BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH

KHOA ĐÀO TẠO CHẤT LƯỢNG CAO

ĐỒ ÁN CNTT

NHÓM 05

CHỦ ĐỀ: AN TOÀN CHO HỆ THỐNG MẠNG IOT

Mã môn học: PROJ215879_22_1_16CLC

Thành viên thực hiện:

Huỳnh Trung Nhân 20110532

Huỳnh Hùng Phú 20110540

GVHD: TS Huỳnh Nguyên Chính

Tp. Hồ Chí Minh, tháng 12 năm 2022

Mục lục

DANH MỤC CHỮ VIẾT TẮT

IoTs	Internet of Things	Mạng lưới vạn vật kết nối Internet
RFID	Radio Frequency Identification	Nhận dạng tần số vô tuyến
IIoTs	Industrial Internet of Things	Cấu trúc Internet of Things
IP	Internet Protocol	Giao thức mạng
IoM	Internet of Media	Mạng đa phương tiện
IoS	Internet of Services	Dịch vụ mạng
MEMS	Microelectromechanical system	Hệ vi điện cơ
RF	Radio Frequence	Tần số vô tuyến
LF	Low frequence	Dải tần số thấp
WSNs	Wireless sensor network	Mạng cảm biến không dây
MAC	Medium Access Control	Điều khiển truy nhập truyền thông
WPAN	Wireless Personal Area Networks	Mạng cá nhân không dây
RSN	Network senson RFID	Mạng cảm biến nhận dạng tần số vô tuyến điện
NFC	Near Field Communication	Giao thức giao tiếp trường gần
BLE	Bluetooth Low Energy	Bluetooth năng lương thấp
PHY	Physical layer	Lớp vật lý
GATT	Generic Access Profile	Cấu hình truy cập chung

Wifi	Wireless Fidelity	Wifi
LAN	Local Area Network	Mạng cục bộ
LR-WPAN	Low rate- wireless private area networks	Mạng tư nhân không dây tốc độ thấp
QoS	Quality of Service	Chất lượng dịch vụ
DSSS	Direct sequence spread spectrum	Phương pháp trực tiếp phổ chuỗi lây lan
PAN	Personal Area Networks	Mạng cá nhân
LTE	Long-Term Evolution	Phát triển dài hạn
LTE-A	Long Term Evolution Advanced	Phát triển tiến hóa dài hạn
MTC	Machine Type Communication	Loại máy truyền thông
OFDMA	Orthogonal Frequency Division Multiple Access	Phân chia đa truy nhập tần số trực giao
PRB	Physical resource blocks	Khối tài nguyên vật lý
RAN	Radio Access Network	Mạng truy nhập vô tuyến
CN	Core Network	Mạng lõi
MTCG	MTC gate	Cổng MTC
RTOS	Real Time Operating Syste	Hệ thống điều hành thời gian thực
BAS	Building Automation	Hệ thống tự động hóa

	Systems	
ITS	lntelligent Transport System	Hệ thống giao thông thông minh
T-CPS	Transportation Cyber Physical Systems	Hệ thống vật lý máy ảnh trong giao thông vận tải
RDF	Resource Description Framework	Khung mô tả nguồn
EXI	Efficient XML Interchange	Sự trao đổi XML hiệu quả
XML	Xtensible Markup Language	Mở rộng ngôn ngữ đánh dấu
CoAP	Constrained Application Protocol	Giao thức ứng dụng ép buộc
REST	Presentational State Transfer	Chuyển đổi trạng thái biểu diễn
HTTP	Hypertext Transfer Protocol	Giao thức siêu chuyển đổi

UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
DTLS	Datagram TLS	Bảo mật lớp vận chuyển dữ liệu
MQTT	Message Queue Telemetry Transport	Chuyển giao từ xa dòng bản tin

TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
XMPP	Extensible Messaging and Presence Protocol	Bản tin mở rộng và giao thức hiện tại
IM	instant messaging	Tin nhắn nhanh
AMQP	Advanced Message Queuing Protocol	Giao thức hàng đợi bản tin cấp cao
DDS	Data Distribution Service	Dịch vụ phân phối dữ liệu
OMG	Object Management Group	Nhóm Squản lí đối tượng
DCPS	Data-Centric PublishSubscribe	Trung tâm dữ liệu theo dõi công khai
DLRL	Data-Local Reconstruction Layer	Lớp tái tạo dữ liệu cục bộ
RPL	Routing Protocol for Low Power and Lossy Networks	Giao thức định tuyến cho mạng suy hao và mạng công suất thấp
DAO	Destination Advertisement Object	Đối tượng đến đích
6LowPAN	Low power Wireless Personal Area Networks	Mạng cá nhân không dây công suất thấp
HAN	Home Automation Networks	Mạng tự động trong nhà
TLS	Transport Layer Security	Bảo mật lớp vận chuyển

API	Application Programming Interfaces	Giao thức lập trình ứng dụng
OEM	Original Equipment Manufacturers	Sản xuất thiết bị nguồn
ISP	Internet service provider	Nhà cung cấp dịch vụ Internet
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông châu Âu
PMI	Physical Mobile Interaction	Giao diện di động lớp vật lý
ERP	Enterprise Resource Planning	Hoạch định nguồn lực doanh nghiệp
CIM	City Information Model	Mô hình thông tin thành phố
W3C	World Wide Web Consortium	Nhiệm vụ hướng dẫn World Wide Web
IETF	Internet Engineering Task Force	Lực lượng đặc nhiệm kỹ thuật Internet
IEEE	EPCglobal IEEE	Viện kỹ nghệ Điện và Điện Tử EPCglobal
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông châu Âu

ICT	Information and Communications Technology.	Công nghệ thông tin và truyền thông
TTDL	Data Center Downtime	Trung tâm dữ liệu

Danh mục hình ảnh

LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành đến trường Đại học sư phạm kỹ thuật thành phố Hồ Chí Minh đã đưa môn học Đồ án công nghệ thông tin vào chương trình giảng dạy. Đặc biệt, chúng em xin cảm ơn sâu sắc thầy Huỳnh Nguyên Chính đã dạy dỗ, truyền đạt những kiến thức quý báu cho chúng em trong suốt kỳ học vừa qua. Trong suốt thời gian qua, chúng em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập, làm việc nhóm hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu và là hành trang để chúng em có thể vững bước sau này.

Do sự tiếp nhận kiến thức của mỗi chúng em luôn tồn tại những hạn chế nhất định, nên trong đồ án cuối kỳ không tránh khỏi những thiếu sót. Vì vậy, chúng em mong nhận được những đóng góp ý kiến đến từ thầy để đồ án của chúng em đạt được kết quả tốt nhất.

Chúng em xin kính chúc thầy sức khoẻ, hạnh phúc, thành công trên con đường sự nghiệp của mình!

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong quá trình phát triển của con người, những cuộc các mạng về công nghệ đóng một vai trò rất quan trọng, chúng làm thay đổi từng ngày, từng giờ cuộc sống của con người, theo hướng hiện đại hơn. Trong đó có thể kể đến Internet of Things – IoTs, là một xu hướng công nghệ mới đang được phát triển rất nhanh chóng làm thay đổi cách sống và phương thức làm việc của con người.

Yếu tố chính cho phép của mô hình IoTs là sự tích hợp của nhiều công nghệ và giải pháp truyền thông, công nghệ nhận dạng và theo dõi, các mạng cảm biến và bộ truyền động có dây và không dây, giao thức truyền thông nâng cao, và khả năng phân tán cho các đối tượng thông minh là phù hợp nhất. Là một trong những thứ có thể dễ dàng hình dung, đóng góp cho sự tiến bộ của Internet of Things đó chính là kết quả của các hoạt động trong các lĩnh vực kiến thức khác nhau như viễn thông, tin học, điện tử và khoa học xã hội cho thấy tầm nhìn phát triển của Internet áp dụng vào cuộc sống của con người.

IoTs được coi là giai đoạn phát triển kế tiếp của Internet, mở ra một cuộc cách mạng trong việc giao tiếp giữa con người - đồ vật và giữa các đồ vật với nhau. Tuy nhiên, để có thể khai thác được những tiềm năng lớn mà IoTs mang lại, còn nhiều vấn đề cần phải giải quyết, trong đó có vấn đề bảo mật cho các thiết bị và hệ thống IoTs.

Xuất phát từ những lý do đó, cùng với sự định hướng của GV. Huỳnh Nguyên Chính , nhóm em đã chọn đề tài nghiên cứu: “AN TOÀN CHO HỆ THỐNG MẠNG IOT” để hiểu rõ hơn về an toàn, bảo mật của công nghệ này.

2. Tổng quan về vấn đề nghiên cứu

Thực tế, Internet of things (IoTs) đã được nhắc đến từ nhiều thập kỷ trước. Tuy nhiên mãi đến năm 1999 cụm từ IoTs mới được đưa ra bởi Kevin Ashton, Ông là một nhà khoa học đã sáng lập ra Trung tâm Auto-ID ở đại học Massachusetts Institute of Technology (MIT), nơi thiết lập các quy chuẩn toàn cầu cho RFID (một phương thức giao tiếp không dây dùng sóng radio) cũng như một số loại cảm biến khác. Đơn giản hơn IoTs là tất cả các thiết bị có thể kết nối với nhau. Việc kết nối có thể thực hiện qua Wi-Fi, mạng viễn thông băng rộng (3G, 4G), Bluetooth, ZigBee, hồng ngoại… Các thiết bị có thể là điện thoại thông minh, máy fax, máy giặt, tai nghe, quạt điện, hệ thống chiếu sáng đều có thể kết nối với nhau.

Hình 1: Tổng quan Internet of things (IoTs)

Internet of Things hay nói cách khác là mạng lưới vạn vật kết nối Internet viết tắt là IoTs (Internet of Things). Đây là một mô hình mới của truyền thông không dây hiện đại, là sự xuất hiện của nhiều vật hay nhiều đối tượng – đặc biệt đó là thẻ Radio Frequency Identification (RFID), cảm biến, thiết bị truyền động, điện thoại di động.

Công nghệ truy cập Internet đóng vai trò chủ chốt. Bất kỳ thiết bị với một địa chỉ IP đều có thể được định vị và truy cập bởi các dịch vụ web thiết lập một mạng lưới mở chung cho tất cả các thiết bị trên một khung làm việc Internet. IoTs bao gồm tất cả, từ việc định nghĩa một mạng mà có thể thu thập dữ liệu của "bất cứ thứ gì" trên thế giới, bộ giám sát sức khỏe cá nhân, giám sát thời tiết, nhà thông minh, quản lý, đến các nhà máy công nghiệp. Khi nói về các nhà máy (nơi mà những thiết bị công nghiệp như cảm biến, công tắc, robot, máy móc tự động hóa, cơ điện tử, là "những thứ" được kết nối), tập hợp này của Internet of Things được gọi là Industrial Internet of Things (IIoTs). Industrial Internet of Things sẽ liên kết giữa người tiêu dùng và các doanh nghiệp trên một cấu trúc Internet, khối lượng lớn thông tin được thu thập bởi các thành phần trong mạng, có thể được tận dụng để ứng dụng cho các doanh

nghiệp để đưa ra các quyết định kinh doanh một cách nhanh chóng, kịp thời.

Khi Internet là một phương tiện truyền thông kỹ thuật số phổ biến trên toàn thế giới, việc sử dụng dữ liệu kết nối toàn cầu qua Internet phục vụ cho các lợi ích của việc sản xuất công nghiệp vẫn còn là lý thuyết, vì rất ít các giải pháp công nghệ trong công nghiệp sẵn có để có thể triển khai trên thực tế.

Mặc dù vậy trong tương lai các nhà máy sẽ tìm hiểu để khai thác triệt để sức mạnh của Internet không chỉ để kết nối các thiết bị tại nhà máy, mà còn để đồng bộ các dữ liệu cần thiết thông qua mạng.

Dự đoán trong tương lai" những thiết bị có thể được kết nối, những thứ gì sẽ được kết nối". Nhưng tại sao lại muốn chúng kết nối với nhau? Chẳng hạn vấn đề giao thông thường hay bị tắc nghẽn ở các giờ cao điểm, nếu IoTs được ứng dụng giúp con người có thể tham khảo lịch làm việc và đề xuất tuyến đường đi tốt nhất để tránh tắc đường và không bị trễ giờ.

Đặc biệt ứng dụng của IoTs trong phạm vi lớn hơn, như IoTs có thể được áp dụng trong mạng lưới giao thông vận tải trong thành phố (smart city), giúp giảm thiểu lãng phí và nâng cao hiệu quả hạ tầng và sử dụng năng lượng. IoTs có rất nhiều ưu thế cho phép kết nối mọi thứ ở tất cả mọi nơi. Tuy nhiên, tác động của nó bên cạnh giá trị mang lại thì IoTs cũng phải trải qua những thách thức như bảo mật là một trong những vấn đề lớn khi hàng tỉ thiết bị kết nối với nhau và phải làm sao cho dữ liệu kết nối giữa thiết bị được an toàn. Và thành phần trong mạng lưới này tăng lên do khối lượng dữ liệu khổng lồ mà các thiết bị kết nối sản sinh ra. Vì thế cần lên kế hoạch lưu trữ, theo dõi, phân tích và xử lý thông tin có ý nghĩa từ lượng dữ liệu lớn đó.

- IoTs có thể điều khiển chức năng ngành công nghiệp và đời sống hàng ngày.
- Cải thiện tỷ lệ sử dụng nguồn năng lượng.
- Tích hợp hệ thống vật lý và hệ thống xã hội con người, có cấu hình linh động.
- Kết nối mạng và giao thông trên thế giới.
- Đóng vai trò tích hợp công nghệ, kết nối các thiết bị tương tác với nhau.

Như vậy khi mọi thứ đã được "Internet hóa", sự điều khiển, quản lý cấp cao có thể truy cập vào các thiết bị kết nối ở bất cứ nơi đâu, chỉ cần một chiếc

điện thoại, máy tính bảng hay đồng hồ thông minh đều có thể kết nối Internet.

Trong luận văn này vấn đề an ninh trong IoTs sẽ được giới thiệu một cách chi tiết về đặc điểm thành phần, các nguy cơ, kiến trúc, ứng dụng cùng với những thách thức phải vượt qua của một ngành công nghệ phát triển, xu hướng tất yếu của tương lai.

Đề tài thảo luận về các vấn đề sau:

Chương 1: Tổng quan và an toàn bảo mật trong internet of things

Chương 2: Kiến trúc cơ sở hạ tầng và các kỹ thuật an ninh chủ yếu trong IoTs

Chương 3: Một số thách thức cùng hướng phát triển trong tương lai và ứng dụng bảo mật iots dựa trên công nghệ lấy mẫu nén Kết luận

3. Phân công công việc

STT	Tên SV	Công việc thực hiện	Phần trăm đóng góp
1	Huỳnh Trung Nhân	- TỔNG QUAN VÀ AN TOÀN BẢO MẬT TRONG IOTS , KIẾN TRÚC CƠ SỞ HẠ TẦNG VÀ CÁC KỸ THUẬT AN NINH CHỦ YẾU TRONG IOTS - Nghiên cứu thuật toán xử lý dữ liệu dựa trên biến đổi wavelet	50 %
2	Huỳnh Hùng Phú	- MỘT SỐ THÁCH THỨC CÙNG HƯỚNG PHÁT TRIỂN TRONG TƯƠNG LAI VÀ ỨNG DỤNG BẢO MẬT IOTS DỰA TRÊN CÔNG NGHỆ LẤY MẪU NÉN - Thuật toán xử lý dữ liệu dựa trên công nghệ lấy mẫu nén (cs) , thiết kế cisco packet tracer	50 %

CHƯƠNG 1: TỔNG QUAN VÀ AN TOÀN BẢO MẬT TRONG IOTS

IoTs là một mô hình mới nhanh chóng phát triển trên nền tảng của truyền thông không dây hiện đại. Ý tưởng cơ bản của khái niệm này là sự hiện diện phổ biến của nhiều thiết bị hay đối tượng - như thẻ Radio Frequency Identification (RFID), cảm biến, thiết bị truyền động, điện thoại di động… Với tác động của Internet of things (IoTs) có thể thay đổi hoàn toàn cách sống của con người. Khi mọi vật đã được "internet hóa" người dùng có thể điều khiển chúng từ bất cứ nơi nào, không bị giới hạn về mặt không gian và thời gian chỉ cần một thiết bị thông minh có kết nối internet. Các ứng dụng IoTs sẽ đóng góp to lớn cho sự phát triển của thế giới và Internet of things đang bắt đầu được khai thác.

1.1 Khái niệm công nghệ IoTs

IoTs tạm dịch là vạn vật kết nối Internet, là một tập hợp các thiết bị có khả năng kết nối với nhau, với Internet và với thế giới bên ngoài để thực hiện việc thu thập dữ liệu, giám sát và điều khiển hệ thống.

Hình 1.1: Mọi vật đều có thể được kết nối

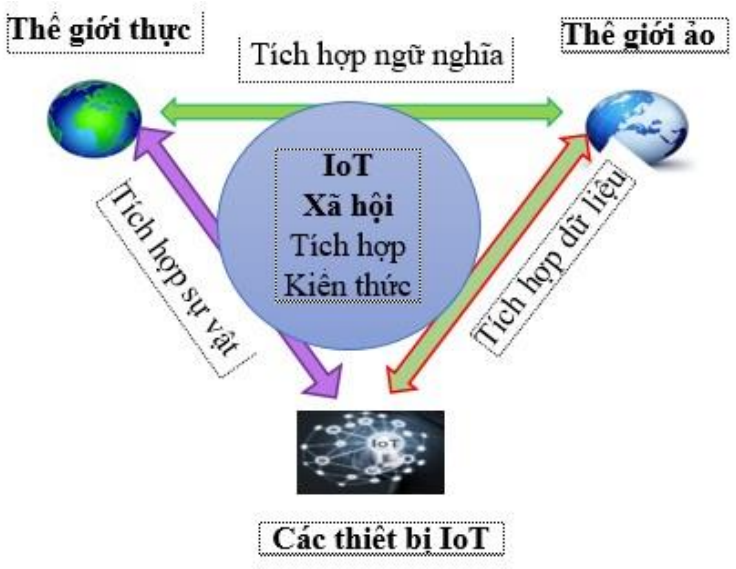
"Things" là sự vật trong Internet of Things, bao gồm tất cả các sự vật thiết bị thông minh và ngay cả con người cũng tham gia vào mạng lưới này, có thể là một con người với màn hình cấy ghép tim, một động vật trang trại với bộ tiếp sóng chip sinh học, một chiếc xe ô tô tích hợp các cảm biến để cảnh báo lái xe khi lốp quá non hoặc bất kỳ đồ vật nào do tự nhiên sinh ra hoặc do con người sản xuất ra được gán với một địa chỉ IP và được cung cấp khả năng truyền tải dữ liệu qua mạng lưới. Con người dễ dàng gán một địa chỉ IP vào một "vật". Tuy nhiên, sự gia tăng

của số lượng các nút thông minh, cũng như số lượng dữ liệu mà các nút tạo ra, gây ra lo ngại về các vấn đề riêng tư, an ninh và chủ quyền dữ liệu.

Internet of Things đòi hỏi: Sự hiểu biết về tình hình của người sử dụng và các thiết bị của con người còn Internet sẽ liên kết chặt chẽ với các giao tiếp gửi nhận thông tin liên lạc.

Mỗi đồ vật, con người đều được cung cấp một địa chỉ riêng biệt và tất cả có khả năng truyền tải trao đổi thông tin dữ liệu qua một mạng duy nhất mà không cần sự tương tác trực tiếp giữa người với người hay giữa người với máy tính. Các thiết bị sẽ có thể chỉ đạo việc chuyển giao, thích nghi với môi trường tương ứng, tự bảo vệ, tự bảo trì, tự sửa chữa và cuối cùng thậm chí còn đóng vai trò tích cực trong việc xử lý riêng. Mọi thứ được "thông minh hóa", đặc biệt là sự có mặt của sensor (cảm biến) để thu thập mọi dữ liệu, có thể tương tác với nhau bất cứ lúc nào, bất cứ nơi đâu và dưới bất kỳ hình thức nào [1, 2].

IoTs không chỉ liên quan đến phần cứng (từ các thiết bị nhỏ cho đến các thiết bị mạng không dây) mà còn có sự can thiệp của phần mềm. Tuy nhiên, trong công nghệ này các bộ cảm biến là những yếu tố quan trọng để xuất dữ liệu từ các đối tượng và từ môi trường. Công nghệ IoTs dự kiến sẽ được áp dụng cho hàng tỉ thiết bị cũng như ứng dụng, từ những chiếc tủ lạnh cho đến không gian đậu xe hay các ngôi nhà cũng sẽ trở nên thông minh hơn trong tương lai. Theo một số ước tính, trên 30 tỷ vật thể sẽ được kết nối cùng với hơn 200 tỷ kết nối không dây [3] sẽ tạo ra xấp xỉ 714 tỷ Euro vào năm 2020 [4]. Với sự gia tăng nhanh chóng trong việc sử dụng ứng dụng IoTs, sự mở rộng các yếu tố và các hạn chế khác nhau về khả năng của thiết bị cũng có nghĩa là các cơ chế mật mã truyền thống, các giao thức bảo mật và các cơ chế bảo vệ không khả dụng hoặc không đủ [6]. An ninh cơ bản phải thiết thực và kiến trúc an ninh phải được thiết kế sao cho chu kỳ của hệ thống dài (> 20 năm), điều đó thực sự là một thách thức. Do đó, phương pháp và công nghệ mới phải được phát triển để đáp ứng các yêu cầu IoTs về mặt an ninh và bảo mật [3]. Trong đó có thể kể đến một số công nghệ hỗ trợ IoTs, như: công nghệ nhận dạng (mạng cảm biến không dây WSN và nhận dạng tần số vô tuyến RFID [1, 5, 8]), công nghệ mạng lưới và truyền thông (công nghệ dây và không dây, ví dụ: GSM và UMTS, Wi-Fi, Bluetooth, ZigBee [9-10]), công nghệ phần mềm và phần cứng (nghiên cứu về các thiết bị nano điện tử tập trung vào việc thu nhỏ, chi phí thấp và tăng chức năng trong thiết kế hệ thống nhận dạng không dây [8]).



Hình 1.2: Tương tác của mạng lưới thiết bị kết nối Internet.

Các giao diện trong hình thức của các dịch vụ dễ dàng tương tác với các vật thông minh qua Internet, truy vấn và thay đổi trạng thái của vật và bất kì thông tin liên quan đến vật đồng thời tham gia bảo mật tài khoản và vấn đề riêng tư. Tầm nhìn của Internet tương lai dựa trên các giao thức truyền thông kết hợp với sự hợp nhất của mạng máy tính, Internet of Media- IoM, Internet of Services- IoS, và IoTs vào một nền tảng IT toàn cầu của mạng và các thiết bị được kết nối. IoS là thành phần nền tảng được sử dụng qua các mạng khác nhau. Mạng tương lai sẽ gồm cơ sở hạ tầng công cộng, cá nhân và khả năng mở rộng cải thiện bằng 'things' đặt gần nhau và kết nối với nhau. Các kết nối không chỉ giữa con người với con người mà còn giữa con người với môi trường. Truyền thông được bao gồm nhiều thiết bị đầu cuối và các trung tâm dữ liệu (dữ liệu nhà, điện toán đám mây..) tăng khả năng lưu trữ và tính sẵn sàng kết nối.

Tuy nhiên IoTs tạo ra mạng lưới hàng tỉ các thiết bị kết nối không dây liên lạc với nhau, nên việc quản lí, giám sát và bảo mật trog IoTs trở nên rất khó khăn, sự phát triển của IoTs trong tương lai sẽ có rất nhiều thách thức cần phải giải quyết như: độ tin cậy, tính di động, hiệu suất, khả năng mở rộng, tương tác, bảo mật, quản lí giám sát…Giải quyết các thách thức này cho phép các nhà cung cấp dịch vụ và người lập trình ứng dụng cần thực hiện các dịch vụ của họ một cách hiệu quả. Đặc biệt là an toàn, bảo mật thông tin.

1.2 Một số ứng dụng trong công nghệ IoTs

1.2.1. Trong giao thông:

Tiềm năng của IoT nằm ở công nghệ cảm ứng trang bị ở mặt đường hoặc phương tiện xe máy, ô tô, tàu điện, xe buýt… IoT cho phép quản lý và kiểm soát giao thông, diều này có thể được thực hiện với sự phối hợp và hợp tác của hạ tầng hệ thống quản lý và kiểm soát giao thông

của thành phố thông minh. Sự kết nối của các phương tiện giao thông với Internet tạo ra vô số những khả năng và ứng dụng mới mang lại những chức năng mới cho cá nhân hoặc việc làm cho việc đi lại dễ dàng và an toàn hơn.

Đối với công tác vận chuyển, điều này mang lại ý nghĩa kinh tế rất lớn. Ngoài ra, việc tiến hành xe không người lái với hệ thống IoT mang tính chính xác và an toàn cao hơn khi từng thông tin nhỏ nhất về những chuyển động trên mặt đường và chuyển động của các phương tiện di chuyển lân cận được thu thập và phân tích theo thời gian thực. Việc xử phạt vi phạm giao thông, do đó, cũng có thể được thực hiện một cách hiệu quả, công bằng, và chính xác.

Hình 1.3: Mô hình thu thập mật độ và cảnh báo tắc nghẽn giao thông

1.2.2 Thành phố thông minh:

Công viên thông minh: giám sát không gian đỗ xe của thành phố.

- Kiểm tra xây dựng: giám sát các rung động và các điều kiện vật chất trong tòa nhà, cầu và các công trình lịch sử.
- Tắc nghẽn giao thông: giám sát các phương tiện và mức độ người đi bộ để tối ưu việc lại xe và đi lại.
- Chiếu sáng thông minh: chiếu sáng thông minh và tương ứng với thời tiết trong hệ thống đèn đường.
- Quản lí chất thải: phát hiện mức độ rác thải trong các container để tối
ưu đường đi thu lượm rác.
- Hệ thống vận tải thông minh: các tuyến đường và đường cao tốc thông minh với việc cảnh báo và điều chỉnh theo điều kiện thời tiết và giảm tránh tai nạn tắc đường.

1.2.3. Trong chăm sóc sức khỏe:

Việc biến bác sĩ và bệnh nhân thành những điểm thu thập dữ liệu với công nghệ theo dõi (tracking), kết hợp với công nghệ xác định (identification) và nhận dạng (authentication), có thể giảm thiểu nguy cơ sai sót trong quá trình khám chữa bệnh, trị bệnh như cho uống nhầm thuốc, nhầm liều thuốc, sai thời gian, sai quy cách, hỗ trợ kịp thời bệnh nhân hay theo dõi tình trạng sức khỏe cộng đồng. Khi từng hành vi của bác sĩ, y tá cũng như bệnh nhân đều được theo dõi và số hóa thành dữ liệu để phân tích, công việc khám chữa bệnh sẽ mang tính chính xác cao hơn.

Hình 1.4: Mô hình chăm sóc sức khỏe

1.2.4. Nhà thông minh:

Các sản phẩm thông minh trong gia đình có thể tự thay đổi nhiệt độ phòng tùy theo cảm ứng nhiệt độ ngoài trời hoặc theo ý thích của người dùng, thay đổi độ sáng của phòng theo thời gian trong ngày…

Đóng mở từng hệ thống rèm tại các phòng riêng, hoặc tất cả các phòng theo lệnh.

Tắt bật từng hệ thống điện chiếu sáng tại toàn bộ các phòng hoặc từng nhóm phòng, từng phòng theo lệnh

Bật nhạc + đèn theo chủ điểm cho từng hệ thống phòng hoặc nhóm phòng theo lệnh.

Với bộ cảm biến IoT, nông dân có thể thu thập dữ liệu về thời tiết, đất, chất lượng không khí và sự phát triển của cây trồng để đưa ra những quyết định thông minh hơn.

Hình 1.5: Mô hình hệ thống nhà thông minh

Đã có nhiều nỗ lực để tiêu chuẩn hóa các dạng phần cứng, phần mềm, điện tử và giao diện giao tiếp cần thiết để xây dựng hệ thống môi trường thông minh. Một số tiêu chuẩn sử dụng thêm dây dẫn liên lạc và điều khiển, một số truyền dẫn thông tin ngay trên hệ thống dây điện sẵn có trong ngôi nhà, một số sử dụng tín hiệu ở tần số vô tuyến điện và một số sử dụng kết hợp đồng thời các giải pháp truyền dẫn khác nhau.

1.2.5. Trong phạm trù cá nhân và xã hội:

IoT có thể giúp thúc đẩy việc kết nối con người với con người ngày càng mạnh mẽ hơn nữa. Tiềm năng của lĩnh vực công nghệ nhận dạng tần số vô tuyến trong ngày có thể bao gồm việc tự động cập nhật các hoạt động sinh hoạt lên mạng xã hội.

Những khả năng này mang đến nhiều lo ngại và nguy cơ tiềm ẩn đến đạo đức thông tin trong môi trường dữ liệu ngày càng nhiều lên, và ngày càng nhanh hơn. Một tiềm năng khác cho công nghệ này là việc người dùng có thể tìm lại và sống lại một cách chính xác lịch sử sinh hoạt của mình vào một thời điểm bất kì trong quá khứ, cũng như có thể giúp người dùng tìm lại được chính xác những vật thể họ đã đánh mất, hoặc đặt nhầm ở đâu đó.

Hình 1.6: Cá nhân và xã hội

1.2.6. Môi trường thông minh:

- Phát hiện cháy rừng: giám sát khí gas đốt cháy và các điều kiện cảnh báo cháy rừng để đưa ra vùng cảnh báo.
- Ô nhiễm không khí: điều khiển khí CO2 thải ra từ nhà máy, các khí gây ô nhiễm từ phương tiện và khí độc trong các nông trại.
- Phòng ngừa lũ quét và chống lở đất: giám sát độ ẩm, các rung chấn, và mật độ đất để phát hiện các mối nguy hiểm theo điều kiện đất. Ngoài ra phát hiện động đất.

1.2.7. Điều khiển trong công nghiệp:

- Các ứng dụng M2M: kiểm soát tài khoản và máy móc chuẩn đoán.
- Chất lượng không khí trong nhà: giám sát khí độc và mức độ khí oxi trong các thiết bị hóa học để đảm bảo cho công nhân và hàng hóa an toàn.
- Giám sát nhiệt độ: kiểm soát nhiệt độ trong công nghiệp.
- Sự có mặt của khí Ozone trong khi làm kho các sản phẩm thịt trong các nhà máy thực phẩm.
- Định vị trong nhà: vị trí tài sản trong nhà bằng cách sử dụng các thẻ tích cực (ZigBee) và bị động (RFID/NFC).
- Các phương tiện tự chuẩn đoán: thu thập thông tin từ CanBus để gửi hình ảnh cảnh báo thời gian thực để nhanh chóng đưa lời khuyên cho lái xe.

1.2.8. Nông nghiệp thông minh:

- Nhà thân thiện với môi trường: kiểm soát điều kiện thời tiết nhỏ để tăng sản lượng rau quả và sản lượng của chúng.
- Mạng lưới trạm thời tiết: nghiên cứu thời tiết trong vùng để dự báo băng, tuyết, mưa, hạn hán, …

- Phân trộn: điều kiện độ ẩm, mức nhiệt trong đất, cỏ rơm để chống nấm, chất chứa vi khuẩn.

1.3. Tầm quan trọng của bảo mật IoTs.

Internet của vạn vật hay IoTs mang tới một viễn cảnh về sự hợp nhất thông tin, nơi không chỉ hệ thống máy tính mà còn là tất cả những thiết bị điện tử xung quanh con người, đều sở hữu khả năng cảm biến, có thể hợp tác với nhau nhằm tạo được sự tiện lợi và thông minh nhất cho cuộc sống con người. Tuy nhiên, chính do sự đa dạng từ mẫu mã, thiết kế, nguồn điện năng tiêu thụ cũng như khả năng xử lý chênh lệch lại gây ra các thách thức vô cùng lớn trong việc định hình một cấu trúc chung cho IoTs cũng như việc đảm bảo an ninh theo cấu trúc chung đó.

Vấn đề quyền riêng tư và bảo mật thông tin, kiểm duyệt thông tin đang đặt ra các bài toán cần giải quyết, với IoTs số lượng các bài toán này còn lớn hơn bởi 3 nguyên nhân chính:

- Các mô hình kinh doanh, ứng dụng, chuẩn hóa giao thức và hạ tầng cơ sở giữa các nhà sản xuất là vấn đề mà các bên tham gia phải cùng giải quyết.
- Việc kết nối hàng tỉ các thiết bị trên thế giới đòi hỏi sự kiểm soát, quản lý chặt chẽ trở nên phức tạp hơn rất nhiều.
- Khi máy móc can thiệp tự động và sâu rộng vào cuộc sống, sự hoạt động ổn định của chúng và cơ chế chống lỗi cũng là vấn đề cần kiểm soát.

1.4. Nguy cơ hệ thống và các hình thức tấn công

Ba vấn đề cốt lõi với IoT là sự riêng tư cho con người, tính bảo mật của các quy trình kinh doanh và khả năng phụ thuộc của bên thứ ba. Người ta thừa nhận rằng trong thiết lập IoTs, có bốn thành phần tương tác (con người, đồ vật, phần mềm và phần cứng) giao tiếp với các mạng công cộng, không đáng tin cậy. Đây là những ràng buộc phải đối mặt với an ninh, bảo mật và tổ hợp những vấn đề mở. Do đó, các câu hỏi liên quan đến người dùng, máy chủ và bên thứ ba đáng tin cậy phải được giải quyết. Trong tình hình như vậy, an ninh có thể được định nghĩa là một khuôn khổ có tổ chức bao gồm các khái niệm, nguyên tắc, chính sách, thủ tục, kỹ thuật và biện pháp cần thiết để bảo vệ hệ thống tài sản cá nhân cũng như toàn thể hệ thống khi chống lại sự đe dọa bất kỳ cố ý hoặc không cố ý. Tất cả những tương tác này cũng phải được đảm bảo bằng cách này hay cách khác, để cung cấp dữ liệu và dịch vụ quan trọng cho tất cả các đối tượng và hạn chế số lượng các sự cố sẽ ảnh hưởng đến toàn bộ IoTs.

1.4.1. Nguy cơ hệ thống

Nguy cơ hệ thống được hình thành bởi sự kết hợp giữa các mối đe dọa tấn công đến an toàn hệ thống và lỗ hổng của hệ thống.

1.4.1.1. Các mối đe dọa

Các mối đe dọa đến hệ thống có thể được phân loại thành:

+ Mối đe dọa bên trong hệ thống: như password, data, update,..

+ Mối đe dọa bên ngoài hệ thống: hacker, virut, internet,..

Mục tiêu đe dọa tấn công: chủ yếu là các dịch vụ an ninh (DNS, www…), user ID, file mật khẩu, vị trí file, địa chỉ mạng,…nhằm lợi dụng quyền truy cập, thay đổi, phá hủy, nghe lén thông tin, ăn cắp phần mềm hoặc phần cứng, nhờ đó làm thay đổi cấu trúc nội dung thông tin hoặc lấy cắp thông tin.

1.4.1.2. Lỗ hổng hệ thống

Là nơi mà đối tượng tấn công có thể khai thác để thực hiện các hành vi tấn công hệ thống. Lỗ hổng hệ thống có thể tồn tại trong hệ thống mạng hoặc trong thủ tục quản trị mạng như:

- Lỗ hổng lập trình (back-door).
- Lỗ hổng Hệ điều hành.
- Lỗ hổng ứng dụng.
- Lỗ hổng vật lý.
- Lỗ hổng trong thủ tục quản lý (mật khẩu, chia sẻ,…).

1.4.2. Các hình thức tấn công mạng.

Vòng đời của mọi thiết bị đều phải trải qua 3 giai đoạn: sản xuất, cài đặt/vận hành và hoạt động. Có rất nhiều tấn công gây ra mất an toàn thông tin và xâm phạm tính riêng tư cho người dùng có thể được thực hiện trong suốt vòng đời của thiết bị.

- *Giai đoạn sản xuất:* Các thiết bị trong IoTs có xu hướng được thiết kế hướng tới một nhiệm vụ cụ thể và không chỉ được phát triển bởi cùng một hãng sản xuất. Điều này dẫn đến các tấn công trong giai đoạn sản xuất như việc sao chép và làm giả thiết bị bất hợp pháp. Các thiết bị sao chép thường được bán với giá rẻ hơn rất nhiều dù có cùng chức năng như các sản phẩm chính hãng. Phần mềm của thiết bị có thể bị thay đổi hoặc cài đặt thêm các chức năng gây hại tới người dùng (ví dụ cửa hậu để ăn cắp thông tin).

- *Giai đoạn cài đặt/vận hành:* thiết bị được cài đặt một định danh và một khóa bí mật được sử dụng trong toàn bộ giai đoạn hoạt động. Thiết bị có thể bị thay thế bởi thiết bị khác có chất lượng thấp hơn nếu quá trình cài đặt không đáng tin cậy. Tấn công giai đoạn này sẽ giúp kẻ tấn công tiết kiệm được tiền cài đặt và có thể thu được lợi nhuận bằng việc bán các sản phẩm chính hãng đã thay thế. Những cuộc tấn công khác trong giai đoạn cài đặt liên quan tới việc chiếm dụng định danh và khóa bí mật gây tổn hại đến quá trình cài đặt trong mạng.

• *Giai đoạn hoạt động:* Những tấn công trong giai đoạn này có thể bao gồm: chặn bắt trên môi trường vật lý, làm gián đoạn hoạt động mạng, từ chối dịch vụ, tấn công nghe lén và các cuộc tấn công điều khiển.

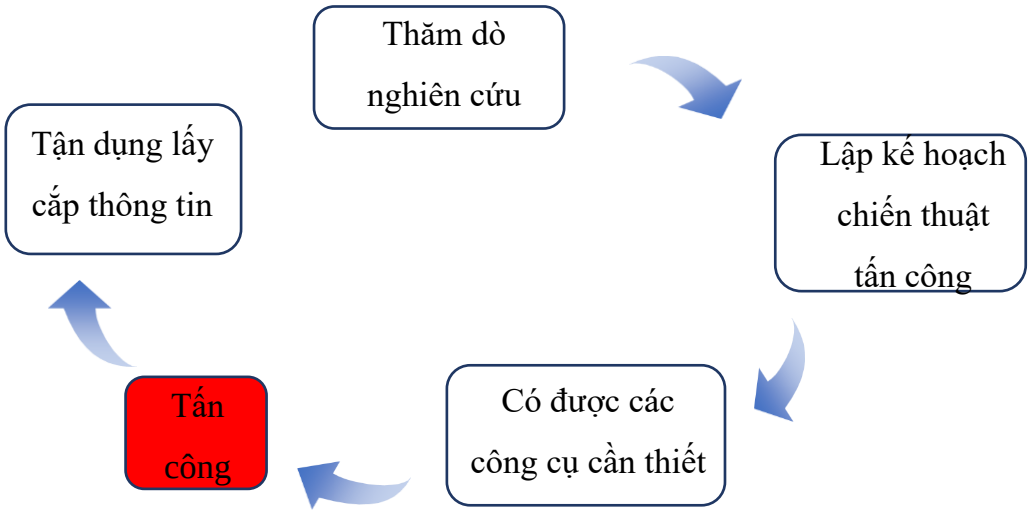
Những hiểm họa an toàn đối với các dịch vụ trong IoTs là do nguyên nhân hạn chế về năng lực tính toán, năng lượng và băng thông kết nối. Để có thể kiểm thử và nhận biết được những mối đe dọa an toàn và các cuộc tấn công vào IoT, dưới đây sẽ khảo sát các hình thức tấn công cụ thể:

- ***Tấn công mạo danh:*** là ăn cắp quyền truy cập của người sử dụng có thẩm quyền, có thể dẫn tới một loạt các tấn công khác như: cung cấp các thông tin điều khiển sai, kiểm soát nút mạng hoặc ảnh hưởng tới truyền thông trên toàn mạng. Một nút mạng giả mạo hình thành khi tấn công giả mạo vào một nút hợp pháp thành công. Khi có nhiều nút giả mạo có thể thực hiện cuộc tấn công trên toàn mạng bằng những nút này.

- ***Tấn công tiêu hao tài nguyên nút:*** xảy ra khi kẻ tấn công liên tục xâm nhập vào mạng, làm tràn bộ nhớ lưu trữ của nút mạng và còn có thể ảnh hưởng xuống nút phía dưới của mạng, gây tiêu hao tài nguyên mạng.

- ***Tấn công nghe lén thụ động:*** nghe lén dữ liệu được truyền đi giữa các nút bằng cách phân tích lưu lượng truyền thông. Qua đó, kẻ tấn công có thể tìm hiểu được về hệ thống mạng. Để chống lại những tấn công này, có thể dùng biện pháp mã hóa dữ liệu khi truyền trên kênh. Mạng IoTs sử dụng mã hóa an toàn với tấn công nghe lén nhưng lại tồn tại nhiều điểm yếu từ những tấn công khai thác nút bị tổn thương.

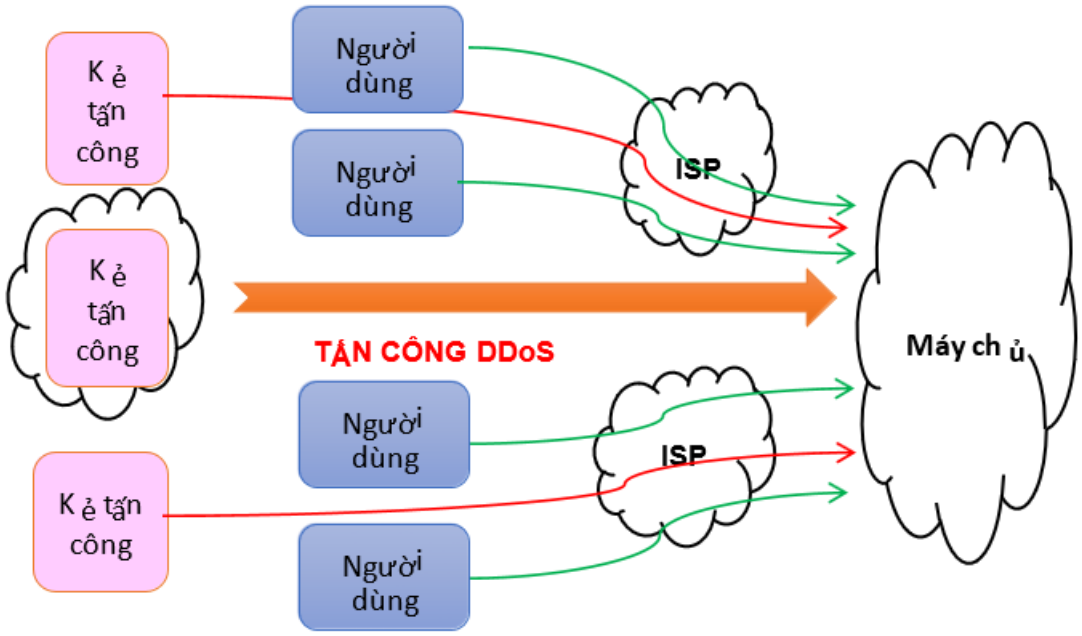
- ***Kỹ thuật đánh lừa (Social Engineering):*** Tấn công này với hai mục đích chính là đùa cợt và trục lợi . Kỹ thuật này phụ thuộc nhiều vào sơ hở của nhân viên, hacker có thể gọi điện thoại hoặc gửi e-mail giả danh người quản trị hệ thống, từ đó lấy mật khẩu của nhân viên và tiến hành tấn công hệ thống. Cách duy nhất để ngăn chặn nó là giáo dục khả năng nhận thức của nhân viên về cách đề phòng.



Hình 1.7: kỹ thuật đánh lừa

- ***Tấn công tính bí mật:*** diễn ra tại tầng mạng nhằm mục đích dò tìm những thông tin định tuyến hoặc dữ liệu trao đổi định tuyến. Cuộc tấn công này xảy ra khi thực thể định tuyến để lộ thông tin trong khi kết nối với một thực thể định tuyến ngoài mạng do lỗi cấu hình hoặc một cuộc tấn công vào điểm yếu của thực thể định tuyến. Để có thể chống lại tấn công này thì tất cả các nút mạng cần phải được xác thực. Việc truyền thông giữa các nút nên theo phương thức ngang hàng (peer-to-peer) để đảm bảo không có nút nào gửi thông tin tới bên nhận chưa được biết. Những biện pháp trên không thể ngăn chặn được hết các cuộc tấn công dò tìm thông tin định tuyến sơ hở, nhưng có thể hạn chế được chúng. Để thành công thì các cuộc tấn công này phải làm cho các nút tổn thương hoạt động nhiều hơn, nhằm làm lộ, lọt các thông tin định tuyến.

- ***Tấn công từ chối dịch vụ DDoS (Denial of Service***): Trên đường truyền giữa hai nút trong IoTs, dễ dàng xảy ra những tấn công chặn bắt luồng dữ liệu. Những cuộc tấn công này có thể khai thác được những dữ liệu mật, khóa,… từ thiết bị. Dựa vào đó, những kẻ tấn công có thể khởi động lại thiết bị khi cần. Nếu kẻ tấn công chặn bắt được khóa riêng thì chỉ làm tổn thương một nút mạng, nhưng nếu là khóa chung thì tấn công này có thể ảnh hưởng tới toàn bộ mạng. IoTs cũng có thể phải đối mặt với các cuộc tấn công từ chối dịch vụ DDoS từ lớp vật lý làm tắc nghẽn mạng, cản trở thiết bị gây ra mất kết nối, ở hình thức tấn công này. Hệ thống được chọn sẽ bị tấn công dồn dập bằng các gói tin với các địa chỉ IP giả mạo.



Hình 1.8: Tấn công DdoS

- ***Tấn công tính toàn vẹn:*** sửa đổi bất hợp pháp thông điệp trên đường truyền hoặc dữ liệu lưu trữ. Những tấn công này có thể dễ dàng được ngăn chặn bằng cách tăng thêm quyền kiểm soát truy cập với dữ liệu lưu trữ và cài đặt các dịch vụ toàn vẹn dữ liệu trên đường truyền cho thông điệp.

- ***Tấn công định tuyến:*** nhằm mục đích thay đổi mô hình logic của mạng và các thông tin định tuyến bằng cách tạo ra các tuyến đường sai. Tấn công này có thể chống được bằng cách xác định các tuyến đường xấu thông qua các gói tin cũ và thiết kế mô hình mạng phân vùng hạn chế quyền truy cập.

- ***Tấn công dùng lại các thông tin định tuyến:*** xảy ra khi kẻ tấn công ghi lại những thông điệp đã được gửi đi trên mạng và gửi chúng quay trở lại nhằm làm gián đoạn hoạt động của mạng. Giao thức định tuyến cho mạng LLN là RPL (RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks) trên nền IPv6 được IETF thiết kế để chống lại loại tấn công này. Trong RPL, thông điệp sẽ có nhiều phiên bản và những thông điệp phiên bản cũ sẽ bị loại bỏ mà không ảnh hưởng tới hoạt động định tuyến bình thường [RFC6550].

- ***Tấn công tính sẵn sàng:*** là những cuộc tấn công chuyển tiếp lựa chọn mục tiêu gây ảnh hưởng tới các tuyến đường định tuyến, nhằm mục đích làm gián đoạn truyền thông trong mạng. Trong Hình 5, có thể thấy một nút bị tổn thương có thể tạo bộ lọc chọn ngẫu nhiên các gói tin đi qua gây rối loạn trong mạng. Nếu như nút mạng loại bỏ tất cả các gói tin nhận được thì được

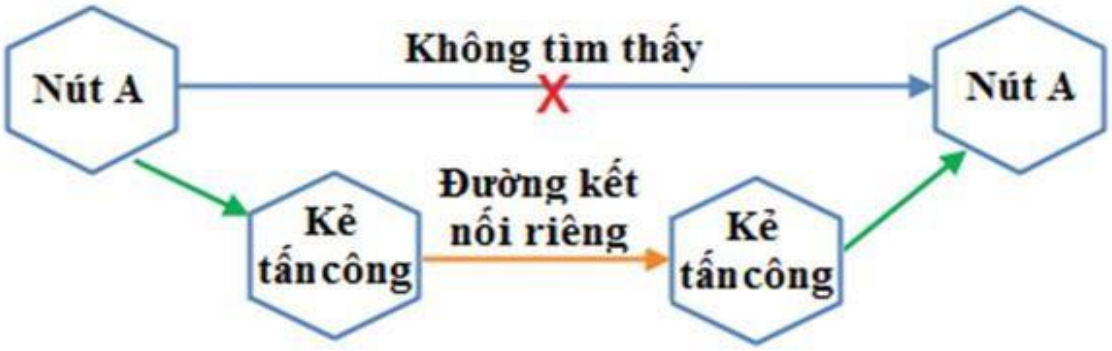
gọi là cuộc tấn công hố đen. Có hai biện pháp ngăn chặn tấn công này là định tuyến đa điểm trên các tuyến đường tách biệt không giao nhau hoặc mỗi nút phải có cơ chế lựa chọn ngẫu nhiên điểm đến tiếp theo trong tập hợp những điểm đến.

Phương pháp định tuyến đa đường tốn nhiều năng lượng nên không được sử dụng trong IoTs.

Hình 1.9: Tấn công chuyển tiếp lựa chọn

- ***Tấn công giả mạo gói ACK và HELLO Flood của giao thức TCP trong IoTs:*** có thể được thực hiện bởi những cách thức khác nhau nhằm mục đích khiến cho các nút tin rằng tồn tại những tuyến đường mà thực tế không có. Cách tối ưu để chống lại những cuộc tấn công này là thông qua kết nối hai hướng trong đó có sự điều khiển xác nhận kết nối hợp lệ ở lớp liên kết dữ liệu.

- ***Tấn công Wormhole:*** là khi hai nút bị tổn thương hoặc nhiễm mã độc, nên ngộ nhận rằng có một tuyến đường ngắn và tốt hơn cho chúng. Một cuộc tấn công Wormhole thuần túy rất khó phát hiện, vì nó không ảnh hưởng tới dữ liệu cũng như lưu lượng truyền thông. Trong trường hợp xấu, tấn công Wormhole sẽ khiến thiết bị mạng tính toán lại các tuyến đường. Khi kết hợp Wormhole với tấn công khác như tấn công chuyển tiếp lựa chọn mục tiêu có thể làm gián đoạn truyền thông mạng.



Hình 1.10: Tấn công Wormhole

- ***Tấn công Sinkhole:*** sử dụng một nút tổn thương để đánh lừa về tuyến đường tốt, nhằm thu hút lưu lượng mạng truy cập đến. Tấn công này chỉ có thể thực hiện bởi một nút bên trong mạng. Nếu Sinkhole kết hợp với tấn công chuyển tiếp có lựa chọn, thì một phần mạng có thể bị

vô hiệu hóa. Biện pháp để ngăn chặn tấn công này là, cần phải có một ngưỡng nhất định tiếp nhận lưu lượng mạng trong mỗi nút, hoặc cơ chế lựa chọn điểm đến kế tiếp cho thông điệp trong một tập hợp các điểm đến có thể.

1.5. Kết chương 1

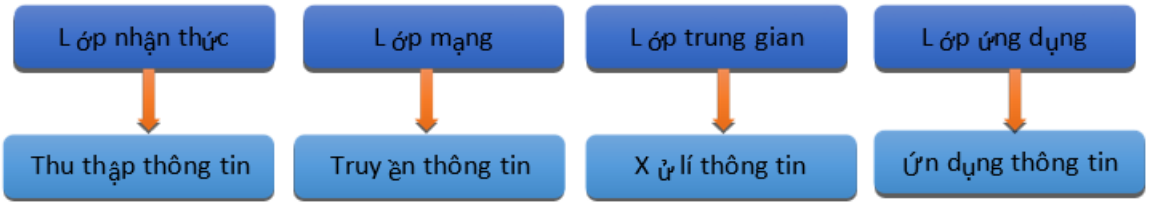
Chương 1 tập trung làm rõ về khái niệm IoTs và một số mô hình ứng
dụng, các nguy cơ mất an ninh bảo mật. Thông qua đó giúp chúng ta có cái nhìn tổng quan về tầm quan trọng trong an ninh bảo mật IoTs.

CHƯƠNG 2: KIẾN TRÚC CƠ SỞ HẠ TẦNG VÀ CÁC KỸ THUẬT AN NINH CHỦ YẾU TRONG IOTS

2.1. Kiến trúc an ninh trong IoTs

Các vấn đề an ninh tương ứng với mỗi lớp của kiến trúc IoTs cần được thảo luận, phân tích và giải quyết ở mức tối đa có thể [11]. Do đó, các yêu cầu bảo mật chung của Internet of Things bao gồm an ninh các nút vật lý, an ninh thu nhận thông tin, an ninh truyền tải thông tin và an ninh xử lý thông tin, để đạt được tính xác thực, bí mật và toàn vẹn của thông tin [12].

Kiến trúc trong IoTs có thể chia làm 4 lớp chính:



Hình 2.1: Xây dựng kiến trúc an ninh trong IoTs

Chức năng của mỗi lớp:

- Lớp cảm quan (lớp nhận thức): Thu thập tất cả các loại thông tin thông qua các thiết bị vật lý (cảm biến, đầu đọc RFID, GPS…) và nhận diện thế giới vật chất. Các thông tin thu thập bao gồm các thuộc tính đối tượng, điều kiện môi trường v.v.. Các phần quan trọng trong lớp này là cảm biến để nhận diện và thu thập thông tin thế giới vật chất.

- Lớp mạng: Truyền tải thông tin từ lớp cảm quan, xử lý sơ bộ, phân loại thông tin. Truyền tải thông tin được dựa trên một số mạng cơ bản, đó là mạng Internet, mạng truyền thông di động, mạng lưới truyền hình vệ tinh, mạng không dây, cơ sở hạ tầng mạng và các giao thức truyền thông.

- Lớp trung gian: Thiết lập một nền tảng hỗ trợ cho lớp ứng dụng. Đóng

vai trò kết hợp lớp ứng dụng phía trên và lớp mạng phía dưới. Quyền hạn sẽ được tổ chức thông qua mạng lưới điện và điện toán đám mây.

- Lớp ứng dụng: Cung cấp các dịch vụ cá nhân hoá theo nhu cầu của người sử dụng (truy cập internet, truyền hình …).Người dùng có thể truy cập vào internet thông qua giao diện lớp ứng dụng sử dụng của truyền hình, máy tính cá nhân hoặc thiết bị di động …

2.1.1. Đặc điểm an ninh

• ***Lớp cảm quan***: Thiết bị giản đơn và có công suất thấp do đó không thể áp dụng liên lạc qua tần số và thuật toán mã hóa phức tạp.

- Chịu tác động của tấn công bên ngoài mạng như tấn công DDoS.
- Các dữ liệu cảm biến cần được đảm bảo toàn vẹn, xác thực và bảo mật.

• ***Lớp mạng***: Các mối nguy cơ trong lớp mạng bao gồm:

- Tấn công Man-in-the-middle và giả mạo thông tin.
- Thư rác (junk mail) và virus.
- Tắc nghẽn mạng do gửi lưu lượng lớn dữ liệu cũng dễ xảy ra.

• ***Lớp trung gian***: Có vai trò trong việc xử lý tín hiệu khối và đưa ra quyết định thông minh nên quá trình xử lý có thể bị ảnh hưởng bởi những thông tin "độc", vì vậy cần tăng cường việc kiểm tra nhận diện thông tin.

• ***Lớp ứng dụng***: Đối với những ứng dụng khác nhau thì yêu cầu an ninh khác nhau.

- Chia sẻ dữ liệu là đặc tính của lớp ứng dụng, điều này nảy sinh các vấn đề liên quan đến thông tin cá nhân, điều khiển truy cập và phát tán thông tin.

2.1.2. Yêu cầu an ninh

Đối với toàn hệ thống, để đảm bảo IoTs chống lại các cuộc tấn công, trong một số lĩnh vực đòi hỏi phải có công nghệ tiên tiến. Cụ thể hơn, xác thực, bảo mật, và toàn vẹn dữ liệu là những vấn đề chính liên quan đến bảo mật IoTs [1]. Xác thực là cần thiết để tạo kết nối giữa hai thiết bị và trao đổi một số khóa công cộng và cá nhân thông qua các node để ngăn ngừa trộm cắp dữ liệu. Tính bảo mật đảm bảo rằng dữ liệu bên trong thiết bị IoTs bị ẩn khỏi các thực thể không được phép. Tính toàn vẹn dữ liệu ngăn cản bất kỳ sự sự thay đổi bằng con người nào đối với dữ liệu đảm bảo rằng dữ liệu đến node nhận ở dạng không thay đổi và vẫn được truyền bởi người gửi.

Đối với từng lớp, yêu cầu an ninh cụ thể:

Lớp cảm quan:

• Xác thực: chứng thực tại node đầu tiên rất cần thiết để ngăn chặn truy cập bất hợp pháp vào node.

- Mã hóa là tuyệt đối cần thiết để bảo mật khi truyền tải thông tin.
- Thỏa thuận khóa: cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên. Đây là quy trình quan trọng nâng cao, được thực hiện trước khi mã hóa.

Lớp mạng:

Cơ chế bảo mật hiện tại khó có thể áp dụng ở tầng này, cần đưa ra kỹ thuật phù hợp.

- Chứng thực nhận dạng (Identity authentication) nhằm ngăn chặn các node bất hợp pháp, là tiền đề cho các cơ chế an toàn, bảo mật.
- DDoS là phương pháp tấn công phổ biến trong hệ thống mạng, rất nghiêm trọng nếu xảy ra đối với IoTs => cần có Anti-DDoS.

Lớp trung gian:

Tầng này cần nhiều hệ thống ứng dụng bảo mật như an ninh điện toán đám mây, điện toán đa nhóm (Secure multiparty computation)… gần như tất cả các thuật toán mã hóa mạnh và giao thức mã hóa, kỹ thuật bảo mật, diệt virus đều tập trung ở lớp này.

Lớp ứng dụng:

Để giải quyết vấn đề an toàn của tầng ứng dụng, chúng ta cần quan tâm 2 mặt:

- Chứng thực qua mạng không đồng nhất.

- Bảo vệ quyền riêng tư của người dùng.

Thêm vào đó, việc đào tạo và quản lý là rất quan trọng với bảo mật thông tin, đặc biệt là quản lý password.

2.2. Các kỹ thuật an ninh chủ yếu

Đối với Internet hiện có, có rất nhiều các giao thức và công nghệ sẵn có để giải quyết hầu hết các vấn đề bảo mật, nhưng các công cụ hiện tại có tính ứng dụng hạn chế trong lĩnh vực IoTs do hạn chế về các nodes, phần cứng IoTs và mạng cảm biến không dây. Hơn nữa, các giao thức bảo mật thông thường tiêu thụ một lượng lớn bộ nhớ và các tài nguyên máy tính. Một yếu tố khác hạn chế việc thực hiện các công cụ bảo mật hiện tại là các thiết bị IoTs thường phải làm việc trong các môi trường xung quanh khắc nghiệt, không thể đoán trước, và thậm chí là môi trường thù địch bao quanh, ở đó chúng có thể dễ bị hư hỏng. Do đó, việc triển khai các công cụ

bảo mật hiện tại vẫn là một nhiệm vụ đầy thách thức và do đó đòi hỏi phải có kiến thức chuyên sâu về kỹ thuật an ninh trong IoTs.

IoTs tạo ra mạng lưới hàng tỉ các thiết bị kết nối không dây liên lạc với nhau, nên việc quản lí giám sát và bảo mật trở nên rất khó khăn, tất cả những thông tin cá nhân của chúng ta đều có khả năng bị theo dõi do những hacker (tin tặc) xâm nhập và đánh cắp. Đối với một người dùng bình thường, những thông tin mật chúng ta đôi khi chỉ là những tin nhắn, dòng chat, tài liệu thông thường, nhưng ở mức độ cao hơn điều này gây ra hậu quả vô cùng nghiêm trọng đối với các công ty, tập đoàn do những thông tin mật nếu bị tiết lộ ra ngoài sẽ gây thiệt hại rất lớn. Tuy nhiên, nếu như những dữ liệu quan trọng được bảo mật và mã hóa, sẽ rất khó để hacker có thể theo dõi và đánh cắp được. Các kỹ thuật an ninh bao gồm: kỹ thuật mã hóa, kỹ thuật bảo mật dữ liệu cảm biến.

2.2.1. Kỹ thuật mã hóa

Việc mã hóa dữ liệu, đơn giản là việc tăng thêm một lớp bảo mật cho dữ liệu bằng cách chuyển đổi dữ liệu sang một dạng khác thông qua một mã khóa với những quy tắc tùy biến, vì vậy, kể cả khi dữ liệu có bị đánh cắp, việc giải mã dữ liệu cũng là rất khó khăn. Một ví dụ đơn giản cho việc mã hóa dữ liệu. Nếu như chỉ đặt mật khẩu cho máy tính, laptop, hacker chỉ cần một vài thủ thuật để bỏ qua lớp mật khẩu (bypass) là có thể truy cập được dữ liệu, hoặc đơn giản chỉ là cắm thiết bị lưu trữ sang một hệ thống khác, tuy nhiên nếu như dữ liệu được mã hóa, kể cả khi có được dữ liệu rồi cũng rất khó để giải mã được như ban đầu nếu không có mã khóa.

2.2.1.1. Cơ chế mã hóa

By-hop: Mỗi thiết bị nhận được tin sẽ giải mã và mã hóa, sau đó gửi cho thiết bị kế tiếp.

+ Ưu điểm: Tất cả các dữ liệu được mã hóa, bao gồm tiêu đề, địa chỉ và thông tin định tuyến.

+ Nhược điểm: Các gói tin được giải mã ở mỗi bước nhảy.

End-to-end: Bên gửi sẽ mã hóa tin, tin được mã hóa truyền qua các thiết bị và chỉ được giải mã khi nó đến được bên nhận.

+ Ưu điểm: Mỗi hop trên mạng không cần phải có 1 chìa khóa để giải mã, độ phức tạp, linh hoạt cao hơn so với By-hop.

+ Nhược điểm: tiêu đề, địa chỉ và các thông tin định tuyến không được mã hóa.

Trong IoT, tầng mạng và tầng ứng dụng kết nối gần với nhau, nên phải lựa chọn:

- Với yêu cầu bảo mật cao, ta sử dụng mã hóa end-to-end.

- Với yêu cầu bảo mật thấp, ta sử dụng mã hóa by-hop.

2.2.1.2. Các thuật toán mã hóa

Mã hóa đối xứng (symmetric encryption algorithm)

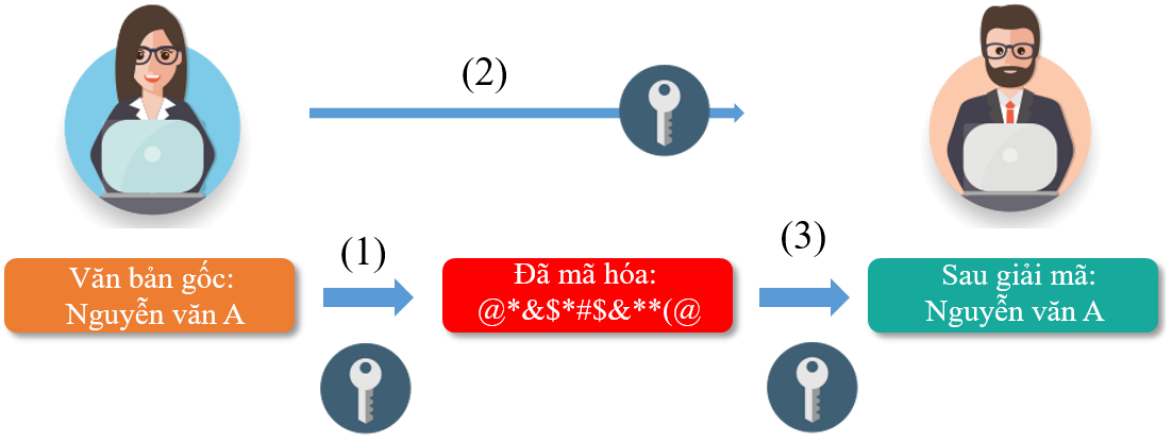
Là phương pháp mã hóa trong đó việc mã hóa và giải mã sử dụng chung 1 khóa (secret key).

Giả sử A cần mã hóa một tập tin để gửi cho B, thì quy trình sẽ như sau:

1. A sử dụng một thuật toán mã hóa, cộng với khóa của A để mã hóa file gửi.

2. Bằng cách nào đó, A giao cho B một khóa giống với khóa của A, có thể là giao trước hoặc sau khi mã hóa tập tin đều được.

3. Khi B nhận tập tin, B sẽ dùng khóa này để giải mã ra tập tin gốc có thể đọc được.



Hình 2.2: Mã hóa đối xứng

Vấn đề ở đây, đó là A phải làm sao để chuyển khóa cho B một cách an toàn. Nếu khóa này bị lộ ra thì bất kì ai cũng có thể dùng thuật toán nói trên để giải mã tập tin, như vậy thì tính bảo mật sẽ không còn nữa.

Thường dùng password như là khóa mã hóa, và bằng cách này có thể nhanh chóng nhắn cho người nhận cùng đoạn password đó để dùng làm khóa giải mã.

Thuật toán đối xứng có thể được chia ra làm hai loại, mã luồng (stream ciphers) và mã khối (block ciphers). Mã luồng mã hóa từng bit của thông điệp trong khi mã khối gộp một số bit lại và mã hóa chúng như một đơn vị. Cỡ khối được dùng thường là các khối 64 bit. Thuật toán tiêu chuẩn mã hóa tân tiến AES (Advanced Encryption Standard), được NIST công nhận tháng 12 năm 2001, sử dụng các khối gồm 128 bit.

Một số ví dụ các thuật toán đối xứng nổi tiếng: Twofish, Serpent, AES , Blowfish, CAST5, RC4, Tam phần DES (Triple Data Encryption Algorithm), và IDEA (International Data Encryption Algorithm – Thuật toán mật mã hóa dữ liệu quốc tế).

Tốc độ

Các thuật toán đối xứng nói chung đòi hỏi công suất tính toán ít hơn các thuật toán khóa bất đối xứng. Trên thực tế, một thuật toán khóa bất đối xứng có khối lượng tính toán nhiều hơn gấp hằng trăm, hằng ngàn lần một thuật toán khóa đối xứng có chất lượng tương đương.

Hạn chế

Hạn chế của các thuật toán khóa đối xứng bắt nguồn từ yêu cầu về sự phân hưởng chìa khóa bí mật, mỗi bên phải có một bản sao của chìa. Do khả năng các chìa khóa có thể bị phát hiện bởi đối thủ mật mã, chúng thường phải được bảo toàn trong khi phân phối và trong khi dùng. Hậu quả của yêu cầu về việc lựa chọn, phân phối và lưu trữ các chìa khóa một cách không có lỗi, không bị mất mát là một việc làm khó khăn, khó có thể đạt được một cách đáng tin cậy.

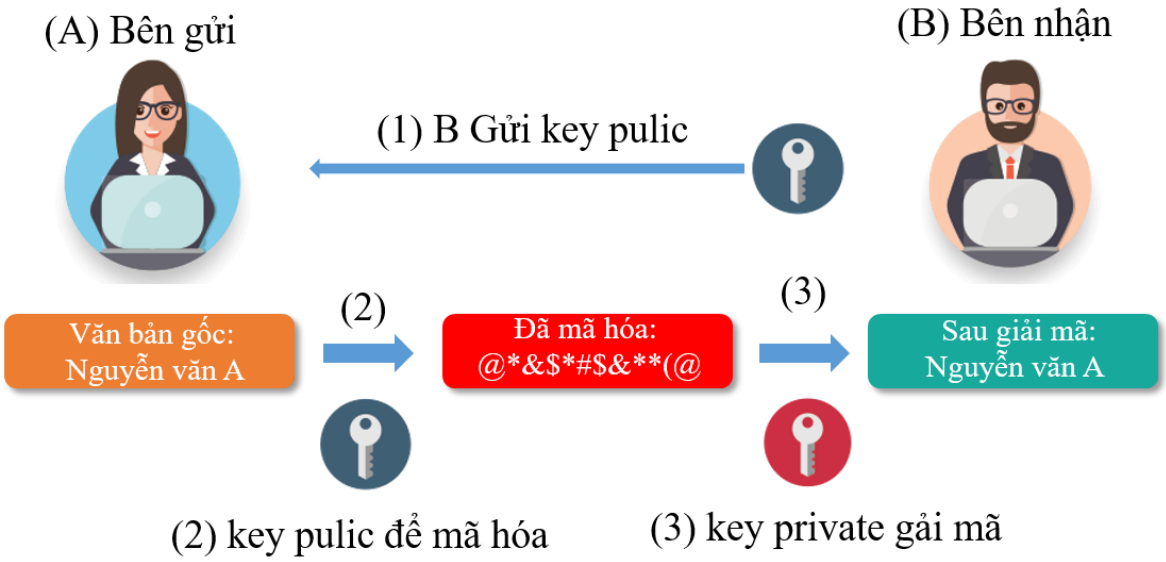
Để đảm bảo giao thông liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người, tổng số lượng chìa khóa cần phải có là $\frac{n(n-1)}{2}$.

Hiện nay người ta phổ biến dùng các thuật toán bất đối xứng có tốc độ chậm hơn để phân phối chìa khóa đối xứng khi một phiên giao dịch bắt đầu, sau đó các thuật toán khóa đối xứng tiếp quản phần còn lại. Vấn đề về bảo quản sự phân phối chìa khóa một cách đáng tin cậy cũng tồn tại ở tầng đối xứng, song ở một điểm nào đấy, người ta có thể kiểm soát chúng dễ dàng hơn.

Tuy thế, các khóa đối xứng hầu như đều được sinh tạo tại chỗ..

Mã hóa bất đối xứng (asymmetric key algorithms)

Là thuật toán trong đó việc mã hóa và giãi mã dùng hai khóa khác nhau là pulic key (khóa công khai hay khóa công cộng) và private key (khóa riêng). Nếu dùng public key để mã hóa thì private key sẽ dùng để giải mã và ngược lại. Cặp key được tạo ra ngẫu nhiên với nhiều chữ số hiển thị, sẽ không thể giải mã ra private key nếu biết public key, khối lượng tính toán lớn, gấp hàng trăm hàng ngàn lần so với thuật toán mã hóa đối xứng.



Hình 2.3: Mã hóa bất đối xứng

Về khía cạnh an toàn, các thuật toán mã hóa bất đối xứng cũng không khác nhiều với các thuật toán mã hóa đối xứng. Có những thuật toán được dùng rộng rãi, có thuật toán chủ yếu trên lý thuyết; có thuật toán vẫn được xem là an toàn, có thuật toán đã bị phá vỡ… lưu ý là những thuật toán được dùng rộng rãi không phải lúc nào cũng đảm bảo an toàn. Một số thuật toán có những chứng minh về độ an toàn với những tiêu chuẩn khác nhau. Nhìn chung, chưa có thuật toán nào được chứng minh là an toàn tuyệt đối (như hệ thống mật mã sử dụng một lần). Vì vậy, cũng giống như tất cả các thuật toán mật mã nói chung, các thuật toán mã hóa khóa công khai cần phải được sử dụng một cách thận trọng.

Ứng dụng

Ứng dụng rõ ràng nhất của mã hóa khóa công khai là bảo mật: một văn bản được mã hóa bằng khóa công khai của một người sử dụng thì chỉ có thể giải mã với khóa bí mật của người đó.

Các thuật toán tạo chữ ký số khóa công khai có thể dùng để nhận thực. Một người sử dụng có thể mã hóa văn bản với khóa bí mật của mình. Nếu một người khác có thể giải mãvới khóa công khai của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khóa công khai đó.

Các đặc điểm trên còn có ích cho nhiều ứng dụng khác như: tiền điện tử, thỏa thuận khóa…

Điểm yếu

- Tồn tại khả năng một người nào đó có thể tìm ra được khóa bí mật. Không giống với hệ thống mật mã sử dụng một lần (one-time pad) hoặc tương đương, chưa có thuật toán mã hóa

khóa bất đối xứng nào được chứng minh là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán. Khả năng một mối quan hệ nào đó giữa 2 khóa hay điểm yếu của thuật toán dẫn tới cho phép giải mã không cần tới khóa hay chỉ cần khóa mã hóa vẫn chưa được loại trừ. An toàn của các thuật toán này đều dựa trên các ước lượng vềkhối lượng tính toán để giải các bài toán gắn với chúng. Các ước lượng này lại luôn thay đổi tùy thuộc khả năng của máy tính và các phát hiện toán học mới.

- Khả năng bị tấn công dạng kẻ tấn công đứng giữa (man in the middle attack): kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã rồi lại mã hóa với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khóa an toàn nhằm đảm bảo nhận thực người gửi vàtoàn vẹn thông tin. Một điều cần lưu ý là khi các chính phủ quan tâm đến dạng tấn công này: họ có thể thuyết phục (hay bắt buộc) nhà cung cấp chứng thực số xác nhận một khóa giả mạo và có thể đọc các thông tin mã hóa. *Khối lượng tính toán*

Để đạt được độ an toàn tương đương đòi hỏi khối lượng tính toán nhiều hơn đáng kể so với thuật toán mật mã hóa đối xứng. Vì thế trong thực tế hai dạng thuật toán này thường được dùng bổ sung cho nhau để đạt hiệu quả cao. Trong mô hình này, một bên tham gia trao đổi thông tin tạo ra một khóa đối xứng dùng cho phiên giao dịch. Khóa này sẽ được trao đổi an toàn thông qua hệ thống mã hóa khóa bất đối xứng. Sau đó 2 bên trao đổi thông tin bí mật bằng hệ thống mã hóa đối xứng trong suốt phiên giao dịch.

Một vài thuật toán mã hóa bất đối xứng: RSA-Rivest shamir adleman, Diffie-hellman, ECC- Error correcting code -mã sửa lỗi

Thuật toán trao đổi khóa Diffie–Hellman cho phép hai bên (người, thực thể giao tiếp) thiết lập một khóa bí mật chung để mã hóa dữ liệu sử dụng trên kênh truyền thông không an toàn mà không cần có sự thỏa thuận trước về khóa bí mật giữa hai bên.

Trong thiết kế hệ thống bảo mật hiện đại, hai thuật toán mã hóa đối xứng và bất đối xứng được sử dụng phối hợp để tận dụng các ưu điểm của cả hai. Những hệ thống sử dụng cả hai thuật toán bao gồm: SSL (Secure Sockets Layer), PGP (Pretty Good Privacy) và GPG (GNU Privacy Guard) v.v. Các thuật toán chìa khóa bất đối xứng được sử dụng để phân phối chìa khóa mật cho thuật toán đối xứng có tốc độ cao hơn.

2.3. Kỹ thuật bảo mật dữ liệu cảm biến không dây

Mạng cảm biến không dây (WSN) có thể hiểu đơn giản là mạng liên kết các node với nhau bằng kết nối sóng vô tuyến, trong đó các node mạng thường là các thiết bị đơn giản, nhỏ gọn, … và có số lượng lớn, được phân bố một cách không có hệ thống trên một diện tích rộng, sử dụng nguồn năng lượng hạn chế và có thể hoạt động trong môi trường khắc nghiệt.

Cấu trúc của mạng cảm biến không dây:

Một node cảm biến được cấu tạo bởi 3 thành phần cơ bản sau: Vi điều khiển, Sensor, bộ phát radio. Ngoài ra còn có các cổng kết nối máy tính.

- *Vi điều khiển bao gồm:* CPU; bộ nhớ ROM, RAM; bộ phận chuyển đổi tín hiệu tương tự thành tín hiệu số và ngược lại.

- *Sensor là chức năng:* cảm nhận thế giới bên ngoài, sau đó chuyển dữ liệu qua bộ phận chuyển đổi để xử lý.

- *Bộ phát radio bao gồm:* các node cảm biến và là thành phần quan trọng nhất trong mạng cảm biến không dây, do vậy việc thiết kế các node cảm biến sao cho có thể tiết kiệm được tối đa nguồn năng lượng là vấn đề quan trọng hàng đầu.

Lớp nhận thức là lớp thấp nhất của kiến trúc IoTs và chịu trách nhiệm thu thập thông tin trên toàn bộ mạng IoTs. Trong lớp này, các vấn đề an ninh quan trọng nhất bao gồm bảo mật thu nhận thông tin và an ninh vật lý của phần cứng như thiết bị cảm biến, các nút RFID và thiết bị đầu cuối cảm biến. Do các ứng dụng chức năng của các nút cảm biến khác nhau có hệ thống bảo vệ yếu, chủ yếu trong môi trường xung quanh khắc nghiệt, IoTs không thể thực hiện được một giao thức bảo mật đơn lẻ và vì vậy thiếu các thiết bị an ninh thích hợp sẽ ảnh hưởng đến an ninh của các nút cảm biến RFID, mạng cảm biến không dây, [7]. Việc thực thi bảo mật vật lý ở lớp nhận thức phải cung cấp cho sự an toàn vật lý của phần cứng cảm biến như các nút RFID, mạng cảm biến và các đầu cuối cảm biến.

2.3.1. Hệ thống an ninh RFID

Vì phần lớn các nút cảm biến RFID được triển khai trong môi trường khắc nghiệt, do đó chúng vẫn dễ bị hư hỏng hoặc trộm cắp và các chính sách phải được thiết kế và thực hiện để thay thế các nút bị hỏng trên mạng cảm biến không dây. Các vấn đề an ninh liên quan đến RFID bao gồm rò rỉ thông tin vị trí của thẻ RFID và người sử dụng, các cuộc tấn công lại, các cuộc tấn công man-in-the-middle, các cuộc tấn công nhân bản và giả mạo. Sự cân bằng giữa chi phí và

an ninh cần được cân bằng và các chính sách an ninh phù hợp phải được thiết kế cho các ứng dụng RFID.

An ninh RFID chủ yếu được thực hiện thông qua các phương pháp vật lý hoặc cơ chế mã hoặc kết hợp cả hai phương pháp. Một số loại phương pháp vật lý đã được thảo luận [9]:

- Mã hóa dữ liệu: Thuật toán mã hóa có thể được áp dụng để đảm bảo tính bảo mật của thông tin thẻ RFID.

- Thẻ chặn: Các thẻ này có thể được sử dụng để che giấu số serial của các thẻ RFID khác bằng cách phát ra một tần số liên tục của số sê-ri nhãn giả [10].

- Sửa đổi tần số thẻ: Tần số của các thẻ có thể được sửa đổi để gây khó khăn cho người dùng độc hại để truy cập vào giao tiếp giữa thẻ RFID và người đọc.

- Méo: Các tín hiệu vô tuyến có thể được sử dụng để gây nhiễu cho các hoạt động của các đầu đọc RFID gần đó.

- Xóa bỏ chính sách đặt hàng: Theo chính sách này, các thẻ sẽ bị hủy .

Các vấn đề bảo mật RFID cũng có thể được giải quyết thông qua việc thực hiện các cơ chế mã. Các cơ chế mã này liên quan đến việc thiết kế các giao thức có xu hướng giải quyết các vấn đề bảo mật liên quan đến các nút RFID. Một số giao thức bảo mật RFID là giao thức Hash Lock, giao thức

LCAP, giao thức chuỗi Hash, giao thức mã hóa lại, vv [11-13]

2.3.2. Bảo mật mạng an ninh cảm biến

Các mối liên quan đến an ninh liên quan đến công nghệ mạng cảm biến bao gồm chụp các nút cảm biến và nút cổng, tấn công toàn vẹn, các cuộc tấn công nghẽn, các cuộc tấn công DOS và các cuộc tấn công nhân bản nút. Các thẻ RFID khác với các nút cảm biến trong đó các thẻ RFID liên quan đến các tính chất tĩnh của vật, trong khi các cảm biến liên quan đến tính năng động của mọi thứ [14]. Xây dựng khuôn khổ an ninh cho mạng cảm biến bao gồm việc tích hợp một số chính sách bảo mật như các thuật toán mã hóa, chính sách phân phối chính, cơ chế phát hiện xâm nhập và các chính sách định tuyến bảo mật [15]. Một số các khung bảo mật hiện có là TinySec, giao thức

LEAP, tần số nhảy tần số, vv

2.5.2.1. Các chính sách phân phối chính:

Thông thường, các mạng cảm biến sẽ chọn ngẫu nhiên các giá trị phân bố trước, trong đó mỗi nút cảm biến ngẫu nhiên chọn vài phím từ các nút có sẵn sao cho mỗi tập hợp của hai nút có thể chia sẻ các khóa với xác suất cao hơn.

2.5.2.2.Cơ chế phát hiện xâm nhập:

Các cơ chế này cung cấp thêm một lớp bảo mật trong Internet of Things khi họ kịp thời phát hiện ra các lỗ hổng bảo mật trong các mạng và do đó có thể cung cấp các biện pháp bảo mật an toàn [15, 17-18].

2.5.2.3. Các chính sách định tuyến bảo mật:

Các bộ định tuyến bảo mật có thể được triển khai qua mạng để tăng cường bảo mật. Một số chính sách định tuyến bảo mật được sử dụng rộng rãi nhất bao gồm chính sách định tuyến đa đường có thể được áp dụng để bảo vệ chống lại các cuộc tấn công chuyển tiếp. Ngoài ra, các cuộc tấn công lũ lụt cần phải được giải quyết bằng cách hạn chế việc định tuyến các nút đến một phạm vi cụ thể [16].

2.5.2.4. Bảo mật thiết bị đầu cuối cảm biến.

Các vấn đề an ninh liên quan đến các đầu cuối của cảm biến trên Internet of Things bao gồm truy cập trái phép, trộm cắp hoặc thiệt hại của thông tin bí mật, sao chép thông tin SIM, truy cập và bắt chước thông tin giao diện không khí, vv Dữ liệu được cảm nhận thông qua nhiều nút cảm biến, Được truyền đến hệ thống con xử lý dữ liệu và cuối cùng nó sẽ đến được với những người dùng và ứng dụng dự định.

Các thiết bị đầu cuối cảm biến được triển khai rộng rãi bao gồm điện thoại thông minh, máy tính cá nhân, máy tính xách tay, máy tính bảng ... Các chính sách bảo mật được sử dụng phổ biến nhất cho các thiết bị đầu cuối cảm biến bao gồm các thuật toán mật mã, chính sách xác thực danh tính, chính sách kiểm soát luồng dữ liệu, cơ chế lọc dữ liệu ... [7].

2.4. Kỹ thuật bảo mật thông tin liên lạc

2.4.1. Bảo mật thu thập Thông tin

Bên cạnh các vấn đề an ninh vật lý, lớp nhận thức cũng cần phải giải quyết các vấn đề liên quan đến an ninh thu thập thông tin. Các vấn đề bảo mật thu thập thông tin bao gồm các cuộc gọi ngầm, gian lận, gian lận và phát lại.

Chính sách bảo mật liên quan đến thu thập dữ liệu đã được thảo luận:

- Phải đảm bảo tính xác thực, bảo mật và tính toàn vẹn của dữ liệu trong giai đoạn thu thập dữ liệu.

- Cần phải tăng cường các giao thức quản lý then chốt trong lớp nhận thức, bao gồm việc áp dụng chính sách quản lý chìa khóa đối xứng và cân bằng trọng lượng nhẹ.

- Chính sách định tuyến an toàn phải được áp dụng để đảm bảo phát hiện đường chính xác và an ninh mạng hiệu quả.

- Các chính sách xác thực nút cảm biến phải được tận dụng để ngăn chặn việc truy cập dữ liệu của người dùng trái phép và độc hại [8].

2.4.2. Bảo mật xử lý thông tin

Trong kiến trúc IoTs, lớp trung gian chủ yếu chịu trách nhiệm xử lý thông tin và nó cũng cung cấp giao diện truyền thông giữa các lớp mạng và ứng dụng của kiến trúc lớp IoTs. Việc triển khai thực hiện an ninh tại lớp trung gian cần đảm bảo bí mật và lưu trữ an toàn thông tin cũng như sự an toàn của phần mềm trung gian. Vẫn tồn tại một số vấn đề kỹ thuật liên quan đến độ tin cậy, sự riêng tư và an ninh của xử lý thông tin trong lớp trung gian của kiến trúc IoTs [7]. Lớp ứng dụng có thể cung cấp nhiều ứng dụng khác nhau như nông nghiệp xanh, nhà thông minh, vận chuyển thông minh ... và các vấn đề bảo mật chính mà các hệ thống ứng dụng đang phải đối mặt bao gồm các chương trình nguy hiểm và lỗi thiết kế.

2.4.3. Bảo mật truyền thông tin

Trong kiến trúc IoTs, trách nhiệm chính của lớp mạng là truyền tải thông tin qua mạng. Kiến trúc IoTs, được thực hiện trên cơ sở truyền thông cơ bản, vẫn dễ bị rủi ro liên quan như các cuộc tấn công từ chối dịch vụ, truy cập trái phép, tấn công người trung gian, các cuộc tấn công của virus ngoài sự thỏa hiệp về tính bí mật và tính toàn vẹn của dữ liệu. Khi IoTs liên quan đến việc cảm nhận và thu thập dữ liệu từ vô số thiết bị, với dữ liệu được thu thập trong các định dạng dữ liệu khác nhau.

Các dữ liệu thu thập có được tính chất không đồng nhất, và điều này mang lại trong các vấn đề khác liên quan đến mạng phức tạp như số lượng lớn các nút chuyển dữ liệu dẫn đến tắc nghẽn mạng.

Các chiến lược bảo mật ở tầng mạng cần duy trì tính xác thực, bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu trong khi nó đang được truyền qua mạng. Các ứng dụng IoTs liên quan đến việc chuyển một lượng lớn dữ liệu qua mạng IoT và điều này đòi hỏi phải áp dụng các cơ chế xác thực, lọc và phát hiện khác nhau để đảm bảo an toàn cho dữ liệu. Dữ liệu cũng phải được

bảo vệ chống lại các cuộc tấn công DDoS bằng cách sử dụng công cụ phát hiện tấn công DDoS. Ngoài ra, tính chất không đồng nhất của kết nối mạng dẫn đến lỗ hổng trao đổi thông tin, các cuộc tấn công lại,… Các cơ chế xác thực, cơ chế quản lý và cơ chế đàm phán, và cơ chế phát hiện xâm nhập có thể được tận dụng để làm cho mạng chống lại các cuộc tấn công như vậy.

2.4.4. Bảo mật ứng dụng thông tin

Khi lớp ứng dụng của kiến trúc IoTs xử lý với số lượng lớn dữ liệu, các ứng dụng phải đối mặt với một số vấn đề bảo mật dữ liệu cũng như vấn đề bảo mật dữ liệu. Bảo vệ dữ liệu, sao lưu dữ liệu và cơ chế phục hồi phải được đặt đúng chỗ để đạt được bảo mật dữ liệu. Để đảm bảo an ninh dữ liệu ở lớp ứng dụng, phải áp dụng các thuật toán quản lý bảo mật dữ liệu và các thuật toán mã hóa/giải mã để bảo đảm cơ sở dữ liệu. Truy cập cơ chế quản lý để ngăn chặn truy cập trái phép vào cơ sở dữ liệu và quản lý đặc quyền quản trị cơ sở dữ liệu, cả hai chiến lược có thể được thực hiện để bảo vệ cơ sở dữ liệu.

Một thành phần khác của việc thực hiện bảo mật ở cấp lớp ứng dụng là sự riêng tư của dữ liệu. Trong nhiều ứng dụng IoTs, bảo vệ sự riêng tư của dữ liệu giả định có ý nghĩa. Thuật ngữ bảo mật dữ liệu cho thấy chủ sở hữu dữ liệu không muốn tập dữ liệu nhạy cảm của họ được tiết lộ để truy cập trái phép. Để ngăn chặn truy cập trái phép và sử dụng dữ liệu, quyền truy cập phải được giới hạn và các hoạt động liên quan đến dữ liệu phải dựa trên mức độ bảo mật hoặc quyền truy cập. Công nghệ biến dạng dữ liệu, công nghệ mã hóa dữ liệu hoặc các đại lý bảo mật là một số công nghệ mà những công nghệ bảo vệ sự riêng tư phổ biến có thể được dựa trên để đảm bảo sự riêng tư của cơ sở dữ liệu.

Mạng máy tính ngang hàng và web ngữ nghĩa là hai chiến lược bảo vệ sự riêng tư lớn. Máy tính peer-to-peer cho phép các nút máy tính ngang hàng chia sẻ các dịch vụ và tài nguyên máy tính của họ với nhau trong khi các trang web ngữ nghĩa xác định và tổ chức thông tin thông qua các tiêu chuẩn cụ thể để làm cho thông tin ngữ nghĩa trở nên rõ ràng hơn và dễ hiểu hơn cho máy móc và để thực hiện các hoạt động của con người, Máy truyền thông [17]. Nhiều kỹ thuật bảo mật dữ liệu khác bao gồm mạng riêng ảo, TLS, SSL, IP security các phần mở rộng bảo mật DNS và bảo vệ sự riêng tư của vị trí [18].

• TLS/SSL: được thiết kế để mã hóa các liên kết trong lớp trung gian. Tiêu chuẩn TLS - transport layer security hay còn gọi là giao thức bảo mật tầng giao vận (tần trung gian), giao thức này được phát triển dựa trên tiêu chuẩn SSL v3.0 (Secure Socket Layer)

- Do giao thức TLS được phát triển dựa trên giao thức SSL nên ta tìm hiểu một chút về cấu trúc của giao thức SSL trước:

Giao thức Secure Socket Layer (SSL) theo hình mình hoạ 3.3 phía dưới thì cấu trúc và giao thức SSL được đặt giữa lớp trung gian và lớp ứng dụng, nó cung cấp khả năng bảo mật thông tin, xác thực và toàn vẹn dữ liệu đến người dùng:

+ Xác thực: đảm bảo tính xác thực của trang mà sẽ làm việc ở đầu kia của kết nối.

+ Mã hoá: đảm bảo thông tin không thể bị truy cập bởi đối tượng thứ ba. Để loại trừ việc nghe trộm thông tin khi truyền qua Internet, dữ liệu phải được mã hoá để không thể bị đọc được bởi những người khác ngoài người gửi và người nhận.

+ Toàn vẹn dữ liệu: đảm bảo thông tin không bị sai lệch và nó phải thể hiện chính xác thông tin gốc gửi đến.

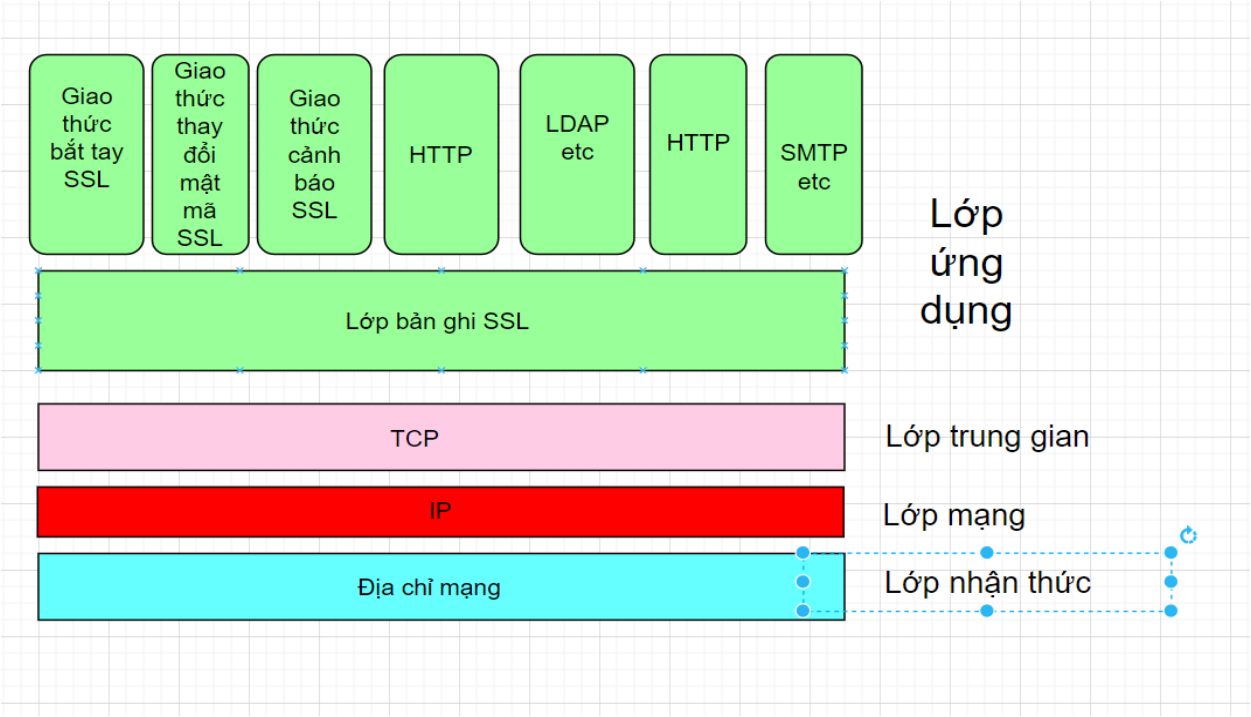
Giao thức SSL cung cấp giao thức bảo mật truyền thông có 3 đặc điểm nổi bật:

- Các bên giao tiếp (nghĩa là client và server) có thể xác thực nhau bằng cách sử dụng mật mã khóa chung

- Sự bí mật của lưu lượng dữ liệu được bảo vệ vì nối kết được mã hóa trong suốt sau khi một sự thiết lập quan hệ ban đầu và sự thương lượng khóa session đã xảy ra.

- Tính xác thực và tính toàn vẹn của lưu lượng dữ liệu cũng được bảo vệ vì các thông báo được xác thực và được kiểm tra tính toàn vẹn một cách trong suốt bằng cách sử dụng MAC.

Tổ chức IETF (Internet Engineering Task Force) đã chuẩn hoá SSL và đặt lại tên là TLS (Transport Layer Security). Mặc dù là có sự thay đổi về tên nhưng TLS chỉ là một phiên bản mới của SSL. Phiên bản TLS 1.0 tương đương với phiên bản SSL 3.1. Tuy nhiên SSL là thuật ngữ được sử dụng rộng rãi hơn.



Hình 2.4: Giao thức Secure Socket Layer (SSL)

Mục tiêu chính của giao thức TLS là cung cấp sự riêng tư và toàn vẹn dữ liệu giữa hai ứng dụng trong môi trường mạng. Cũng như giao thức SSL thì giao thức TLS cũng theo mô hình client-server. Giao thức TLS gồm có hai lớp là Lớp bản ghi (Record Layer) và lớp bắt tay (Handshake Layer).

+ Lớp bản ghi: là lớp thấp nhất bao gồm TLS record protocol

Đặc tính kết nối riêng tư: mã hoá đối xứng được sử dụng để mã hoá dữ liệu (mã hoá AES...) Các khoá để mã hoá đối xứng được sinh ra cho mỗi lần kết nối và được thoả thuận bí mật của giao thức khác. Chính vì vậy giao thức TLS cũng có thể được sử dụng mà không cần mã hoá.

Đặc tính kết nối đáng tin cậy: Một thông điệp vận chuyển thông báo sẽ bao gồm kiểm tra tính toàn vẹn (sử dụng hàm Băm ví dụ SHA-1). Ngoài ra giao thức TLS còn được sử dụng để phân mảnh, nén, đóng gói, mã hoá dữ liệu, cho phép máy chủ xác nhận nhau và thoả thuận thuật toán mã hoá. Mỗi cấu trúc dữ liệu bao gồm 4 trường thông tin:

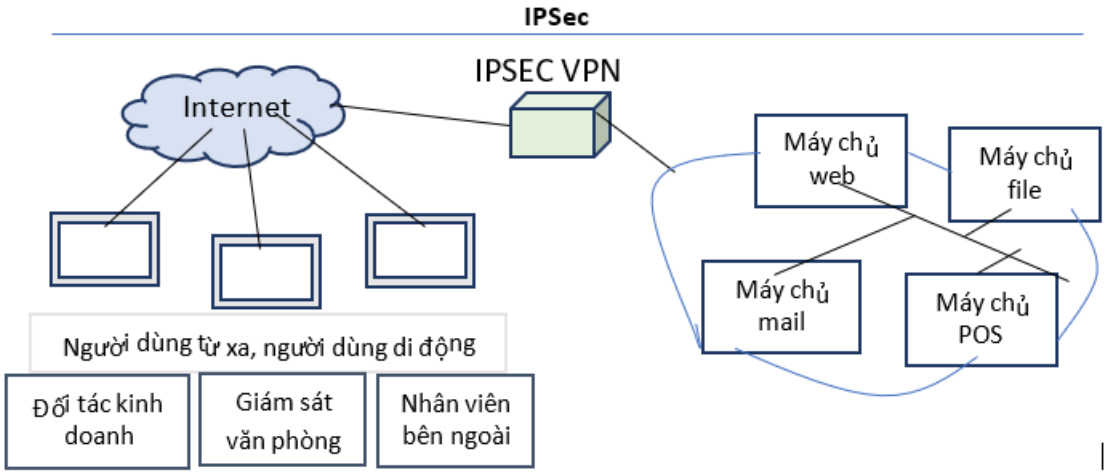
- Type o Version o Length o Fragment

  + Lớp bắt tay SSL: nằm trên lớp bản ghi

- Định danh của điểm kết nối có thể được xác thực bằng cách sử dụng mã hóa bất đối xứng hoặc khóa công khai (RSA)

- Quá trình thỏa thuận khóa bí mật chia sẻ được an toàn o Quá trình thỏa thuận đáng tin cậy + Ứng dụng của giao thức TLS

- Đóng gói các giao thức ví dụ như HTTP, FTP, SMTP, NNTP và XMPP.
- Cho phép trao đổi riêng tư trên mạng.
- Cho phép các ứng dụng client-server giao tiếp với nhau an toàn.
- IPSec: được thiết kế để bảo vệ an ninh của các lớp mạng, nó có thể cung cấp tính toàn vẹn, tính xác thực và bảo mật trong mỗi lớp.



Hình 2.5: Giao thức Secure Socket Layer (SSL)

IPsec (IP security) bao gồm một hệ thống các giao thức để bảo mật quá trình truyền thông tin trên nền tảng Internet Protocol (IP). Bao gồm xác thực hoặc mã hoá (Authenticating and/or Encrypting) cho mỗi gói IP trong quá trình truyền thông tin. Giao thức IPsec được làm việc tại tầng mạng – layer 3 của mô hình OSI.

+ Bảo mật (mã hóa)-Confidentiality: Người gửi có thể mã hóa dữ liệu trước khi truyền chúng qua mạng. Bằng cách đó, không ai có thể nghe trộm trên đường truyền.

+ Toàn vẹn dữ liệu-Data integrity: Người nhận có thể xác minh các dữ liệu được truyền qua mạng Internet mà không bị thay đổi.

+ Xác thực-Authentication: Xác thực đảm bảo kết nối được thực hiện và các đúng đối tượng. Người nhận có thể xác thực nguồn gốc của gói tin, bảo đảm, xác thực nguồn gốc của thông tin.

+ Antireplay protection: xác nhận mỗi gói tin là duy nhất và không trùng lặp.

2.5. Kết chương 2

Chương 2 giới thiệu về kiến trúc cơ sở hạ tầng, đặc điểm an ninh, một số các kỹ thuật bảo mật phổ biến đang được áp dụng và nêu rõ chính sách bảo mật dựa trên mô hình kiến trúc của IoT của từng lớp, nhằm nâng cao tối đa hiệu quả an ninh và tiện lợi cho cả nhà sản xuất cũng như người sử dụng.

CHƯƠNG 3: MỘT SỐ THÁCH THỨC CÙNG HƯỚNG PHÁT TRIỂN TRONG TƯƠNG LAI VÀ ỨNG DỤNG BẢO MẬT IOTS DỰA TRÊN CÔNG NGHỆ LẤY MẪU NÉN

3.1. Thách thức và hướng phát triển

3.1.1. Thách thức

Internet of Things là một môi trường đa lĩnh vực với một số lượng lớn các thiết bị và dịch vụ kết nối với nhau để trao đổi thông tin. Mỗi lĩnh vực có thể áp dụng các yêu cầu về bảo mật, riêng tư và tin tưởng của riêng nó. Để thiết lập các thiết bị và dịch vụ IoTs an toàn hơn và có sẵn với chi phí thấp, có rất nhiều thách thức an ninh và bảo mật cần vượt qua. Trong đó những thách thức gồm:

3.1.1.1. Bảo vệ sự riêng tư và bảo vệ dữ liệu của người dùng

Bảo mật là một vấn đề quan trọng trong bảo mật IoTs dựa trên đặc tính phổ biến của môi trường IoTs. Mọi thứ được kết nối, dữ liệu được truyền đạt và trao đổi qua internet, tạo ra cho người sử dụng sự riêng tư một chủ đề nhạy cảm trong nhiều nghiên cứu [13, 14]. Mặc dù đã có rất nhiều nghiên cứu đã được đề xuất về vấn đề bảo mật nhưng nhiều chủ đề vẫn cần được nghiên cứu thêm. bảo mật trong việc thu thập dữ liệu, cũng như chia sẻ và quản lý dữ liệu, và các vấn đề bảo mật dữ liệu vẫn là những vấn đề nghiên cứu mở nên được thực hiện [15].

3.1.1.2. Xác thực và nhận dạng quản lí

Xác thực và IDM là sự kết hợp của các quy trình và công nghệ nhằm quản lý và bảo đảm tiếp cận với thông tin và các nguồn lực đồng thời bảo vệ các hồ sơ cá nhân. IDM duy nhất xác định các đối tượng và xác thực đòi hỏi phải nhận dạng việc thành lập giữa hai bên giao tiếp [16]. Cần phải xem xét làm thế nào để quản lý xác thực danh tính trong IoTs, vì nhiều người dùng và thiết bị cần phải xác thực lẫn nhau thông qua các dịch vụ tin cậy. Nhiều vấn đề nghiên cứu mở như vậy đã được trình bày. Để xác định tất cả mọi thứ một cách độc đáo, cần phải xác định cách tiếp cận quản lý nhận dạng hiệu quả. Tính di động, sự riêng tư, giả mạo, và các khía cạnh ẩn danh đòi hỏi phân tích và nghiên cứu sâu hơn [15] thường IoTs không chắc chắn, sự tin cậy đóng một vai trò quan trọng trong việc thiết lập giao tiếp an toàn giữa các vật. Hai khía cạnh của sự tin cậy nên được xem xét trong IoTs: tin vào sự tương tác giữa các tổ chức, và tin tưởng vào hệ thống từ quan điểm người sử dụng. Để lấy được lòng tin của người dùng, cần có một cơ chế hiệu quả của việc xác định niềm tin trong một môi trường năng động và hợp tác IoTs. Mục tiêu chính của nghiên cứu tin tưởng trong khuôn khổ IoTs là những điều sau đây: đầu tiên, khái niệm về

các mô hình mới cho niềm tin không tập trung; Thứ hai, việc thực hiện các cơ chế niềm tin cho điện toán đám mây; Thứ ba, sự phát triển của các ứng dụng dựa trên sự tin cậy của nút (ví dụ, định tuyến, tập hợp dữ liệu,…) [15].

Phương pháp SL: cách tiếp cận SL thậm chí còn cho phép tin tưởng tiêu cực (mất lòng tin), đó là một sự trừu tượng hữu ích khi truyền đạt lòng tin với người sử dụng. Trong các hệ thống IoTs được quản lý, dự đoán cho tổ chức quản lý IoTs là một trung tâm tin cậy cho tất cả các thiết bị được quản lý. Sự tin cậy có thể là tính chuyển đổi giữa các hệ thống nhưng cần phải tuân theo các thoả thuận. Một mô hình có khả năng làm việc là mô hình thỏa thuận roaming được tìm thấy trong các hệ thống di động, theo đó một thuê bao có thể sử dụng các dịch vụ trong các mạng khác với điều kiện các nhà khai thác có một thỏa thuận roaming tại chỗ. Niềm tin cuối cùng sẽ đòi hỏi một nền tảng, một yếu tố trong đó là đáng tin cậy. Trong ngữ cảnh của chúng ta, một thiết bị đáng tin phải có khả năng tránh lật đổ. Bài báo "Reflections on Trust In Devices" tiếp tục điều tra sự tin cậy vào các thiết bị từ góc nhìn của con người và cung cấp các phân tích quan trọng về các giới hạn của sự tin tưởng vào phần mềm và phần cứng. Trong bối cảnh hậu Snowdon, một khuôn khổ chính sách tốt là mong muốn kết hợp mức tin tưởng được đánh giá và mức độ đe dọa hiện tại trước khi đưa ra quyết định.

3.1.1.3. Cho phép và kiểm soát truy cập

Ủy quyền cho phép xác định nếu người hoặc đối tượng, sau khi xác định, nguồn lực có được phép hay không. Kiểm soát truy cập có nghĩa là kiểm soát việc tiếp cận các nguồn lực bằng cách cho phép hoặc từ chối theo một loạt các tiêu chí. Sự ủy quyền thường được thực hiện thông qua việc sử dụng kiểm soát truy cập. Sự cho phép và kiểm soát truy cập là rất quan trọng trong việc thiết lập một kết nối an toàn giữa một số thiết bị và dịch vụ. Vấn đề chính cần được giải quyết trong nội dung này là tạo ra các quy tắc kiểm soát truy cập dễ dàng hơn để tạo, hiểu và vận dụng. Thông tin bổ sung về kiểm soát truy cập được cung cấp tiếp theo.

3.1.1.4. An ninh giữa các điểm cuối

An ninh ở các điểm cuối giữa các thiết bị IoTs và máy chủ Internet cũng rất quan trọng. Áp dụng các sơ đồ mật mã cho mã hoá và mã xác thực cho các gói dữ liệu là không đủ cho IoTs hạn chế nguồn lực. Đối với an ninh đầu cuối hoàn chỉnh, việc xác minh nhận diện cá nhân trên cả hai đầu, các giao thức như TLS, IPsec,.. và các thuật toán (ví dụ các thuật toán AES và Hash) phải được an toàn thực hiện. Trong IoTs với an ninh đầu cuối, cả hai đầu thường dựa vào thông tin liên lạc thực tế của họ không hiển thị cho bất kỳ ai khác và không ai khác có thể sửa đổi dữ

liệu khi chuyển tiếp. Chính xác và đầy đủ an ninh đầu cuối là cần thiết, mà không có nó, nhiều ứng dụng sẽ không được tốt.

3.1.1.5. Giải pháp an ninh chống tấn công

Có nhiều loại thiết bị khác nhau với bộ nhớ khác nhau và nguồn lực tính toán hạn chế được kết nối với internet của sự vật. Vì những thiết bị này dễ bị tấn công, nên có các giải pháp bảo mật chống tấn công và các giải pháp an ninh ít quan trọng có sẵn. Các mức độ ít quan trọng cần được cung cấp trên các thiết bị để giải quyết các cuộc tấn công từ bên ngoài, chẳng hạn như tấn công từ chối dịch vụ, các trận lụt, ...

3.1.1.6. Nguy cơ thất thoát thông tin cá nhân

Ý tưởng về các thiết bị gia dụng thông minh nói chung và IoTs bị coi là bất khả thi chỉ vào khoảng một vài năm về trước khi công nghệ IPv4 vẫn còn giữ vị trí chủ yếu trên thế giới. Với công nghệ IPv4 chỉ có tổng cộng khoảng 4,3 tỉ địa chỉ public cho toàn bộ các thiết bị trên mạng Internet, kéo theo đó là khó kiểm soát các private IP trong từng mạng nội bộ. Ngược lại, với IPv6 ra đời phát triển cao hơn của IPv4 sẽ có khoảng 340 x 1036 tỷ địa chỉ. Số lượng địa chỉ này được đánh giá là sẽ đủ để trong tương lai gần ngay cả chiếc bếp trong nhà cũng sẽ có thể có một địa chỉ độc nhất trên toàn thế giới (tuy rằng không phải thiết bị nào cũng sẽ cần IP riêng đặc biệt là những thứ nhỏ bé cỡ công tắc đèn). Nhờ khả năng định danh chi tiết đến từng thiết bị, con người dễ dàng tạo ra các dịch vụ đánh giá, theo dõi từ xa cho từng tòa nhà, và cho từng vật dụng. Tuy nhiên với quá nhiều thiết bị tham gia vào mạng lưới sẽ có nguy cơ thất thoát thông tin hay vấn đề bảo mật, an toàn.

An toàn là một thách thức đáng kể cho việc triển khai IoTs do thiếu các tiêu chuẩn và kiến trúc thông thường cho an toàn IoTs. Trong các mạng không đồng nhất như trong trường hợp của IoTs, không phải là dễ dàng để đảm bảo an toàn và bảo mật của người sử dụng. Các chức năng cốt lõi của IoTs được dựa trên việc trao đổi thông tin giữa hàng tỷ của các đối tượng kết nối Internet. Vấn đề bảo mật và các hoạt động truy cập đến các thiết bị IoTs là cực kỳ quan trọng. Tuy nhiên, việc đảm bảo sự trao đổi dữ liệu là cần thiết để tránh mất hoặc ảnh hưởng đến bảo mật thông tin của khách hàng. Các thiết bị IoTs tham gia ngày càng nhiều vào mạng lưới với các dữ liệu nhạy cảm đòi hỏi phải quản lý kiểm soát truy cập trong suốt thời gian một cách chuẩn xác.

Một số thách thức như kiến trúc tổng thể và an ninh đã thu hút rất nhiều chú ý trong khi tính sẵn sàng, độ tin cậy và hiệu suất vẫn cần được quan tâm hơn đòi hỏi cần nghiên cứu đưa ra biện pháp để IoTs phát triển tối ưu hơn nữa.

3.1.1.7. Thách thức tại việt nam

Tại việt Nam, IoTs hiện tại mới phát triển ở giai đoạn đầu. Bên cạnh cơ sở hạ tầng ICT, một trong những thách thức lớn nhất để triển khai IoTs là chi phí cao và những nguy cơ an ninh tiềm ẩn, chúng tôi đang cố gắng hạ thấp chi phí để ngày càng nhiều cá nhân và doanh nghiệp có thể tiếp cận được với IoTs. Các tổ chức trong nước nếu muốn triển khai IoTs thì phải tối ưu hóa trung tâm dữ liệu (TTDL) để sẵn sàng cho IoTs. Một điểm được nhấn mạnh, cùng những phiên bản và tiêu chuẩn mới hỗ trợ cho IoTs, 4G là điều không thể thiếu nếu muốn phát triển IoTs tại Việt Nam.

TTDL đang thay đổi từng ngày, bên cạnh IoTs có một xu hướng khác đang ảnh hưởng tới TTDL là sự phát triển của sự phi tập trung hóa (edge computing). Phi tập trung hóa là quá trình chuyển dịch năng lực tính toán từ phần lõi của TTDL tới biên mạng, gần hơn với nơi khách hàng đặt trụ sở và nơi diễn ra các tương tác số. Các nhà cung cấp dịch vụ di động khi họ đang chuyển dịch hạ tầng cơ sở gần hơn tới khu vực biên khi ngày càng có nhiều khách hàng xem video và nghe nhạc trực tuyến hơn. Chính vì vậy cần phải cân nhắc sự linh hoạt trong thiết kế. Các tổ chức cần nghĩ đến phát triển cả theo chiều dọc và chiều ngang.

Việc quản lý nhiều thiết bị từ xa có thể là một thách thức và thường đòi hỏi có thêm nhân lực có kỹ năng và gây tốn kém. Để tiết kiệm chi phí trong khi vẫn đảm bảo có thể nắm bắt được các hệ thống TTDL lân cận, các tổ chức phải cho phép hiển thị thời gian thực của tất cả mạng lưới IT, từ trung tâm đến phần biên. Các thiết bị phân phối năng lượng thông minh như Liebert® MPH, thiết bị chuyển mạch KVM và các giải pháp DCIM cho phép quản lý tập trung các máy chủ từ xa, người vận hành có thể chủ động phát hiện và nhận dạng rủi ro tiềm ẩn và xử lý ngay lập tức. Khả năng phục hồi ở mọi mức độ cũng cần được quan tâm hàng đầu. Trong xã hội kết nối ngày nay, người dùng kì vọng các ứng dụng luôn luôn sẵn có. Nghiên cứu mới đây của Ponemon về Thời gian chết của TTDL được tài trợ bởi Emerson Network Power cho thấy, chi phí downtime đã tăng tới $8.851 mỗi phút hoặc trung bình $740.357. Lỗi UPS vẫn được xem là nguyên nhân hàng đầu gây ra gián đoạn trung tâm dữ liệu. Điều này có thể tránh được đối với những UPS đáng tin cậy, có khả năng chịu được sự cố như Liebert GXT4 [50]. Mặt khác các nhà khai triển IoTs tham gia trực tiếp vào việc triển khai, hỗ trợ khách hàng bằng việc cung cấp các giải pháp phần cứng và phần mềm để bảo vệ và tối ưu hóa hạ tầng then chốt, hỗ trợ khối bán lẻ, ngân hàng, viễn thông và thậm chí cả ngành công nghiệp sản xuất trong việc cung cấp các giải pháp quản lý IT, quản lý nhiệt và quản lý năng lượng cho dù họ phải đối mặt với những thách thức nào.

3.2.2. Hướng phát triển tương lai

Theo báo cáo Ericsson Mobility Report, tới năm 2021, dự kiến sẽ có 28 tỉ thiết bị kết nối trong đó có 15 tỉ thiết bị kết nối IoT bao gồm thiết bị M2M như đồng hồ đo thông minh, cảm biến trên đường, địa điểm bán lẻ, các thiết bị điện tử tiêu dùng như ti vi, đầu DVR, thiết bị đeo. 13 tỉ còn lại là điện thoại di động, máy tính xách tay PC, máy tính bảng…

Dự kiến năm 2019, toàn cầu sẽ chi 1.300 tỉ đô la Mỹ cho IoTs. Tới năm 2020, theo dự đoán của Gartner thì giá trị gia tăng do IoTs mang lại sẽ là 1.900 tỉ đô la Mỹ. Và theo McKinsey, tới năm 2025 IoTs sẽ đóng góp vào nền kinh tế toàn cầu là 11.000 tỉ đô la Mỹ.

Tới năm 2021, dự kiến số thuê bao sẽ lên tới 9,1 tỉ. Số thuê bao này cao hơn số dân bởi mỗi người có thể sở hữu nhiều thiết bị. Trong các kết nối IoTs như vậy, sẽ có bao gồm cả những có đăng ký thuê bao SIM/eSIM được gắn ngay trong thiết bị và cả những thiết bị như điện tử tiêu dùng không cần dùng SIM (Non-SIM).

IoTs đang diễn ra một cách mạnh mẽ. Khoảng 50% doanh nghiệp đã bắt đầu triển khai những dự án về IoTs. IoTs mang lại một cơ hội doanh thu cho rất nhiều ngành và những giải pháp đó bắt đầu thương mại hóa với tốc độ rất nhanh. Ngành dịch vụ tiện ích, giao thông, tòa nhà thông minh và các ngành bán lẻ là những ngành đi đầu trong việc ứng dụng IoTs [18].
Trước việc IoTs phát triển mạnh mẽ trên thế giới, hiện tại các nhà mạng

Việt Nam đã bắt đầu thử nghiệm triển khai 4G, các dịch vụ IoTs cũng có tiềm năng phát triển và triển khai trên nền tảng này. IoTs sẽ có tác động trực tiếp lên các nhà khai thác viễn thông. Các nhà khai thác viễn thông [18] đã cho biết hiện giờ thường chia thành 3 nhóm phụ thuộc vào chiến lược của từng

nhà cung cấp. IoTs có ảnh hưởng khác nhau tới từng nhóm đó.

- Thứ nhất “Các nhà khai thác viễn thông và các công ty thuộc các ngành công nghiệp khác nhau đang nắm bắt cơ hội từ IoTs". Với các công ty đặt chiến lược vào hệ thống mạng tối ưu (Network Developer), họ sẽ thu lợi nhuận từ việc cung cấp mạng như dịch vụ tiện ích cho các nhà cung cấp dịch vụ khác khai thác.

- Nhóm hai là các công ty thúc đẩy nền tảng cung cấp dịch vụ (Services Enabler), họ tập trung vào việc quản lý mạng mang tính linh hoạt cao, với hệ thống giám sát và quản lý vận hành rất tốt để tích hợp giải pháp hiệu quả và hợp tác với các doanh nghiệp IT khác để cung cấp các dịch vụ sáng tạo.

- Nhóm thứ ba là các công ty tạo ra các dịch vụ và ứng dụng sáng tạo mới (Services Creator) – nhóm công ty này rất tích cực trong việc tạo ra hệ sinh thái, xây dựng hệ thống mạng chất lượng cao, trải nghiệm tốt để cung cấp các dịch vụ sáng tạo trong các lĩnh vực như giao thông, dịch vụ tiện ích, tài chính, y tế, truyền thông.

Sự phát triển của IoTs tạo ra bốn bước chuyển dịch trong vai trò của các nhà khai thác viễn thông. Vai trò đầu tiên là thu thập dữ liệu để nâng cao hiệu quả nội bộ như hệ thống báo cáo và roaming. Vai trò thứ hai là phân tích thông tin tương tác của khách hàng, để cung cấp những dịch vụ IoTs mang tính cá nhân cho các thuê bao của mình. Vai trò thứ ba là sử dụng cơ sở dữ liệu phân tích là giá trị, kết nối với các công ty cung cấp dịch vụ ở lĩnh vực khác tạo ra sản phẩm hiệu quả. Vai trò thứ tư là cung cấp dịch vụ quản lý dữ liệu cho các kết nối IoTs, làm cầu nối giữa các công ty cung cấp ứng dụng

IoTs với chính các kết nối IoT có SIM và không có SIM để các bên đều mua được dịch vụ mình cần và bán được dịch vụ mình có một cách hiệu quả. Như vậy để có thể triển khai IoTs thành công và bền vững, cần phải cân nhắc đến bốn yếu tố là nền tảng phần mềm, hệ sinh thái giữa các ngành, quá trình chuẩn hóa về công nghệ và đảm bảo tính riêng tư và an toàn cho khách hàng.

Tại Việt Nam: Ba thách thức được đề cập lâu nay là giá thành thiết bị, năng lượng pin, vùng phủ kết nối. Mới đây nổi trội hai thách thức mới là yêu cầu về độ linh hoạt và tính đa dạng. Tính linh hoạt là rất cần thiết bởi khi có nhiều thiết bị IoTs kết nối thì tốc độ kết nối diễn ra nhanh hơn tốc độ kết nối của băng rộng di động hiện tại. Mật độ kết nối thiết bị IoTs không đồng bộ tạo ra lưu l ượng lớn đột ngột đối với một số cells. Sự đa dạng cũng đặc biệt quan trọng. Hiện tại, người dùng smartphone có chung sự kỳ vọng về vùng phủ và dung lượng và họ thỏa mãn khi ứng dụng họ dùng hoạt động tốt bất cứ lúc nào và ở đâu khi họ muốn sử dụng. Nhưng đối với các kết nối IoTs thì mọi yêu cầu trở nên phức tạp hơn, đa dạng hơn, công suất và cường độ lớn hơn, đòi hỏi các nhà mạng phải nâng cao nỗ lực quản lý và vận hành.

Theo cuộc khảo sát về an ninh và bảo mật IoTs, rất nhiều nghiên cứu là cần thiết để làm cho mô hình IoTs trở thành hiện thực. Trong phần này, hướng nghiên cứu trong tương lai được đề xuất:

- Vấn đề an ninh và bảo mật cần được xem xét rất nghiêm túc vì IoTs không chỉ giải quyết những lượng lớn dữ liệu nhạy cảm (dữ liệu cá nhân, dữ liệu kinh doanh ...) mà còn có khả năng ảnh hưởng đến môi trường vật lý với khả năng kiểm soát của nó. Các môi trường Cyber-vật lý phải được bảo vệ khỏi bất kỳ loại tấn công nguy hiểm nào.

- Xác định, phân loại và phân tích các công nghệ, thiết bị và dịch vụ của IoTs sẽ thúc đẩy sự phát triển IoTs và hỗ trợ cho tầm nhìn IoTs.

- Thiết kế các tiêu chuẩn kiến trúc cần phải có các mô hình, giao diện và giao thức dữ liệu trừu tượng, cùng với các ràng buộc bê tông cho các công nghệ trung lập để hỗ trợ phạm vi rộng nhất của con người, phần mềm, đồ vật thông minh hoặc thiết bị.

- Phát triển các khuôn khổ mới nhằm giải quyết các sơ đồ ID toàn cầu, quản lý nhận dạng, mã hoá/mã hoá nhận dạng, xác thực cũng như tạo ra các dịch vụ tìm kiếm và khám phá thư mục toàn cầu cho các ứng dụng IoTs với các chương trình nhận diện khác nhau.

3.2. Tăng cường bảo mật trong hệ thống iots dựa trên công nghệ lấy mẫu nén

Internet of Things (IoT) đang cung cấp nhiều ứng dụng trong các lĩnh vực khác nhau. Mục tiêu chính là tạo một mạng dựa trên internet để kết nối mọi thứ bao gồm các thiết bị điện tử và nhu cầu của con người. Các hệ thống trong nhà thông minh hoặc các lĩnh vực công nghiệp/quân sự có thể liên lạc với nhau cho các mục đích khác nhau. IoT hỗ trợ các mạng khác để đạt hiệu quả cao hơn.

Mạng cảm biến không dây truyền thống (WSN) thu thập dữ liệu từ khu vực cảm biến được gửi đến trạm gốc (BS). BS có thể ở các vị trí cố định để thu thập dữ liệu cảm biến. Với sự tích hợp giữa các IoT và WSN, dữ liệu có thể được gửi qua đám mây hoặc internet để được lưu trữ ở mọi nơi cần thiết.

BS có thể được thiết lập ở mọi nơi để có thể thu thập dữ liệu.

Với sự gia tăng nhanh chóng trong việc sử dụng ứng dụng IoT, một số vấn đề bảo mật và riêng tư được quan sát thấy. Khi gần như mọi thứ sẽ được kết nối với nhau, vấn đề này sẽ trở nên rõ ràng hơn, và tiếp xúc thường xuyên sẽ tiết lộ lỗ hổng bảo mật và điểm yếu. Những hiểm họa an toàn đối với các dịch vụ trong IoT là do nguyên nhân hạn chế về năng lực tính toán, năng lượng và băng thông kết nối. Các loại mối đe dọa khác nhau đến mô hình IoT được mô tả gồm: tấn công từ chối dịch vụ (DoS), loại tấn công này làm cho máy tính hoặc tài nguyên mạng không khả dụng cho người sử dụng như dự kiến. Do khả năng bộ nhớ thấp và nguồn lực tính toán hạn chế, phần lớn nguồn tài nguyên của các thiết bị trong IoTs dễ bị tấn công đe dọa; Các cuộc tấn công vật lý, loại tấn công này can thiệp vào các thành phần phần cứng. Do tính chất không được giám sát và phân phối của IoT, hầu hết các thiết bị thường hoạt động trong môi trường ngoài trời,

rất nhạy cảm với các cuộc tấn công vật lý. Những cuộc tấn công này có thể khai thác được những dữ liệu mật, khóa… từ thiết bị.

Trong nghiên cứu này, sử dụng một số phương pháp mới với mục đích chính là nén dữ liệu và tăng cường bảo mật cho dữ liệu dựa trên công nghệ lấy mẫu nén. Các phương pháp này không chỉ tiết kiệm năng lượng truyền khi dữ liệu truyền giảm đáng kể mà còn bảo mật được dữ liệu truyền. Những đóng góp chính của nghiên cứu này được liệt kê như sau:

- Thuật toán truyền dữ liệu từ IoTs được thiết lập dựa trên phép biến đổi Wavelet.
- Thuật toán dựa trên công nghệ lấy mẫu nén xử lý dữ liệu từ IoTs.
- Cung cấp các kết quả mô phỏng xử lý dữ liệu để làm rõ hiệu quả các các thuật toán.

3.2.1. Công nghệ lấy mẫu nén

Công nghệ lấy mẫu nén (CS – Compressive sensing) cho phép khôi phục toàn bộ dữ liệu dựa trên một số lượng mẫu nhỏ hơn rất nhiều so với các phướng pháp nén và lấy mẫu thông thường như Shannon /Nyquist. Điều kiện tiên quyết để sử dụng công nghệ này là tín hiệu phải "thưa - rỗng" trong miền thích hợp.

Tín hiệu cảm biến

Một tín hiệu, ví dụ $X = [x_1 x_2 \ldots x_N]^T \in$ RN, được định nghĩa là rỗng mức k nếu nó có biểu diễn tín hiện ở một miền nào đó thích hợp, ví dụ $\boldsymbol{\psi} = [\psi i, j] \in R^{NxN}$ và $X = \boldsymbol{\psi}\theta$ và θ có k thành phần khác 0 và các thành phần nhỏ còn lại có thể coi như bằng không.

Lấy mẫu tín hiệu và ma trận lấy mẫu

Các mẫu cảm biến được tạo ra dựa trên công thức $Y = \Phi X$, where $\Phi = [\varphi_{i,j}] \in R^{MxN}$ bao gồm các thành phần là các hệ số Gaussian được tạo ra một cách ngẫu nhiên. Vector các mẫu cảm biến còn có thể được viết như sau: Y =

$[y_1 y_2 \ldots y_M]^T \in R^M$.

Khôi phục tín hiệu

Với số lượng mẫu cảm biến nhất định $M = O(klogN/k)$ có thể khôi phục được toàn bộ dữ liệu cảm biến như dã được đề cập ở [ ]. $\Theta\hat{} = argmin||\Theta||$, $st.\ to\ Y = \Phi\Psi\Theta$ (1)

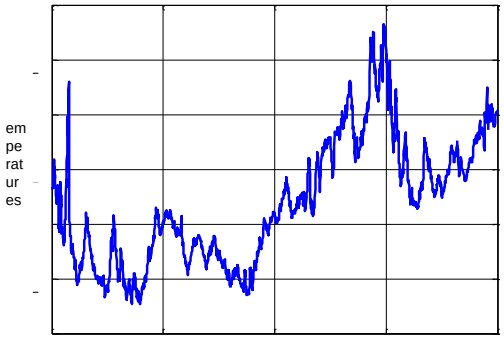
1

Trên thực tế, những mẫu cảm biến khi thu thập được sẽ thường gắn với nhiễu như sau: $Y = \Phi X + e, trongđó||e|| = \epsilon$. Và dữ liệu sẽ được khôi phục theo 2 thuật toán sau:

$$\Theta = argmin||\Theta||_1, st.\ to\ ||Y - \Phi\Psi\Theta||_2 < \epsilon \quad (2)$$

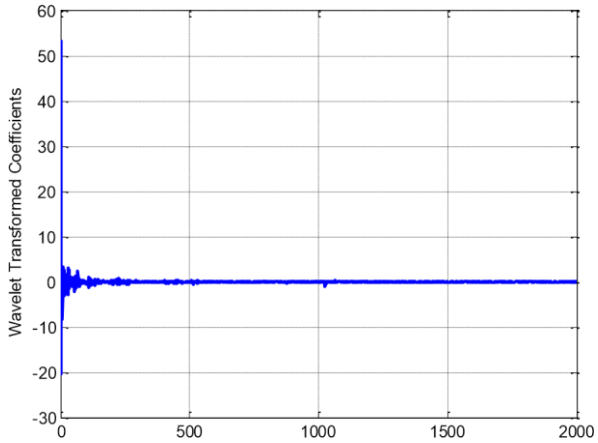
3.2.2. Thuật toán xử lý dữ liệu dựa trên biến đổi wavelet

Trong phần này, áp dụng lý thuyết biến đổi Wavelet để xử lý dữ liệu thu được từ các hệ thống IoTs để nén dữ liệu cảm biến và truyền đi một số lượng nhất định mẫu. Hình 3.1 thể hiện 2000 giá trị cảm biến thu từ 2000 bộ cảm biến trong hệ thống IoTs.



Hình 3.1: Dữ liệu cảm biến nhiệt độ thu từ 2000 bộ cảm biến trong hệ thống IoTs

Wavelet



Hình 3.2: Dữ liệu cảm biến sau biến đổi Wavelet sẽ trở thành các hệ số lớn và còn lại là các hệ số bé có thể coi bằng không ('0')

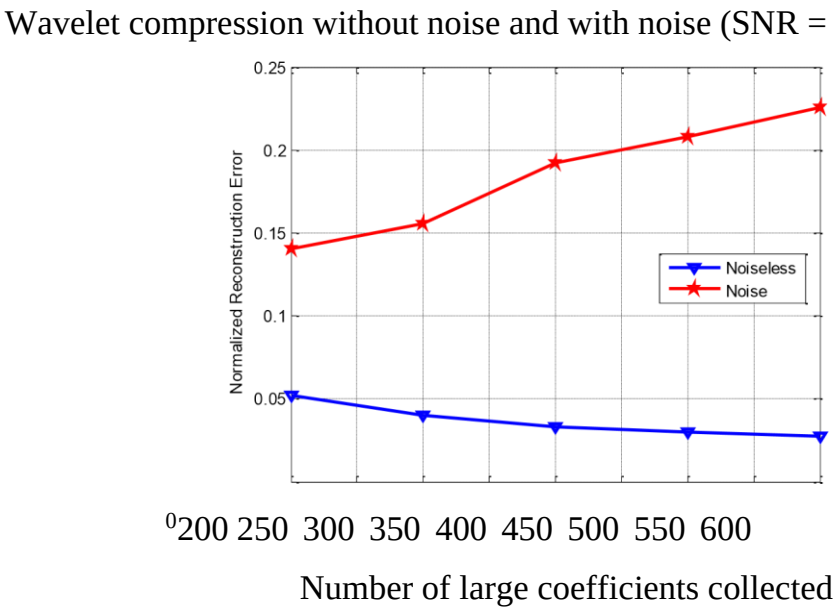
Dữ liệu thu thập được từ IoTs sẽ được nhân với các hệ số Wavelet hay ma trận Wavelet với kích cỡ tùy thuộc vào kích cỡ của dữ liệu để nhận được các hệ số đã biến đổi. Các hệ số này tự phân loại hệ số lớn và bé như trong Hình 3.2. thuật toán này sẽ chỉ gửi các hệ số lớn đến trạm

gốc (BS) hoặc trung tâm xử lý dữ liệu. Do vậy, theo như Hình 3.2, chỉ một lượng mẫu rất nhỏ cần phải gửi đi nên sẽ tiết kiệm được nhiều năng lượng truyền.

BS thu thập các hệ số lớn và khôi phục lại tất cả dữ liệu ban đầu. Hệ số nhỏ được coi bằng không ('0') ở phía đầu thu. BS sẽ nhân trở lại các hệ số với ma trận Wavelet để thu được toàn bộ dữ liệu ban đầu.

Đặc tính bảo mật ở đây là phần hệ số lớn được chuyển đi hoàn toàn an toàn cho dữ liệu gốc và giảm chi phí truyền dẫn. Người truy cập khác không thể khôi phục dữ liệu dựa trên các hệ số lớn nếu không biết thông tin về biến đổi Wavelet.

Tuy nhiên, phương pháp này không cản trở được nhiễu xâm nhập vào dữ liệu, như Hình 3.3. Do vậy, phương pháp này nên chỉ sử dụng ở môi trường truyền ngắn, ít bị ảnh hưởng bởi nhiễu.



Hình 3.3: Hệ số lớn tăng và chất lượng khôi phục dữ liệu trong các môi trường có nhiễu và không có nhiễu.

3.2.3. Thuật toán xử lý dữ liệu dựa trên công nghệ lấy mẫu nén (cs)

Thuật toán này với khả năng xử lý được nhiễu nhờ công nghệ lấy mẫu nén như đã trình bày ở phần 3.1.1

Thuật toán này bao gồm 3 pha như sau:

Pha thứ nhất – Thu dữ liệu từ IoTs

Trong pha này, dữ liệu được tập hợp lại từ hệ thống IoTs chờ xử lý. Dữ liệu có thể là hình ảnh, videos, nhiệt độ, độ ẩm, … sẽ được phân chia theo từng cụm, từng khoảng thời gian tùy vào ứng dụng để chờ xử lý

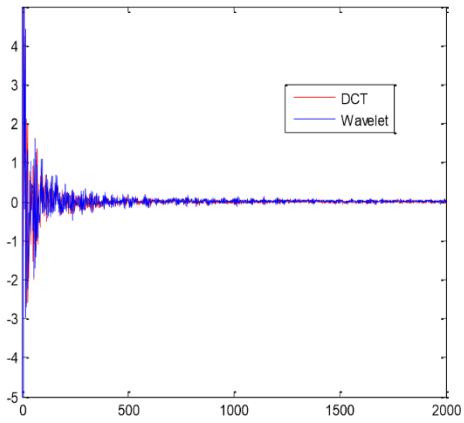
Pha thứ hai – Tạo ra các mẫu cảm biến

Ở pha này, bộ xử lý sẽ tạo ra một ma trận Gaussian rồi đem nhân với toàn bộ dữ liệu mà nó lưu trữ để tạo ra được một số lượng mẫu cảm biến nhất định. Kích cỡ của ma trận sẽ quyết định số mẫu cảm biến truyền đi ***Pha thứ ba – Thu thập mẫu cảm biến và khôi phục dữ liệu***

Số lượng mẫu cảm biến tạo ra sẽ được gửi về trạm gốc. Dựa trên thuật toán khôi phục dữ liệu của CS theo công thức (1) và (2), toàn bộ dữ liệu từ bộ cảm biến ở trong các hệ thống IoTs sẽ được khôi phục.

Với thuật toán trên, hai cơ sở Wavelet và DCT được lựa chọn để làm rỗng dữ liệu đảm bảo áp dụng được công nghệ nén cảm biến. Hình 3.4 đưa ra so sánh khả năng phân tích và phân loại dữ liệu của Wavelet và DCT. Hai phương pháp biến đổi về cơ bản là giống nhau, đảm bảo số lượng mẫu lớn và năng lượng của tín hiệu tập trung ở phần đầu như hình vẽ.

5Sparse S signal from real sensor reading X = psi*S, N = 2000



Hình 3.4: Sử dụng hai cơ sở là Wavelet và DCT để làm rỗng dữ liệu trong quá trình khôi phục dữ liệu với công nghệ nén cảm biến.

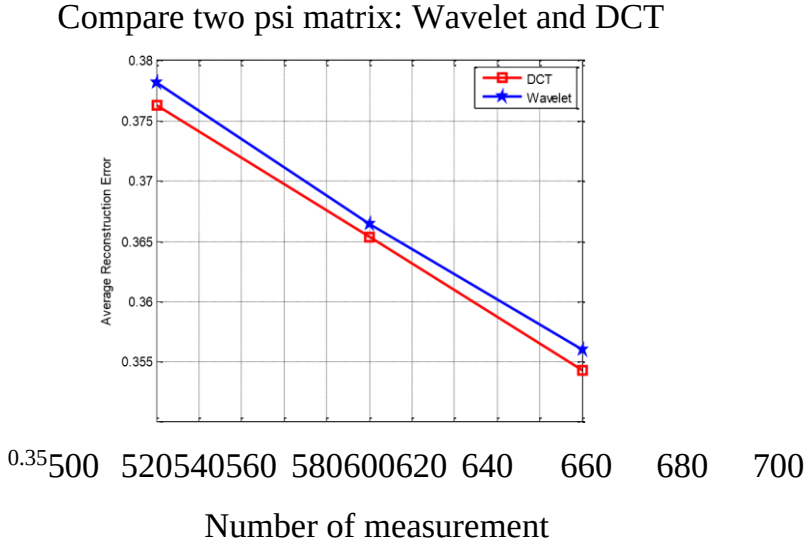
Với số lượng mẫu cảm biến nhất định được gửi về BS để khôi phục toàn bộ dữ liệu. Ở đây dữ liệu từ IoTs được chọn có thể là dữ liệu cảm biến nhiệt độ, độ ẩm đọc từ các bộ cảm biến, dữ liệu ngẫu nhiên, dữ liệu ảnh, .v.v.

Tất cả dữ liệu có thể nén hay nói cách khác có độ tương quan cao đều có thể áp dụng được công nghệ lấy mẫu nén. Trong phần này, chọn một hình ảnh để thực hiện mô phỏng như Hình 3.5.

Hình 3.5: Hình ảnh được chọn để thực hiện mô phỏng nén và khôi phục dữ liệu sử dụng công nghệ lấy mẫu nén.

Sau khi thực hiện khôi phục dữ liệu sử dụng công nghệ lấy mẫu nén.

Đã được đánh giá để làm rõ chất lượng khôi phục dữ liệu dựa trên số lượng mẫu sử dụng. Chú ý ở đây là, số lượng mẫu càng lớn sẽ cho chất lượng khôi phục dữ liệu càng cao. Điều đó có nghĩa là lỗi khôi phục sẽ nhỏ dần và được thể hiện ở Hình 3.6.



Hình 3.6: Chất lượng khôi phục ảnh với tổng số dữ liệu ảnh là 2000 giá trị vô hướng số mẫu nén tăng trong khi lỗi khôi phục giảm dần.

Kết quả trong việc so sánh khôi phục ảnh với cả DCT và Wavelet là tương đương nhau.

Tính bảo mật được đóng góp ở nghiên cứu này là với số mẫu bảo mật có thể bị mất mát, dữ liệu vẫn được khôi phục đầy đủ. Tuy nhiên, hackers nhận được một số mẫu cảm biến cũng không thể khôi phục được dữ liệu của hệ thống IoTs hiện tại.

3.3. Kết chương 3

Chương 3 tập chung chính về công nghệ lấy mẫu nén áp dụng trong mạng IoTs đã chứng minh được hiệu quả. Với số mẫu chuyển đi rất nhỏ so với toàn bộ khối lượng dữ liệu ban đầu, kết quả khôi phục dữ liệu đáp ứng được yêu cầu sử dụng của hệ thống và người dùng. Hơn nữa, các thuật toán đã đáp ứng được nhu cầu bảo mật trong hệ thống IoTs.

Cũng nêu rõ một số thách thức cần giải quyết về các vấn đề an ninh của Iots nói chung và tại Việt Nam nói riêng. Qua đó có phương hướng tích cực hạn chế tiềm ẩn nguy cơ mất an toàn trong tương lai.

ĐẶC TẢ PROJECT

Những ngôi nhà của thế kỷ 21 sẽ ngày càng trở nên tự kiểm soát và tự động hóa hơn do sự thoải mái mà nó mang lại, đặc biệt là khi được làm việc trong một ngôi nhà riêng. Hệ thống tự động hóa gia đình là một phương tiện cho phép người dùng điều khiển các thiết bị điện thuộc nhiều loại khác nhau. Nhiều hệ thống tự động hóa gia đình hiện có, được thiết lập tốt dựa trên giao tiếp có dây. Điều này không gây ra vấn đề gì cho đến khi hệ thống được lên kế hoạch tốt trước và được lắp đặt trong quá trình xây dựng vật lý của tòa nhà. Nhưng đối với các tòa nhà đã có sẵn, chi phí thực hiện rất cao.

Ngược lại, hệ thống không dây có thể giúp ích rất nhiều cho các hệ thống tự động hóa. Với sự tiến bộ của các công nghệ không dây như Wi-Fi, mạng đám mây trong thời gian gần đây, các hệ thống không dây được sử dụng hàng ngày và mọi nơi.

Ưu điểm của hệ thống tự động hóa gia đình:

Trong những năm gần đây, các hệ thống không dây như Wi-Fi ngày càng trở nên phổ biến hơn trong mạng gia đình. Ngoài ra, trong các hệ thống tự động hóa gia đình và tòa nhà, việc sử dụng các công nghệ không dây mang lại một số lợi thế không thể đạt được chỉ bằng cách sử dụng mạng có dây.

1) Giảm chi phí lắp đặt: Đầu tiên và quan trọng nhất, chi phí lắp đặt giảm đáng kể vì không cần cáp. Các giải pháp có dây yêu cầu cáp, trong đó vật liệu cũng như việc đặt cáp chuyên nghiệp (ví dụ như vào tường) rất tốn kém.

2) Khả năng mở rộng hệ thống và mở rộng dễ dàng: Triển khai mạng không dây đặc biệt thuận lợi khi, do các yêu cầu mới hoặc thay đổi, việc mở rộng mạng là cần thiết. Trái ngược với cài đặt có dây, trong đó phần mở rộng cáp là tẻ nhạt. Điều này làm cho việc cài đặt không dây trở thành một khoản đầu tư quan trọng.

3) Lợi ích thẩm mỹ: Ngoài việc bao phủ một khu vực lớn hơn, thuộc tính này cũng giúp đáp ứng đầy đủ các yêu cầu thẩm mỹ. Ví dụ bao gồm các tòa nhà đại diện với kiến trúc hoàn toàn bằng kính và các tòa nhà lịch sử nơi lý do thiết kế hoặc nhà kính không cho phép đặt cáp.

4) Tích hợp các thiết bị di động: Với các mạng không dây, việc liên kết các thiết bị di động như PDA và Điện thoại thông minh với hệ thống tự động hóa trở nên khả thi ở mọi nơi và bất cứ lúc nào, vì vị trí vật lý chính xác của thiết bị không còn quan trọng đối với kết nối (miễn là thiết bị nằm trong tầm với của mạng).

Vì tất cả những lý do này, công nghệ không dây không chỉ là một lựa chọn hấp dẫn trong việc cải tạo và tân trang, mà còn cho các cài đặt mới.

Tự động hóa gia đình là tự động hóa nhà cửa, việc nhà hoặc hoạt động gia đình. Nói cách khác, nó đề cập đến việc sử dụng CNTT / máy tính để điều khiển các thiết bị gia dụng. Nó tích hợp các thiết bị điện trong một ngôi nhà với nhau. Ví dụ: Nó có thể bao gồm kiểm soát tập trung ánh sáng, thiết bị, khóa an ninh của cổng và cửa ra vào để cung cấp sự tiện lợi, thoải mái, năng lượng, hiệu quả và an toàn được cải thiện. Trong thế giới CNTT ngày nay, tự động hóa gia đình đang trở nên phổ biến do sự dễ dàng, phương tiện linh hoạt để xem / giám sát và điều khiển các thiết bị và những thứ khác theo sự thoải mái và nhu cầu của người dùng. Phần thách thức nằm ở sự đơn giản và chi phí lắp đặt chúng trong nhà và thay đổi theo số lượng dịch vụ ngày càng tăng được theo dõi và kiểm soát. Dự án có tên 'HOME AUTOMATION USING PACKET TRACER' này là ý tưởng về tự động hóa gia đình bằng cách sử dụng Cisco Packet Tracer. Sự phổ biến của tự động hóa gia đình đã tăng lên rất nhiều trong những năm gần đây do khả năng chi trả đáng kể và sự đơn giản thông qua kết nối điện thoại thông minh và máy tính bảng. Một hệ thống tự động hóa gia đình tích hợp các thiết bị điện trong một ngôi nhà với nhau. Các kỹ thuật được sử dụng trong tự động hóa gia đình bao gồm các kỹ thuật trong tự động hóa tòa nhà cũng như kiểm soát các hoạt động trong nước, chẳng hạn như hệ thống điều khiển ánh sáng và sử dụng các thiết bị điện khác. Các thiết bị có thể được kết nối thông qua mạng gia đình để cho phép điều khiển bằng máy tính cá nhân và có thể cho phép truy cập từ xa từ internet. Thông qua việc tích hợp các công nghệ thông tin với môi trường gia đình, các hệ thống và thiết bị có thể giao tiếp theo cách tích hợp dẫn đến sự tiện lợi, hiệu quả năng lượng và lợi ích an toàn. Do sự tiến bộ của công nghệ không dây, có một số kết nối khác nhau được giới thiệu như GSM, WIFI và Bluetooth. Mỗi kết nối có thông số kỹ thuật và ứng dụng độc đáo của riêng họ. Trong số bốn kết nối không dây phổ biến thường được triển khai trong dự án Tự động hóa gia đình, WIFI đang được lựa chọn với khả năng phù hợp của nó. Các khả năng của WIFI là quá đủ để được thực hiện trong thiết kế. Ngoài ra, hầu hết các máy tính xách tay / máy tính xách tay hoặc điện thoại thông minh hiện tại đều đi kèm với bộ chuyển đổi WIFI tích hợp. Nó sẽ gián tiếp làm giảm chi phí của hệ thống này.

Dự án này đề cập đến việc triển khai nhà thông minh bằng cách sử dụng trình theo dõi gói cisco được phát hành mới vì tính năng này bao gồm các cảm biến khác nhau, bộ truyền động và thiết bị thông minh khác nhau được sử dụng để tự động hóa gia đình. Một số thiết bị là cửa sổ thông minh, ánh sáng thông minh, cửa thông minh, quạt thông minh với máy dò và cảm biến khác nhau. Để triển khai nhà thông minh, tôi đã sử dụng phần mềm mô phỏng theo dõi gói cisco mới được phát hành để thiết kế và định cấu hình thiết bị IOE với thiết bị mạng cổ điển.

Công dụng

Các mục tiêu chính của dự án của chúng tôi như sau:

i. Để điều khiển từ xa các thiết bị gia dụng và giám sát chúng.

Ii. Để tiết kiệm thời gian và sử dụng năng lượng hiệu quả

Iii. Để tăng tính độc lập của bạn và đạt được sự kiểm soát tốt hơn đối với môi trường gia đình

Iv. Để giúp giao tiếp với gia đình dễ dàng hơn

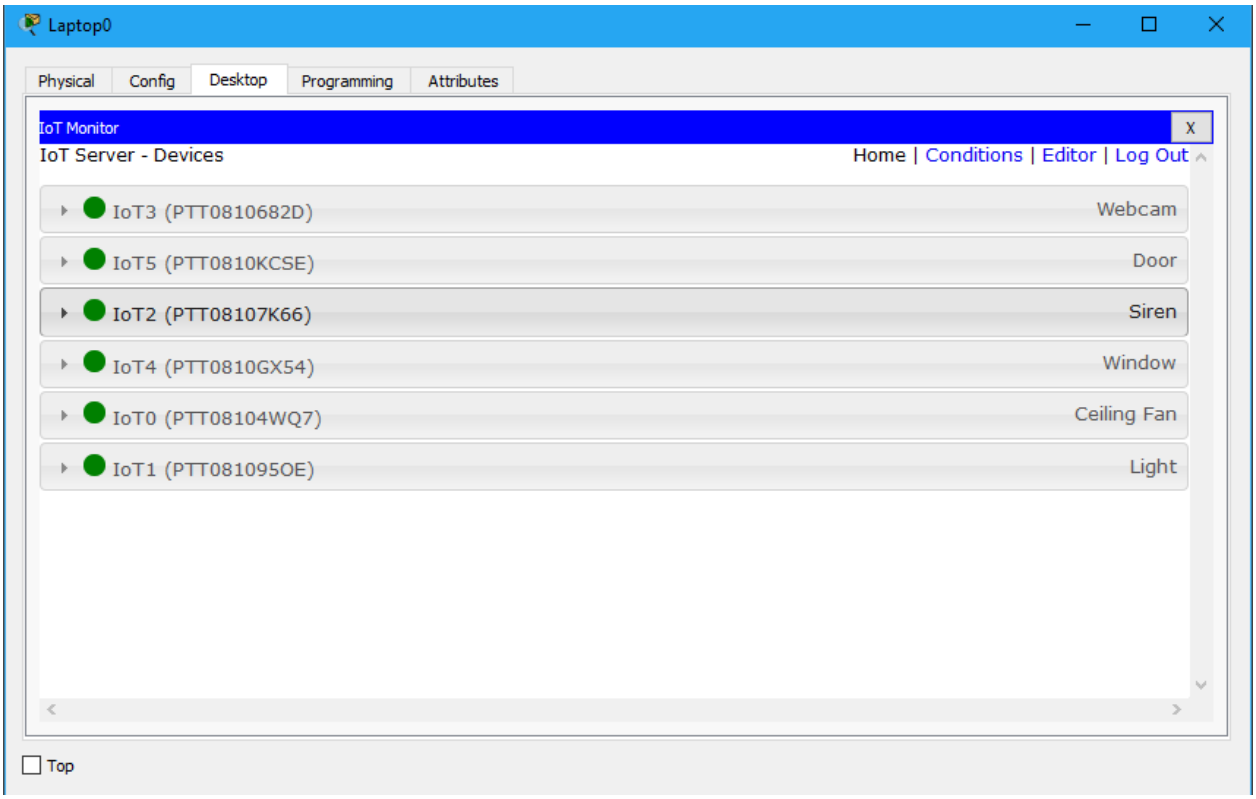
v. Để cải thiện an toàn cá nhân

Vi. Để cảnh báo trực quan về các tình huống khẩn cấp

THIẾT KẾ

Để triển khai nhà thông minh, tôi đã sử dụng trình theo dõi gói cisco được phát hành mới, bao gồm các đối tượng thông minh khác nhau được sử dụng để tự động hóa gia đình như quạt thông minh, cửa sổ thông minh, cửa thông minh, ánh sáng thông minh, còi báo động thông minh, webcam thông minh và các cảm biến khác nhau được bao gồm.

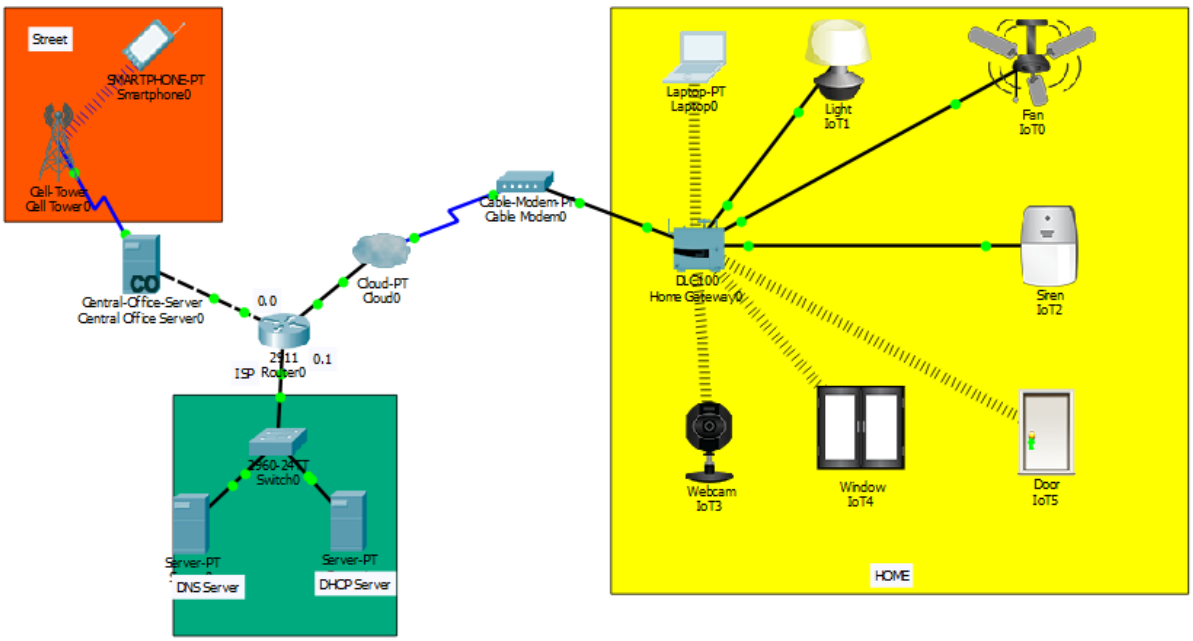
Để điều khiển đối tượng và cảm biến thông minh này, Home Gateway được sử dụng, vì nó cung cấp môi trường lập trình để điều khiển đối tượng thông minh được kết nối với nó và cung cấp các cơ chế điều khiển bằng cách đăng ký thiết bị thông minh với Home Gateway tương ứng.



Cổng trang chủ:

Home Gateway có 4 cổng Ethernet ngoài một điểm truy cập không dây được định cấu hình với SSID "Home Gateway". Để bảo mật kết nối không dây WEP / WPA-PSK / WPA2 Enterprise có thể được cấu hình trên cổng chính.

LẮP ĐẶT THIẾT BỊ



CẤU HÌNH

Phần cấu hình CLI định tuyến và bảo mật :

Router>

Router>enable

Router#conf terminal

Router(config)#hostname ISP

ISP(config)#intgigabitEthernet 0/2

ISP(config-if)#ip address 10.10.220.1 255.255.255.0

ISP(config-if)#no shutdown

ISP(config)#intgigabitEthernet 0/0

ISP(config-if)#ip address 209.165.200.225 255.255.255.224

ISP(config-if)#no shutdown

ISP(config)#intgigabitEthernet 0/1

ISP(config-if)#ip address 209.165.201.225 255.255.255.224

ISP(config-if)#no shutdown

Configurating dhcp server for cell and IOE device

ISP(config)#ipdhcp excluded-address 209.165.201.225 209.165.201.230

ISP(config)#ipdhcp pool cell

ISP(dhcp-config)#network 209.165.201.225 255.255.255.224

ISP(dhcp-config)#default-router 209.165.201.225

ISP(dhcp-config)#dns-server 10.10.220.10

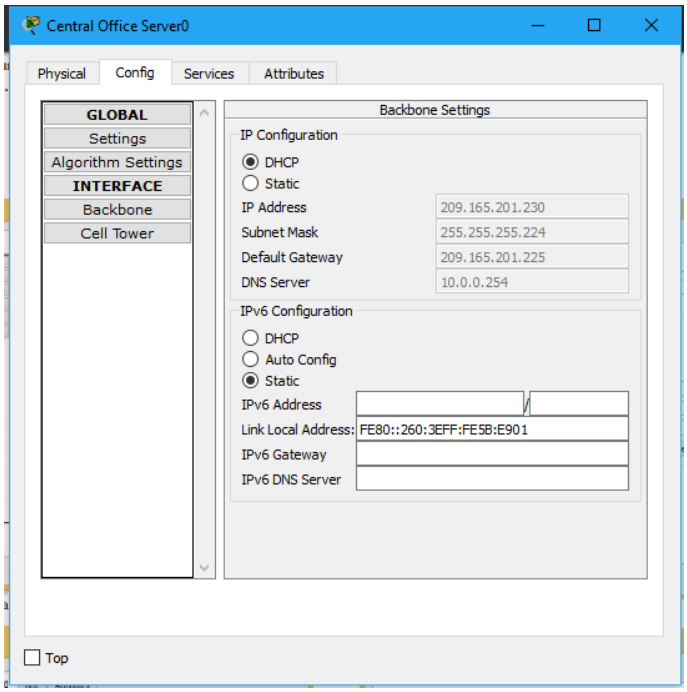
ISP(config)#ipdhcp excluded-address 209.165.200.225 209.165.200.230

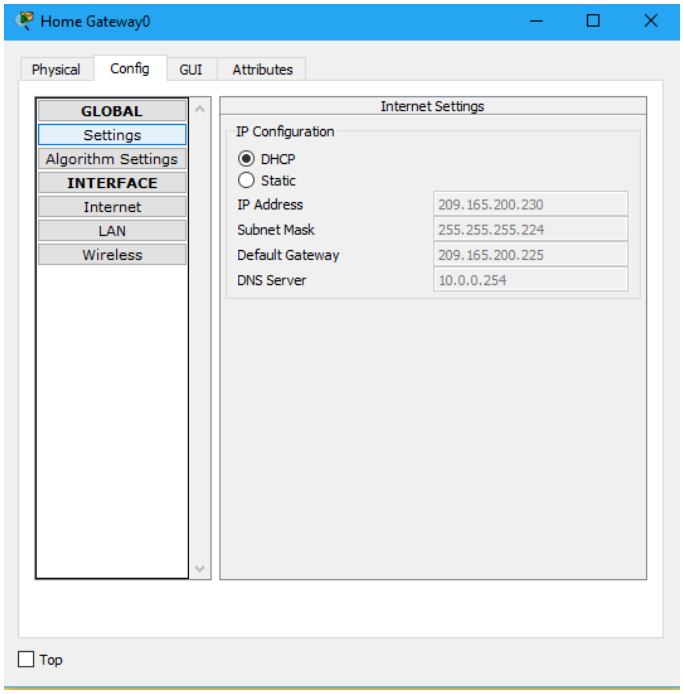
ISP(config)#ipdhcp pool ioe

ISP(dhcp-config)#network 209.165.200.224 255.255.255.224

ISP(dhcp-config)#default-router 209.165.200.225

ISP(dhcp-config)#dns-server 10.10.220.10




Home Gateway0
Physical
Config
GUI
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Internet
LAN
Wireless
Internet Settings
IP Configuration
DHCP
Static
IP Address
209.165.200.230
Subnet Mask
255.255.255.224
Default Gateway
209.165.200.225
DNS Server
10.0.0.254
Top

KẾT LUẬN

Trong những nghiên cứu tới, sẽ làm tăng hiệu quả việc áp dụng công nghệ nén cảm biến không chỉ với các đối tượng dữ liệu nêu trên mà còn triển khai đa dạng hơn. Ngoài ra, mã hóa cũng đang được nghiên cứu để áp dụng công nghệ nén cảm biến để tăng cường khả năng bảo mật cho hệ thống IoTs.

Luận văn này đã giới thiệu khái quát về các khía cạnh an ninh của IoTs, những ứng dụng đã và đang triển khai, làm rõ một số nguy cơ, thách thức và đưa ra các biện pháp phòng vệ và hướng giải quyết quyết cho an ninh IoTs trong tương lai. Còn rất nhiều khó khăn và thách thức liên quan đến IoTs vẫn đang phải đối mặt.

TÀI LIỆU THAM KHẢO

[1] L. Atzori, A. Iera, and G. Morabito, *"The internet of things: A survey",* Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online].

Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[2] D. Bandyopadhyay and J. Sen, *"Internet of things: Applications and challenges in technology and standardization",* Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

[3] O. Vermesan and P. Friess, *"Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems",* River Publishers, 2013.

[4] O. Mazhelis, H. Warma, S. Leminen, P. Ahokangas, P. Pussinen, M. Rajahonka, R. Siuruainen, H. Okkonen, A. Shveykovskiy, and J. Myllykoski, *"Internet-of-things market, value networks, and business models : State of the art report",* 2013.

[5] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffle,

"Vision and challenges for realising the internet of things," Cluster of

European Research Projects on the Internet of Things, European Commision, 2010.

[6] H. Suo, J. Wan, C. Zou, and J. Liu, *"Security in the tnternet of things: A review,"* in Computer Science and Electronics Engineering

(ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648– 651.

[7] G. Yang, J. Xu, W. Chen, Z.-H. Qi, and H.-Y. Wang, *"Security characteristic and technology in the internet of things,"* Nanjing Youdian

Daxue Xuebao(Ziran Kexue Ban)/ Journal of Nanjing University of Posts and Telecommunications(Natural Nanjing University of Posts and

Telecommunications), vol. 30, no. 4, 2010.

[8] A. de Saint-Exupery, *"Internet of things, strategic research roadmap,"* 2009.

[9] L. Tan and N. Wang, *"Future internet: The internet of things,"*

in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5. IEEE, 2010, pp. V5–376.

[10] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, *"Identity authentication and capability based access control (iacac) for the internet of things,"* Journal of Cyber Security and Mobility, vol. 1, no. 4, pp.

309–348, 2013.

[11] Q. Gou, L. Yan, Y. Liu and Y. Li, *"Construction and Strategies in IoT Security System,"* IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Aug 2023, 2013, 1129-1132.

[12] L. Li, *"Study on Security Architecture in the Internet of Things,"* International Conference on Measurement, Information and Control (MIC), 2012, vol. 1, May 18-20, pp. 374-377.

[13] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis, *"State-of-the-art in privacy preserving data mining,"* ACM Sigmod Record, vol. 33, no. 1, pp. 50–57, 2004.

[14] M. Langheinrich, *"Privacy by designprinciples of privacy-aware ubiq-uitous systems,"* in Ubicomp 2001: Ubiquitous Computing. Springer, 2001, pp. 273–291.

[15] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A.

Bouabdallah, *"A systemic approach for iot security,"* in Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE, 2013, pp. 351–355.

[16] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, *"Identity manage-ment framework towards internet of things (iot): Roadmap and key challenges,"* in Recent Trends in Network Security and Applications.

Springer, 2010, pp. 430–439.

[17] A. Josang, *"Conditional reasoning with subjective logic,"* Journal of Multiple-Valued Logic and Soft Computing, vol. 15, no. 1, pp. 5– 38, 2008.