nhắm vào hệ thống. Cùng với đó các kỹ thuật được sử dụng để triển khai các hệ thống phát hiện xâm nhập được cũng đề cập và phân tích. Kỹ thuật được sử dụng nhiều trong các IDS truyền thống là sử dụng các bộ luật, tuy nhiên do lượng thông tin trong các hệ thống IoT là rất lớn nên các kỹ thuật giúp máy tính có thể tự học như học có giám sát, học không giám sát, học tăng cường hoặc học

sâu rất cần thiết. Trong chương 3, kỹ thuật sử dụng Fuzzy để thiết hệ một hệ thống phát hiện xâm nhập sẽ được trình bày và đánh giá.

CHƯƠNG 3: GIẢI PHÁP SỬ DỤNG LOGIC MỜ CHO HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS

3.1. Lý thuyết nền tảng

3.1.1. Tổng quan về Logic mờ

Logic mờ (Fuzzy Logic) là một phần mở rộng của Logic nhị phân được phát triển bởi Lotfi Zadeh trưởng khoa điện tử thuộc trường đại học California, một nhà toán học và logic học người Hà Lan vào năm 1965 dựa trên lý thuyết toán học về các tập mờ, nó là sự tổng quát hoá của lý thuyết tập hợp cổ điển.

Lý thuyết tập mờ đã khái quát hóa hai tập xác định có giá trị thành một hàm thuộc của tập mờ. Chúng được sử dụng để xử lý các khái niệm về sự chính xác một phần cho phép mô hình hóa sự không chắc chắn của ngôn ngữ tự nhiên. Thuật ngữ *ngôn ngữ mờ* được sử dụng để mô tả các trường hợp hoặc tình huống dưới góc nhìn của sự mơ hồ trong ngôn ngữ tự nhiên. Ví dụ với câu: *khi trời rất nhiều mây, trời có thể sẽ mưa,* có các thuật ngữ ngôn ngữ *rất* và *có thể* – mà bộ não con người có thể hiểu được. Các tập mờ, cùng với các hệ thống suy luận mờ, được cung cấp các công cụ để viết phần mềm, cho phép các hệ thống máy tính hiểu các thuật ngữ mơ hồ đó và suy luận với các thuật ngữ này.

Lý thuyết tập mờ cho phép sử dụng các khái niệm ngôn ngữ để biểu diễn các giá trị định lượng. Tiện ích của tập mờ nằm ở khả năng mô hình hóa dữ liệu không chắc chắn hoặc mơ hồ, thường gặp trong cuộc sống thực.

Các hệ thống động phức tạp có thể được mô tả một cách hiệu quả bằng cách sử dụng kỹ thuật mô hình hóa hệ thống mờ.

Khung cơ bản được sử dụng trong cách tiếp cận này liên quan đến việc biểu diễn mối quan hệ được mô hình hóa bằng một tập hợp các luật mờ IF-THEN.

3.1.1.1. Định nghĩa tập mờ

Tập mờ bao gồm một miền diễn ngôn (universe of discourse) và một hàm liên thuộc (membership function) ánh xạ mọi phần tử trong miền diễn ngôn thành một giá trị trong khoảng đóng từ 0 đến 1. Như vậy tập mờ có định nghĩa là giả sử X là miền và $x \in X$ là một phần tử cụ thể của miền X thì tập mờ A được đặc trưng bởi một hàm ánh xạ liên thuộc:

$$\mu_A(x): X \to [0,1] \qquad (1)$$

Vậy nên, với mọi phần tử $x \in X$, $\mu_A(x)$ thể hiện mức độ chắc chắn của phần tử x thuộc tập A. Với tập A là tập 2 giái trị thì $\mu_A(x)$ sẽ có thể là 2 giá trị 0 hoặc 1.

3.1.1.2. Hàm liên thuộc

Hàm thành viên là một biểu diễn hình học về độ liên thuộc của mỗi đầu vào. Hàm được sử dụng để liên kết một mức độ liên thuộc của từng phần tử trong miền của tập mờ tương ứng. Các hàm thành viên của tập mờ có thể có bất kỳ hình dạng hoặc kiểu nào được xác định bởi các chuyên gia trong lĩnh vực mà tập hợp được xác định. Các hàm đó phải thỏa mãn các ràng buộc sau:

- Một hàm liên thuộc phải có cận dưới là 0 và cận trên là 1.
- Với mỗi $x \in X$, $\mu_A(x)$ phải là duy nhất.

Biểu diễn hình học của các hàm liên thuộc có thể bao gồm nhiều hình dạng như:

Hàm hình tam giác, được xác định bởi công thức:

$$\mu_A(x) = \begin{cases} 0 & x < \alpha_{\min} \\ \dfrac{x - \alpha_{\min}}{\beta - \alpha_{\min}} & x \in (\alpha_{\min}, \beta) \\ \dfrac{\alpha_{\max} - x}{\alpha_{\max} - \beta} & x \in (\beta, \alpha_{\max}) \\ 0 & x > \alpha_{\max} \end{cases}$$

Hàm hình thang, được xác định bởi công thức:

$$\mu_A(x) = \begin{cases} 0 & x < \alpha_{\min} \\ \dfrac{x - \alpha_{\min}}{\beta_1 - \alpha_{\min}} & x \in (\alpha_{\min}, \beta_1) \\ \dfrac{\alpha_{\max} - x}{\alpha_{\max} - \beta_2} & x \in (\beta_2, \alpha_{\max}) \\ 0 & x > \alpha_{\max} \end{cases}$$

Hàm liên thuộc Γ , được định nghĩa bởi công thức:

$$\mu_A(x) = \begin{cases} 0 & x < \alpha \\ 1 - e^{\gamma(x-\alpha)^2} & x > \alpha \end{cases}$$

Hàm liên thuộc S, được định nghĩa bởi công thức:

$$\mu_A(x) = \begin{cases} 0 & x < \alpha_{\min} \\ 2\left(\dfrac{x-\alpha_{\min}}{\alpha_{\max}-\alpha_{\min}}\right)^2 & x \in (\alpha_{\min}, \beta) \\ 1 - 2\left(\dfrac{x-\alpha_{\min}}{\alpha_{\max}-\alpha_{\min}}\right)^2 & x \in (\beta, \alpha_{\max}) \\ 0 & x > \alpha_{\max} \end{cases}$$

Hàm logistic, được định nghĩa bởi;

$$\mu_A(x) = 1 / \left(1 + e^{-\gamma x}\right)$$

Hàm Gaussian, được định nghĩa bởi:

$$\mu_A(x) = e^{-\alpha(x-\beta)^2}$$

Nhiệm vụ của chuyên gia trong miền là xác định hàm nắm bắt các đặc điểm của tập mờ để lựa chọn và tùy chỉnh các tham số cho các hàm liên thuộc sao cho tối ưu nhất.

3.1.1.3. Các biến mờ

Trong khi các biến trong toán học thường nhận các giá trị số, thì trong các ứng dụng logic mờ, các biến ngôn ngữ phi số thường được sử dụng để tạo thuận lợi cho việc biểu diễn các quy tắc và sự kiện. Biến mờ cho phép tính toán với các ngôn ngữ thay vì số. Các biến ngôn ngữ là các biến có giá trị là các từ hoặc câu từ ngôn ngữ tự nhiên.

Các biến ngôn ngữ và ngữ nghĩa cho phép dịch ngôn ngữ tự nhiên thành logic hoặc số để cung cấp các công cụ cho việc suy luận gần đúng. Trong ngôn ngữ tự nhiên, danh từ thường được kết hợp với tính từ để lượng hóa những danh từ này. Trong lý thuyết hệ thống mờ, những tính từ này được gọi là ngữ nghĩa (hedges).

3.1.1.4. Các toán tử trong logic mờ

Với logic nhị phân, ta có tập các toán tử truyền thống như AND, OR, NOT. Thì trong logic mờ các toán tử này vẫn được sử dụng, tuy nhiên trong logic mờ sẽ không giới hạn các đầu vào. Các toán tử khi này cần được biểu diễn dưới dạng các hàm cho tất cả các giá trị mờ có thể xảy ra, cụ thể là tất cả các số thực trong khoảng từ 0 đến 1. Với X là miền, A và B là các tập mờ được xác định trên miền X ta có:

Toán tử AND, Nếu A và B là các tập mờ, thì:

$$\mu_{A\cap B}(X) = \min\left(\mu_A(x), \mu_B(x)\right) \quad \forall x \in X$$

Toán tử OR, nếu A và B là hai tập mờ, thì:

$$\mu_{A\cup B}(X) = \max\left(\mu_A(x), \mu_B(x)\right) \quad \forall x \in X$$

Toán tử NOT:

$$\mu_{\bar{A}}(X) = 1 - \mu_A(x) \quad \forall x \in X$$

3.1.1.5. Các luật trong logic mờ

Nói chung, các hành vi mang tính động của một hệ mờ được đặc trưng bởi một tập các luật ngôn ngữ mờ. Các luật này là các câu lệnh if-then liên quan đến các tập mờ, logic mờ và hệ thống suy luận mờ. Các quy tắc này dựa trên kiến thức và kinh nghiệm của một chuyên gia về con người trong lĩnh vực đó. Các luật mờ có dạng tổng quát:

If $\rightarrow$ *[tiền đề (s)]* $\rightarrow$ *then [hệ quả (s)]*

Tiền đề và hệ quả của một luật mờ là các mệnh đề chứa các biến ngôn ngữ. Các phần tiền đề và hệ quả của luật ngôn ngữ có thể tạo thành tổ hợp các tập mờ được kết hợp bằng cách sử dụng các toán tử logic như phép cộng, phép hợp và phép giao. Có hai loại luật mờ chính, luật mờ Mamdani và luật mờ Takagi-Sueno (TS).

Luật mờ Mamdani, có thể được công thức hóa như sau:

IF v_1 *is* S_1 *AND ... AND* v_m *is* S_m*, THEN* z_1 *is* W_1 *AND... AND* z_p *is* W_p

Trong đó v_i,i=1,…M là biến đầu vào thứ i và z_i,i=1,…p là biến đầu ra thứ i. S_i và W_i tương ứng là các tập mờ đầu vào và đầu ra.

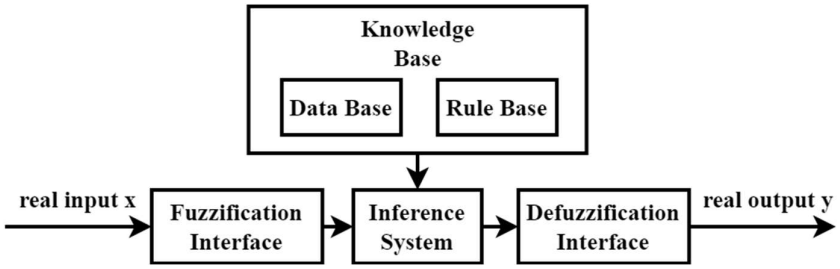
Luật mờ TS, các luật mờ TS sử dụng các phương trình toán học của các biến đầu vào làm phần hệ quả cho luật. Một luật mờ TS chung có thể được biểu diễn như sau:

IF v_1 is S_1 AND ... AND v_m is S_m, THEN $z_1=f_1(v_1,...v_m)$ AND... AND $z_p=f_p(v_1,...v_m)$

Trong đó f_i có thể là các hàm số thực.

3.1.2. Hệ thống suy luận mờ

Hệ thống suy luận mờ FIS được xây dựng dựa trên các kiến thức nền tảng bao gồm các tập mờ và luật mờ. Ngoài ra, hệ thống suy luận mờ còn bao gồm ba thành phần khác, mỗi thành phần thực hiện một nhiệm vụ cụ thể trong quá trình suy luận là mờ hóa (fuzzification), suy luận (inference) và giải mờ (defuzzication), như minh họa trong Hình 3.1.



Hình 3.1. Mô hình chung của hệ thống suy luận mờ

Phần mờ hóa trong hệ thống suy luận mờ là một thủ tục toán học để chuyển đổi một giá trị đầu vào thành một giá trị liên thuộc của tập mờ. Để minh họa, giả sử các tập mờ A B và các hàm thành viên tương ứng đã được xác định. Quá trình mờ hóa nhận đầu vào là a,b $\in$ X với X là không gian các giá trị đầu vào, và chuyển đổi thành các đầu ra là các độ liên thuộc $\mu_A(a)$, $\mu_A(b)$, $\mu_B(a)$, và $\mu_B(b)$.

Cơ chế suy luận cho phép ánh xạ một đầu vào đã cho tới một đầu ra bằng cách sử dụng logic mờ; các hàm liên thuộc, các phép toán logic và các luật if-then. Nó là một quá trình ánh xạ các đầu vào mờ hóa (nhận được từ quá trình mờ hóa) tới cơ sở các luật if-then và để tạo ra một đầu ra mờ cho mỗi quy luật. Nghĩa là, đối với các hệ quả trong không gian đầu ra của luật, mức độ liên thuộc của tập hợp đầu ra sẽ được xác định dựa trên mức độ liên thuộc trong tập hợp đầu vào và mối quan hệ giữa các tập hợp đầu vào. Mối quan hệ giữa các bộ đầu vào được xác định bởi các toán tử logic kết hợp các bộ trong tiền đề. Các tập mờ đầu ra trong hệ quả sau đó được kết hợp để tạo thành một hàm liên thuộc tổng thể

cho đầu ra của luật. Giả sử tập mờ đầu vào A và B với miền ngôn ngữ X1 và tập mờ đầu ra C với X2 là miền ngôn ngữ:

IF A is a AND B is b THEN C is C

Từ quá trình mờ hóa, bộ phận suy luận nhận được các giá trị $\mu_A(a)$ và $\mu_B(a)$. Bước đầu tiên trong quá trình suy luận là tính *firing strength* thông qua sự kết hợp của các tập tiền đề thông qua các toán tử. Với ví dụ ở trên, giá trị *firing strength* sẽ được tính là:

$$min(\mu_A(a), \mu_B(a))$$

Với mỗi luật k, giá trị *firing strength* α_k sẽ được tính bằng cách tương tự. Sau đó, bước tiếp theo là tích lũy và xử lý tất cả các kết quả nhận được. Trong bước này, một giá trị mờ duy nhất được xác định cho mỗi $c_i \in C$. Thông thường, giá trị mờ cuối cùng β_j liên kết với mỗi kết quả c_i được tính toán bằng cách sử dụng toán tử **max**, nghĩa là:

$$\beta_j = \max_{\forall k}(a_{k_i})$$

Kết quả cuối cùng của quá trình suy luận là một loạt các giá trị đầu ra mờ.

Phần giải mờ là một quá trình toán học được sử dụng để chuyển đổi một tập mờ thành số thực. Các tập mờ được tạo ra bởi suy luận mờ trong các luật mờ phải được kết hợp về mặt toán học để tạo ra một số duy nhất làm đầu ra của một hệ mờ. Đối với hệ mờ có nhiều hơn một biến đầu ra, quá trình giải mờ được tính riêng cho từng biến nhưng cách giống nhau. Có nhiều phương pháp giải mờ khác nhau. Tuy nhiên kỹ thuật phổ biến được sử dụng cho quá trình giải mờ đó là phương pháp suy luận Mamdani.

Phương pháp suy luận Mamdani có thể được tóm tắt thành các bước sau:

- Hàm liên thuộc của mỗi tập hợp bị cắt bớt tại giá trị thuộc tương ứng được tìm thấy từ cơ sở luật.
- Các hàm liên thuộc kết quả được cộng lại với nhau dưới dạng hàm OR để hợp nhất chúng thành một vùng mô tả đầu ra.
- Tìm trọng tâm của khu vực hợp nhất làm giá trị đầu ra thực cho hệ thống.

3.1.3. Thuật toán tối ưu TLBO

Các thuật toán heuristic dựa trên quần thể có hai nhóm quan trọng: thuật toán tiến hóa (Evolutionary Algorithm - EA) và thuật toán dựa trên trí thông minh bầy đàn (Swarm Intelligence - SI). Một vài thuật toán tiến hóa như: Genetic Algorithm (GA), Evolution Strategy (ES), Evolution Programming (EP). Một vài thuật toán dựa trên trí thông minh bầy đàn nổi tiếng như: Particle Swarm Optimization (PSO), Shuffled Frog Leaping (SFL), Ant Colony Optimization (ACO), Artificial Bee Colony (ABC).

Tất cả các thuật toán dựa trên tiến hóa và trí thông minh bầy đàn đều là thuật toán xác suất và yêu cầu các tham số kiểm soát chung như quy mô dân số, số thế hệ, v.v. Bên cạnh các tham số điều khiển chung, các thuật toán khác nhau còn yêu cầu các tham số điều khiển dành riêng cho mỗi thuật toán. Ví dụ, GA sử dụng xác suất đột biến, xác suất đan xen, toán tử lựa chọn; PSO sử dụng tham số quán tính, các tham số xã hội và nhận thức; ABC sử dụng số lượng ong quan sát, ong thợ, ong trinh sát và giới hạn; Thuật toán HS sử dụng tốc độ xem xét bộ nhớ hòa âm, tốc độ điều chỉnh cao độ và số lượng ứng biến. Tương tự, các thuật toán khác như ES, EP, DE, SFL, ACO, FF, CSO, AIA, GSA, BBO, FPA, ALO, IWO, v.v. cần điều chỉnh các tham số cụ thể của thuật toán tương ứng. Việc điều chỉnh phù hợp các tham số dành riêng cho thuật toán là một yếu tố rất quan trọng ảnh hưởng đến hiệu suất của các thuật toán đã đề cập ở trên. Việc điều chỉnh không đúng các tham số dành riêng cho thuật toán hoặc làm tăng chi phí tính toán hoặc mắc kẹt tại các giải pháp tối ưu cục bộ. Trước thực tế đó, Rao et al. (2011) đã giới thiệu thuật toán tối ưu hóa dựa trên dạy-học (TLBO) không yêu cầu bất kỳ tham số riêng nào. Thuật toán TLBO chỉ yêu cầu các tham số kiểm soát chung như quy mô dân số và số thế hệ để hoạt động.

Thuật toán TLBO là một thuật toán lấy cảm hứng từ quá trình dạy-học và dựa trên tác động ảnh hưởng của giáo viên đến đầu ra của học viên trong một lớp học. Thuật toán mô tả hai chế độ học tập cơ bản: (i) thông qua giáo viên (được gọi là giai đoạn giáo viên) và (ii) thông qua tương tác với những học viên khác (được gọi là giai đoạn học viên). Trong thuật toán tối ưu hóa này, một nhóm học viên được coi là dân số và các môn học khác nhau được cung cấp cho học viên được coi là các biến thiết kế khác nhau của bài toán tối ưu hóa và kết quả của học viên tương tự như giá trị 'độ phù hợp' của bài toán tối ưu hóa.

Giải pháp tốt nhất trong toàn dân được coi là giáo viên. Các biến thiết kế thực chất là các tham số tham gia vào hàm mục tiêu của bài toán tối ưu đã cho và lời giải tốt nhất chính là giá trị tốt nhất của hàm mục tiêu.

3.1.3.1. Giai đoạn giáo viên

Đây là phần đầu tiên của thuật toán, trong giai đoạn này học viên sẽ học thông qua giáo viên. Trong giai đoạn này, giáo viên cố gắng nâng cao kết quả trung bình của cả lớp về môn học do mình giảng dạy tùy thuộc vào khả năng của mình. Tại mỗi lần lặp i, giả sử rằng có m môn học (tức là các biến thiết kế), n học viên (tức là quy mô dân số là k=1,2,…,n) và $M_{j,i}$ là kết quả trung bình của học viên trong một môn học cụ thể j (j=1,2,…,m), Kết quả tổng thể tốt nhất $X_{total\text{-}kbest,i}$ trên tất cả các môn học cùng nhau đạt được trong toàn bộ học viên, có thể được coi là kết quả tốt nhất học viên *kbest*. Tuy nhiên, vì giáo viên thường được coi là người có học thức cao, người đào tạo học viên để họ có kết quả tốt hơn, nên học viên giỏi nhất được thuật toán xác định là giáo viên. Sự khác biệt giữa kết quả trung bình hiện có của từng môn học và kết quả tương ứng của giáo viên cho từng môn học được cho bởi:

$$Difference\_Mean_{j,k,i} = r_i \left(X_{j,kbest,i} - T_F M_{j,i}\right) \qquad (1)$$

Trong đó, $X_{j,kbest,i}$ là kết quả của học viên giỏi nhất môn j. T_F là hệ số giảng dạy quyết định giá trị trung bình bị thay đổi và r_i là số ngẫu nhiên trong khoảng [0, 1]. Giá trị của T_F có thể là 1 hoặc 2. Giá trị của TF được quyết định ngẫu nhiên với xác suất bằng nhau,

$$T_F = round\,[1+rand\,(0,1)\{2-1\}] \qquad (2)$$

T_F không phải là một tham số của thuật toán TLBO. Giá trị của TF không được cung cấp làm đầu vào cho thuật toán và giá trị của nó được quyết định ngẫu nhiên bởi thuật toán sử dụng biểu thức (2). Sau khi tiến hành một số thử nghiệm trên nhiều hàm chuẩn, người ta kết luận rằng thuật toán hoạt động tốt hơn nếu giá trị của T_F nằm trong khoảng từ 1 đến 2. Tuy nhiên, thuật toán được cho là hoạt động tốt hơn nhiều nếu giá trị của TF là 1 hoặc 2 và do đó để đơn giản hóa thuật toán, hệ số giảng dạy được đề xuất lấy 1 hoặc 2 tùy thuộc vào tiêu chí làm tròn do biểu thức (2) đưa ra. Dựa trên $Difference\_Mean_{j,k,i}$, giải pháp hiện tại được cập nhật trong giai đoạn giáo viên theo biểu thức sau.

$$X'_{j,k,i} = X_{j,k,i} + \text{Difference\_Mean}_{j,k,i}$$

Trong đó, $X'_{j,k,i}$ là giá trị cập nhật của $X_{j,k,i}$. $X'_{j,k,i}$ được chấp nhận nếu nó mang lại giá trị chức năng tốt hơn. Tất cả các giá trị chức năng được chấp nhận ở cuối giai đoạn giáo viên được duy trì và các giá trị này trở thành đầu vào cho giai đoạn học viên.

3.1.3.2. Giai đoạn học viên

Đây là phần thứ hai của thuật toán nơi học viên nâng cao kiến thức của họ bằng cách tương tác với nhau. Một học viên tương tác ngẫu nhiên với những học viên khác để nâng cao kiến thức của mình. Một học viên sẽ học được những điều mới nếu học viên kia có nhiều kiến thức hơn họ. Xem xét quy mô dân số là n, quá trình học tập của giai đoạn này được giải thích như sau:

Chọn ngẫu nhiên hai học viên P và Q sao cho $X'_{\text{total-P,i}} \neq X'_{\text{total-Q,i}}$ (trong đó $X'_{\text{total-P,i}}$ và $X'_{\text{total-Q,i}}$ là các giá trị hàm cập nhật của $X_{\text{total- P,i}}$ và $X_{\text{total-Q,i}}$ tương ứng của P và Q khi kết thúc giai đoạn giáo viên)

$$X''_{j,P,i} = X'_{j,P,i} + r_i\,(X'_{j,P,i} - X'_{j,Q,i}), \text{ If } X'_{\text{total-P,i}} < X'_{\text{total-Q,i}}$$

$$X''_{j,P,i} = X'_{j,P,i} + r_i\,(X'_{j,Q,i} - X'_{j,P,i}), \text{ If } X'_{\text{total-Q,I}} < X'_{\text{total-P,i}}$$

$X''_{j,P,i}$ được chấp nhận nếu nó cho giá trị hàm mục tiêu tốt hơn.

3.1.4. Tập dữ liệu Iot-23

Tập dữ liệu IoT-23 là một tập dữ liệu do phòng thí nghiệm Avast AIC tạo ra. Bộ dữ liệu chứa 20 bản ghi của các phần mềm độc hại từ các thiết bị IoT khác nhau và 3 bản ghi cho các bất thường lành tính. Dữ liệu được thu thập với sự hợp tác của Đại học Kỹ thuật Séc ở Praha, với dữ liệu được thu thập từ năm 2018 đến 2019. Tập dữ liệu ở dạng hoàn chỉnh chứa: tệp .pcap, là tệp dữ liệu mạng ban đầu; tệp conn.log.labeled, được tạo bằng cách chạy trình phân tích mạng có tên Zeek.

Do thực tế là làm việc sử dụng các tệp conn.log.labeled sẽ dễ dàng hơn nên dữ liệu để đánh giá mô hình được đề xuất sẽ được trích xuất từ những tệp này. Các tệp .pcap được tạo bởi chương trình thu thập mạng Wireshark và chỉ có thể được mở bằng chương trình này, việc làm việc với các tệp này tỏ ra khó khăn không cần thiết đối với dự án này, vì vậy chúng đã bị loại bỏ. Cách tiếp cận này dường như cũng được những người tạo tập dữ liệu

chấp nhận, cung cấp hai tùy chọn tải xuống là phiên bản hoàn chỉnh chứa tất cả tệp được trình bày ở trên và phiên bản nhẹ hơn, chỉ chứa tệp conn.log.có nhãn và thông tin. Phiên bản sau đã được chọn cho dự án này.

Tập dữ liệu chứa tổng cộng 325.307.990 bản ghi, trong đó 294.449.255 là độc hại. Tập dữ liệu chứa các loại tấn công sau: Attack, C&C, C&C- FileDownload, C&C- Mirai, C&C- Torii, DDoS, C&C- HeartBeat, C&C- HeartBeat -Attack, C&C- HeartBeat – FileDownload, C&CpartOfAHorizontalPortScan, Okiru, OkiruAttack, PartOfA-HorizontalPortScan, PartOfAHorizontalPortScan-Attack và luồng dữ liệu an toàn Benign.

Mỗi tệp conn.log.labelled chứa 23 cột thuộc tính như được trình bày trong bảng 3.1.

Cột	**Mô tả**	**Kiểu dữ liệu**	**Cột**	**Mô tả**	**Kiểu dữ liệu**
ts	Thời gian thực giám sát	Int	local_orig	Khi kết nối là cục bộ	Bool
uid	ID của giám sát	Str	local_resp	Khi phản hồi là cục bộ	Bool
id_orig.h	Địa chỉ IP tấn công	Str	missed_bytes	Số byte bị mất mát	Int
id_orig.p	Công được dùng trên thiết bị phản hồi	Int	history	Lịch sử trạng thái kết nối	Str
id_resp.h	Địa chỉ IP của thiết bị được giám sát	Str	orig_pkts	Số gói tin được gửi tới thiết bị	Int
id_resp.p	Cổng được sử dụng cho phản hồi	Int	orig_ip_bytes	Số byte được gửi tới thiết bị	Int
proto	Giao thức mạng	Str	resp_pkts	Số gói tin được gửi từ thiết bị	Int
service	Giao thức tầng ứng dụng	str	resp_ip_bytes	Số byte được gửi từ thiết bị	Int

duration	Thời gian di chuyển của gói tin	Float	tunnel_parents	Id của kết nối nếu là kết nối đường hầm	Str
orig_bytes	Lượng dữ liệu được gửi tới thiết bị	Int	label	Nhãn của mẫu giám sát	Str
resp_bytes	Lượng dữ liệu được gửi bởi thiết bị	Int	detailed_label	Kiểu tấn công cụ thể	Str
conn_state	Trạng thái kết nối	str	-	-	-

Bảng 3.1. Các loại thông tin trong tập dữ liệu

Cột trạng thái kết nối (conn-state) là một biến dành riêng cho Zeek và biểu thị trạng thái kết nối giữa hai thiết bị. Ví dụ: S0 có nghĩa là một thiết bị đã thử kết nối nhưng phía bên kia không trả lời. Trong tập dữ liệu này, tất cả các giá trị bị thiếu trong bất kỳ mục nhập nào đều được đánh dấu bằng dấu gạch ngang ("-"), ngoại trừ địa chỉ IP, được đánh dấu bằng hai dấu hai chấm ("::").

3.2. Mô hình đề xuất hệ thống phát hiện xâm nhập

3.2.1. Xử lý dữ liệu

Giai đoạn đầu tiên liên quan đến việc xử lý lưu lượng mạng thô. Quá trình này trích xuất các thuộc tính mạng từ tệp conn.log.labeled trong bộ dữ liệu. Các thuộc tính không mang các đặc trưng chung trong tập dữ liệu như *ID flow, timestamp, label, local resp* và *local orig* sẽ bị xóa khỏi tất cả các tập dữ liệu. Sau đó các giá trị *NaN* (Not a Number) được thay thế bởi giá trị 0. Các cột thuộc tính danh định của toàn bộ tập dữ liệu được mã hóa bằng *one-hot encoding*, với mỗi danh định trong tập dữ liệu được biểu thị bằng một chuỗi nhị phân. Sau đó, để loại bỏ sự chênh lệch về giá trị của dữ liệu cũng như để tăng tốc độ tính toán, các cột thuộc tính sẽ được chuẩn hóa về khoảng (-1, 1). Nhãn các kiểu tấn công và an toàn sau đó cũng được mã hóa lần lượt từ 0 đến 4.

Tệp dữ liệu có hai cột loại địa chỉ IPv4, *'id.orig h'* và *'id.resp h'*, mỗi cột chứa giá trị của các địa chỉ IP khác nhau. Thư viện 'ipaddress' được sử dụng để chuyển đổi dữ liệu địa chỉ IPv4 sang định dạng kỹ thuật số làm tiêu chuẩn cho mã hóa địa chỉ IP. Thư viện

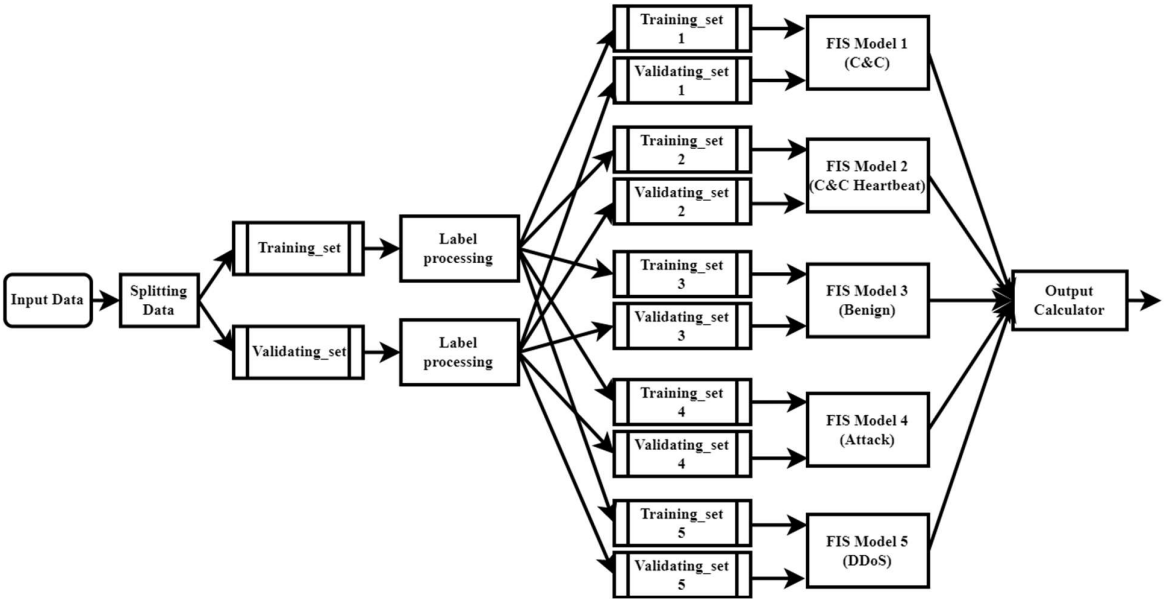
này sẽ chuyển đổi địa chỉ IP sang định dạng kỹ thuật số bằng cách chuyển đổi từng octet thành nhị phân 8 bit và sau đó ghép 4 octet để tạo ra chuỗi nhị phân 32 bit. Và từ hệ nhị phân 32-bit, chúng ta sẽ chuyển ngược lại sang số thập phân.

Việc xử lý dữ liệu bị thiếu được xử lý bằng cách sử dụng giá trị trung bình của từng loại tấn công liên quan đến tính năng đó. Điều này có nghĩa là các giá trị bị thiếu trong cột tính năng sẽ được thay thế bằng giá trị trung bình tương ứng.

Do mô hình được phát triển với mục đích phân loại và phát hiện bốn luồng lưu lượng bị tấn công là C*&C, C&C Hearbeat, Attack, DDos* và một luồng lưu lượng an toàn *Benign* nên sau khi tập dữ liệu được xử lý các mẫu có nhãn như trên sẽ được tách ra để được tập dữ liệu chuẩn sử dụng cho giai đoạn tối ưu và đánh giá hệ thống. Qua thử nghiệm với các tập dữ liệu có số lượng mẫu khác nhau thì để giảm chi phí xử lý cũng như giảm thời gian mô phỏng nhưng vẫn giữ được hiệu năng tối ưu thì mỗi kiểu tấn công và an toàn sẽ có tổng 800 mẫu dữ liệu.

3.2.2. Mô hình được đề xuất

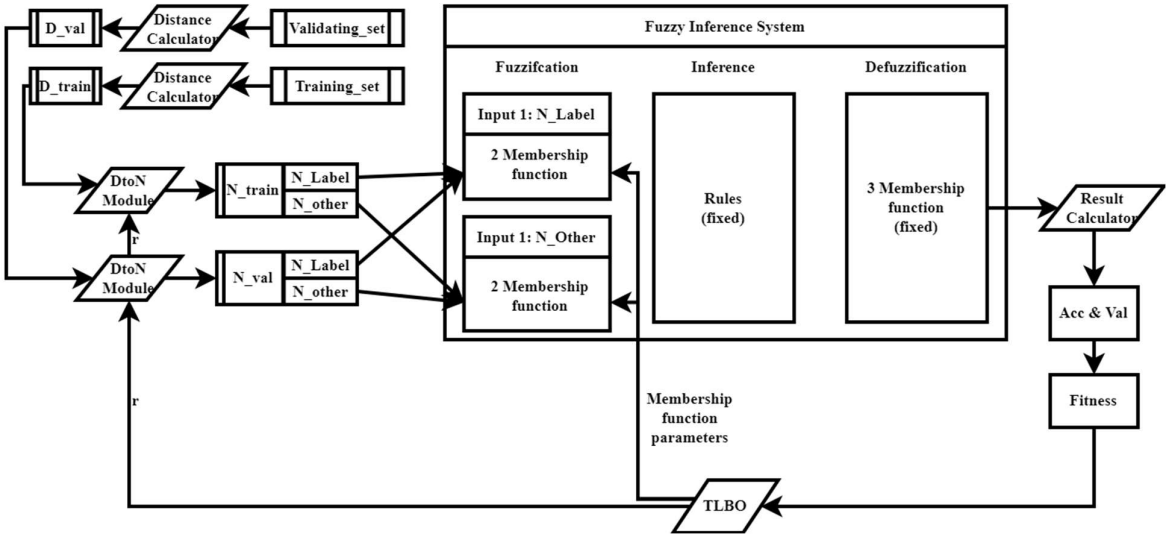
Mô hình hệ thống phát hiện xâm nhập (IDS) đề xuất được xây dựng với mục đích phát hiện bốn kiểu tấn công nghiêm trọng và dữ liệu an toàn có trong tập dữ liệu IoT-23 là*: C&C, C&C Hearbeat, Attack, DDos và Benign*. Ứng với mỗi kiểu tấn công hoặc an toàn là các hệ thống suy luận mờ chuyên dụng được tối ưu riêng biệt để phân loại từng kiểu tấn công hoặc an toàn như được được thể hiện trong Hình 3.2. Với mô hình được đề xuất, dữ liệu sau khi được xử lý tại bước xử lý dữ liệu sẽ được tách thành ba tập dữ liệu là *Trainning_set*, *Validating_set* và *Testing_set* với tỉ lệ lần lượt là 80% - 10% - 10%. Hai tập *Trainning_set* và *Validating_set* được sử dụng trong giai đoạn đào tạo mô hình, còn lại tập Testing_set được sử dụng để đánh giá mô hình sau khi đã qua giai đoạn đào tạo.



Hình 3.2. Kiên trúc của mô hình IDS được đề xuất

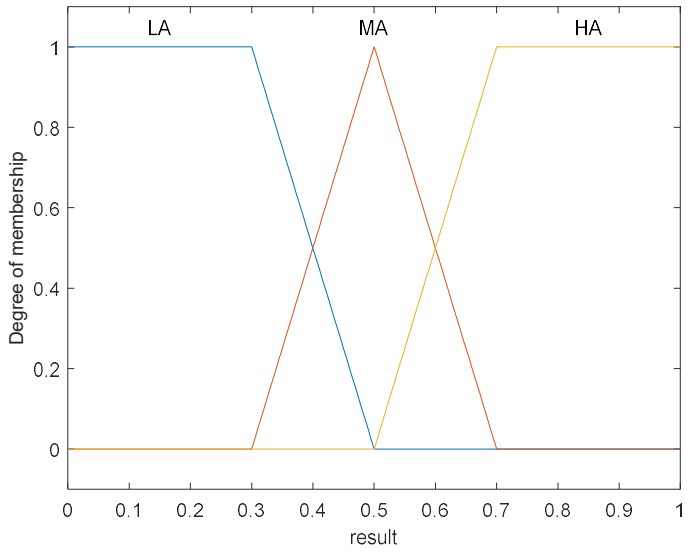
Như được thể hiện trong Hình 3.2, hai tập dữ liệu *Trainning_set* và *Validating_set* trước khi được đưa vào các hệ thống suy luận mờ (FIS) chuyên dụng sẽ được xử lý nhãn sao cho phù hợp với từng hệ thống suy luận mờ. Tại bước này, ứng mới mỗi hệ thống suy luận mờ chuyên dụng hai tập dữ liệu sẽ được điều chỉnh riêng biệt với một phương thức chung: các mẫu dữ liệu trong hai tập dữ liệu có nhãn tương ứng với nhãn mà hệ thống suy luận mờ chuyên dụng muốn phân loại sẽ được mã hóa thành 1, các mẫu dữ liệu có nhãn khác sẽ được mã hóa thành 0. Ví dụ, với hệ thống suy luận mờ chuyên dụng có mục đích phân loại các mẫu có nhãn *C&C* thì trong bước xử lý nhãn, các mẫu dữ liệu trong hai tập Trainning_set và *Validating_set* có nhãn là *C&C* sẽ được mã hóa thành 1, còn lại các mẫu dữ liệu có nhãn là *C&C Hearbeat, Attack, DDos* hoặc *Benign* sẽ được mã hóa thành 0.

Hai tập dữ liệu *Trainning_set* và *Validating_set* sau khi được xử lý nhãn sẽ được đưa vào từng hệ thống suy luận mờ chuyên dụng tương ứng để thực hiện tối ưu các tham số cho các hệ thống suy luận mờ chuyên dụng đó.



Hình 3.3. Kiến trúc tối ưu một hệ thống suy luận mờ chuyên dụng

Đi sâu vào từng hệ thống suy luận mờ chuyên dụng, mỗi hệ thống được cấu tạo từ hệ thống suy luận mờ (FIS) với các tham số được tối ưu một các riêng biệt bằng thuật toán TLBO như được thể hiện trong Hình 3.3. Hệ thống suy luận mờ được triển khai là hệ thống suy luận mờ Mamdani, bao gồm hai đầu vào *N_attack, N_other* và một đầu ra. Mỗi đầu vào có hai hàm liên thuộc L (Low) và H (High). Đầu ra của hệ thống suy luận mờ được sử dụng có ba hàm liên thuộc tương ứng là LA (Low Attack), MA (Medium Attack) và HA (High Attack) được cố định như thể hiện trong Hình 3.4. Bảng 3.2 thể hiện các luật được sử dụng trong miền suy luận của hệ thống.



Hình 3.4. Ba hàm liên thuộc đầu ra của mỗi hệ thống suy luận mờ

N_Benign	N_DDoS	Output
L	L	FA
L	H	HA
H	L	FA
H	H	MA

Bảng 3.2. Hệ luận được sử dụng trong hệ thống suy luận mờ

Mỗi hàm liên thuộc đầu vào trong mỗi hệ thống là các hàm hình thang (Trapezoid) được đặc trưng bởi bốn tham số (a, b, c, d). Tuy nhiên để giảm số lượng tham số cho hệ thống khi tối ưu bốn tham số này sau đó được mã hóa thành 3 tham số (x, y, z) với mối quan hệ được thể hiện như sau:

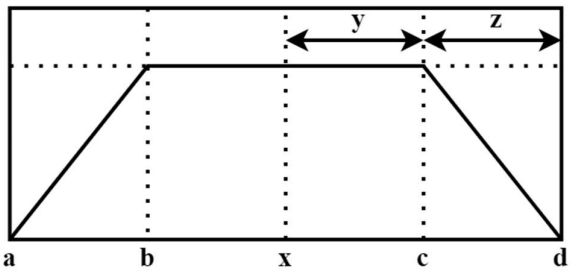
$$a = x - y - z$$

$$b = x - y$$

$$c = x + y$$

$$d = x + y + z$$

Hình 3.5 minh họa cụ thể hơn cho cách mã hóa này.



Hình 3.5. Cách mã hóa tham số

Sau đó ứng với từng hệ thống suy luận mờ chuyên dụng, các tham số của bốn hàm liên thuộc ứng với hai đầu vào sẽ được kết nối lại và kết nối với tham số bán kính r để trở thành cấu trúc của một thành viên cho thuật toán tối ưu TLBO.

Quá trình tối ưu cho cả hệ thống được thực hiện theo hai giai đoạn là Giai đoạn khởi tạo và Giai đoạn tối ưu. Hai giai đoạn này được áp dụng lần lượt cho từng hệ thống suy luận mờ để tối ưu một cách riêng biệt. Các hệ thống suy luận mờ sau khi được tối ưu sẽ

được ghép lại và ghép với bộ xử lý đầu ra để tạo thành hệ thống hoàn chỉnh. Bộ xử lý đầu ra sẽ có nhiệm vụ thu thập đầu ra của năm hệ thống mờ chuyên dụng để tìm ra giá trị lớn nhất từ đó đưa ra đầu ra là giá trị ứng với hệ thống suy luận có đầu ra lớn nhất đó.

3.2.2.1. Giai đoạn khởi tạo

Hai tập dữ liệu Training_set và Validating_set được đưa vào khối tính toán khoảng cách (Distance Calculator). Tại khối này, các điểm dữ liệu trong tập dữ liệu Training_set được sử dụng làm không gian chuẩn để tính khoảng cách. Đối với tập *Traning_set* khi đi vào khối tính toán khoảng cách, từng điểm trong tập này sẽ được tính khoảng cách đến cách điểm trong không gian chuẩn để được ma trận khoảng cách D_train. Tương tự với tập *Validating_set*, khi được đưa vào khối tính toán khoảng cách, mỗi điểm trong tập *Validating_set* sẽ được tính khoảng cách với không gian chuẩn để được ma trận khoảng cách D_val.

Tiếp đó thuật toán TLBO khởi tạo ngẫu nhiên n thành viên với chiều dài của mỗi thành viên là 13 theo cấu trúc là sự kết nối của các tham số của các hàm liên thuộc đầu vào và tham số bán kính r. Các tham số của các hàm liên thuộc đầu vào được khởi tạo trong khoảng từ 0 đến 1, còn bán kính r qua thử nghiệm với các khoảng khởi tạo khác nhau thì hệ thống sẽ đạt được kết quả tốt nhất khi bán kính r được khởi tạo trong khoảng từ 0 đến trung bình khoảng cách trong tập D_train.

Bán kính r sau khi được khởi tạo sẽ cùng với mỗi tập D_train và D_val trở thành đầu vào của bộ *DtoN (DtoN Module).* Tại đây thuật toán sẽ duyệt từng dòng trong ma trận đầu vào và so sánh dữ liệu với bán kính r để tìm ra cách điểm dữ liệu có khoảng cách nhỏ hơn hoặc bằng bán kính r so với điểm đang được xét. Sau đó dựa vào nhãn đã được xử lý của các điểm thuật toán sẽ tính ra tổng số điểm ứng với kiểu tấn công đang xét *N_attack* và tổng số điểm thuộc các kiểu tấn công còn lại *N_other*. Hai giá trị này sau đó được chuẩn hóa về khoảng từ 0 đến 1 để làm đầu vào cho bộ suy luận mờ chuyên dụng.

3.2.2.2. Giai đoạn tối ưu (hình đào tạo)

Mục tiêu của giai đoạn tối ưu là thay đổi giá trị của các tham số và tham số bán kính r bằng thuật toán TLBO theo từng vòng để dần tối thiểu hóa hàm chi phí J đối với từng hệ thống suy luận mờ chuyên dụng. Hàm mục tiêu được sử dụng trong mô hình là:

$$J = \frac{1}{n}\sum_{i=0}^{n}(F(x^{(i)}) - y^{(i)})^2$$

Trong đó: n là tổng số mẫu trong tập đào tạo

$x^{(i)}$ là mẫu thứ i trong tập đào tạo

$y^{(i)}$ là nhãn của mẫu thứ i trong tập đào tạo

$F(x^{(i)})$ là đầu ra dự đoán của hệ thống suy luận mờ chuyên dụng khi đầu vào là mẫu thứ i trong tập đào tạo

Để thực hiện tối thiểu hóa hàm J, giá trị *fitness* được sử dụng để đánh giá các thành viên trong thuật toán TLBO được tính như sau:

$$fitness^{(k)} = \frac{100}{J^{(k)} + 1}$$

Tại vòng đầu tiên, các tham số hàm liên thuộc của hệ thống suy luận mờ sau khi được khởi tạo sẽ được truyền vào các hệ thống suy luận mờ. Sau đó hai đầu vào *N_attack* và *N_other* sẽ được đưa vào để thực hiện tính toán. Trải qua 3 lớp xử lý mờ hóa, suy luận và giải mờ hóa của hệ thống suy luận mờ đầu ra của hệ thống được sử dụng để tính giá trị đánh giá cho các thành viên (tức các trường hợp tối ưu cho hệ thống) theo công thức:

$$fit^{(k)} = \frac{100}{J^{(k)} + 1}$$

Và để đảm bảo cho hệ thống không bị over-fit, tức giá trị fit tăng cao nhưng khả năng phát hiện thực sự của hệ thống lại giảm, giá trị *val* là giá trị *fit* khi đầu vào là các mẫu trong tập *Validating_set* được sử dụng để đánh giá khả năng thực của hệ thống trong quá trình đào tạo. Kết quả tối ưu cuối cùng được chọn là kết quả có giá trị *val* cao nhất.

Giá trị *fit* sau khi được tính cho mỗi thành viên sẽ được đưa về thuật toán TLBO để thực hiện thay đổi theo hai giai đoạn: *Giai đoạn giáo viên* và *Giai đoạn học viên* như đã trình bày trong phần trước để tối ưu dần cho hệ thống sau mỗi vòng lặp.

3.3. Mô phỏng đánh giá

3.3.1. Các tham số đánh giá

Mô hình khi mô phỏng sẽ được đánh giá với cả các tham số riêng cho từng bộ suy luận mờ cũng như cả tham số chung để đánh giá tổng thể cả hệ thống. Các tham số đánh giá riêng bao gồm *accuracy*, *precision*, *recall*, *F1-score* và *False Positive Rate (FPR).* Tham số chung để đánh giá cho toàn hệ thống được sử dụng là độ chính xác *Accuracy*.

Độ chính xác *accuracy* riêng được tính là tỉ lệ của tổng số mẫu dự đoán đúng trên tổng số mẫu của tập dữ liệu đầu vào. Với công thức được biểu diễn như sau:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision được tính là tỉ lệ của tổng các dự đoán dương tính đúng chia cho tổng các dự đoán dương tính đúng và dương tính giả:

$$Precision = \frac{TP}{TP + FP}$$

Recall là tỉ lệ của các dự đoán dương tính đúng chia cho tổng số mẫu dương tính, tức là tổng của các dự đoán dương tính đúng và âm tính giả

$$Recall = \frac{TP}{TP + FN}$$

F1-score là sự kết hợp của hai giá trị *Precision* và *Recall* giúp đánh giá chính xác mô hình sau khi được đào tạo

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Cuối cùng là FPR tức tỉ lệ dương tính giả. FPR được đính là tỉ lệ của tổng số mẫu âm tính, tức là tổng của các mẫu được dự đoán là dương tính giả và âm tính đúng

$$FPR = \frac{FP}{FP + TN}$$

Tương tự với độ chính xác khi tính trên một hệ thống suy luận mờ chuyên dụng, độ chính xác Accuracy chung cho cả mô hình cũng được tính dựa trên tỉ lệ của tổng số lượng mẫu dự đoán đúng từ hệ thống chia cho tổng số mẫu đầu vào.

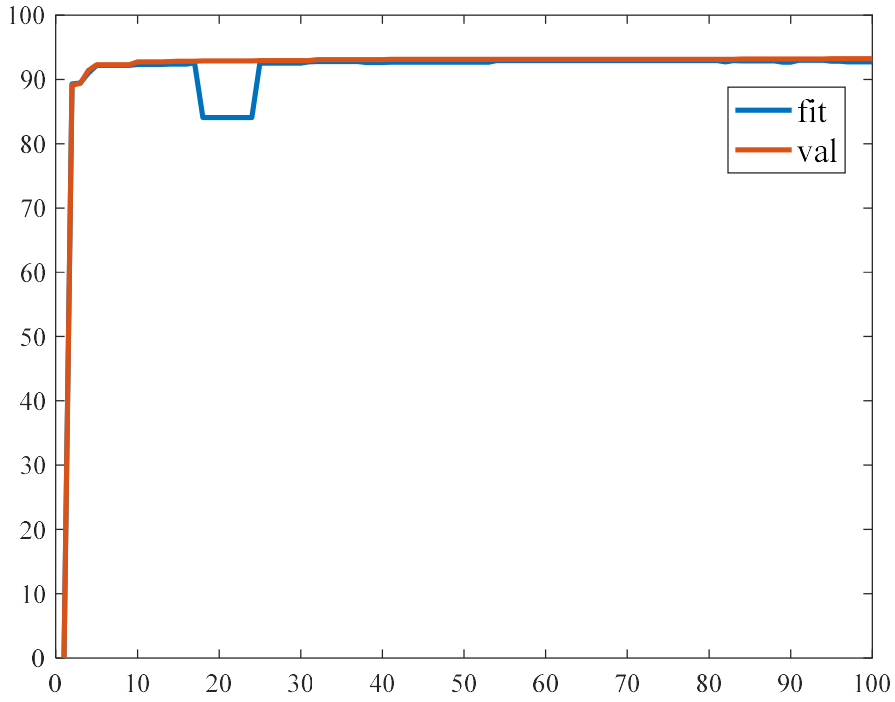
3.3.2. Mô phỏng và kết quả

Toàn bộ các thử nghiệm của mô hình IDS sử dụng các hệ thống suy luận mờ được xây dựng và thực hiện trên Matlab. Hai tập dữ liệu *Traning_set* và *Validating_set* được sử dụng trong quá trình tối ưu mô hình thông qua thuật toán TLBO, sau đó mô hình sẽ được đánh giá qua tập *Testing_set* để thu được kết quả cuối cùng. Các tham số được sử dụng trong mô phỏng được thể hiện trong Bảng 3.3:

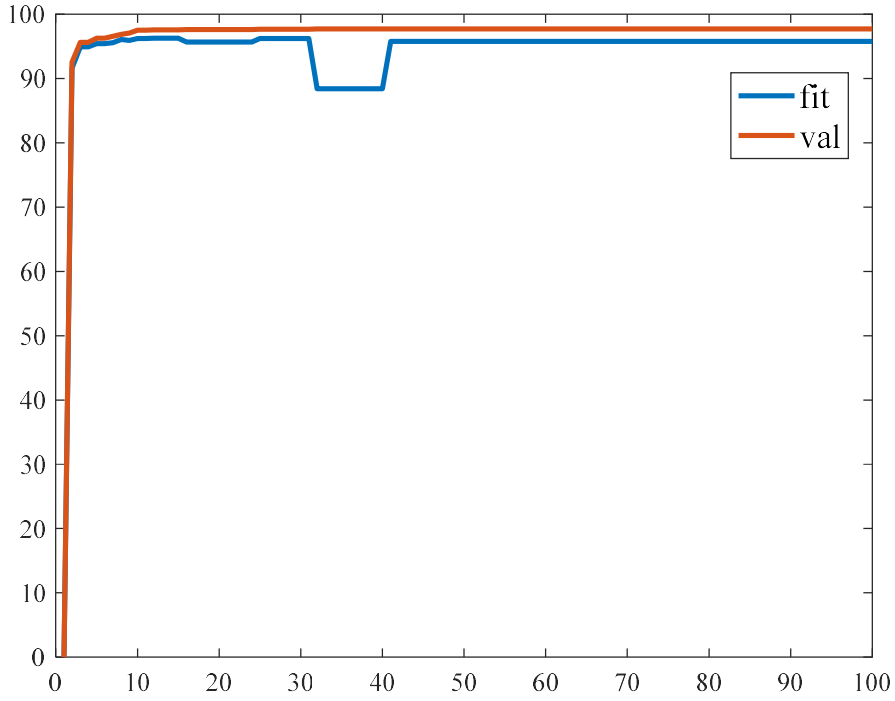
Tham số	**Giá trị**
Số mẫu tập train	3200
Số mẫu tập valid	400
Số mẫu tập test	400
Dân số	50
Chiều dài 1 thành viên	13
Số vòng tối ưu cho mỗi hệ thống	100

Bảng 3.3. Các tham số được sử dụng trong giai đoạn tối ưu

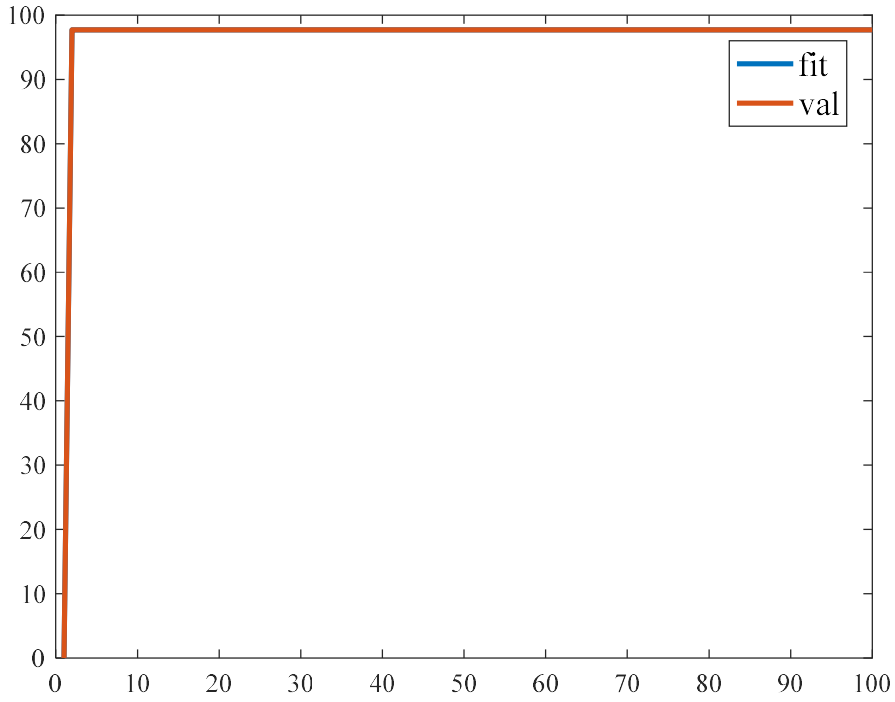
Mô hình sau khi được triển khai và mô phỏng, lần lượt các hệ thống suy luận mờ chuyên dụng sẽ được tối ưu. Hình 3.6-10 thể hiện độ hội tụ trong quá trình tối ưu của từng hệ thống.



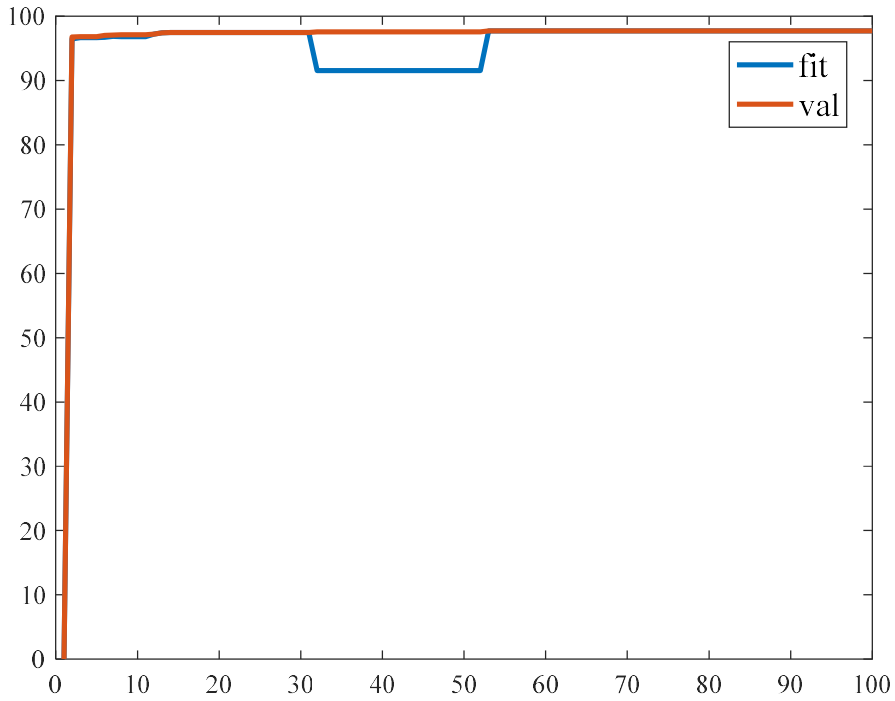
Hình 3.6. Độ hội tụ tối ưu đối với hệ thống suy luận mờ thứ nhất (Benign)



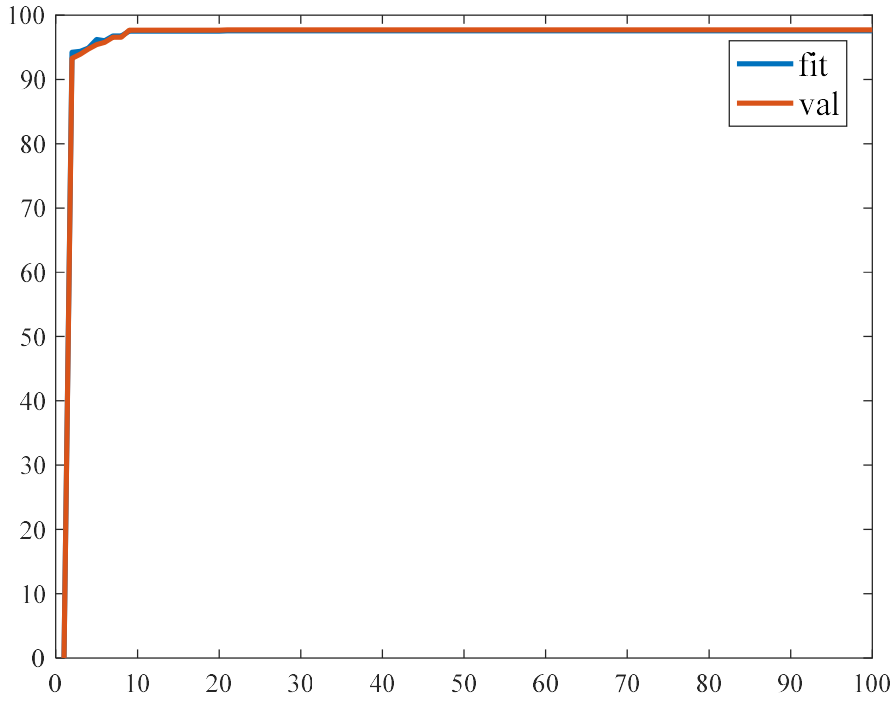
Hình 3.7. Độ hội tụ tối ưu đối với hệ thống suy luận mờ thứ hai (Attack)



Hình 3.8. Độ hội tụ tối ưu đối với hệ thống suy luận mờ thứ ba (C&C)



Hình 3.9. Độ hội tụ tối ưu đối với hệ thống suy luận mờ thứ tư (C&C-HeartBeat)



Hình 3.10. Độ hội tụ tối ưu đối với hệ thống suy luận mờ thứ năm (DDoS)

Sau giai đoạn tối ưu, các hệ thống suy luận mờ chuyên dụng được ghép lại thành một hệ thống hoàn chỉnh và đánh giá trên tập *Testing_set*. Kết quả chung đạt được độ chính xác trên 99%. Điều này chứng tỏ khả năng phát hiện 4 kiểu tấn công và an toàn của mô hình IDS được đề xuất là vượt trội. Đặc biệt khi so sánh với các hệ thống phát hiện xâm nhập hiện tại dựa trên rule thì mô hình IDS được đề xuất có khả năng phát hiện tốt hơn và tỉ lệ cảnh báo sai là rất thấp.

Hệ thống suy luận mờ chuyên dụng	**Accuracy**	**precision**	**recall**	**FPR**	**F1-score**
Benign	0.99	0.96	1	0.0094	0.98
Attack	0.99	1	0.96	0	0.98
C&C	1	1	1	0	1
C&C-HeatBeat	1	1	1	0	1
DDoS	1	1	1	0	1
Accuracy chung	0.9925				

Bảng 3.4. Kết quả đánh giá mô hình IDS được đề xuất

3.4. Kết luận chương

Trong chương 3, một hệ thống phát hiện xâm nhập dựa trên các tiếp cận sử dụng logic mờ đã được trình bày. Mô hình được đề xuất là sự kết hợp của các hệ thống suy luận mờ được tối ưu bằng thuật toán TLBO giúp phân loại và phát hiện 4 kiểu tấn công nghiêm trong trong hệ thống IoT là C*&C, C&C Hearbeat, Attack, DDos* và *Benign*. Mô hình được thiết kế với sự đơn giản và hiệu quả giúp có thể dễ dàng triển khai trong các mạng IoT. Mô hình sau khi đào tạo được đánh giá bằng tập dữ liệu IoT-23 và đã thu được kết quả tốt với khả năng phát hiện chính xác lên đến 99.25% và có tỉ lệ cảnh báo giả là rất thấp so với các hệ thống phát hiện xâm nhập truyền thống.

KẾT LUẬN

Sau một thời gian tìm hiểu, nghiên cứu với sự nỗ lực của bản thân và sự hướng dẫn tận tình của TS. Hoàng Trọng Minh, đề tài "Nghiên cứu giải pháp phát hiện đa tấn công cho hệ thống phát hiện xâm nhập trong mạng IoT sử dụng logic mờ" của sinh viên đã hoàn thành với một số kết quả sau đây.

- Về mặt lý thuyết, đồ án đã trình bày chi tiết các nội dung gồm:
- Tổng quan về mạng IoT và các rủi ro về an ninh mạng;
- Khảo sát các giải pháp cũng như kỹ thuật được được sử dụng để thiết kế và triển khai một hệ thống phát hiện xâm nhập;

Đề xuất một hệ thống phát hiện xâm nhập với hướng tiếp cận sử dụng logic mờ để phân loại và phát hiện luồng an toàn và bốn luồng mạng tấn công nghiệp trong hệ thống IOT;

Về mặt ứng dụng, hệ thống được đề xuất được được mô phỏng thông qua Matlab từ đó thể hiện được khả năng phát hiện chính xác cao khi được đánh giá với tập dữ liệu IoT-23.

Do thời gian nghiên cứu có hạn nên đồ án không thể tránh khỏi những thiếu sót, vì vậy em rất mong nhận được các ý kiến đóng góp từ các thầy cô giáo và các bạn.

Một lần nữa em xin chân thành cảm ơn Thầy giáo TS. Hoàng Trọng Minh cùng các thầy cô giáo, gia đình và bạn bè đã giúp đỡ em trong quá trình thực hiện đồ án.

Em xin chân thành cảm ơn.

TÀI LIỆU THAM KHẢO

1. Parmisano, & Maria Jose Erquiaga. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo.
2. Cherkassky, V. (1998). Fuzzy Inference Systems: A Critical Review. In: Kaynak, O., Zadeh, L.A., Türkşen, B., Rudas, I.J. (eds) Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications. NATO ASI Series, vol 162. Springer, Berlin, Heidelberg.
3. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications. Volume 84. 2017. Pages 25-37
4. Laghari, A.A., Wu, K., Laghari, R.A. et al. A Review and State of Art of Internet of Things (IoT). Arch Computat Methods Eng 29, 1395–1413 (2022).
5. Stoian, N.A. (2020) Machine Learning for anomaly detection in IoT networks : Malware analysis on the IoT-23 data set.
6. Sabri, Naseer. (2013). Fuzzy inference system: Short review and design. Source of the DocumentInternational Review of Automatic Control.
7. D. Mudzingwa and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (IDPS)," 2012 Proceedings of IEEE Southeastcon, 2012, pp. 1-6, doi: 10.1109/SECon.2012.6197080.
8. Thakkar, A., Lohiya, R. A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. Arch Computat Methods Eng 28, 3211–3243 (2021).
9. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, A survey of intrusion detection in Internet of Things, Journal of Network and Computer Applications, Volume 84, 2017, Pages 25-37, ISSN 1084-8045.
10. Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, Computer Networks, Volume 54, Issue 15, 2010, Pages 2787-2805, ISSN 1389-1286.