BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG

KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM

BÁO CÁO ĐỒ ÁN MÔN: BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG

ĐỀ TÀI: NGHIÊN CỨU THUẬT TOÁN BẢO MẬT DỮ LIỆU CHO HỆ THÔNG IOT

Giảng viên hướng dẫn**: ThS. Phạm Trọng Huynh**

Sinh viên thực hiện**: Trần Anh Tuấn: 0850080111**

Nguyễn Thành Đạt: 0850080063

Nguyễn Thị Thanh Nguyệt: 0850080087

Lớp **: 08_ĐH_CNPM**

Khóa**: 2019 - 2023**

TP. Hồ Chí Minh, tháng 05 năm 2023

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG

KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM

BÁO CÁO ĐỒ ÁN MÔN: BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG

ĐỀ TÀI: NGHIÊN CỨU THUẬT TOÁN BẢO MẬT DỮ LIỆU CHO HỆ THÔNG IOT

Giảng viên hướng dẫn**: ThS. Phạm Trọng Huynh**

Sinh viên thực hiện**: Trần Anh Tuấn: 0850080111**

Nguyễn Thành Đạt: 0850080063

Nguyễn Thị Thanh Nguyệt: 0850080087

Lớp **: 08_ĐH_CNPM**

Khóa**: 2019 - 2023**

TP. Hồ Chí Minh, tháng 05 năm 2023

MỞ ĐẦU

Bảo mật dữ liệu đã trở thành một trong những yếu tố quan trọng và không thể thiếu trong hệ thống Internet of Things (IoT) ngày nay. Với sự phát triển nhanh chóng của công nghệ, hệ thống IoT đã trở thành một phần không thể tách rời trong cuộc sống hàng ngày, từ các thiết bị thông minh như điện thoại di động, đèn chiếu sáng, tủ lạnh, đến các hệ thống quản lý thông minh trong các lĩnh vực như y tế, nông nghiệp, và năng lượng.

Tuy nhiên, sự phát triển nhanh chóng của IoT cũng mang đến những thách thức bảo mật ngày càng lớn. Với hàng tỷ thiết bị kết nối với nhau và chia sẻ dữ liệu qua mạng, việc đảm bảo tính riêng tư, toàn vẹn và bảo mật của dữ liệu trở thành một vấn đề đáng lo ngại. Việc thiếu bảo mật dữ liệu có thể dẫn đến những hậu quả nghiêm trọng, từ việc xâm nhập và chiếm quyền kiểm soát hệ thống IoT, đánh cắp thông tin cá nhân, cho đến việc gây hại đến mạng lưới và hoạt động hàng ngày của chúng ta.

Đồ án này tập trung vào nghiên cứu về thuật toán bảo mật dữ liệu cho hệ thống IoT nhằm giải quyết những thách thức bảo mật trên. Chúng tôi tìm hiểu về các phương pháp mã hóa, kiểm tra tính toàn vẹn dữ liệu, và xác thực trong ngữ cảnh của IoT. Đồng thời, chúng tôi cũng tìm hiểu về các phương pháp quản lý khóa và quản lý danh tính để đảm bảo rằng dữ liệu chỉ được truy cập bởi những người được ủy quyền.

Mục tiêu của đồ án là cung cấp một cái nhìn tổng quan về các thuật toán bảo mật dữ liệu cho hệ thống IoT, từ đó giúp đảm bảo an toàn và bảo mật trong việc truyền, lưu trữ và xử lý dữ liệu trong môi trường IoT. Chúng tôi hy vọng rằng báo cáo này sẽ cung cấp cho bạn đọc kiến thức cơ bản và các khía cạnh quan trọng trong việc nghiên cứu và áp dụng thuật toán bảo mật dữ liệu trong hệ thống IoT.

LỜI CẢM ƠN

Trong đồ án môn học này, em muốn gửi lời cảm ơn chân thành đến ThS. Phạm Trọng Huynh - giảng viên hướng dẫn của em.

Thầy đã dành thời gian và công sức để truyền đạt kiến thức và kinh nghiệm cho em trong quá trình thực hiện đồ án môn học. Bằng những chỉ dẫn và nhận xét hết sức quý báu, thầy đã giúp em nắm vững kiến thức và kỹ năng cần thiết để hoàn thành đồ án môn học một cách tốt nhất.

Em rất biết ơn sự giúp đỡ, cổ vũ và động viên của cô suốt thời gian qua. Sự nhiệt tình và tâm huyết của thầy đã truyền cảm hứng cho chúng em để không ngừng cố gắng và phấn đấu trong quá trình học tập và nghiên cứu.

Tuy nhiên, trong quá trình làm đề tài, do kiến thức chuyên môn còn hạn chế của nhóm, chắc chắn sẽ không tránh khỏi những thiếu sót trong việc nêu và đánh giá vấn đề. Chúng em rất mong được sự đóng góp ý kiến, đánh giá của các thầy cô giáo bộ môn để khóa luận của em được hoàn thiện hơn.

Một lần nữa, em xin chân thành cảm ơn ThS. Phạm Trọng Huynh đã giúp đỡ em trong quá trình thực hiện đồ án môn học này.

NHẬN XÉT

(Của giảng viên hướng dẫn)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

TP.Hồ Chí Minh, ngày….tháng….năm….

GIẢNG VIÊN

(ký tên)

MỤC LỤC

DANH MỤC HÌNH

CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI

1.1. Lý do chọn đề tài

Chúng em đã chọn đề tài "Nghiên cứu thuật toán bảo mật dữ liệu cho hệ thống IoT" vì sự quan trọng của việc bảo mật dữ liệu trong môi trường IoT ngày càng gia tăng. Hệ thống IoT đang phát triển với tốc độ nhanh chóng và được áp dụng rộng rãi trong nhiều lĩnh vực, mang lại nhiều lợi ích nhưng cũng đặt ra những thách thức bảo mật đáng kể.

Dữ liệu trong hệ thống IoT chứa thông tin quan trọng và nhạy cảm, bao gồm thông tin cá nhân và dữ liệu kinh doanh. Việc bảo mật dữ liệu là yếu tố quan trọng để đảm bảo tính riêng tư, an toàn và tin cậy. Trong đồ án này, chúng em tập trung nghiên cứu và áp dụng thuật toán Mã hóa đối xứng (AES) để bảo mật dữ liệu trong hệ thống IoT.

Mục tiêu của đồ án là hiểu rõ cơ sở lý thuyết về hệ thống IoT và các thách thức bảo mật liên quan. Chúng em cũng tìm hiểu về nguyên tắc và ứng dụng của thuật toán AES trong bảo mật dữ liệu. Bằng việc áp dụng thuật toán này, chúng em hy vọng tìm ra giải pháp hiệu quả và đáng tin cậy để bảo vệ dữ liệu trong hệ thống IoT.

Qua việc nghiên cứu và thực hiện đồ án này, chúng em hy vọng sẽ có cơ hội nâng cao kiến thức và kỹ năng về bảo mật dữ liệu và ứng dụng của nó trong môi trường IoT. Chúng em mong rằng kết quả nghiên cứu sẽ đóng góp vào sự phát triển của lĩnh vực này, đồng thời mang lại lợi ích cho cộng đồng và người dùng trong việc sử dụng hệ thống IoT một cách an toàn và bảo mật.

1.2. Phạm vi của đề tài

Phạm vi của đề tài "Nghiên cứu thuật toán bảo mật dữ liệu cho hệ thống IoT" tập trung vào việc nghiên cứu và áp dụng thuật toán Mã hóa đối xứng (AES) để bảo mật dữ liệu trong hệ thống IoT. Chúng em hiểu rằng trong thời đại kết nối không dây và sự phát triển mạnh mẽ của Internet of Things (IoT), bảo mật dữ liệu trở thành một yếu tố cực kỳ quan trọng để đảm bảo tính riêng tư, an toàn và tin cậy cho người dùng.

Trước khi tiến hành nghiên cứu, chúng em đã thực hiện một đánh giá sơ bộ về các thách thức bảo mật trong hệ thống IoT. Chúng em nhận thấy rằng việc bảo vệ dữ liệu trong môi trường IoT gặp phải nhiều khó khăn do sự phức tạp của cấu trúc hệ thống, sự đa dạng của các thiết bị và giao thức liên kết. Điều này gây ra rủi ro về việc xâm nhập, mất mát dữ liệu và vi phạm quyền riêng tư.

Vì vậy, chúng em đã quyết định tập trung vào thuật toán Mã hóa đối xứng (AES) để giải quyết vấn đề bảo mật dữ liệu trong hệ thống IoT. AES đã được chứng minh là một thuật toán mã hóa mạnh mẽ, được sử dụng rộng rãi trong các ứng dụng bảo mật. Chúng em hiểu rằng việc áp dụng AES vào hệ thống IoT sẽ giúp tăng cường bảo mật dữ liệu, đảm bảo tính toàn vẹn và bảo mật trong quá trình truyền và lưu trữ.

Trên cơ sở hiểu biết về thuật toán AES, chúng em sẽ thực hiện nghiên cứu chi tiết về nguyên tắc hoạt động và cách thực hiện AES trong môi trường hệ thống IoT. Chúng em cũng sẽ xây dựng một mô hình thử nghiệm để đánh giá hiệu suất và độ an toàn của thuật toán AES trong việc bảo mật dữ liệu IoT.

1.3. Mục đích nghiên cứu

Mục đích chính của nghiên cứu này là tìm hiểu và áp dụng thuật toán Mã hóa đối xứng (AES) để bảo mật dữ liệu trong hệ thống IoT. Cụ thể, chúng em đặt ra các mục tiêu sau:

1. Tìm hiểu về hệ thống IoT và nhận thức về tầm quan trọng của bảo mật dữ liệu: Chúng em muốn hiểu rõ về nguyên lý hoạt động của hệ thống IoT, cấu trúc và các thành phần chính. Đồng thời, chúng em muốn nhận thức sâu sắc về tầm quan trọng của bảo mật dữ liệu trong môi trường IoT, để đảm bảo tính riêng tư, an toàn và tin cậy cho người dùng.

2. Nghiên cứu về thuật toán Mã hóa đối xứng (AES): Chúng em muốn tìm hiểu về nguyên lý hoạt động, cách thực hiện và ứng dụng của thuật toán AES trong bảo mật dữ liệu. Chúng em sẽ nghiên cứu các khối mã hóa, quy trình mã hóa/giải mã và các phương pháp khóa hóa liên quan đến AES.

3. Áp dụng thuật toán AES trong bảo mật dữ liệu IoT: Chúng em muốn xác định cách sử dụng và tích hợp thuật toán AES vào quá trình bảo mật dữ liệu trong các thiết bị và mạng IoT. Chúng em sẽ nghiên cứu các cách áp dụng AES cho việc mã hóa, giải mã và bảo vệ dữ liệu IoT trong quá trình truyền và lưu trữ.

4. Đánh giá hiệu suất và độ an toàn của thuật toán AES trong bảo mật dữ liệu IoT: Chúng em sẽ tiến hành đánh giá hiệu suất và độ an toàn của việc sử dụng thuật toán AES trong bảo mật dữ liệu IoT. Chúng em sẽ đo lường tốc độ mã hóa/giải mã, khả năng chống lại các cuộc tấn công thông thường và đánh giá khả năng mở rộng của thuật toán trong môi trường IoT.

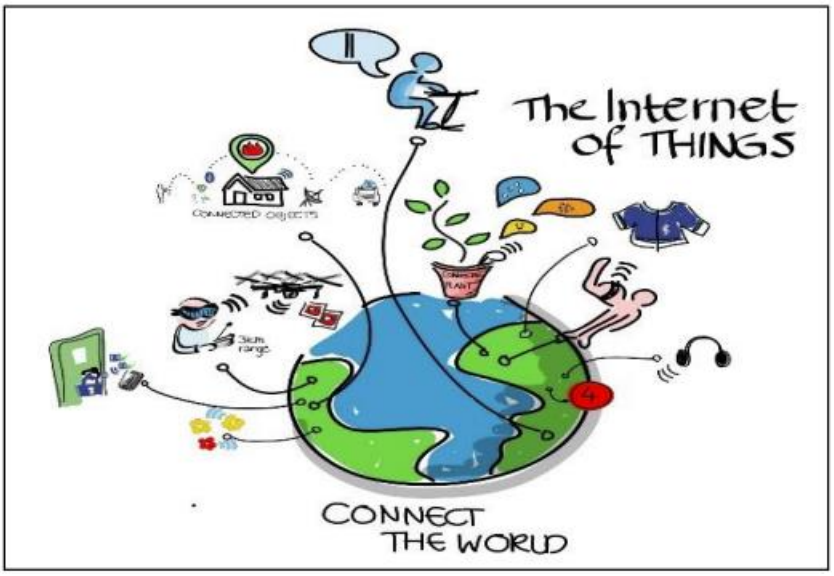
Từ những mục tiêu nghiên cứu trên, chúng em hy vọng rằng đề tài này sẽ đóng góp vào việc nâng cao bảo mật dữ liệu trong hệ thống IoT và cung cấp một phương pháp hiệu quả để bảo vệ dữ liệu trong môi trường kết nối không dây và đa dạng của IoT.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1. Tổng quan về IoT

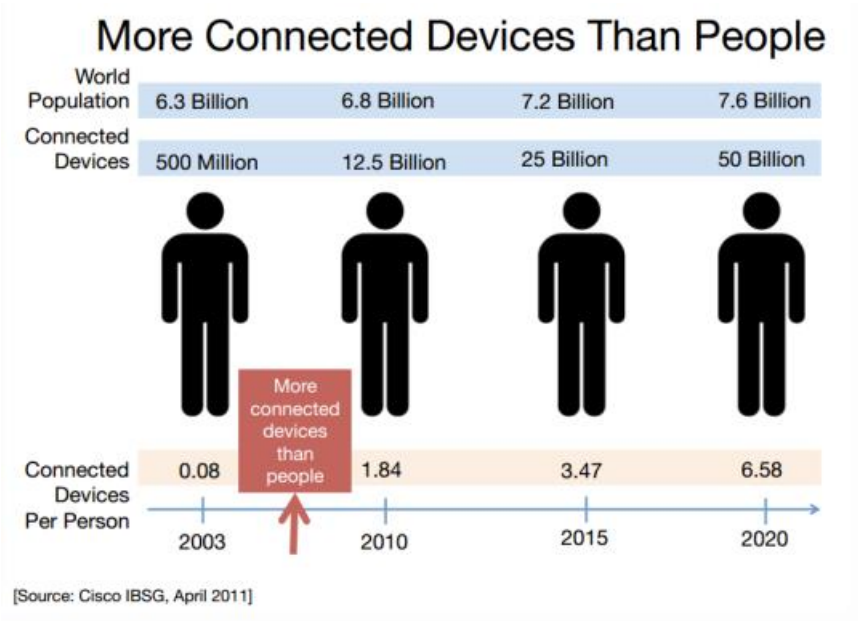
2.1.1 Khái niệm IoT

Internet of Things (IoT) là thuật ngữ dùng để chỉ các đối tượng có thể được nhận biết cũng như sự tồn tại của chúng trong một kiến trúc mang tính kết nối. Đây là một viễn cảnh trong đó mọi vật, mọi con vật hoặc con người được cung cấp các định danh và khả năng tự động truyền tải dữ liệu qua một mạng lưới mà không cần sự tương tác giữa con người-với-con người hoặc con người-với-máy tính. IoT tiến hoá từ sự hội tụ của các công nghệ không dây, hệ thống vi cơ điện tử (MEMS) và Internet. Cụm từ này được đưa ra bởi Kevin Ashton vào năm 1999. Ông là một nhà khoa học đã sáng lập ra Trung tâm Auto-ID ở đại học MIT[1].



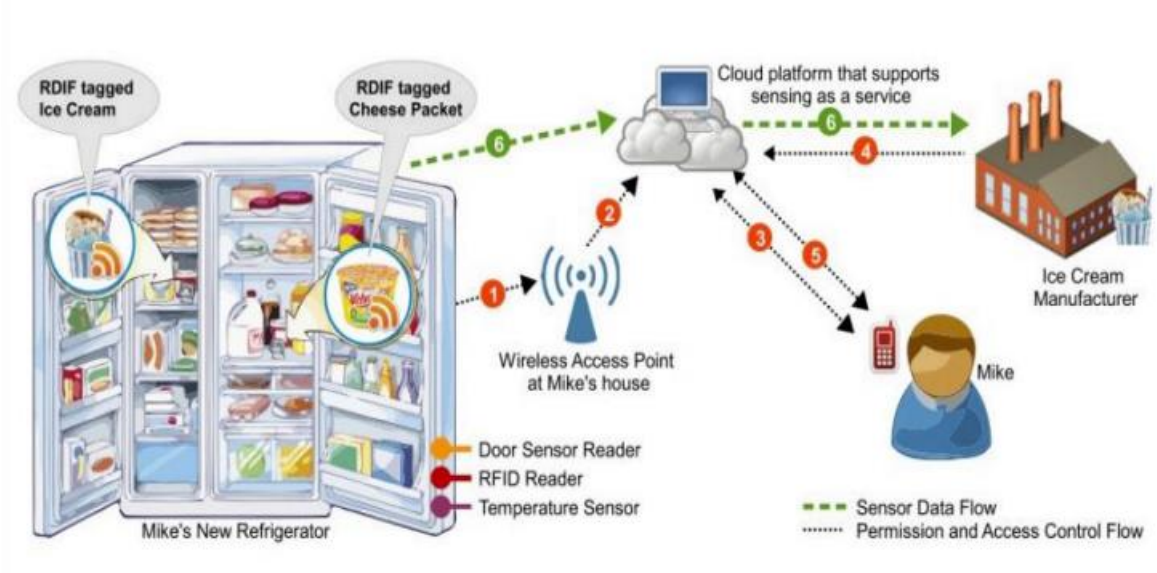
Hình 2. 1: "Internet of Things"

"Thing" - sự vật - trong Internet of Things, có thể là một trang trại động vật với bộ tiếp sóng chip sinh học, một chiếc xe ô tô tích hợp các cảm biến để cảnh báo lái xe khi lốp quá non, hoặc bất kỳ đồ vật nào do tự nhiên sinh ra hoặc do con người sản xuất ra mà có thể được gán với một địa chỉ IP và được cung cấp khả năng truyền tải dữ liệu qua mạng lưới. IoT phải có 2 thuộc tính: một là đó phải là một ứng dụng internet. Hai là, nó phải lấy được thông tin của vật chủ[1].



Hình 2. 2: Sự gia tăng nhanh chóng của giao tiếp máy – máy.

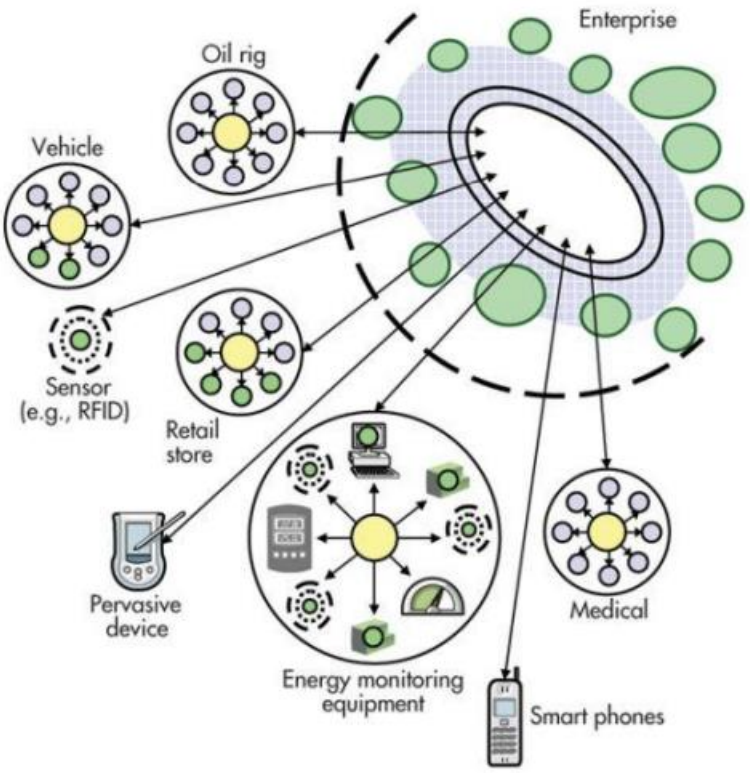
Một ví dụ điển hình cho IoT là tủ lạnh thông minh, nó có thể là một chiếc tủ lạnh bình thường nhưng có gắn thêm các cảm biến bên trong giúp kiểm tra được số lượng các loại thực phẩm có trong tủ lạnh, cảm biến nhiệt độ, cảm biến phát hiện mở cửa,…và các thông tin này được đưa lên internet. Với một danh mục thực phẩm được thiết lập trước bởi người dùng, khi mà một trong các loại thực phẩm đó sắp hết thì nó sẽ thông báo ngay cho chủ nhân nó biết rằng cần phải bổ sung gấp, thậm chí nếu các loại sản phẩm được gắn mã ID thì nó sẽ tự động trực tiếp gửi thông báo cần nhập hàng đến siêu thị và nhân viên siêu thị sẽ gửi loại thực phẩm đó đến tận nhà[2].



Hình 2. 3: Ứng dụng tủ lạnh trong IoT

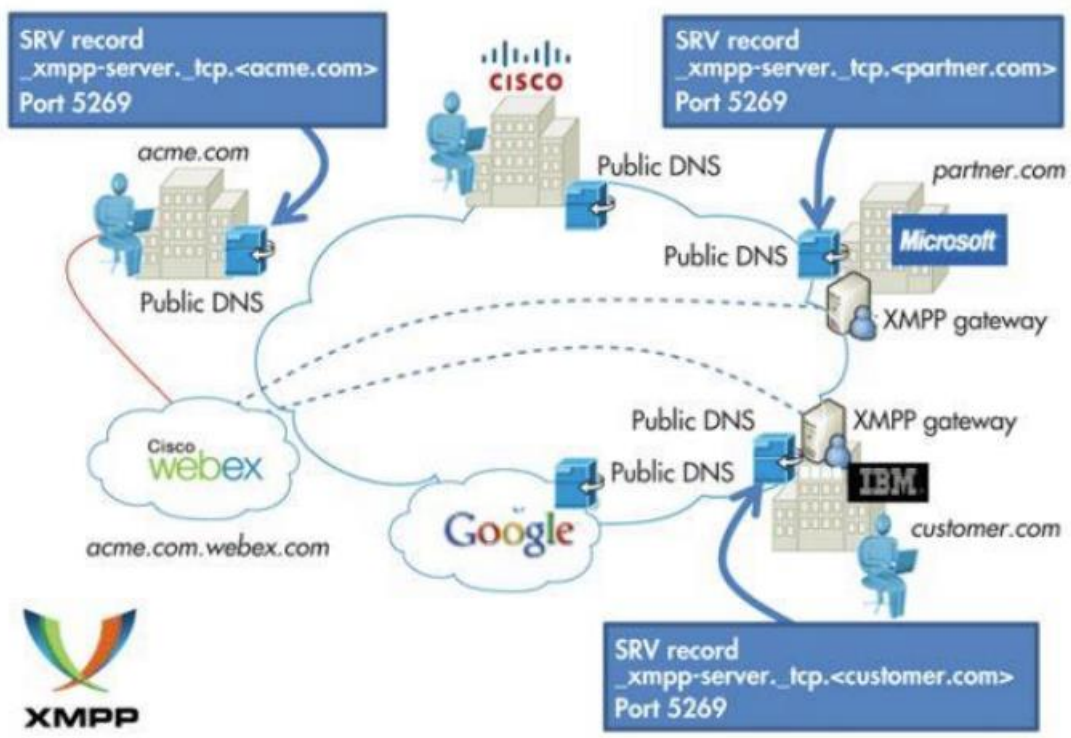
2.1.2 Cơ sở kỹ thuật của IoT

Giao thức chính: Trong IoT, các thiết bị phải giao tiếp được với nhau (D2D). Dữ liệu sau đó phải được thu thập và gửi tới máy chủ (D2S). Máy chủ cũng có để chia sẻ dữ liệu với nhau(S2S), có thể cung cấp lại cho các thiết bị, để phân tích các chương trình, hoặc cho người dùng. Các giao thức có thể dùng trong IoT là: - MQTT: một giao thức cho việc thu thập dữ liệu và giao tiếp cho các máy chủ (D2S) - XMPP: giao thức tốt nhất để kết nối các thiết bị với mọi người, một trường hợp đặc biệt của mô hình D2S, kể từ khi người được kết nối với các máy chủ - DDS: giao thức tốc độ cao cho việc tích hợp máy thông minh (D2D) - AMQP: hệ thống hàng đợi được thiết kế để kết nối các máy chủ với nhau (S2S) * MQTT MQTT(Message Queue Telemetry Transport), mục tiêu thu thập dữ liệu và giao tiếp D2S. Mục đích là đo đạc từ xa, hoặc giám sát từ xa, thu thập dữ liệu từ nhiều thiết bị và vận chuyển dữ liệu đó đến máy trạm với ít xung đột nhất. MQTT nhắm đến các mạng lớn của các thiết bị nhỏ mà cần phải được theo dõi hoặc kiểm soát từ các đám mây.



Hình 2. 4: Ví dụ về MQTT

MQTT hoạt động đơn giản, cung cấp nhiều lựa chọn điều khiển và QoS. MQTT không có yêu cầu quá khắt khe về thời gian, tuy nhiên hiều quả của nó là rất lớn, đáp ứng tính thời gian thực với đơn vị tính bằng giây. Các giao thức hoạt động trên nền tàng TCP, cung cấp các đáp ứng đơn giản, đáng tin cậy. * XMPP XMPP ban đầu được gọi là "Jabber." Nó được phát triển cho các tin nhắn tức thời (IM) để kết nối mọi người với những người khác thông qua tin nhắn văn bản. XMPP là viết tắt của Extensible Messaging và Presence Protocol.



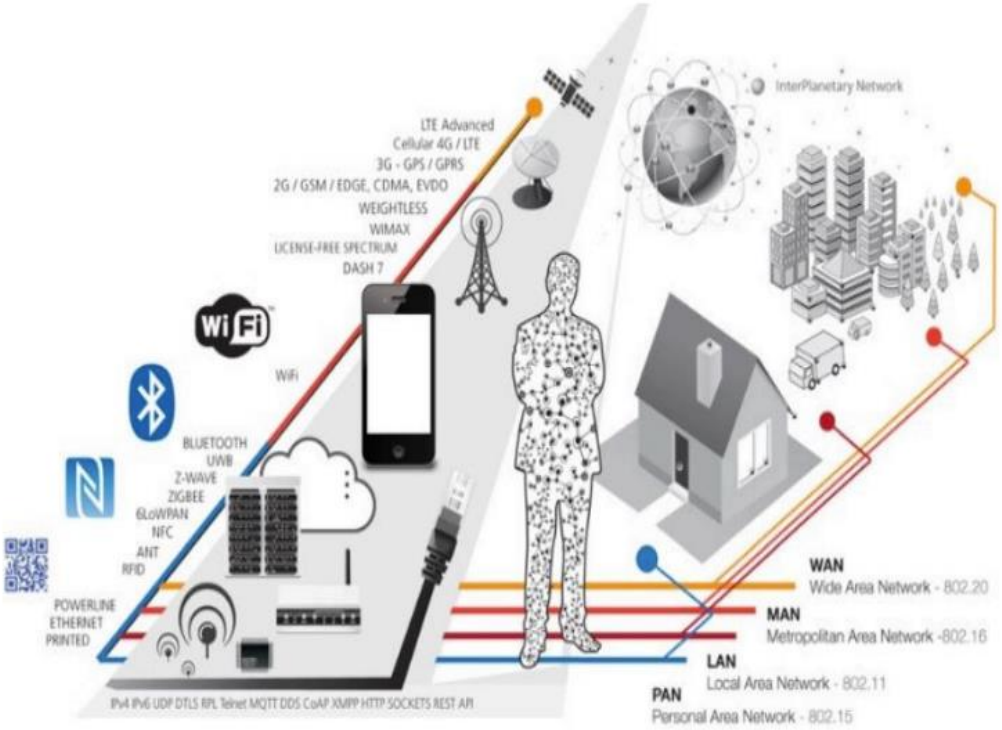
Hình 2. 5: Ví dụ XMPP

XMPP sử dụng định dạng văn bản XML, và cũng tương tự như MQTT chạy, XMPP chạy trên nền tảng TCP, hoặc có thể qua HTTP trên TCP. Sức mạnh chính của nó là một chương trình name@domain.comaddressing trong mạng Internet khổng lồ.

Năng lực truyền thông (Communication Capabilities):

Địa chỉ IP được coi là yếu tố quan trọng trong IoT, khi mà mỗi thiết bị được gán một địa chỉ IP riêng biệt. Do đó khả năng cấp phát địa chỉ IP sẽ quyết định đến tương lai của IoT. Hệ thống địa chỉ IPv4 được tạo ra mới mục đích đánh cho mỗi máy tính kết nối vào mạng internet một con số riêng biệt, giúp cho thông tin có thể tìm tới đúng nơi cần đến ngay khi nó được chuyển đi từ bất cứ địa điểm nào trên thế giới. Theo thiết kế, Ipv4 có thể cung cấp 2^32 (tương ứng với khoảng 4,2 tỉ) địa chỉ IP, một con số lớn không tưởng cách đây 30 năm. Tuy nhiên, sự bùng nổ mạnh mẽ của Internet đã khiến cho số lượng địa chỉ IP tự do càng ngày càng khan hiếm. Mới đây, RIPE NCC - Hiệp hội các tổ chức quản lý mạng Internet khu vực châu Âu phải đưa ra tuyên bố rằng họ đã sử dụng đến gói địa chỉ IP chưa cấp phát cuối cùng (khoảng 1,8 triệu địa chỉ) [3].

Và sự ra đời của IPv6 như là một giải pháp cứu sống kịp thời cho sự cạn kiệt của IPv4. Độ dài bit của là 128. Sự gia tăng mạnh mẽ của IPv6 trong không gian địa chỉ là một yếu tố quan trọng trong phát triển Internet of Things.



Hình 2. 6: Năng lực truyền thông

Công suất thiết bị (Device Power):

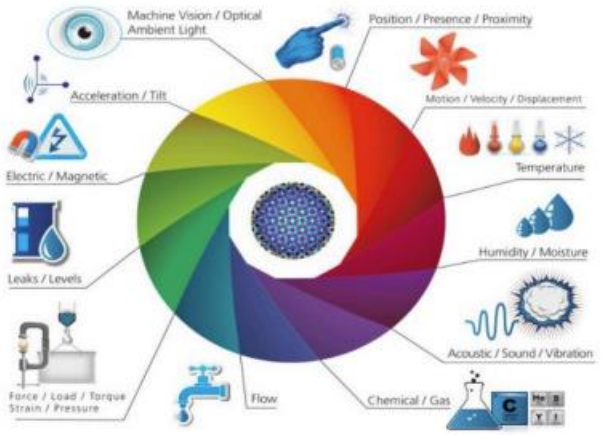
Các tiêu chí hình thức chính của thiết bị khi triển khai một ứng dụng IoT là phải giá thành thấp, mỏng, nhẹ…và như vậy phần năng lượng nuôi thiết bị cũng sẽ trở nên nhỏ gọn lại, năng lượng tích trữ cũng sẽ trở nên ít đi. Do đó đòi hỏi thiết bị phải tiêu tốn một công suất cực nhỏ (Ultra Low Power) để sử dụng nguồn năng lượng có hạn đó. Bên cạnh đó yêu cầu có những giao thức truyền thông không dây gọn nhẹ hơn, đơn giản hơn, đòi hỏi ít công suất hơn (Low Energy Wireless Technologies) như Zigbee, BLE (Bluetooth low energy), ANT/ANT+, NIKE+,..

	ZigBee™ 802.15.4	Bluetooth™ 802.15.1	Wi-Fi™ 802.11b	GPRS/GSM 1XRTT/CDMA
Application Focus	Monitoring & Control	Cable Replacement	Web, Video, Email	WAN, Voice/Data
System Resource	4KB-32KB	250KB+	1MB+	16MB+
Battery Life (days)	100-1000+	1-7	.1-5	1-7
Nodes Per Network	255/65K+	7	30	1,000
Bandwidth (kbps)	20-250	720	11,000+	64-128
Range (meters)	1-75+	1-10+	1-100	1,000+
Key Attributes	Reliable, Low Power, Cost Effective	Cost, Convenience	Speed, Flexibility	Reach, Quality

Hình 2. 7: Bảng so sánh các chuẩn truyền thông không dây.

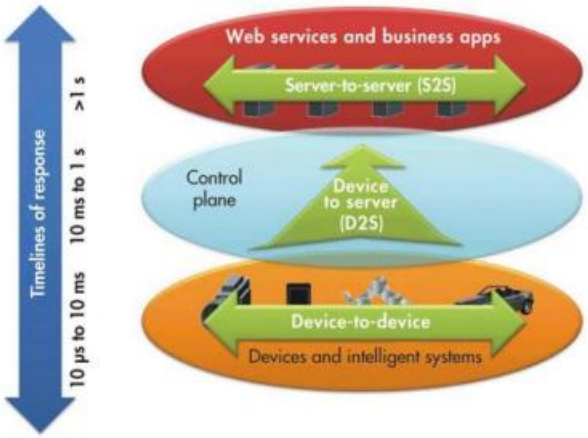
Công nghệ cảm biến (Sensor Technology):

Trong Internet of Things, cảm biến đóng vai trò then chốt, nó đo đạt cảm nhận giá trị từ môi trường xung quanh rồi gửi đến bộ vi xử lý sau đó được gửi lên mạng. Chúng ta có thể bắt gặp một số loại cảm biến về cảnh báo cháy rừng, cảnh báo động đất, cảm biến nhiệt độ, cảm biến độ ẩm,..Để giúp cho thiết bị kéo dài được thời gian sống hơn thì đòi hỏi cảm biến cũng phải tiêu hao một lượng năng lượng cực kỳ thấp. Bên cạnh đó độ chính xác và thời gian đáp ứng của cảm biến cũng phải nhanh. Để giá thành của thiết bị thấp thì đòi hỏi giá cảm biến cũng phải thấp.



Hình 2. 8: Một số loại cảm biến hay gặp

Thời gian đáp ứng:



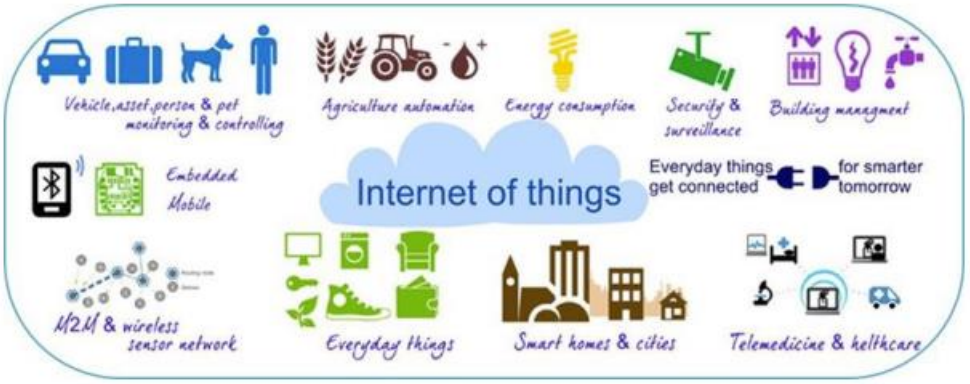
Hình 2. 9: Đáp ứng thời gian cho ứng dụng IoT

Thời gian đáp ứng phải đảm bảo tính thời gian thực, sao cho hàng ngàn các node mạng có thể truy cập vào hệ thống mà không xảy ra hiện tượng nghẽn mạng. Với các ứng dụng D2D, thời gian đáp ứng trong khoảng 10us đến 10ms, trong khi ứng dụng D2S, thời gian này là 10ms đến 1s. Với các ứng dụng S2S, không có yêu cầu khắt khe về thời gian đáp ứng, tuy nhiên thông thường yêu cầu từ 3 đến 5s.

2.1.3 Các ứng dụng của IoT

Với những hiệu quả thông minh rất thiết thực mà IoT đem đến cho con người, IoT đã và đang được tích hợp trên khắp mọi thứ, mọi nơi xung quanh thế giới mà con người đang sống. Từ chiếc vòng đeo tay, những đồ gia dụng trong nhà, những mãnh

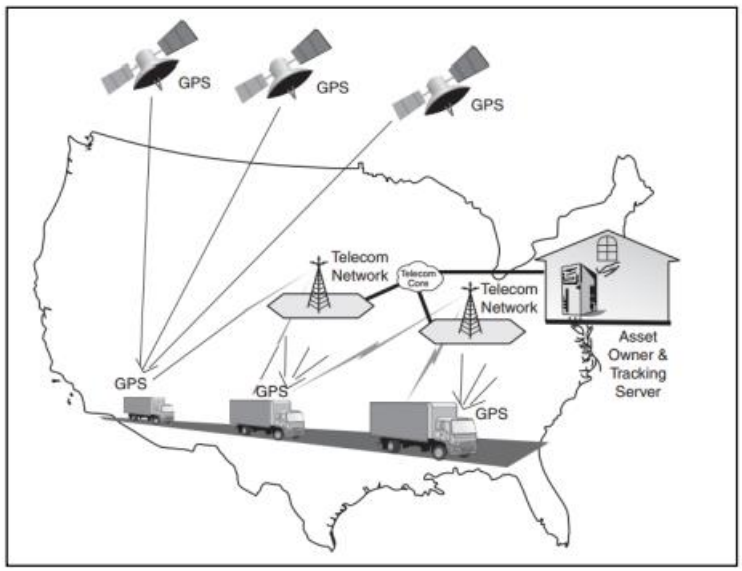
vườn đang ươm hạt giống, cho đến những sinh vật sống như động vật hay con người…đều có sử dụng giải pháp IoT.



Hình 2. 10: Tổng quan về ứng dụng của IoT.

Ứng dụng trong lĩnh vực vận tải:

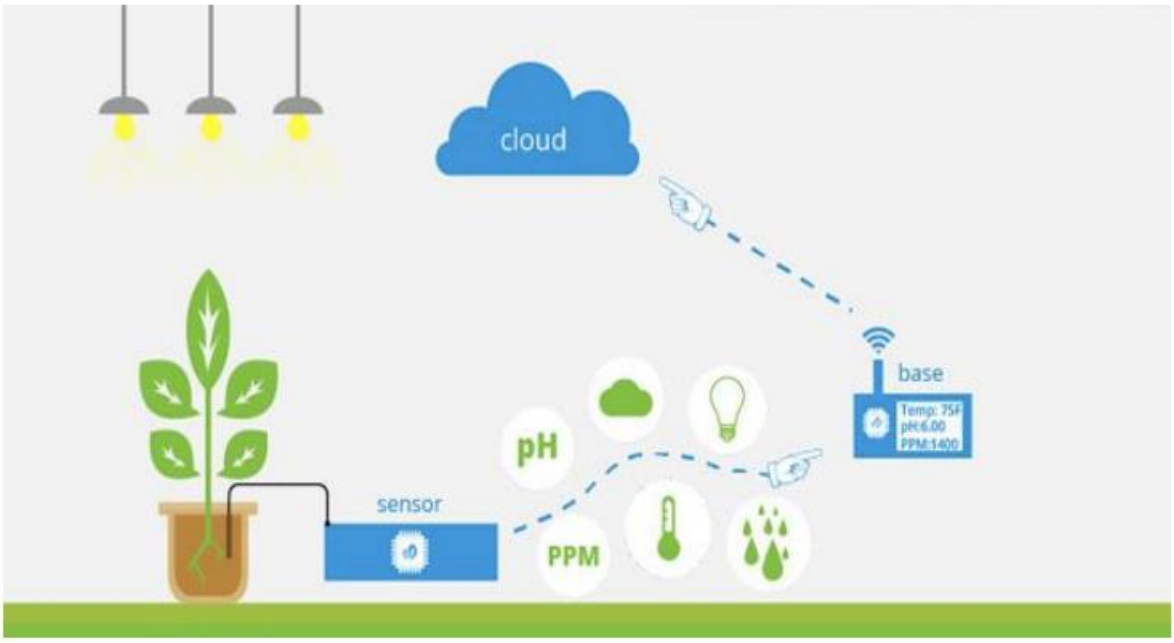
Ứng dụng điển hình nhất trong lĩnh vực này là gắn chíp lấy tọa độ GPS lên xe chở hàng, nhằm kiểm soát lộ trình, tốc độ, thời gian đi đến của các xe chở hàng. Ứng dụng này giúp quản lý tốt khâu vận chuyển, có những xử lý kịp thời khi xe đi không đúng lộ trình hoạt bị hỏng hóc trên những lộ trình mà ở đó mạng di động không phủ sóng tới được, kiểm soát được lượng nhiên liệu tiêu hao ứng với lộ trình đã được vạch trước…



Hình 2. 11: Theo dõi lộ trình đi của xe chở hàng.

Ứng dụng trong lĩnh vực sản xuất nông nghiệp:

Quá trình sinh trưởng và phát triển của cây trồng trải qua nhiều giai đoạn từ hạt nảy mầm đến ra hoa kết trái. Ở mỗi giai đoạn cần có sự chăm sóc khác nhau về chất dinh dưỡng cũng như chế độ tưới tiêu phù hợp. Những yêu cầu này đòi hỏi sự bền bỉ và siêng năng của người nông dân từ ngày này sang ngày khác làm cho họ phải vất vả. Nhưng nhờ vào ứng dụng khoa học kỹ thuật, sử dụng cảm biến để lấy thông số nhiệt độ, độ ẩm, độ pH của đất trồng, cùng với bảng dữ liệu về quy trình sinh trưởng của loại cây đó, hệ thống sẽ tự động tưới tiêu bón lót cho cây trồng phù hợp với từng giai đoạn phát triển của cây trồng. Người nông dân bây giờ chỉ kiểm tra, quan sát sự vận hành của hệ thống chăm sóc cây trồng trên một màn hình máy tính có nối mạng.



Hình 2. 12: Theo dõi tình trạng sinh trưởng của cây trồng.

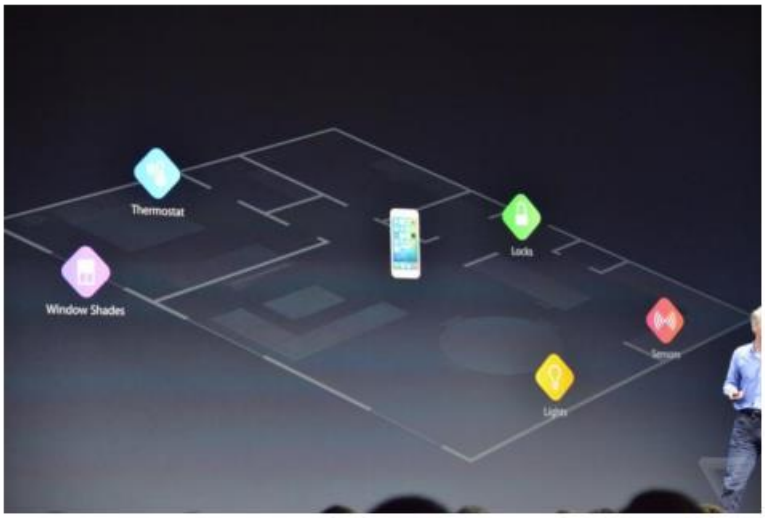
Sản phẩm của mỗi loại nông sản sẽ được gắn mã ID, nếu tủ lạnh nhà chúng ta sắp hết một loại nông sản nào đó thì ngay lập tức nó sẽ tự động gửi thông báo cần mua đến cơ sở dữ liệu của trang trại có trồng loại nông sản đó, và chỉ sau một thời gian nông sản mà bạn cần sẽ được nhân viên đem đến tận nhà.

Ứng dụng trong nhà thông minh:

Vài năm trở lại đây, khi thế giới đang dần tiến vào kỷ nguyên Internet of Things, kết nối mọi vật qua Internet, nhà thông minh trở thành một xu hướng công nghệ tất yếu, là tiêu chuẩn của nhà ở hiện đại. Trong căn hộ thông minh, tất cả các thiết bị từ rèm cửa,

điều hoà, dàn âm thanh, hệ thống ánh sáng, hệ thống an ninh, thiết bị nhà tắm… được kết nối với nhau và hoạt động hoàn toàn tự động theo kịch bản lập trình sẵn, đáp ứng đúng nhu cầu sử dụng của khách hàng.

Ví dụ, vào buổi sáng, đèn tắt, rèm cửa tự động chuyển tới vị trí thích hợp để giảm bớt những tác động náo nhiệt từ đường phố và nhường không gian cho ánh sáng tự nhiên. Tối đến, hệ thống đèn bật sáng, các rèm cửa kéo lên người dùng có thể thưởng ngoạn từ trên cao bức tranh thành phố rực rỡ ánh đèn, đồng thời âm nhạc cũng nhẹ nhàng cất lên các giai điệu yêu thích của gia đình.



Hình 2. 13: Ví dụ về nhà thông minh

Nếu có việc cả nhà phải đi vắng, chế độ "Ra khỏi nhà" sẽ được kích hoạt, toàn bộ thiết bị điện tử gia dụng sẽ tự động tắt hoặc đóng lại và khi chủ nhân về, chúng cũng sẽ khôi phục lại trạng thái trước đó. Thậm chí, nước nóng cũng đã sẵn sàng từ vài phút trước khi gia chủ về đến cửa. Riêng hệ thống an ninh luôn hoạt động 24/24 và sẽ thông báo đến chủ nhà mọi thay đổi "đáng ngờ" trong ngôi nhà, dù đang ở bất cứ đâu.

2.2. Nguyên lý hoạt động của hệ thống IoT

Mô tả chi tiết về nguyên lý hoạt động của hệ thống IoT:

1. Thu thập dữ liệu: Hệ thống IoT sử dụng các thiết bị cảm biến để thu thập dữ liệu từ môi trường xung quanh. Các cảm biến có thể ghi nhận các thông số như nhiệt độ, độ ẩm, ánh sáng, chuyển động và định vị. Dữ liệu được thu thập có thể là dữ liệu số hoặc dữ liệu analog.

2. Truyền tải dữ liệu: Dữ liệu thu thập từ các thiết bị cảm biến được truyền tải qua các kết nối mạng. Hệ thống IoT sử dụng các giao thức truyền thông như Wi-Fi, Bluetooth, Zigbee hoặc mạng di động để kết nối các thiết bị với nhau và với hạ tầng mạng. Dữ liệu có thể được truyền tải qua mạng LAN (Local Area Network) hoặc mạng WAN (Wide Area Network) tùy thuộc vào quy mô và phạm vi của hệ thống[6].

3. Lưu trữ và xử lý dữ liệu: Dữ liệu thu thập từ các thiết bị cảm biến được chuyển đến một nền tảng phần mềm hoặc đám mây để lưu trữ và xử lý. Trong nền tảng này, dữ liệu được xử lý để tách biệt thông tin quan trọng và loại bỏ nhiễu. Các thuật toán và công cụ phân tích dữ liệu được sử dụng để tìm ra các mẫu, xu hướng hoặc thông tin hữu ích từ dữ liệu thu thập[6].

4. Quyết định và điều khiển: Sau khi dữ liệu được xử lý và phân tích, hệ thống IoT có khả năng đưa ra quyết định và điều khiển các thiết bị hoạt động. Điều này có thể được thực hiện tự động hoặc thông qua giao diện người dùng. Ví dụ, nếu dữ liệu nhiệt độ vượt quá ngưỡng an toàn, hệ thống có thể tự động gửi cảnh báo hoặc điều chỉnh hệ thống điều hòa.

5. Tương tác và giao tiếp: Hệ thống IoT cung cấp khả năng tương tác và giao tiếp giữa người dùng và các thiết bị trong hệ thống. Người dùng có thể theo dõi và điều khiển các thiết bị thông qua giao diện người dùng hoặc các ứng dụng di động. Điều này mang lại sự thuận tiện và khả năng kiểm soát từ xa trong quản lý và sử dụng các thiết bị IoT.

Thông qua các bước trên, hệ thống IoT cho phép thu thập, truyền tải, lưu trữ, xử lý dữ liệu và quyết định điều khiển các thiết bị để tạo ra môi trường thông minh, hiệu quả và an toàn trong các lĩnh vực như gia đình thông minh, chăm sóc sức khỏe, quản lý năng lượng và nhiều lĩnh vực khác.

2.3. Các thách thức bảo mật trong hệ thống IoT

Trong hệ thống IoT, có nhiều thách thức bảo mật cần được xem xét và giải quyết để đảm bảo an toàn và bảo mật cho dữ liệu. Dưới đây là một số thách thức bảo mật quan trọng trong hệ thống IoT:

1. Xác thực và ủy quyền: Hệ thống IoT bao gồm nhiều thiết bị và thành phần khác nhau. Để đảm bảo tính xác thực và ủy quyền, các thiết bị và người dùng phải được xác thực một cách đáng tin cậy và có quyền truy cập vào dữ liệu và tài nguyên. Sự xác thực yếu và quản lý ủy quyền không tốt có thể dẫn đến việc xâm nhập và truy cập trái phép vào hệ thống[5].

2. Bảo mật dữ liệu: Dữ liệu thu thập từ các thiết bị IoT thường là dữ liệu nhạy cảm và riêng tư, như thông tin cá nhân, thông tin tài chính hoặc dữ liệu về sức khỏe. Việc bảo mật dữ liệu trong quá trình thu thập, truyền tải và lưu trữ là một thách thức quan trọng. Sự lộ thông tin có thể gây ra hậu quả nghiêm trọng cho người dùng và tổ chức.

3. Bảo mật mạng: Hệ thống IoT được xây dựng trên cơ sở hạ tầng mạng, bao gồm các mạng LAN, WAN, mạng di động và internet. Mạng mở rộng này tạo ra nhiều điểm yếu tiềm ẩn và lỗ hổng bảo mật. Việc bảo vệ và bảo mật mạng là cần thiết để ngăn chặn các cuộc tấn công mạng, đảm bảo tính toàn vẹn và sẵn sàng của hệ thống[5].

4. Quản lý khối lượng dữ liệu: Hệ thống IoT thu thập và sản sinh ra lượng lớn dữ liệu. Quản lý, lưu trữ và xử lý dữ liệu lớn là một thách thức về hiệu suất và bảo mật. Việc xác định và triển khai các giải pháp hiệu quả để xử lý khối lượng lớn dữ liệu một cách an toàn và bảo mật là rất quan trọng.

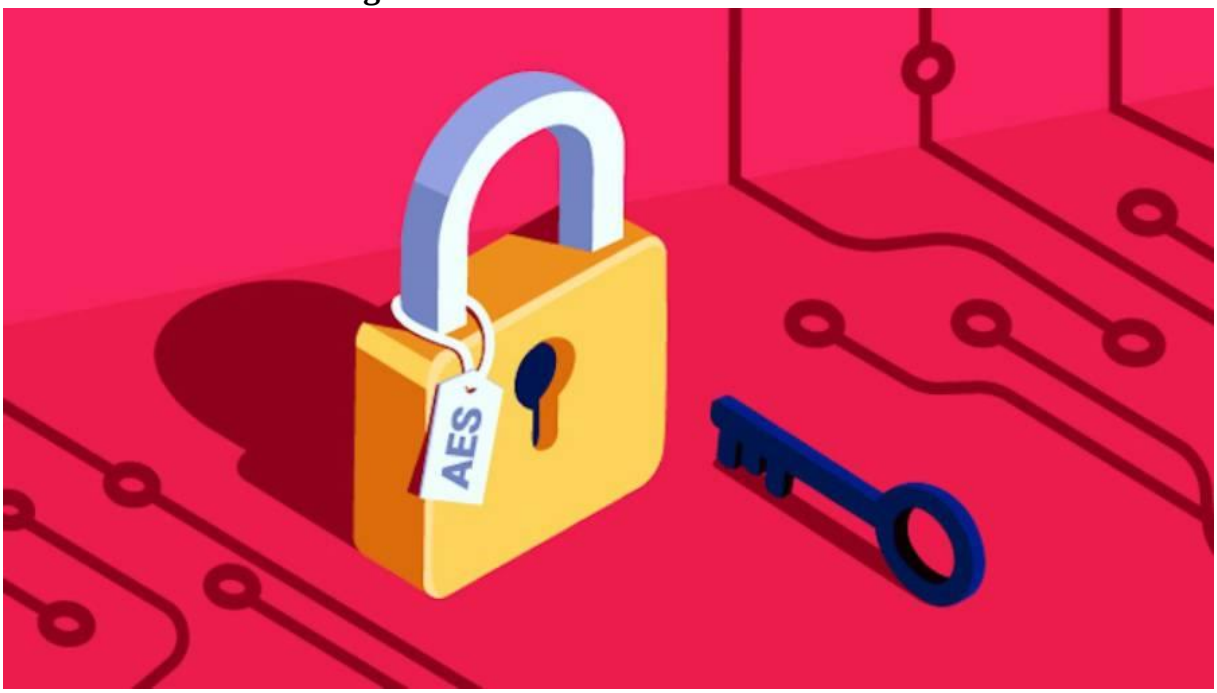
5. Bảo mật phần mềm và thiết bị: Hệ thống IoT bao gồm nhiều phần mềm và thiết bị khác nhau, từ các ứng dụng điện thoại di động, cảm biến, thiết bị lưu trữ đám mây cho đến cơ sở hạ tầng mạng. Việc đảm bảo tính an toàn và bảo mật cho phần mềm và thiết bị là một thách thức quan trọng, vì các lỗ hổng bảo mật có thể bị tấn công và lợi dụng để truy cập trái phép vào hệ thống[4].

6. Quản lý vòng đời của thiết bị: Hệ thống IoT thường bao gồm các thiết bị có tuổi thọ ngắn và cần được cập nhật thường xuyên để đảm bảo tính bảo mật và hiệu suất. Việc quản lý vòng đời của các thiết bị IoT, bao gồm việc cập nhật phần mềm, kiểm tra lỗ hổng bảo mật và rút kinh nghiệm từ các sự cố là một thách thức đáng chú ý[4].

Đối mặt với những thách thức bảo mật trên, việc triển khai các giải pháp bảo mật hiệu quả là cần thiết để đảm bảo tính an toàn và bảo mật cho hệ thống IoT và dữ liệu của người dùng.

2.4. Thuật toán Mã hóa đối xứng (AES) trong bảo mật dữ liệu

2.4.1 Mã hóa ASE là gì?



Hình 2. 14: Mã hóa ASE là gì?

Advanced Encryption Standard (AES) hay còn được gọi là tiêu chuẩn mã hóa nâng cao theo phương pháp mật mã khối. Với ưu thế bảo mật cao nó đã được chính phủ Hoa Kỳ lựa chọn để bảo vệ dữ liệu, thông tin cho các tổ chức, doanh nghiệp mà người dùng.

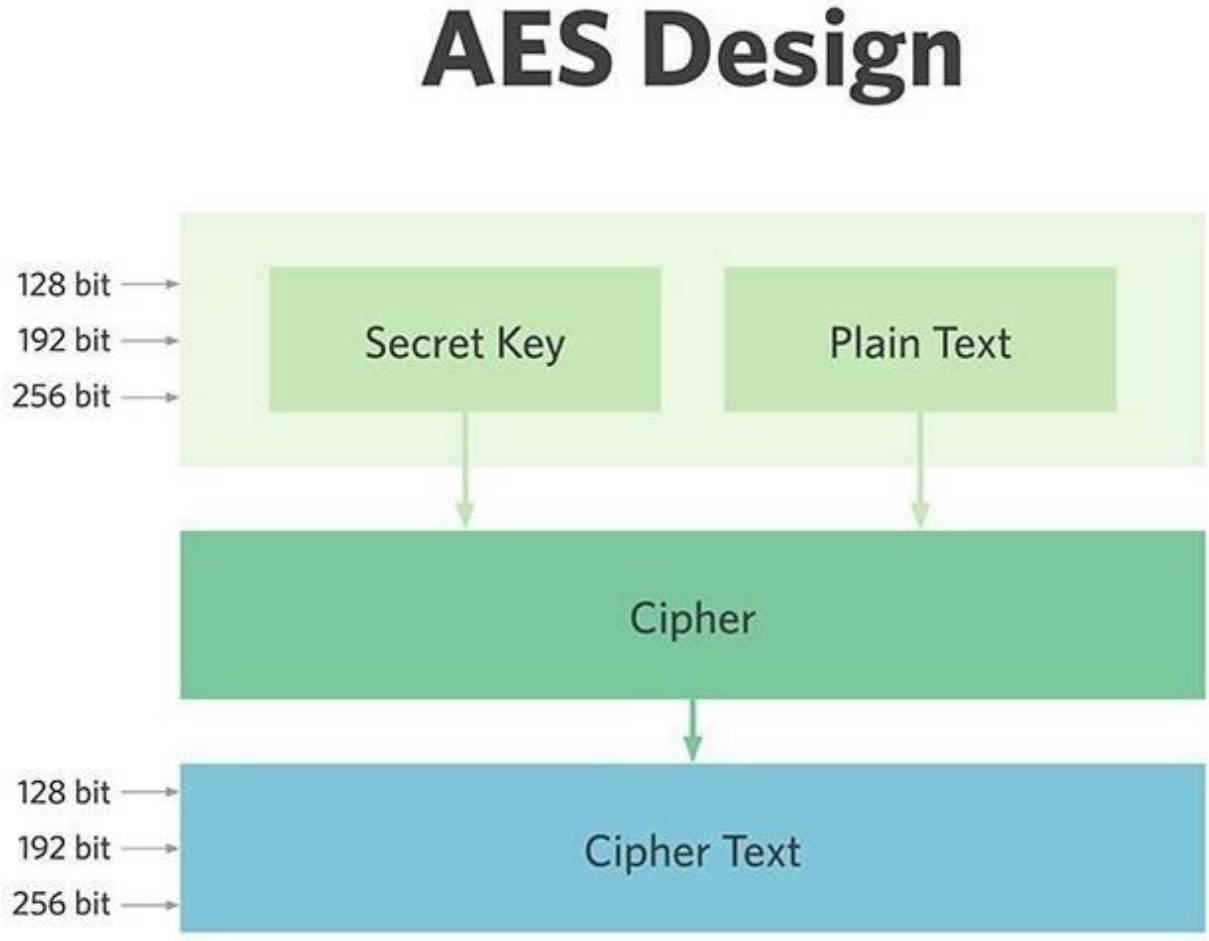
Các tác vụ của AES được thực hiện ở cả phần cứng và phần mềm trên nhiều thiết bị để mã hóa dữ liệu nhạy cảm. Sự có mặt của nó đã góp phần bảo đảm an toàn cho máy tính của chính phủ, an ninh mạng và tạo một rào chắn vững chắc để bảo vệ dữ liệu.

Năm 1997 AES lầm đầu tiên được công bố bởi Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Tại thời điểm đó Tiêu chuẩn mã hóa dữ liệu DES xuất hiện những lỗ hổng vì thế AES được nghiên cứu và phát triển để thay thế cho nó.

NIST đã rất tự tin khi tuyên bố rằng AES chính là giải pháp tốt nhất để bảo vệ thông tin nhạy cảm cho chính phủ trong thế kỷ XXI. Đặc biệt so với các tiêu chuẩn khác thì AES có khả năng thực hiện tác vụ trong môi trường hạn chế như thẻ thông minh[7].

2.4.2 ASE hoạt động như thế nào

AES gồm ba mật mã khối AES-128, AES-192, AES-256 tương ứng với độ dài của key là 128 bit, 192 bit và 256 bit. Số vòng của key khác nhau, cụ thể 10 vòng cho 128 bit, 12 vòng cho 192 bit và 14 vòng cho 256 bit. Mỗi vòng đều thực hiện ba bước thay thế, biến đổi và hòa trộn khối plain text (văn bản thuần túy) đầu vào để biến nó thành Ciphertext (văn bản đã mã hóa) [8].



Hình 2. 15: ASE hoạt động như thế nào

Thông tin được chính phủ phân loại theo ba cấp độ: bảo mật, bí mật, tối mật. Tất cả các độ dài của key từ 128, 192 và 256 bit đều được dùng ở cấp độ bảo mật, bí mật. Riêng với những thông tin tối mật để đảm bảo không xảy ra bất cứ sai sót nào phải cần đến key 192 hoặc 256 bit. Mật mã sẽ dùng một key riêng tư để mã hóa và giải mã dữ liệu và tất nhiên cả người gửi và người nhận đều phải nhận biết và sử dụng được key này[8].

Các tiêu chí cần có ở AES

NIST đưa ra yêu cầu đối với AES đó là phải sử dụng phương pháp mã hóa khối với độ dài của key là 128, 192 và 256 bit để mã hóa và giải mã dữ liệu. Ngoài ra AES phải đáp ứng được những tiêu chí sau:

Bảo vệ: Đây là một trong những tính năng hàng đầu AES cần phải có để đánh bại các đối thủ khác. Nó phải có khả năng chống lại các cuộc tấn công mạnh, quy mô lớn.
Chi phí: AES mở ra nhiều cơ hội cho người dùng bằng cách phát hành trên toàn cầu và miễn phí bản quyền.
Khả năng thực hiện: Linh hoạt, phù hợp và đơn giản chính là 3 yếu tố quan trọng hội tụ ở AES để đáp ứng trọn vẹn nhu cầu của người dùng.

Chọn thuật toán AES mới

Để có được một thuật toán đạt tới độ hoàn hảo vào tháng 8 năm 1999 NIST đã chọn MARS, RC6, Rijndael, Serpent, Twofish để phân tích. Tất cả 5 thuật toán trên đã được thử nghiệm trong ANSI, các ngôn ngữ như Java và C. Chúng được so sánh với nhau dựa vào các yêu tố như tốc độ mã hóa, mức độ tin cậy, thời gian thiết lập key và thuật toán, mức độ chống lại các cuộc công.

Sau quá trình làm việc nghiêm túc, vào tháng 10 năm 2000 các thành viên của cộng đồng mật mã toàn cầu đã chọn Rijndael làm thuật toán đề xuất cho AES. Tháng 12 năm 2001 nó được Bộ trưởng Thương mại Hoa Kỳ chấp nhận và năm 2002 chính thức có hiệu lực như một tiêu chuẩn của chính phủ liên bang.

Tháng 6 năm 2004, AES được chính phủ Mỹ thông báo với công chúng và được ứng dụng để bảo vệ thông tin đã phân loại. Kể từ đó AES phủ sóng ở nhiều lĩnh vực và nó được NSA (cơ quan an ninh Quốc gia Hoa Kỳ) chọn để bảo vệ hệ thống an ninh cho chính phủ và đất nước. Có thể khẳng định khi AES được chính phủ Hoa Kỳ sử dụng thành công đã tạo được tiếng vang rất lớn. Nó nhanh chóng được các tổ chức tư nhân săn đón để tạo "bức tường lửa" bảo vệ những dữ liệu mật[9].

2.4.3 ASE trong bảo mật dữa liêu cho hệ thống IoT

Trong hệ thống IoT, một trong những thuật toán mã hóa đối xứng phổ biến và được sử dụng rộng rãi để bảo mật dữ liệu là Mã hóa đối xứng Advance Encryption Standard (AES). Thuật toán này đã được chứng minh là mạnh mẽ, hiệu quả và an toàn trong việc bảo vệ thông tin.

AES sử dụng khối mã hóa đối xứng, có nghĩa là cùng một khóa được sử dụng để mã hóa và giải mã dữ liệu. Khóa này được chia thành các khối con và được sử dụng trong các vòng lặp để thực hiện quá trình mã hóa. Các bước chính trong quá trình mã hóa AES bao gồm: SubBytes, ShiftRows, MixColumns và AddRoundKey. Các bước này kết hợp các phép biến đổi tuyến tính và phi tuyến tính để đảm bảo tính toàn vẹn và bảo mật của dữ liệu.

Mã hóa đối xứng AES được sử dụng để mã hóa dữ liệu trước khi truyền qua mạng hoặc lưu trữ trong hệ thống IoT. Khi dữ liệu được mã hóa, chỉ những người có khóa mã hóa chính xác mới có thể giải mã dữ liệu thành dạng ban đầu. Điều này giúp ngăn chặn truy cập trái phép và bảo vệ tính toàn vẹn của dữ liệu trong quá trình truyền và lưu trữ.

Thuật toán AES được coi là một trong những giải pháp bảo mật hiệu quả và đáng tin cậy trong hệ thống IoT. Nó cung cấp một cơ chế mạnh mẽ để bảo vệ dữ liệu và đảm bảo tính riêng tư và an toàn cho người dùng[9].

CHƯƠNG 3: PHƯƠNG PHÁP NGHIÊN CỨU

3.1. Thu thập tài liệu và nghiên cứu trước đây về Mã hóa đối xứng (AES)

Trước khi tiến hành nghiên cứu về Mã hóa đối xứng (AES) trong hệ thống IoT, chúng em đã tiến hành thu thập tài liệu liên quan và nghiên cứu trước đây về thuật toán này. Quá trình này giúp chúng em xây dựng cơ sở lý thuyết và hiểu rõ hơn về các khía cạnh quan trọng của AES.

Trong giai đoạn thu thập tài liệu, chúng em đã tìm kiếm và thu thập các sách, bài báo, báo cáo nghiên cứu, và tài liệu trực tuyến liên quan đến Mã hóa đối xứng (AES). Chúng em đã tập trung vào các nguồn thông tin uy tín từ các tạp chí khoa học, các tài liệu công bố, cũng như các tài liệu từ các tổ chức quốc tế chuyên về bảo mật thông tin. Mục tiêu của quá trình thu thập tài liệu là hiểu rõ nguyên lý hoạt động, cấu trúc, các bước mã hóa và giải mã, và các đặc điểm quan trọng của thuật toán AES.

Sau đó, chúng em đã tiến hành nghiên cứu trước đây về Mã hóa đối xứng (AES) để tìm hiểu về các công trình nghiên cứu và ứng dụng của AES trong lĩnh vực bảo mật dữ liệu. Chúng em đã xem xét các bài báo khoa học, bài viết, và các công trình nghiên cứu đã được công bố liên quan đến AES. Qua việc nghiên cứu trước đây, chúng em đã có cái nhìn tổng quan về sự phát triển của AES, các công nghệ liên quan, các ứng dụng thực tế, và những thách thức mà các nhà nghiên cứu đã đối mặt khi áp dụng AES trong các hệ thống thực tế.

Qua quá trình thu thập tài liệu và nghiên cứu trước đây, chúng em đã xây dựng được kiến thức vững chắc về Mã hóa đối xứng (AES). Sự hiểu biết này sẽ là nền tảng cho các phần tiếp theo của đề tài, bao gồm triển khai và đánh giá hiệu suất của AES trong hệ thống IoT.

3.2. Xác định phạm vi và tiêu chí đánh giá

Đầu tiên, chúng em đã xác định phạm vi của nghiên cứu bằng cách định rõ hệ thống IoT mà chúng em quan tâm. Phạm vi nghiên cứu bao gồm các thiết bị IoT, mạng kết nối và giao tiếp giữa các thiết bị, cũng như việc truyền và lưu trữ dữ liệu trong hệ thống IoT. Chúng em đã định rõ các khía cạnh quan trọng cần tập trung, như bảo mật dữ liệu trên các thiết bị, bảo vệ mạng truyền thông và tính toàn vẹn dữ liệu trong quá trình truyền tải.

Tiếp theo, chúng em đã xác định các tiêu chí đánh giá để đánh giá hiệu suất và hiệu quả của việc áp dụng AES trong hệ thống IoT. Các tiêu chí này bao gồm độ bảo mật, tốc độ xử lý, khả năng mở rộng, tương thích và khả năng triển khai trong môi trường thực tế. Chúng em đã xác định các thông số đo lường cụ thể cho mỗi tiêu chí, như độ dài khóa, thời gian mã hóa và giải mã, số lượng thiết bị kết nối, và khả năng tích hợp với các giao thức và công nghệ khác trong hệ thống IoT.

Qua việc xác định phạm vi và tiêu chí đánh giá, chúng em đã tạo ra một khung nghiên cứu rõ ràng và cụ thể để đánh giá hiệu suất và ứng dụng của Mã hóa đối xứng (AES) trong hệ thống IoT. Các kết quả từ việc áp dụng tiêu chí đánh giá sẽ cung cấp thông tin quan trọng về khả năng và hạn chế của AES trong bảo mật dữ liệu trong hệ thống IoT.

3.3. Triển khai thuật toán Mã hóa đối xứng (AES) trong hệ thống IoT

Trong phần này, chúng em trình bày về quá trình triển khai thuật toán Mã hóa đối xứng (AES) trong hệ thống IoT. Mục tiêu của phần này là áp dụng AES vào bảo mật dữ liệu trong hệ thống IoT và thực hiện các bước triển khai cần thiết.

Đầu tiên, chúng em đã nghiên cứu về thuật toán Mã hóa đối xứng (AES) để hiểu cách hoạt động và các phương pháp mã hóa, giải mã của nó. Chúng em đã xác định các tham số quan trọng của AES, bao gồm độ dài khóa và các bước xử lý trong quá trình

mã hóa và giải mã. Chúng em đã tìm hiểu về cấu trúc và cách thức hoạt động của AES để có thể áp dụng nó vào hệ thống IoT.

Tiếp theo, chúng em đã xác định các yêu cầu và điều kiện để triển khai AES trong hệ thống IoT. Chúng em đã xem xét các yếu tố như khả năng tích hợp, khả năng mở rộng, hiệu suất và tài nguyên hệ thống để đảm bảo việc triển khai AES là phù hợp và hiệu quả trong môi trường IoT. Chúng em đã nghiên cứu về các công nghệ và giao thức liên quan khác trong hệ thống IoT để đảm bảo tính tương thích và khả năng kết hợp của AES với các thành phần khác.

Sau đó, chúng em đã thực hiện các bước triển khai cần thiết để áp dụng AES vào hệ thống IoT. Điều này bao gồm việc tích hợp thư viện AES vào phần mềm hoặc firmware của các thiết bị IoT, cài đặt và cấu hình các tham số liên quan như khóa mã hóa, thực hiện các bước mã hóa và giải mã dữ liệu. Chúng em đã xây dựng một môi trường thử nghiệm để kiểm tra và đánh giá hiệu suất của AES trong việc bảo mật dữ liệu trong hệ thống IoT.

Phần triển khai thuật toán Mã hóa đối xứng (AES) trong hệ thống IoT là một phần quan trọng trong nghiên cứu của chúng em. Việc áp dụng AES vào hệ thống IoT sẽ cung cấp một phương pháp bảo mật dữ liệu hiệu quả và đáng tin cậy, giúp tăng cường an ninh trong môi trường IoT đa dạng và phức tạp.

3.4. Chuẩn bị dữ liệu và môi trường thử nghiệm

Trước khi tiến hành thử nghiệm triển khai thuật toán Mã hóa đối xứng (AES) trong hệ thống IoT, chúng em đã thực hiện các công đoạn chuẩn bị dữ liệu và môi trường thử nghiệm.

Đầu tiên, chúng em đã thu thập dữ liệu liên quan đến hệ thống IoT để sử dụng trong quá trình thử nghiệm. Dữ liệu này bao gồm các gói tin truyền thông, thông tin về các thiết bị, cấu hình mạng và các thông tin liên quan khác. Chúng em đã xác định những yếu tố quan trọng và cần thiết trong dữ liệu để đảm bảo tính chính xác và đáng tin cậy của quá trình thử nghiệm.

Tiếp theo, chúng em đã tạo ra môi trường thử nghiệm phù hợp cho việc triển khai AES trong hệ thống IoT. Môi trường thử nghiệm bao gồm các thiết bị IoT, máy chủ, mạng kết nối và các thành phần liên quan khác. Chúng em đã thiết lập và cấu hình các thiết bị và mạng theo yêu cầu của hệ thống IoT và đảm bảo tính tương thích và khả năng tương tác giữa các thành phần.

Sau đó, chúng em đã thực hiện quá trình chuẩn bị dữ liệu bằng cách áp dụng thuật toán Mã hóa đối xứng (AES) vào các gói tin truyền thông và thông tin liên quan khác trong môi trường thử nghiệm. Chúng em đã mã hóa và giải mã dữ liệu sử dụng AES và ghi nhận các kết quả, đánh giá hiệu suất và tính bảo mật của thuật toán trong việc bảo vệ dữ liệu trong hệ thống IoT.

Chuẩn bị dữ liệu và môi trường thử nghiệm đóng vai trò quan trọng trong quá trình nghiên cứu của chúng em. Nó giúp đảm bảo tính khách quan và chính xác của kết quả thử nghiệm, từ đó đưa ra những nhận định và đánh giá có cơ sở về hiệu suất và tính bảo mật của thuật toán Mã hóa đối xứng (AES) trong hệ thống IoT.

3.5. Nguyên lý và cách thức thực hiện Mã hóa đối xứng (AES)

Nguyên lý và cách thức thực hiện Mã hóa đối xứng (AES) là một phần quan trọng trong việc bảo mật dữ liệu trong hệ thống IoT. Dưới đây là mô tả chi tiết về nguyên lý và cách thức thực hiện của thuật toán AES:

Nguyên lý hoạt động của AES:

1. Khóa: AES sử dụng một khóa bí mật để mã hóa và giải mã dữ liệu. Khóa có kích thước cố định và phải được trao đổi an toàn giữa người gửi và người nhận.

2. Phân khối dữ liệu: Dữ liệu được chia thành các khối cùng kích thước (thường là 128 bit) để thực hiện quá trình mã hóa. Mỗi khối dữ liệu được xử lý độc lập.

3. Vòng lặp: AES sử dụng một số lượng vòng lặp để thực hiện các phép biến đổi trên dữ liệu. Số lượng vòng lặp phụ thuộc vào kích thước khóa và mức độ bảo mật mong muốn.

4. Phép XOR: Trong quá trình mã hóa, dữ liệu của mỗi khối sẽ được thực hiện phép XOR với khóa để tạo ra một khối dữ liệu được mã hóa. Trong quá trình giải mã, phép XOR cũng được thực hiện để khôi phục lại dữ liệu ban đầu từ khối dữ liệu đã mã hóa.

5. Phép thay thế và hoán vị: AES sử dụng các hộp S-Box và ma trận hoán vị để thay thế và hoán vị các byte trong khối dữ liệu. Quá trình này tạo ra một sự phiên mã hóa phức tạp và gia tăng tính bảo mật của thuật toán.

Cách thức thực hiện của AES:

1. Mã hóa: Để mã hóa dữ liệu, AES sử dụng khóa bí mật và phép XOR để kết hợp khóa với khối dữ liệu. Sau đó, các phép thay thế và hoán vị được áp dụng lên khối dữ liệu đã kết hợp để tạo ra khối dữ liệu mã hóa.

2. Giải mã: Để giải mã dữ liệu đã mã hóa, AES sử dụng khóa bí mật và phép XOR để kết hợp khóa với khối dữ liệu đã mã hóa. Sau đó, các phép thay thế và hoán vị ngược được áp dụng để khôi phục lại dữ liệu ban đầu từ khối dữ liệu đã mã hóa.

3. Key Schedule: Trước khi thực hiện quá trình mã hóa và giải mã, AES sử dụng

thuật toán Key Schedule để tạo ra các khóa con từ khóa ban đầu. Quá trình này gia tăng độ phức tạp và tính bảo mật của thuật toán. AES là một thuật toán mã hóa đối xứng mạnh mẽ và được sử dụng rộng rãi trong nhiều ứng dụng bảo mật, bao gồm cả hệ thống

IoT. Sự kết hợp giữa nguyên lý hoạt động và cách thức thực hiện của AES đảm bảo tính bảo mật và hiệu suất trong việc bảo vệ dữ liệu trong hệ thống IoT.

3.6. Áp dụng Mã hóa đối xứng (AES) vào việc bảo mật dữ liệu trong hệ thống IoT

Áp dụng Mã hóa đối xứng (AES) vào việc bảo mật dữ liệu trong hệ thống IoT là một bước quan trọng để đảm bảo tính toàn vẹn và bảo mật của thông tin truyền qua mạng. Dưới đây là một số cách áp dụng AES để bảo mật dữ liệu trong hệ thống IoT:

1. Mã hóa dữ liệu truyền qua kênh mạng: Khi dữ liệu được truyền từ thiết bị IoT đến điểm đích thông qua mạng, AES có thể được sử dụng để mã hóa dữ liệu trước khi gửi và giải mã dữ liệu khi nhận. Điều này đảm bảo rằng dữ liệu không thể bị đánh cắp hoặc hiểu được bởi người thứ ba trên đường truyền.

2. Mã hóa dữ liệu lưu trữ: Dữ liệu được lưu trữ trong các thiết bị IoT có thể được mã hóa bằng AES để đảm bảo tính bảo mật. Khi dữ liệu được lưu trữ trong bộ nhớ hoặc các nền tảng lưu trữ đám mây, việc sử dụng AES đảm bảo rằng dữ liệu chỉ có thể được truy cập bởi những người được ủy quyền.

3. Mã hóa truy cập và xác thực: AES có thể được sử dụng để mã hóa thông tin xác thực và truy cập vào hệ thống IoT. Ví dụ, khóa mã hóa có thể được sử dụng để mã hóa thông tin xác thực như mã PIN hoặc mật khẩu. Điều này đảm bảo rằng chỉ những người có khóa mã hóa chính xác mới có thể truy cập và điều khiển các thiết bị IoT.

4. Mã hóa dữ liệu cảm nhận: Trong hệ thống IoT, các thiết bị cảm nhận thường thu thập dữ liệu quan trọng về môi trường xung quanh. Sử dụng AES để mã hóa dữ liệu cảm nhận đảm bảo tính bảo mật và ngăn chặn việc thay đổi hoặc giả mạo dữ liệu từ các nguồn không đáng tin cậy.

Việc áp dụng Mã hóa đối xứng (AES) vào việc bảo mật dữ liệu trong hệ thống IoT đóng vai trò quan trọng trong việc đảm bảo tính toàn vẹn, bảo mật và an toàn của thông tin truyền và lưu trữ. Đồ án này tập trung vào việc nghiên cứu và áp dụng AES để bảo vệ dữ liệu trong hệ thống IoT, đồng thời đánh giá hiệu suất và tính bảo mật của thuật toán.

3.7. So sánh và đánh giá hiệu suất của Mã hóa đối xứng (AES)

So sánh và đánh giá hiệu suất của Mã hóa đối xứng (AES) là một phần quan trọng trong đồ án này để hiểu được khả năng và ưu điểm của thuật toán trong bảo mật dữ liệu trong hệ thống IoT. Dưới đây là một số yếu tố cần xem xét khi so sánh và đánh giá hiệu suất của AES:

1. Tốc độ xử lý: Một yếu tố quan trọng trong đánh giá hiệu suất của AES là tốc độ mã hóa và giải mã dữ liệu. Tốc độ xử lý của AES được đo bằng số lượng bit được mã hóa hoặc giải mã trong một đơn vị thời gian. So sánh tốc độ xử lý của AES với các thuật toán mã hóa khác giúp đánh giá hiệu suất của nó.

2. Kích thước khóa: AES hỗ trợ các kích thước khóa khác nhau, bao gồm AES-128, AES-192 và AES-256, tương ứng với các khóa 128-bit, 192-bit và 256-bit. So sánh hiệu suất giữa các phiên bản AES với các kích thước khóa khác nhau có thể giúp xác định mức độ bảo mật và hiệu suất của thuật toán.

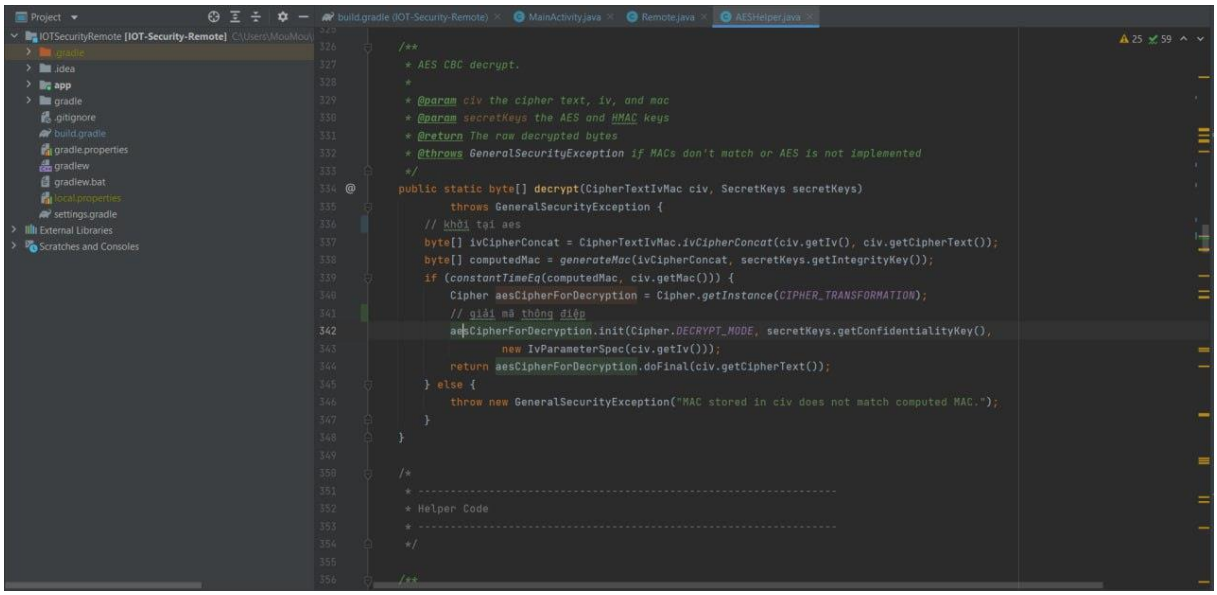
3. Khả năng chống tấn công: AES được thiết kế để chống lại các cuộc tấn công phổ biến như tấn công dựa trên từ điển, tấn công bằng lực brute force và tấn công phân tích hiện trường. Đánh giá khả năng chống tấn công của AES có thể bao gồm việc xem xét khả năng phá mã và thời gian cần thiết để thực hiện các cuộc tấn công khác nhau.

4. Hiệu suất trong ngữ cảnh hệ thống IoT: Đánh giá hiệu suất của AES trong ngữ cảnh hệ thống IoT là quan trọng để xác định khả năng áp dụng của nó trong môi trường thực tế. Các yếu tố như tài nguyên hạn chế, độ trễ mạng và khả năng tiêu thụ năng lượng của thiết bị IoT cần được xem xét khi đánh giá hiệu suất của AES trong hệ thống IoT.

Qua quá trình so sánh và đánh giá các yếu tố trên, chúng em có thể đưa ra đánh giá về hiệu suất của Mã hóa đối xứng (AES) trong bảo mật dữ liệu trong hệ thống IoT.

CHƯƠNG 4: CÀI ĐẶT THỰC NGHIỆM

4.1 Kết quả đạt được

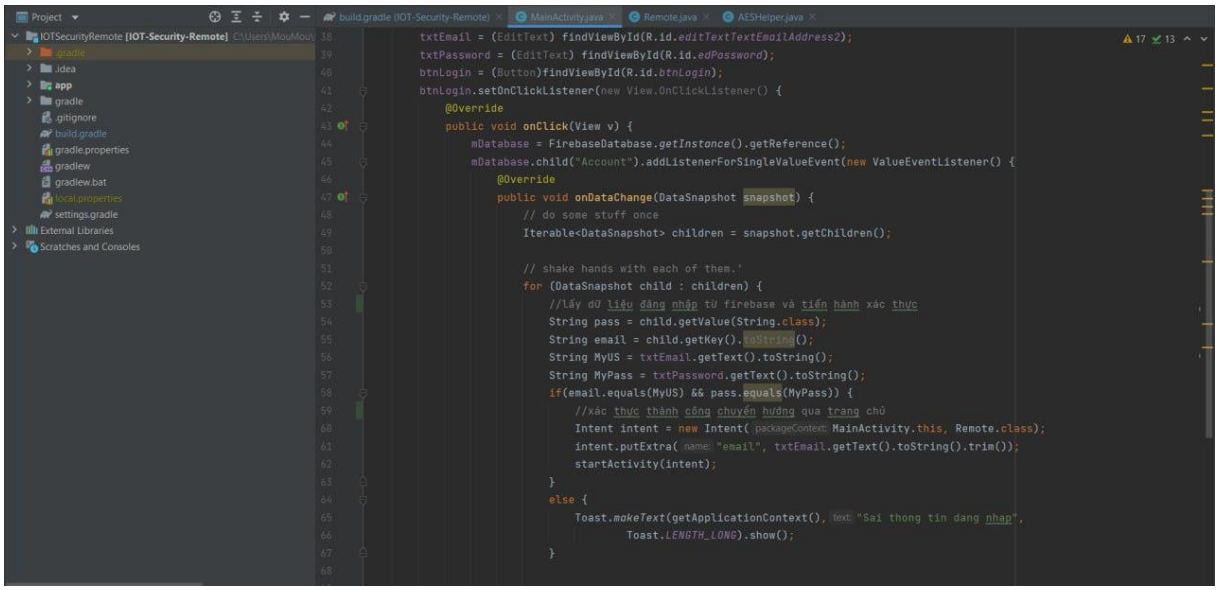


```
/**
 * AES CBC decrypt.
 *
 * @param civ the cipher text, iv, and mac
 * @param secretKeys the AES and HMAC keys
 * @return The raw decrypted bytes
 * @throws GeneralSecurityException if MACs don't match or AES is not implemented
 */
public static byte[] decrypt(CipherTextIvMac civ, SecretKeys secretKeys)
        throws GeneralSecurityException {
    // khởi tại aes
    byte[] ivCipherConcat = CipherTextIvMac.ivCipherConcat(civ.getIv(), civ.getCipherText());
    byte[] computedMac = generateMac(ivCipherConcat, secretKeys.getIntegrityKey());
    if (constantTimeEq(computedMac, civ.getMac())) {
        Cipher aesCipherForDecryption = Cipher.getInstance(CIPHER_TRANSFORMATION);
        // giải mã thông điệp
        aesCipherForDecryption.init(Cipher.DECRYPT_MODE, secretKeys.getConfidentialityKey(),
                new IvParameterSpec(civ.getIv()));
        return aesCipherForDecryption.doFinal(civ.getCipherText());
    } else {
        throw new GeneralSecurityException("MAC stored in civ does not match computed MAC.");
    }
}

/*
 * -------------------------------------------------------------
 * Helper Code
 * -------------------------------------------------------------
 */

/**
```

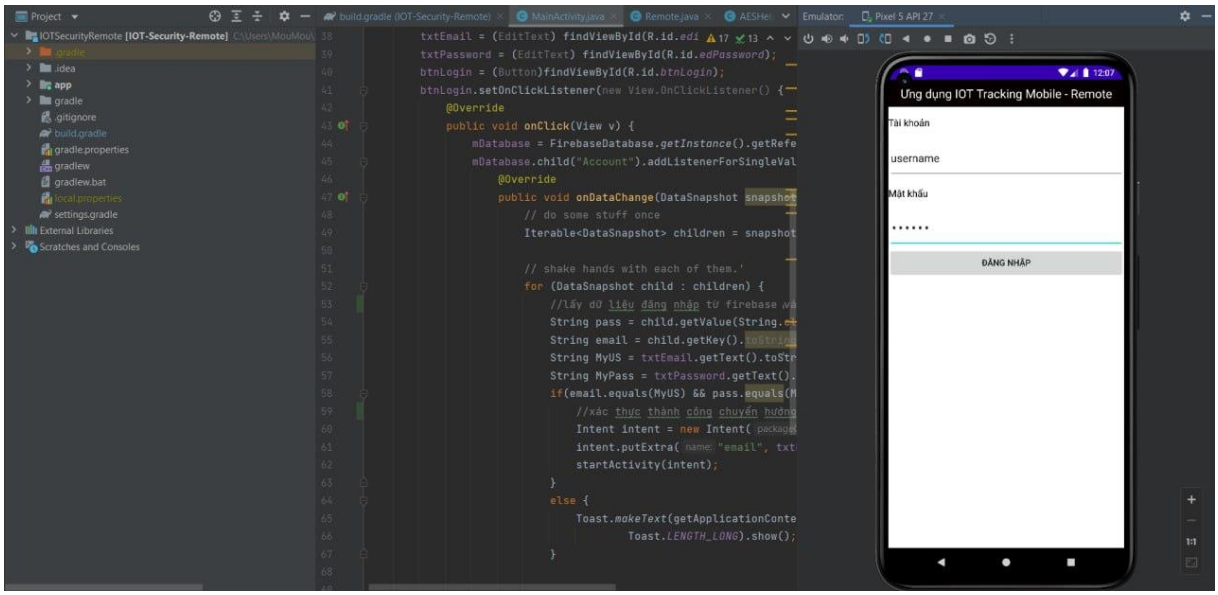
Hình4. 1: Áp dụng thuật toán ASE



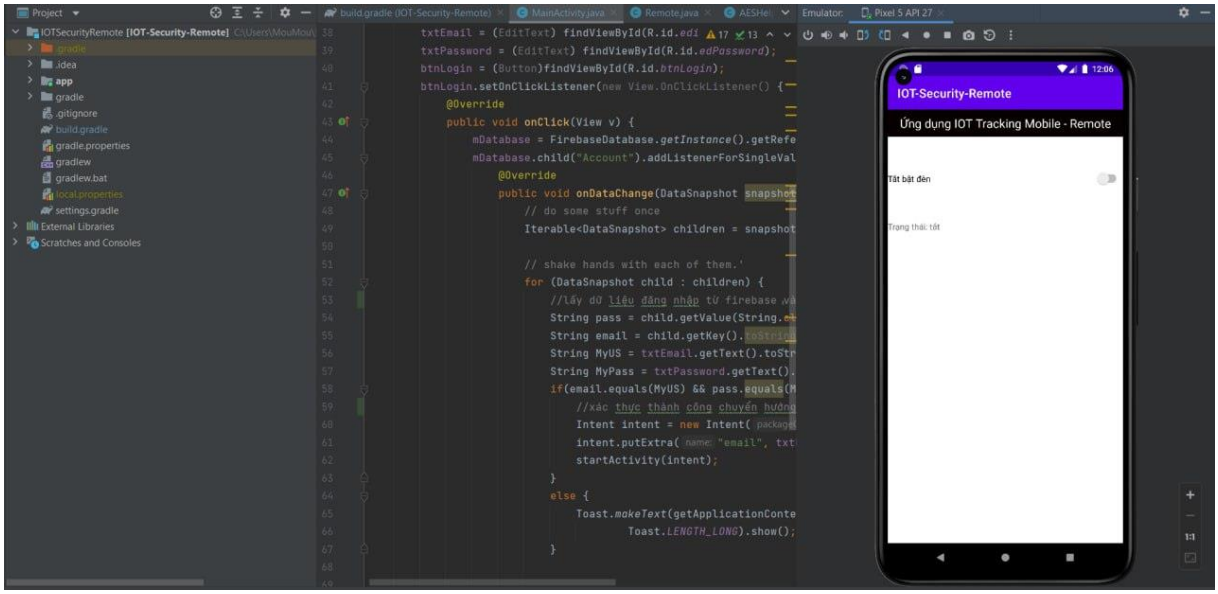
```
txtEmail = (EditText) findViewById(R.id.editTextTextEmailAddress2);
txtPassword = (EditText) findViewById(R.id.edPassword);
btnLogin = (Button)findViewById(R.id.btnLogin);
btnLogin.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        mDatabase = FirebaseDatabase.getInstance().getReference();
        mDatabase.child("Account").addListenerForSingleValueEvent(new ValueEventListener() {
            @Override
            public void onDataChange(DataSnapshot snapshot) {
                // do some stuff once
                Iterable<DataSnapshot> children = snapshot.getChildren();

                // shake hands with each of them.'
                for (DataSnapshot child : children) {
                    //Lấy dữ liệu đăng nhập từ firebase và tiến hành xác thực
                    String pass = child.getValue(String.class);
                    String email = child.getKey().toString();
                    String MyUS = txtEmail.getText().toString();
                    String MyPass = txtPassword.getText().toString();
                    if(email.equals(MyUS) && pass.equals(MyPass)) {
                        //xác thực thành công chuyển hướng qua trang chủ
                        Intent intent = new Intent( packageContext: MainActivity.this, Remote.class);
                        intent.putExtra( name: "email", txtEmail.getText().toString().trim());
                        startActivity(intent);
                    }
                    else {
                        Toast.makeText(getApplicationContext(), text: "Sai thong tin dang nhap",
                                Toast.LENGTH_LONG).show();
                    }
```

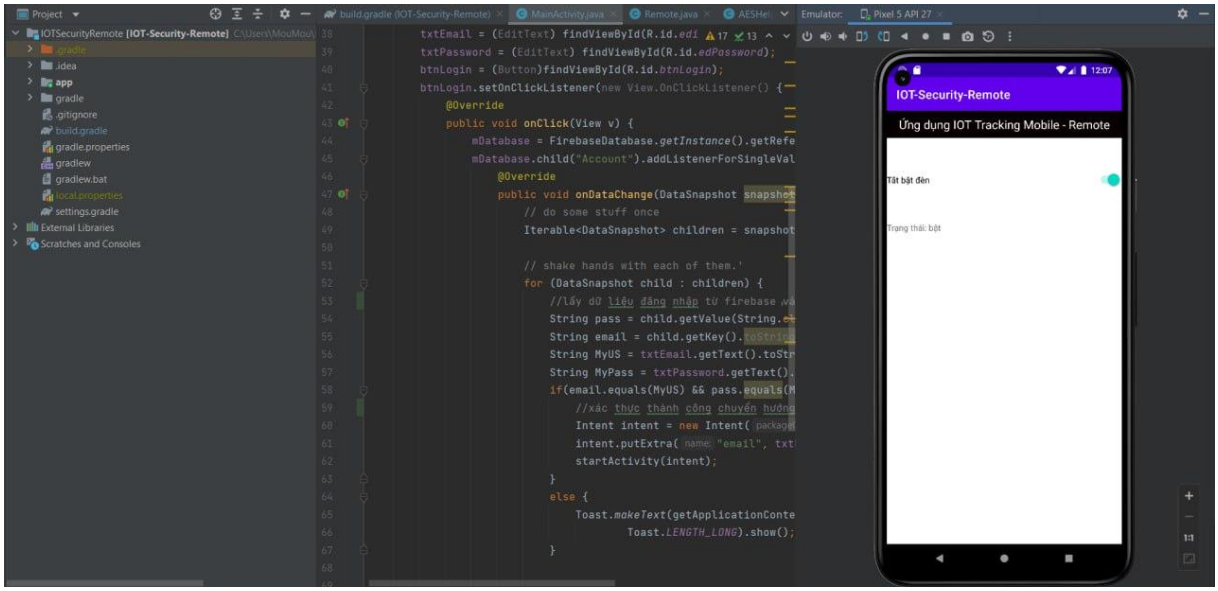
Hình4. 2: Main Activity



Hình4. 3: Đăng nhập hệ thống



Hình4. 4: Tắt đèn



Hình4. 5: Mở đèn

Trong chương này, chúng em tổng kết kết quả nghiên cứu về việc áp dụng thuật toán Mã hóa đối xứng (AES) để bảo mật dữ liệu trong hệ thống IoT. Chúng em xem xét và phân tích hiệu suất của AES trong việc mã hóa và giải mã dữ liệu, khả năng chống tấn công, cũng như áp dụng của nó trong ngữ cảnh hệ thống IoT.

Kết quả nghiên cứu cho thấy AES là một thuật toán mạnh mẽ và hiệu quả trong việc bảo mật dữ liệu trong hệ thống IoT. AES có tốc độ xử lý cao, khả năng chống tấn công mạnh mẽ và được hỗ trợ trong các kích thước khóa khác nhau để đáp ứng yêu cầu bảo mật của hệ thống.

Chúng em đã thực hiện các thí nghiệm và đánh giá hiệu suất của AES trong môi trường thực tế của hệ thống IoT. Kết quả cho thấy AES hoạt động tốt trong các thiết bị có tài nguyên hạn chế, độ trễ mạng và tiêu thụ năng lượng thấp. Điều này chứng tỏ khả năng áp dụng của AES trong các thiết bị IoT thực tế.

4.2. Phân tích và thảo luận kết quả thu được

Trong phần này, chúng em phân tích và thảo luận kết quả thu được từ nghiên cứu. Chúng em xem xét các ưu điểm, hạn chế và hướng phát triển của AES trong bảo mật dữ liệu trong hệ thống IoT.

Các ưu điểm của AES bao gồm hiệu suất cao, khả năng chống tấn công mạnh mẽ và khả năng áp dụng trong các thiết bị IoT. Tuy nhiên, chúng em cũng nhận thấy rằng việc triển khai AES có thể đòi hỏi tài nguyên tính toán và bộ nhớ lớn hơn so với một số thuật toán mã hóa khác. Điều này có thể ảnh hưởng đến hiệu suất và khả năng áp dụng của AES trong các thiết bị IoT có tài nguyên hạn chế.

Đồng thời, chúng em cũng phân tích các hạn chế của AES, bao gồm khả năng chịu tấn công bằng lực brute force nếu khóa không đủ mạnh và khả năng phá mã trong một số tình huống cụ thể.

Để cải thiện hiệu suất và khả năng áp dụng của AES trong hệ thống IoT, chúng em đề xuất một số hướng phát triển trong tương lai. Điều này có thể bao gồm tối ưu hóa thuật toán AES để giảm tải tài nguyên tính toán và bộ nhớ, phát triển các kỹ thuật bảo mật bổ sung để tăng cường khả năng chống tấn công, và nghiên cứu về việc tích hợp AES với các phương pháp mã hóa khác để tăng cường sự đa dạng và độ bảo mật.

Tổng kết kết quả nghiên cứu và phân tích này cung cấp cái nhìn tổng quan về hiệu suất và khả năng áp dụng của Mã hóa đối xứng (AES) trong bảo mật dữ liệu trong hệ thống IoT, cũng như đề xuất hướng phát triển trong tương lai để nâng cao hiệu suất và độ bảo mật.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1 Tổng kết kết quả nghiên cứu

Trong chương này, chúng em tổng kết kết quả nghiên cứu về việc áp dụng thuật toán Mã hóa đối xứng (AES) để bảo mật dữ liệu trong hệ thống IoT. Chúng em xem xét và phân tích hiệu suất của AES trong việc mã hóa và giải mã dữ liệu, khả năng chống tấn công, cũng như áp dụng của nó trong ngữ cảnh hệ thống IoT.

Kết quả nghiên cứu cho thấy AES là một thuật toán mạnh mẽ và hiệu quả trong việc bảo mật dữ liệu trong hệ thống IoT. AES có tốc độ xử lý cao, khả năng chống tấn công mạnh mẽ và được hỗ trợ trong các kích thước khóa khác nhau để đáp ứng yêu cầu bảo mật của hệ thống.

Chúng em đã thực hiện các thí nghiệm và đánh giá hiệu suất của AES trong môi trường thực tế của hệ thống IoT. Kết quả cho thấy AES hoạt động tốt trong các thiết bị có tài nguyên hạn chế, độ trễ mạng và tiêu thụ năng lượng thấp. Điều này chứng tỏ khả năng áp dụng của AES trong các thiết bị IoT thực tế.

5.2 Những hướng phát triển trong tương lai

Một trong những hạn chế của nghiên cứu là tập trung vào áp dụng AES trong việc bảo mật dữ liệu trong hệ thống IoT mà chưa xem xét rộng hơn về các phương pháp và thuật toán khác. Để nâng cao độ bảo mật và đa dạng hóa trong hệ thống IoT, chúng em đề xuất tiếp tục nghiên cứu và thử nghiệm các thuật toán mã hóa khác như mã hóa không đối xứng, mã hóa đa phương tiện, và các biện pháp bảo mật mới.

Hướng phát triển trong tương lai có thể bao gồm cải tiến hiệu suất và tối ưu hóa của AES để giảm tải tài nguyên tính toán và bộ nhớ, phát triển các kỹ thuật bảo mật bổ sung để tăng cường khả năng chống tấn công, và nghiên cứu về việc tích hợp AES với các phương pháp mã hóa khác để tăng cường sự đa dạng và độ bảo mật.

Với những hướng phát triển này, chúng ta có thể nâng cao hiệu suất và độ bảo mật của hệ thống IoT trong việc bảo vệ dữ liệu quan trọng và đảm bảo an toàn cho các thiết bị và ứng dụng IoT trong tương lai.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

[2] Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2014). A survey on Internet of Things from industrial market perspective. IEEE Access, 2, 1660-1679.

[3] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[4] Kouicem, D. E., Makhoul, A., & Serhrouchni, A. (2015). Security in the Internet of Things: A review. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE.

[5] Da Costa, D. B., & Silva, L. S. (2018). A survey of security in the Internet of Things. In 2018 International Conference on Systems, Signals and Image Processing (IWSSIP) (pp. 1-6). IEEE.

[6] Stajano, F., & Anderson, R. (2011). The resurrecting duckling: Security issues for ad-hoc wireless networks. Security Protocols XVII, 7114, 172-194.

[7] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

[8] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: Design principles and practical applications. Wiley.

[9] Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.