HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thành Duy

ỨNG DỤNG BLOCKCHAIN TRONG BẢO MẬT IOT

LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI – NĂM 2020

Nguyễn Thành Duy

ỨNG DỤNG BLOCKCHAIN TRONG BẢO MẬT IOT

Chuyên ngành : KỸ THUẬT VIỄN THÔNG
Mã số : 8.52.02.08

LUẬN VĂN THẠC SĨ KỸ THUẬT

Người hướng dẫn khoa học: TS.VŨ THỊ THÚY HÀ

HÀ NỘI – NĂM 2020

LỜI CAM ĐOAN

Em xin cam đoan đề tài: *"Ứng dụng Blockchain trong bảo mật IoT"* là một công trình nghiên cứu độc lập dưới sự hướng dẫn của TS. Vũ Thị Thúy Hà. Ngoài ra không có bất cứ sự sao chép của người khác. Đề tài, nội dung luận văn là sản phẩm mà em đã nỗ lực nghiên cứu trong quá trình học tập tại trường và tìm hiểu qua các tài hiệu, trang web vv… Các số liệu, kết quả trình bày trong báo cáo là hoàn toàn trung thực, em xin chịu hoàn toàn trách nhiệm về luận văn của riêng em.

Hà Nội, ngày 15 tháng 05 năm 2020

Người cam đoan

Nguyễn Thành Duy

LỜI CẢM ƠN

Lời đầu tiên cho em xin được gửi lời cảm ơn sâu sắc tới toàn thể thầy cô trong Học viện Công nghệ Bưu chính Viễn thông và đặc biệt là các thầy cô Khoa Sau Đại Học đã tận tình truyền đạt kiến thức trong suốt hơn hai năm em học tập tại trường. Với vốn kiến thức được tiếp thu trong quá trình học không chỉ là nền tảng cho quá tình nghiên cứu luận án mà còn là hành trang quý báu để em bước vào đời một cách vững vàng và tự tin.

Em xin trân trọng lời cảm ơn tới cô TS. Vũ Thị Thúy Hà đã trực tiếp hướng dẫn và giúp đỡ em trong suốt quá trình làm luận án tốt nghiệp. Dù bận rộn trong công việc giảng dạy ở trường nhưng cô vẫn luôn dành thời gian trả lời những thắc mắc của em và chỉ ra những thiết sót để em hoàn thành luận án này một cách tốt nhất.Em xin gửi lời cảm ơn sâu sắc nhất đến bố mẹ, gia đình và những người bạn bè luôn bên cạnh ủng hộ, tạo điều kiện cho em làm tốt nhiệm vụ của mình. Dù em đã cố gắng hết sức trong quá trình nghiên cứu, tìm hiểu "Ứng dụng Blockchain trong bảo mật IoT" luận văn này của em khó có thể tránh khỏi những thiếu sót. Em rất mong nhận được sự đóng góp của Thầy Cô để luận án của em hoàn thiện hơn.

Cuối cùng em xin kính chúc Thầy Cô dồi dào sức khỏe và thành công trong sự nghiệp cao quý.

Trân trọng!

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

Viết Tắt	Tiếng Anh	Tiếng Việt
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks	Sử dụng giao thức IPv6 cho các mạng LAN không dây công suất thấp
AC	Access Control	Máy chủ kiểm soát truy cập
AMQP	Advance Message Queuing Protocol	Giao thức hàng đợi tin nhắn tiên tiến
API	Application Programming Interface	Giao diện lập trình ứng dụng
CA	Certificate Authority	Cơ quan cấp chứng chỉ
CoAP	Constrained Application Protocol	Giao thức ứng dụng ràng buộc
DoS	Denial of Service	Tấn công từ chối dịch vụ
DTLS	Datagram Transport Layer Security	Bảo mật lớp vận chuyển gói dữ liệu
EDI	Electronic Data Interchange	Trao đổi dữ liệu điện tử
GPRS	General Packet Radio Service	Dịch vụ vô tuyến gói tổng hợp
GPS	Global Positioning System	Hệ thống định vị toàn cầu
GSM	Global System for Mobile Communication	Hệ thống định vị di động toàn cầu
HMAC	Hash-based Message Authencation Code	Mã nhận thực bản tin dựa trên hàm băm
IoT	Internet of Things	Internet vạn vật

IPv6	Internet Protocol Version 6	Thế hệ địa chỉ Internet phiên bản mới
LAN	Local Area Network	Mạng máy tính cục bộ
M2M	Machine to Machine	Truyền thông từ máy đến máy
MAC	Message Authencation Code	Mã xác thực bản tin
MEMS	Microelectromechanical System	Hệ thống cơ điện tử
MITM	Man-In-The-Middle Attack	Tấn công xen giữa
MQTT	Message Queuing Telemetry Transport	Tin nhắn hàng đợi truyền tải từ xa
QoS	Quality of Service	Chất lượng dịch vụ
RFID	Radio Frequency Identification	Nhận dạng bằng tần số vô tuyến
RPL	Routing Protocol for Low Power and Lossy Network	Giao thức định tuyến cho mạng tổn hao năng lượng thấp
SoA	Service Oriented Architecture	Kiến trúc hướng dịch vụ
TLS	Transport Layer Security	Bảo mật tầng giao vận
TPM	Trusted Platform Module	Mô-đun nền tảng đáng tin cậy
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng
WiFi	Wireless Fidelity	Hệ thống truy cập Internet không dây
WiMax	Worldwide Interoperability for Microwave Access	Hệ thống truy cập không dây băng rộng theo tiêu chuẩn IEE 802.16
WSN	Wireless sensor network	Mạng cảm biến không dây
XMPP	Extensible Messaging and Presence Protocol	Giao thức hiện diện và nhắn tin mở rộng

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

1. Lý do chọn đề tài

Kỷ nguyên IoT (Internet of Things) đang bùng nổ mạnh mẽ. Trên thế giới hiện có 18 tỷ thiết bị kết nối và dự báo đến năm 2030 sẽ có trên 40 tỷ thiết bị kết nối. Song hành cùng sự bùng nổ của IoT là xu thế phát triển như vũ bão của y tế thông minh, tòa nhà thông minh, giao thông thông minh… tại nhiều Quốc gia trên thế giới và tại Việt Nam. Các thiết bị IoT thường có thể can thiệp trực tiếp vào hoạt động, môi trường sống của con, vì vậy trong trường hợp bị tin tặc tấn công, kiểm soát và cài đặt các phần mềm độc hại, thì các thiết bị IoT có thể trở thành công cụ để tin tặc can thiệp, tấn công trực tiếp có chủ đích vào con người. Ngoài ra các công nghệ mới sử dụng trong các thiết bị IoT thường phát triển nhanh hơn khả năng kiểm soát về bảo mật hiện nay.

Công nghệ Blockchain (BC) là một công nghệ mới, có thể hiểu BC là các khối dữ liệu được liên kết với nhau. Những khối dữ liệu (block) này được ghi và xác nhận bởi mỗi chủ thể tham gia vào blockchain. Vì thế, càng có nhiều đối tượng tham gia, thì hệ thống blockchain càng mạnh, tính bảo mật càng cao.

Nền tảng an ninh mạng dựa trên BC có thể bảo mật các thiết bị kết nối bằng cách sử dụng chữ ký điện tử để nhận diện và xác thực các thiết bị này. Sau đó các thiết bị sẽ đóng vai trò là những đối tượng tham gia được ủy quyền trong mạng blockchain. Mỗi thiết bị được xác thực tham gia mạng IoT bảo mật dựa trên blockchain sẽ được coi là một thực thể tham gia, giống như trong mạng blockchain thông thường. Tất cả thông tin liên lạc giữa các thiết bị IoT sẽ được bảo mật bằng mật mã và lưu trữ trong nhật ký chống giả mạo. Mọi thiết bị mới được thêm vào mạng đều được đăng ký bằng cách gán ID kỹ thuật số duy nhất trên hệ thống Blockchain. Nền tảng này sẽ cung cấp các kênh bảo mật để liên lạc giữa các thiết bị và đồng thời tất cả các thiết bị kết nối sẽ có quyền truy cập an toàn vào hệ thống chủ hay cơ sở hạ tầng. Đây cũng chính là lý do em đã chọn luận văn của mình là "Ứng dụng Blockchain trong bảo mật IoT".

2. Tổng quan về vấn đề nghiên cứu

Luận văn tập trung nghiên cứu kiến trúc, mô hình kết nối, khảo sát các giải pháp bảo mật trong IoT, thách thức khi ứng dụng BC trong bảo mật IoT. Nghiên cứu xây dựng mô hình ứng dụng BC trong việc bảo mật thiết bị IoT trong gia đình.

Trong quá trình nghiên cứu, xây dựng đề cương về "Ứng dụng Blockchain trong bảo mật IoT", học viên đã tìm đọc và nghiên cứu một số các bài báo khoa học cùng hướng với Luân văn cụ thể như sau:

Nghiên cứu về tổng quan IoT, khảo sát một số mô hình bảo mật IoT, các kiểu tấn công vào thiết bị IoT [2]

Phân tích các ưu điểm cũng như thách thức của BC khi đưa vào ứng dụng bảo mật cho thiết bị IoT [3],[5],[6].

Nghiên cứu ứng dụng triển khai BC trong bảo mật IoT smart city [8], bảo mật IoT smarthome [4] .Tuy nhiên tất cả các công trình nghiên cứu vẫn chưa có được đánh giá toàn diện về các tham số hiệu năng cải thiện của ứng dụng BC vào bảo mật thiết bị IoT.

Mục đích của luận văn là tập trung làm rõ các nội dung chính như sau:

1. Nghiên cứu tổng quan về IoT và mô hình triển khai ứng dụng IoT
2. Nghiên cứu các mô hình bảo mật cho các thiết bị IoT, các kiểu tấn công vào thiết bị IoT smart home
3. Nghiên cứu bảo mật của BC và ứng dụng BC trong bảo mật các thiết bị IoT, phân tích rõ ưu điểm và những thách thức khi ứng dụng BC.
4. Xây dựng mô hình kiến trúc bảo mật ứng dụng BC cho các thiết bị IoT smart home

3. Mục đích nghiên cứu

Mục đích chính của luận văn nhằm xây dựng giải pháp bảo mật cho các thiết bị IoT trong gia đình (SmartHome) ứng dụng BC. Giải pháp đề xuất nhằm đáp ứng các yêu cầu như sau:

Đề xuất kiến trúc IoT smart home bao gồm 4 lớp: Lớp smart home, Lớp mạng BC, Lớp cloud computing và lớp dịch vụ.

Mô hình đề xuất ứng dụng BC phải có tính hiệu quả, khả năng mở rộng và tính sẵn sàng cao của dịch vụ, bảo vệ và chống lại tấn công DoS/DDoS vào IoT smart home .

Xây dựng thuật toán phân tích phát hiện và chống lại tấn công DoS/DDoS trong IoT smart home.

Đánh giá hiệu năng các tham số bảo mật của mô hình IoT smart home ứng dụng BC qua đó cho thấy ưu việt của mô hình đề xuất.

4. Đối tượng và phạm vị nghiên cứu

Đối tượng nghiên cứu của đề tài:

- Các giải pháp bảo mật cho thiết bị IoT,
- Kiến trúc hệ thống IoT,
- Các công cụ hỗ trợ bảo mật cho thiết bị IoT,

Phạm vi nghiên cứu của đề tài:

Nghiên cứu các kiểu tấn công và bảo mật cho thiết bị IoT trong gia đình.

Nghiên cứu các mô hình kết nối IoT trong gia đình và tiềm năng của BC khi ứng dụng vào bảo mật SmartHome

5. Phương pháp nghiên cứu

a. Phương pháp nghiên cứu lý thuyết

- Cơ sở lý thuyết về IoT,
- Cơ sở lý thuyết về các mô hình bảo mật cho IoT,
- Cơ sở lý thuyết bảo mật BC .

b. Phương pháp thực nghiệm

- Triển khai chính sách bảo mật BC cho thiết bị IoT trong gia đình
- Xây dựng mô hình kết nối và thử nghiệm tấn công DoS/DDoS trong IoT smarthome

Nội dung đồ án gồm 3 chương:

Chương I: Tổng quan về Internet of Things

Chương II: Bảo mật thiết bị IoT.

Chương III: Xây dựng mô hình bảo mật BC cho IoT Smart Home.

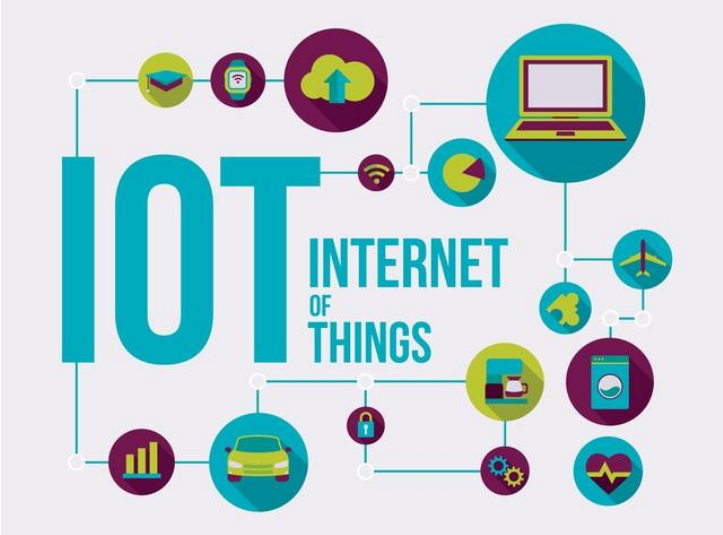
CHƯƠNG 1. NGHIÊN CỨU TỔNG QUAN VỀ INTERNET OF THINGS

1.1 Internet of things

Internet of Things (IoT) đề cập đến mạng lưới các đối tượng vật lý, nó đang phát triển nhanh và đã có hàng tỷ thiết bị được kết nối. Điều này khác với internet hiện tại, nó phần lớn là một mạng máy tính, bao gồm cả điện thoại và máy tính bảng. "Things" trong IoT có thể là bất cứ thứ gì, từ thiết bị gia dụng, máy móc, hàng hóa, tòa nhà và phương tiện cho đến con người, động vật và thực vật. Với IoT, tất cả các đối tượng vật lý được kết nối với nhau, có khả năng trao đổi dữ liệu với nhau mà không cần sự can thiệp của con người. Họ có thể được truy cập và kiểm soát từ xa. Điều này sẽ thay đổi hoàn toàn cuộc sống của chúng ta.

Khái niệm các thiết bị kết nối với nhau không phải là mới. Năm 1982, một máy Coke tại Đại học Carnegie Mellon đã trở thành thiết bị đầu tiên được kết nối với Internet. Nó có thể theo dõi hàng tồn kho và cho biết liệu đồ uống còn lạnh ko. Kể từ đó, tính kết nối đã được mở rộng đáng kể, trong các lĩnh vực điện toán có mặt khắp nơi, truyền thông từ máy đến máy (M2M) và liên lạc từ thiết bị đến thiết bị (D2D). Nhưng thuật ngữ IoT được đưa ra bởi doanh nhân người Anh - Kevin Ashton vào năm 1999, trong một bài thuyết trình mà ông đã thực hiện cho Procter & Gamble. Vào thời điểm đó, ông là người đồng sáng lập và giám độc điều hành của trung tâm Auto-ID tại MIT và tầm nhìn của IoT dựa trên nhận dạng bằng tần số vô tuyển RFID (radio-frequency identification). IoT đã phát triển kể từ đó và ngày càng trở nên phổ biến trong những năm gần đây, do sự hội tụ của một số công nghệ như vi điều khiển, cảm biến, truyền thông không dây, hệ thống nhúng và hệ thống cơ điện tử (MEMS).

Ngày này, IoT được xem như là công nghệ của tương lai, là tương lai của internet. Theo Internet Society, sẽ có khoảng 100 tỷ thiết bị IoT và thị trường toàn cầu hơn 11 nghìn tỷ đô la vào năm 2025. IoT sẽ phát triển theo cấp số nhân giống như những gì Internet đã làm cách đây khoảng hai thập kỷ [1-9-10].



Hình 1.1: Tổng quan về IoT

1.2 Các yêu cầu truyền thông IoT

Có một số bước để làm cho Internet vạn vật (IoT) hoạt động:

Đầu tiên, mỗi phần tử trong mạng phải có một định danh duy nhất. Nhờ địa chỉ IPv6 (Internet Protocol Version 6), địa chỉ IP thế hệ tiếp theo với chiều dài 128 bit sẽ cung cấp một lượng địa chỉ khổng lồ cho hoạt động Internet. Chúng ta có thể chỉ định một ID duy nhất cho một đối tượng vật lý trên hành tinh.

Thứ hai, mỗi đối tượng trong IoT đều phải có khả năng giao tiếp. Có một số công nghệ không dây hiện đại giúp truyền thông có thể thực hiện được, chẳng hạn như WiFi, Bluetooth năng lượng thấp, NFC, RFID, cũng như ZigBee, Z-Wave và 6LoWPAN (sử dụng giao thức IPv6 trong các mạng PAN không dây công suất thấp).

Thứ ba, mỗi đối tượng trong IoT cần phải có cảm biến để chúng ta có thể lấy thông tin về nó. Các cảm biến có thể là nhiệt độ, độ ẩm, ánh sáng, chuyển động, áp suất, hồng ngoại, cảm biến siêu âm, v.v… Các cảm biến mới đang ngày càng nhỏ hơn, rẻ hơn và bền hơn.

Thứ tư, mỗi đối tượng trong IoT cần có một bộ vi điều khiển (hoặc bộ vi xử lý) để quản lý các cảm biến và liên lạc, và để thực hiệc các tác vụ. Có nhiều bộ vi điều khiển có thể được sử dụng trong IoT, nhưng bộ vi điều khiển dựa trên ARM chắc chắn là một trong những bộ vi điều khiển có ảnh hưởng nhiều nhất.

Cuối cùng, chúng ta sẽ hệ thống máy tính sương mù (Fog Computing) để lưu trữ, phân tích và hiển thị dữ liệu để chúng ta có thể thấy những gì đang diễn ra và tương tác qua ứng dụng điện thoại.

1.3 Mô hình kiến trúc của IoT

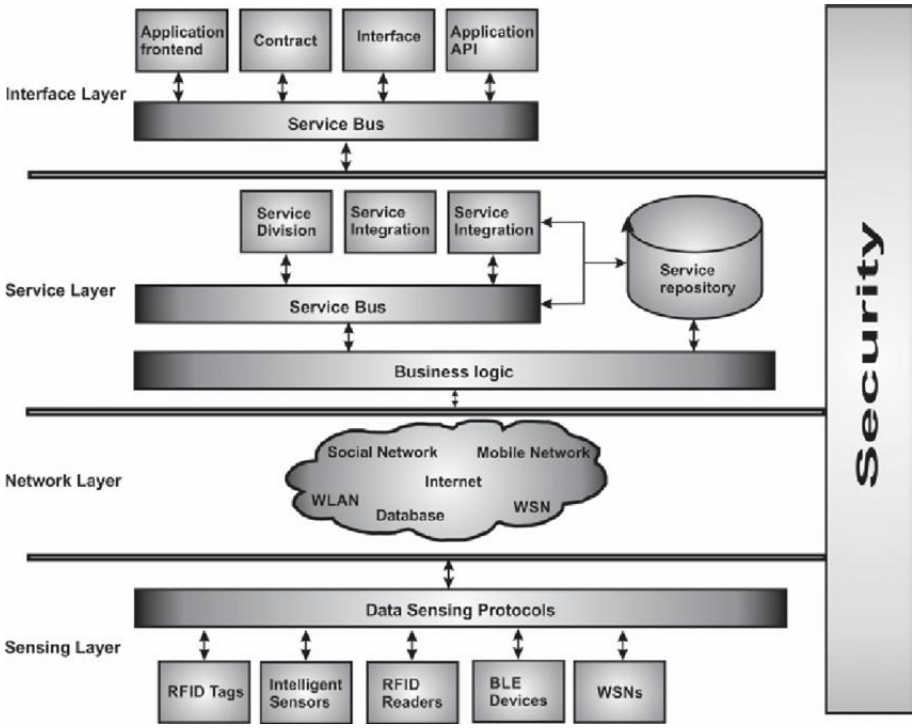
Kiến trúc hệ thống phải cung cấp đảm bảo hoạt động cho IoT, nó là cầu nối khoảng cách giữa các thiết bị vật lý và thế giới ảo. Khi thiết kế, kiến trúc IoT cần xem xét các yếu tố sau: (1) Các yếu tố kỹ thuật, như kỹ thuật cảm biến, phương thức truyền thông, công nghệ mạng, v.v.; (2) Đảm bảo an ninh, như bảo mật thông tin, bảo mật truyền dẫn, bảo vệ quyền riêng tư, v.v.; (3) Các vấn đề kinh doanh, chẳng hạn như mô hình kinh doanh, quy trình kinh doanh, v.v. … Hiện tại, SoA (Service Oriented Architecture - kiến trúc hướng dịch vụ) đã được áp dụng thành công cho thiết kế IoT, nơi các ứng dụng đang hướng tới các công nghệ tích hợp hướng dịch vụ. Trong lĩnh vực kinh doanh, các ứng dụng phức tạp giữa các dịch vụ đa dạng đã xuất hiện. Các dịch vụ nằm trong các lớp khác nhau của IoT như: lớp cảm biến, lớp mạng, lớp dịch vụ và lớp giao diện ứng dụng. Ứng dụng dựa trên dịch vụ sẽ phụ thuộc nhiều vào kiến trúc của IoT. Hình 1.2 dưới đây mô tả một mô hình kiến trúc cho IoT, bao gồm 4 lớp:

Lớp cảm biến được tích hợp với các thành phần cuối của IoT để cảm nhận và thu thập thông tin của các thiết bị.

Lớp mạng là cơ sở hạ tầng để hỗ trợ các kết nối không dây hoặc có dây giữa các đối tượng trong IoT.

Lớp dịch vụ cung cấp và quản lý các dịch vụ theo yêu cầu của người dùng hoặc ứng dụng.

Lớp ứng dụng – giao diện bao gồm các phương thức tương tác với người dùng hoặc ứng dụng.



Hình 1.2: SoA cho IoT

1.3.1 Lớp cảm biến

Đây là nguồn gốc thông tin và là lớp cốt lõi của IoT. Tất cả các loại thông tin của thế giới vật lý được sử dụng trong IoT đều được nhận biết và thu thập qua lớp này. Các cảm biến được sử dụng để xác định các đối tượng cũng như truyền tải dữ liệu được cung cấp tới lớp tiếp theo. Các thiết bị thu thập và tải dữ liệu lên lớp mạng trực tiếp hoặc gián tiếp. Dự kiến tất cả các thiết bị sẽ sử dụng IPv6 trong tương lai. Các công nghệ được sử dụng trong lớp này như mạng cảm biến không dây (WSN), các công nghệ cảm biến, các thẻ đọc và ghi dữ liệu, hệ thống RFID, camera, hệ thống định vị toàn cầu (GPS), thiết bị đầu cuối thông minh, trao đổi dữ liệu điện tử (EDI), v.v…Khi xây dựng lớp cảm biến cho IoT, các mối quan tâm chính như:

Chi phí, kích thước, tài nguyên và mức tiêu thụ năng lượng: Những đối tượng có thể được trang bị các thiết bị cảm biến như thẻ RFID, cảm biến, bộ truyền động, v.v., cần được thiết kế để giảm thiểu các nguồn tài nguyên cần thiết cũng như chi phí.

Triển khai: Các nút cuối của IoT (như đầu đọc RFID, thẻ, cảm biến, v.v.) có thể được triển khai một lần hoặc theo cách tăng dần hoặc ngẫu nhiên tùy theo yêu cầu của ứng dụng.

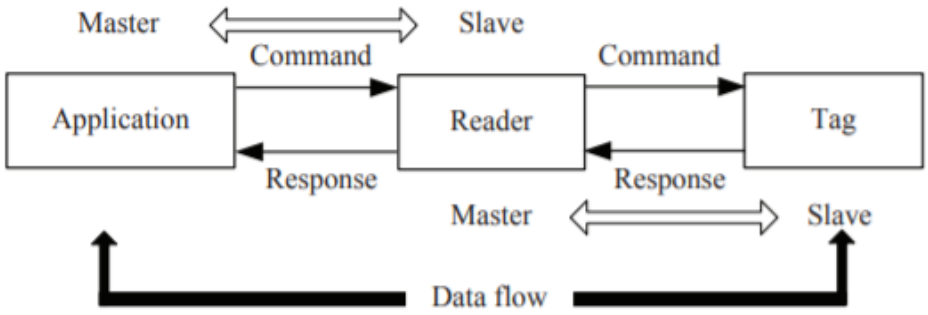
Tính bất đồng bộ: Một loạt các đối tượng hoặc mạng lai làm cho IoT rất không đồng nhất.

Giao tiếp: Các nút cuối IoT phải được thiết kế có khả năng giao tiếp với nhau.

Mạng: IoT liên quan đến các mạng lai, chẳng hạn như mạng cảm biến không dây, mạng lưới không dây và hệ thống kiểm soát và thu thập dữ liệu giám sát.

1.3.1.1 Hệ thống nhận dạng qua tần số vô tuyến (RFID)

Các hệ thống RFID bao gồm 3 thành phần chính: thẻ RFID, đầu đọc, thệ thống ứng dụng.



Hình 1.3: Hệ thống nhận dạng vô tuyến (RFID)

Thẻ RFID: còn được gọi là bộ tiếp sóng được gắn vào các đối tượng để đếm hoặc nhận dạng. Các thẻ có thể là chủ động hoặc thụ động. Thẻ chủ động là những thẻ có năng lượng pin một phần hoặc đầy, có khả năng giao tiếp với các thẻ khác và có thể bắt đầu một phiên trao đổi của riêng chúng với trình đọc thẻ. Mặt khác, thẻ thụ động không cần bất kỳ nguồn năng lượng nào mà được cung cấp bởi trình đọc thẻ. Thẻ bao gồm chủ yếu là ăng-ten cuộn và một vi mạch, mới mục đích chính là lưu trữ dữ liệu.

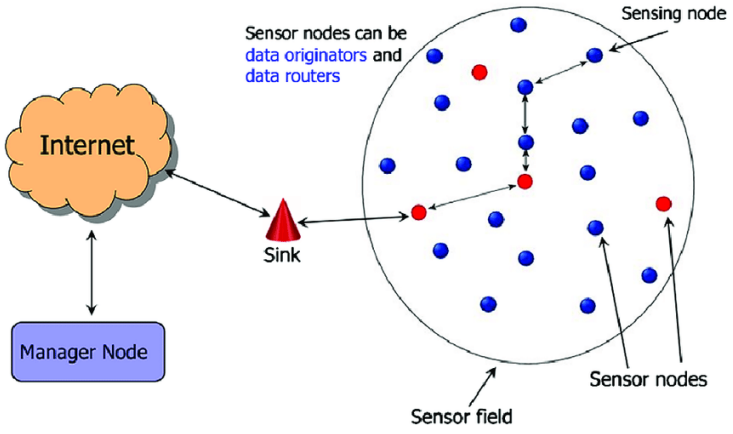
Đầu đọc: còn được gọi là bộ thu phát (máy phát/máy thu) được tạo thành từ mô-đun và bộ điều khiển giao diện tần số vô tuyến (RFI). Chức năng chính của nó

là kích hoạt các thẻ, cấu trúc chuỗi giao tiếp với thẻ và truyền dữ liệu giữa phần mềm ứng dụng và thẻ.

Hệ thống ứng dụng: Còn gọi là hệ thống xử lý dữ liệu, có thể là một ứng dụng hoặc cơ sở dữ liệu, tùy thuộc vào ứng dụng. Phần mềm ứng dụng khởi tạo tất cả các hoạt động đọc thẻ. RFID cung cấp một cách nhanh chóng, linh hoạt và đáng tin cậy để phát hiện, theo dõi và kiểm soát nhiều thiết bị điện tử. Các hệ thống RFID sử dụng truyền phát vô tuyến để gửi năng lượng đến thẻ RFID trong khi thẻ phát ra mã nhận dạng duy nhất trở lại đầu đọc thu thập dữ liệu được liên kết với hệ thống quản lý thông tin. Dữ liệu được thu thập từ thẻ sau đó có thể được gửi trực tiếp đến máy chủ hoặc được lưu trữ trong một trình đọc di động và được tải lên sau đó đến máy chủ.

1.3.1.2 Mạng cảm biến không dây (WSN)

Thông thường các mạng cảm biến không dây (WSN) bao gồm một nhóm các thiết bị cảm biến, nằm rải rác trong một khu vực nhất định thu thập và báo cáo dữ liệu cho một thiết bị thu phát trung tâm (sink), sau đó gửi dữ liệu đến kho lưu trữ dữ liệu để xử lý. Các thiết bị trung tâm này thường mạnh hơn các thiết bị cảm biến vì chúng được yêu cầu xử lý tất cả các thông tin đến, có thể thực hiện một số xử lý thông tin và gửi thông tin đến hệ thống bach-end. Ý tưởng này được mô tả như hình 1.4 dưới đây.



Hình 1.4: Mô hình mạng WSN đơn giản

Do các thiết bị cảm biến có phạm vi giao tiếp hạn chế, chúng có thể không phải lúc nào cũng có thể gửi/báo các thông tin trực tiếp đến sink. Do đó, các mạng

WSN thường chuyển tiếp thông tin qua các nút cảm biến khác cho đến khi đến được sink.

1.3.2 Lớp mạng

Lớp này còn được gọi là lớp giao vận, bao gồm mạng truy nhập và mạng lõi, cung cấp khả năng truyền dữ liệu thu được từ lớp dưới lên lớp trên. Lớp mạng truyền thông tin bằng các phương thức liên lạc liện có bao gồm mạng có dây và không dây như: mạng truy nhập vô tuyến, mạng cảm biến không dây (WSN) và các thiết bị liên lạc khác, hệ thống mạng GSM, GPRS, WiMax, WiFi, Ethernet, v.v. IoT yêu cầu khả năng mở rộng trong việc kết nối một số lượng lớn các thiết bị. Hơn một tỷ thiết bị sẽ được thêm vào hệ thống hàng năm. Vì lý do này, IPv6 sẽ đóng vai trò chính trong việc xử lý khả năng mở rộng lớp mạng.

1.3.2.1 Giao thức 6LoWPAN

6LoWPAN (IPv6 protocol over low-power wireless PANs) có nghĩa là sử dụng giao thức IPv6 trong các mạng PAN không dây công suất thấp được phát triển bởi IEFT cho phép truyền dữ liệu qua giao thức IPv6 và IPv4 trong các mạng không dây công suất thấp với các cấu trúc mạng điểm-điểm (P2P) và dạng lưới (mesh). 6LoWPAN cho phép các gói tin được nhận cũng như gửi qua các mạng dựa trên tiêu chuẩn IEEE 802.15.4. Ngoài ra, nó sử dụng các cơ chế đóng gói và nén tiêu đề để giảm tải cho kênh truyền (tối đa 127 bytes cho IEEE 802.15.4). Với IPv6 là sự kế thừa của IPv4 sẽ cung cấp khoảng 2128 địa chỉ cho tất cả mọi đối tượng trên thế giới, cho phép mỗi đối tượng có một địa chỉ IP duy nhất để kết nối với Internet. Tuy nhiên, giao thức này không đảm bảo an toàn dưới bất kỳ hình thức nào mà dựa vào các giao thức khác cho việc này, ví dự như giao thức IPsec và DTLS.

1.3.2.2 Giao thức RPL

RPL (Routing Protocol for Low Power and Lossy Network) là một giao thức được phát triển bởi IEFT để định tuyến trong môi trường IoT và sử dụng cơ chế vectơ khoảng cách để định tuyến qua môi trường IPv6. Giao thức này được phát triển cho các mạng tiêu thụ và tổn thất năng lượng thấp (LLNs). Các yếu tố cải tiến được sử dụng trong RPL bao gồm:

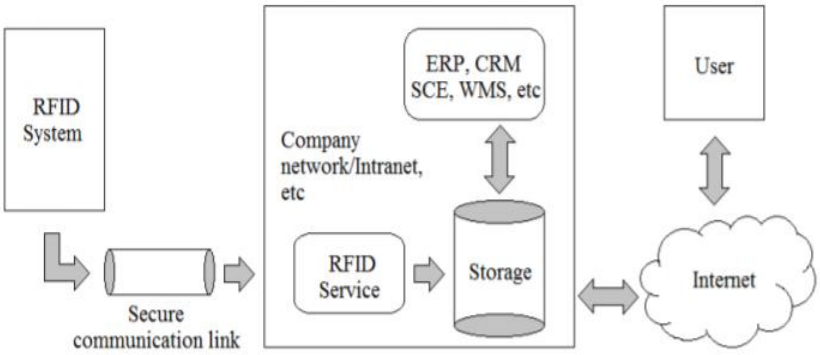
Sử dụng thuật toán "trickle" để quảng bá thông tin định tuyến. Nguyên lý cơ bản của thuật toán này là dựa vào trạng thái của mạng hiện tại và năng lực xử lý của các node để điều chỉnh tần suất gửi thông tin quảng bà phù hợp.

Phân tập theo không gian (spatial diversity): Việc truyền tin trong môi trường vô tuyến thường xuyên phải chịu các yếu tố gây nhiễu, suy hao, v.v… Việc bù tổn hao yêu cầu phải phát tín hiệu với công suất lớn. Khi đó, có node sẽ dễ rơi vào trạng thái mất kết nối khi giá trị năng lượng cung cấp chạm đến ngưỡng suy hao. Đặc điểm phân tập trong không gian cho phép mỗi node có một tập các nút mạng cha để sẵn sang thay thế lẫn nhau khi cần thiết.

Sử dụng giải pháp ước lượng số bước truyền ETX (Estimated number of Transmission) để tính toán thông số (metric) động. Metric động được sử dụng vì là đại lượng liên tục thay đổi giá trị tại mỗi thời điểm và phản ánh được trạng thái của mạng.

1.3.3 Lớp dịch vụ

Lớp dịch vụ bao gồm các chức năng xử lý dữ liệu thu thập được và cung cấp các liên kết đến bộ lưu trữ cho dữ liệu thu được từ lớp phần tử. Lớp này đóng vai trò là giao diện giữa các thiết bị khác nhau của IoT và cung cấp các phương thức giao tiếp giữa các thành phần. Ngoài ra, lớp dịch vụ trên cùng của lớp mạng cung cấp kết nối giữa các cảm biến và lớp ứng dụng. Hình dưới đây cho thấy dữ diệu đi qua lớp dịch vụ dưới dạng một lớp tích hợp.



Hình 1.5: Đường dẫn dữ liệu qua lớp dịch vụ

Điều quan trọng nhất là thiết kế một chiến lược bảo mật hiệu quả để bảo vệ các dịch vụ chống lại các cuộc tấn công trong lớp dịch vụ. Các yêu cầu bảo mật trọng lớp dịch vụ bao gồm:

Yêu cầu bảo mật tổng thể, bao gồm bảo mật, tính toàn vẹn, bảo vệ quyền riêng tư, xác thực, bảo vệ khóa, tính khả dụng, v.v.

Rò rỉ quyền riêng tư. Do một số thiết bị IoT được đặt ở những nơi không đáng tin cậy, điều này gây ra rủi ro tiền tang cho những kẻ tấn công tìm thấy thông tin riêng tư như nhận dạng người dụng, v.v.

Dịch vụ trái phép, trong IoT, cuộc tấn công lạm dụng dịch vụ bao gồm: (1) lạm dụng dịch vụ bất hợp pháp; (2) lạm dụng dịch vụ chưa đăng ký.

Nút xác thực giả danh

Tấn công DoS

Tấn công phát lại, kẻ tấn công gửi lại dữ liệu

Từ chối trong lớp dịch vụ bao gồm từ chối truyền thông và từ chối dịch vụ

1.3.4 Lớp ứng dụng

Lớp ứng dụng – lớp tương tác với người dùng cuối – bao gồm các ứng dụng. Lớp ứng dụng chịu trách nhiệm cung cấp dịch vụ và xác định một bộ các giao thức cho thông tin truyền ở lớp này. Mỗi ứng dụng sử dụng các giao thức lớp ứng dụng riêng. Lớp ứng dụng sử dụng một loạt các giao thức khác nhau như: CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advance Message Queuing Protocol).

1.3.3.1 Giao thức ứng dụng ràng buộc CoAP

CoAP là một giao thức truyền tải dữ liệu theo mô hình client/server dựa trên internet tương tự như giao thức HTTP nhưng được thiết kế cho các thiết bị ràng buộc. Giao thức này được sử dụng trong môi trường bị hạn chế như: các nút bị hạn chế về RAM, ROM hoặc CPU; mạng bị hạn chế chẳng hạn mạng sử dụng năng lượng thấp như mạng cá nhân không dây (WPAN). Môi trường hạn chế này dẫn đến việc mất các gói dữ liệu trong khi truyền. CoAP được phát triển bởi IEFT, chủ yếu được ứng dụng trong mô hình machine-to-machine (M2M) và tự động hóa các hệ

thống để giảm tỉ lệ mất gói, tăng hiệu quả cho việc truyền dữ liệu. Tính năng qua trọng nhất của CoAP là đơn giản và đáng tin cậy, vì nó hỗ trợ yêu cầu unicast và multicast bằng cách dử dụng UDP và cung cấp khả năng trao đổi tin nhắn không đồng bộ. UDP có thể dễ dàng triển khai trên các vi điều khiển hơn TCP nhưng các công cụ bảo mật như SSL/TSL không sẵn có, tuy nhiên có thể sử dụng DTLS để thay thế. CoAP là một giao thức đơn có 2 lớp, lớp đầu tiên là lớp bản tin và lớp thứ hai là lớp yêu cầu/phản hồi. Lớp bản tin nhằm tạo độ tin cậy dựa trên UDP, trong khi lớp yêu cầu/phản hồi nhằm thực hiện các tương tác và giao tiếp.

1.3.3.2 Tin nhắn hàng đợi truyền tải từ xa (MQTT)

MQTT là một giao thức lớp ứng dụng theo mô hình publisher/subcriber (xuất bản/theo dõi). Nó tương tự như như mô hình clinet-server. Tuy nhiên, tính đơn giản và mã nguồn mở của nó làm cho giao thức này chỉ phù hợp với các môi trường bị hạn chế, chẳng hạn như trong môi trường sử dụng công suất thấp, khả năng tính toán, bộ nhớ và băng thông hạn chế. Nó thích hợp cho các ứng dụng IoT và mô hình tương tác giữa máy với máy (M2M). Giao thức MQTT có thể chạy trên TCP/IP. MQTT được phát triển bởi IBM vào năm 2013, nó đã được chuẩn hóa bởi OASIS, nó nhằm mục đích giảm yêu cầu bang thông. Ngoài việc đảm bảo độ tin cậy của việc truyền tải gói, MQTT cung cấp một bộ các tính năng bao gồm: hỗ trợ truyền thông đa điểm và khả năng thiết lập liên lạc giữa các thiết bị từ xa. Ngoài ra, nó cung cấp một cơ chế thông báo khi xảy ra tình huống bất thường. MQTT cung cấp ba tùy chọn để đáp ứng chất lượng dịch vụ nhắn tin: gửi dữ liệu nhiều nhất một lần, gửi dữ liệu ít nhất một lần và gửi dữ liệu đảm bảo bên gửi chỉ nhận đúng một lần.

1.3.3.3 Giao thức hiện diện và nhắn tin mở rộng (XMPP)

Giao thức hiện diện và nhắn tin mở rộng (XMPP) là một trong những giao thức nhắn tin và liên lạc phổ biến nhất trọng IoT, nó đã được IEFT chuẩn hóa. Giao thức này là một giao thức nổi tiếng được sử dụng rộng rãi trong tất cả các mạng. Một số vấn đề hạn chế của IoT có thể được giải quyết bằng giao thức XMPP vì nó hỗ trợ các bản tin dung lượng nhỏ và độ trễ thấp. Những đặc điểm này làm cho giao thức XMPP trở thành một lựa chọn tốt cho truyền thông và nhắn tin IoT. Giao thức XMPP hỗ trợ các mô hình Request/Response (yêu cầu/phản hồi) cho phép truyền

thông hai chiều và mô hình Publish/Subcribe (xuất bản/đăng ký) cho phép truyền thông đa hướng. Khả năng mở rộng cao trong XMPP được cung cấp bởi kiếm trúc phi tập trung. Nhưng mặt khác, nó có một số điểm yếu. Vì giao thức này cần mức tiêu thụ băng thông cao và sử dụng CPU cao, không đảm bảo QoS và nó bị hạn chế ở kiểu dữ liệu đơn giản.

1.3.3.4 Giao thức hàng đợi tin nhắn tiên tiến (AMQP)

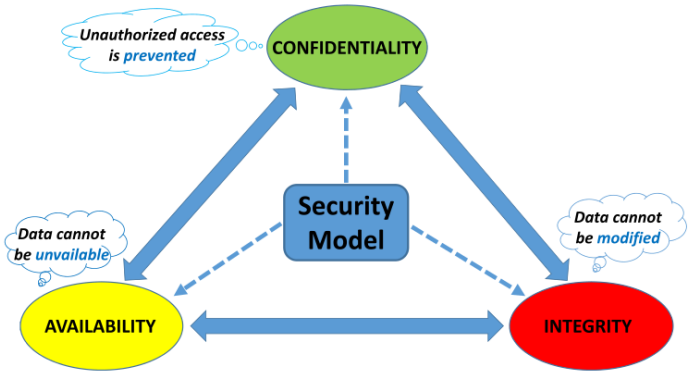
Giao thức hàng đợi và nhắn tin tiên tiến (AMQP) là một giao thức làm trung gian cho các gói tin trên lớp ứng dụng với mục đích thay thế các hệ thống truyền thông tin độc quyền và không tương thích. Các tính năng chính của AMQP là định hướng tin nhắn, hàng đợi, định tuyến. Các hoạt động sẽ được thực hiện thông qua broker, nó cung cấp khả năng điều khiển luồng (Flow Control). Nó được chuẩn hóa bởi OASIS. Ngày nay, AMQP được sử dụng rộng rãi trong các nền tảng kinh doanh và thương mại. Việc sử dụng mô hình publish/subscribe làm cho giao thức này có khả năng mở rộng cao. AMQP hỗ trợ truyền thông đặc tính bất đồng bộ và khả năng tương tác giữa các thiết bị khác nhau hỗ trợ các ngôn ngữ khác nhau. Giao thức AMQP tập trung vào việc thiết lập một tập các thông số kỹ thuật của tin nhắn để đạt được độ tin cậy, bảo mật và hiệu suất.

Giao thức AMQP được sử dụng trong môi trường IoT tập trung vào trao đổi thông tin và liên lạc. AMQP sử dụng các chế độ gửi tin nhắn khác nhau: nhiều nhất 1 lần, ít nhất 1 lần và chính xác 1 lần để đảm bảo độ tin cậy. Giao thức này cũng sử dụng TCP để đảm bảo độ tin cậy. Cách tiếp cận publish/subcribe của AMQP bao gồm hai thành phần: Hàng đợi trao đổi và hàng đợi tin nhắn. Hàng đợi trao đổi có trách nhiệm định tuyến tin nhắn theo thứ tự phù hợp trong hàng đợi. Hàng đợi tin nhắn lưu trữ tin nhắn cho đến khi chúng được gửi đến người nhận. Có một quy trình cụ thể với một bộ quy tắc để trao đổi giữa các thành phần trao đổi và hàng đợi tin nhắn.

1.4 Bảo mật trong IoT

An toàn thông tin trong IoT hướng tới hai khía cạnh của sự an toàn là ngăn chặn sự truy cập bất hợp pháp và thông tin bị rò rỉ dựa trên sự phân loại dựa trên thủ

tục và phạm vi để bảo vệ các thành phần của hệ thống và chính sách an toàn theo tam giác C.I.A



Hình 1.6: Yêu cầu bảo mật cho IoT

1.5 Kết luận chương I

Nội dung chương I phân tích một cách tổng quát về Internet of Things (IoT). Bao gồm định nghĩa về IoT, kiến trúc, mô hình truyền thông IoT, mô hình kết nối IoT, sơ lược các vấn đề bảo mật trong IoT. Qua phân tích cho thấy lỗ hổng bảo mật của các thiết bị IoT cũng như một số các vấn đề cần quan tâm như tính riêng tư, tiêu tốn năng lượng, mào đầu điều khiển, ….vv

CHƯƠNG 2: BẢO MẬT THIẾT BỊ IoT

2.1 Ứng dụng của IoT

2.1.1 Ứng dụng trong Smart Home

Nhà thông minh có lẽ là ứng dụng IoT phổ biến nhất. Bằng cách kết nối tất cả các thiết bị gia dụng, chúng ta có thể tự động hóa nhiều thói quen hàng ngày, chẳng hạn như tự động bật và tắt đèn, tự động sưởi ấm, bắt đầu hoặc ngừng bật bếp ga, v.v… Với lưới điện thông minh và đồng hồ điện thông minh, chúng ta có thể giảm mức sử dụng năng lượng và hóa đơn dịch vụ và với hệ thống an ninh, chúng ta có thể làm cho ngôi nhà an toàn hơn bằng cách tự động phát hiện và ngăn chặn xâm nhập bằng nhiều cảm biến hồng ngoại, chuyển động, âm thanh, rung cũng như hệ thống báo động. Nhà thông minh cũng có thể làm cho người già và người tàn tật thoải mái hơn khi ở nhà. Với IoT, chúng ta có thể thu thập và phân tích dữ liệu từ người già và người tàn tật để chẩn đoán bệnh, dự đoán rủi ro tiềm ẩn, xác định hoặc ngăn ngừa tai nạn như té ngã, mở khóa cửa hoặc cửa sổ từ xa để các thành viên trong gia đình giám sát từ xa. Với IoT, cũng có thể khiến người già và người tàn tật kết nối nhiều hơn với bên ngoài và giảm cảm giác cô đơn. Thị trường nhà thông minh sự đoán sẽ có giá trị thị trường vào khoảng hơn 137 tỷ USD vào năm 2023 (theo Markets and Market, July 2017) [website 2].

Hình 2. 1:*Mô hình nhà thông minh*

2.1.2 Ứng dụng trong theo dõi sức khỏe

IoT cho phép hệ thống thông báo khẩn cấp và theo dõi sức khỏe từ xa. Một cách tiếp cận rất phổ biến là thông qua các thiệt bị công nghệ có thể đeo như vòng đeo tay thông minh, đồng hồ thông minh, v.v… Các thiết bị đeo này có thể thu thập một loạt các dữ liệu về sức khỏe như nhịp tim, nhiệt độ cơ thể và huyết áp, sau đó có thể được lưu trữ vào cơ sở dữ liệu để phân tích và chẩn đoán các chỉ số về sức khỏe cho người dùng. Người dùng có thể tương tác với thiết bị thông minh qua các ứng dụng trên điện thoại do nhà sản suất thiết bị cung cấp.

Hình 2. 2: Đồng hồ thông minh theo dõi sức khỏe Apple Watch2.1.3

2.1.3 Ứng dụng trong giao thông thông minh

IoT có thể cải thiện đáng kể các hệ thống giao thông. Với việc tất cả các xe được kết nối, việc lên kế hoạch cho hành trình sẽ dễ dàng hơn rất nhiều, tránh ùn tắc giao thông, tìm chỗ đỗ xe dễ dàng hơn và giảm tai nạn giao thông. Những chiếc xe không người lái chắc chắn sẽ có tác động rất lớn. Nhiều công ty, như Tesla, Google, Uber, Volvo, Volkswagen, Audi và General Motors đang tích cực phát triển và quảng bá chúng. Những chiếc xe không người lái có thể làm cho cuộc hành trình di chuyển thú vị hơn cà có thể an toàn hơn nhiều. Bằng cách kết nối tất cả các bảng thông tin và bảng quảng cáo tại các nhà gà và sân bay, nó giúp hành khách có được cập nhật thường xuyên và trong trường hợp xảy ra tai nạn để phát hiện nhanh các sự cố và giảm chi phí phát sinh. Bằng cách cải thiện khả năng quản lý đầu cuối, quản lý kho và quản lý tàu, IoT cũng sẽ có lợi cho ngành công nghiệp hậu cần.

Hình 2. 3*:* Giao thông thông minh

2.1.4 Ứng dụng trong quản lý năng lượng

Bằng cách tích hợp các cảm biến và bộ truyền động, IoT có khả năng giảm mức tiêu thụ năng lượng của tất cả các thiết bị tiêu thụ năng lượng. IoT cũng sẽ hiện đại hóa cơ sở hạ tầng ngành điện, để nâng cao hiệu quả và năng suất.

2.1.5 Ứng dụng trong hoạt động sản xuất

Ứng dụng của IoT trong thời kỳ công nghiệp 4.0, hay cuộc cách mạng công nghiệp lần thứ tư là rất lớn. Cuộc cách mạng công nghiệp đầu tiên diễn ra vào thế kỷ thứ mười tám, khi động cơ hơi nước được áp dụng chính trong sản xuất công nghiệp. Cuộc cách mạng công nghiệp lần thứ hai diễn ra vào cuối thế kỷ thứ mười chín. Đó là giai đoạn tăng trưởng của các ngành công nghiệp đã có từ trước và mở rộng các ngành mới như thép, dầu, điện và sử dụng điện để sản xuất hàng loạt. Cuộc cách mạng công nghiệp lần thứ ba, hay cuộc cách mạng kỹ thuật số, diễn ra vào cuối thể kỷ 20, khi công nghệ thông tin và tự động hóa được ứng dụng mạnh mẽ. Công nghiệp 4.0 xây dựng trên các hệ thống vật lý không gian mạng tích hợp chặt chẽ máy móc, phần mềm, cảm biến, Internet và người dùng với nhau. Nó sẽ tạo ra các nhà máy thông minh, trong đó máy móc có thể tự tối ưu hóa, tự cấu hình và thậm trí sử dụng trí tuệ nhân tạo để hoàn thành các nhiệm vụ phức tạp nhằm mang lại chi phí vượt trội, hiệu quả và chất lượng hàng hóa hoặc dịch vụ tốt hơn.

2.1.6 Ứng dụng trong việc bảo vệ môi trường

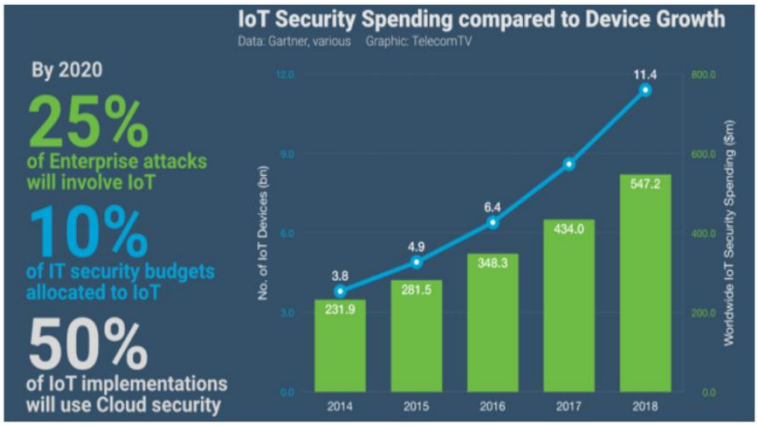
Bằng cách triển khai các cảm biến trong môi trường, chúng ta có thể đo lường và giám sát chất lượng không khí, chất lượng nước, điều kiện đất, bức xạ và hóa chất nguy hiểm hiệu quả hơn. Chúng ta có thể dự đoán động đất và sóng thần tốt hơn và phát hiện cháy rừng, tuyết lở, sạt lở đất nhanh hơn. Tất cả những điều này sẽ giúp con người bảo vệ môi trường tốt hơn. Bằng cách gắn thẻ động vật hoang dã, đặc biệt là các loài có nguy cơ tuyệt chủng, chúng ta có thể nghiên cứu và hiểu rõ hơn hành vi của động vật, và do đó cung cấp sự bảo vệ tốt hơn và môi trường sống an toàn hơn. IoT cũng cho phép canh tác thông minh, cung cấp khả năng hiển thị 24/7 về tình trạng của đất và cây trồng, từ đó giúp nông dân tối ưu hòa việc sử dụng phân bón và các sản phẩm bảo vệ thực vật. Điều này một lần nữa sẽ có tác động tích cực đến môi trường.

2.2 Các vấn đề bảo mật trong IoT

2.2.1 Sự gia tăng của các cuộc tấn công mạng

Với một đô thị chứa hàng triệu thiết bị kết nối với nhau, hacker có phạm vi tấn công rất lớn. Khi đó việc đảm bảo an toàn cho toàn bộ hệ thống là một thách thức lớn. Ngày nay, các cuộc tấn công mạng đang gia tăng và trở nên mạng mẽ hơn. Theo báo cáo mối đe dọa (Threat Report) CenturyLink 2018, Singapore đã phải tạm thời ngừng các sáng kiến quốc gia thông minh (Smart Nation) do vụ việc xâm phạm dữ liệu y tế của tổ chức y tế SingHealth. Nhiều công ty tại các Quốc gia là những nạn nhân của mã độc tống tiền (Ransomware). Một cuộc tấn công vào các hệ thống chăm sóc sức khỏe của Hồng Kông đã diễn ra trong khoảng thời gian hai tuần, trong khi WannaCry tấn công thành công nhà sản xuất chip theo hợp đồng lớn nhất Đài Loan. Việt Nam cũng không ngoại lệ, tính đến 16/5, khoảng 800 máy tính cá nhân và máy chủ tại Việt Nam bị lây nhiễm Ransomeware WannaCry, chủ yếu tập trung ở các tỉnh thành phố lớn. Ví dụ như ở Hà Nội có khoảng 400 máy bị tấn công, còn thành phố HCM là hơn 200 máy, chủ yếu là hệ thống server. Việt Nam nằm trong top 20 quốc gia, vùng lãnh thổ bị ảnh hưởng nhất, bên cạnh Ukraina, Ấn Độ, Trung Quốc, Đài Loan, v.v… IoT càng phát triển thì các mối đe dọa càng gia tăng theo.

Theo báo cáo của Telecom, xu hướng kết nối và triển khai IoT vượt xa bất kỳ hệ thống nối mạng nào khác. Gartner ước tính đến năm 2020. Sẽ có khoảng 50 tỷ thiết bị sẽ được kết nối với internet. Điều này đồng nghĩa với việc sẽ có 50 tỷ mục tiêu mới cho những kẻ tấn công với mục đích đánh sập các máy chủ quan trọng đối với một mạng internet đang hoạt động.



Hình 2. 4*:* Sự phát triển của IoT và vấn đề bảo mật

2.2.2 Sự thiếu đồng bộ về chính sách đảm bảo an ninh

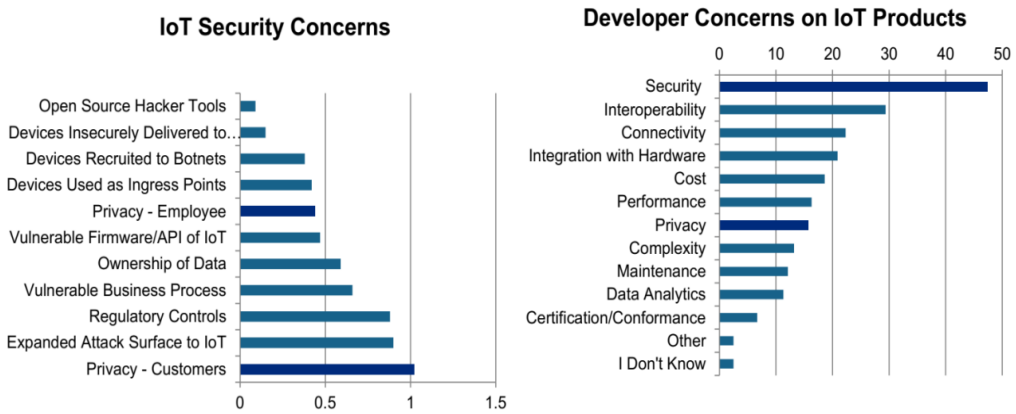
Trong khi các tổ chức khai thác lợi ích của việc có rất nhiều dữ liệu, thì chính điều này lại đặt ra nguy cơ mất an toàn thông tin lên cao hơn. Nhiều công ty đa quốc gia hoạt động và đặt trụ sở trải dài trên nhiều vùng địa lý khác nhau nên các hệ thống của họ sẽ phải tương tác trên nhiều khu vực địa lý khác nhau. Hơn nữa, chuyển đổi số đã thu hẹp khoảng cách giữa khách hàng, công ty và các mạng lưới của bên thứ ba, khiến việc theo dõi dữ liệu được lưu trữ, sử dụng trở thành một rào cản khó trong đảm bảo an ninh thông tin chia sẻ. Các công ty cũng ngày càng có xu hướng chuyển sang các nhà cung cấp dịch vụ bên thứ ba. Do đó, các công ty muốn sử dụng dịch vụ CNTT hoặc nhà cung cấp dịch vụ viễn thông để số hóa, điệu này có nghĩa là dữ liệu được trải rộng trên nhiều quốc gia, vùng lãnh thổ và phải tuân theo các quy định khác nhau của mỗi quốc gia khác nhau. Các quy định chính quan trọng hiện nay bao gồm: Luật bảo vệ dữ liệu chung của Châu Âu, đạo luật bảo vệ dữ liệu cá nhân và báo cáo kiểm toán các nhà cung cấp dịch vụ thuê ngoài của Singapo cũng như Pháp lệnh bảo mật dữ liệu cá nhân của Hồng Kông, v.v… Các quy định này điều tiết việc sử dụng dữ liệu mang tính cá nhân hoặc tài chính.

2.2.3 Thiếu hụt nhân lực an ninh mạng

Con người luôn là yếu tố cốt lõi trong sự phát triển của IoT, luôn phải có đội ngũ nghiên cứu, vận hành, nâng cấp, bảo trì và phát triển nó. Đến năm 2020, sự thiếu hụt tài năng trong lĩnh vực an ninh không gian mạng trên toàn cầu có thể lên tới 1,5 triệu nhân lực. Sự thiếu hụt các tài năng trong lĩnh vực này sẽ tạo nên những hậu quả nghiêm trọng cho các sang kiến số của khu vực. Ở ASEAN, 1.000 công y hàng đầu có thể mất đến 750 tỷ USD vốn hóa thị trường và mối quan tâm về an ninh mạng có thể ảnh hưởng đến sự chuyển đổi số của khu vực. Tại Việt Nam, theo sự báo đến năm 2020, nguồn nhân lực công nghệ thông tin có trình độ cao của Việt Nam có thể thiếu hụt hơn 1,2 triệu người.

2.2.4 Thách thức bảo mật đến từ các thiết bị IoT

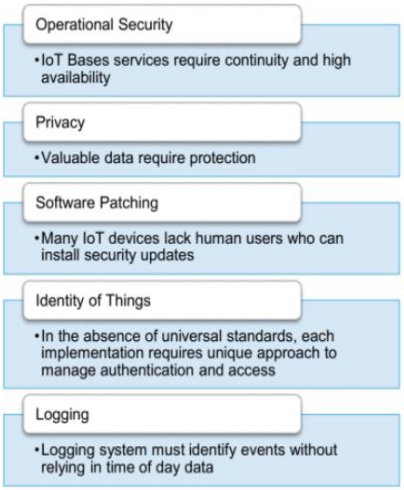
Đặc trưng của các thiết bị IoT là rất nhỏ, có nhiều thiết bị không có hệ điều hành đầy đủ nên rất khó khăn trong việc triển khai phần mềm diệt virus hay bảo mật. Với một số lượng thiết bị IoT khổng lồ, khi một thiết bị IoT gắn vào mạng lưới này thì rất khó nhận biết. Chính điều này khiến cho công tác kiểm soát hệ thống càng trở nên khó khăn. Hơn nữa, các thiết bị IoT thường sử dụng các giao thức mạng không dây phổ biến như WiFi và Bluetooth để kết nối. Mỗi giao thức này đều có các lỗ hổng riêng và dễ bị tấn công bằng cách sử dụng các công cụ như Wifite hoặc Aircracking Suite có thể khiến việc lưu trữ dữ liệu và bảo vệ quyền riêng tư rất khó.



Hình 2. 5: Các mối quan ngại bảo mật từ thiết bị IoT

Các lỗ hổng trên thiết bị IoT cũng có thể là lỗi từ nhà sản xuất. Ví dụ, bàn phím Swiftkey trong các thiết bị Android của Samsung đã được phát hiện rất dễ bị tấn công nghe lén. Hay hệ điều hành iOS của Apple cũng được phát hiện nhiều lỗ hổng, trong đó là "No iOS Zone" – lỗ hổng này cho phép kẻ tấn công làm treo các thiết bị iPhone, iPad và iPod Touch bằng sóng WiFi. Số lượng phần mềm độc hại tấn công vào các thiết bị IoT cũng lớn theo từng ngày, từng giờ với mức độ nguy hiểm ngày càng tăng. Năm 2017, loại mã độc CopyRAT đã tấn công hơn 14 triệu thiết bị Android trên toàn cầu và đã root thành công khoảng 8 triệu thiết bị di động. Đầu năm 2018, Trojan CrossRAT truy cập từ xa trên nhiều nền tảng, có thể tấn công 4 hệ điều hành phổ biến là Window, Solaris, Linux và macOS, cho phép kẻ tấn công điều khiển thiết bị từ xa như sử dụng hệ thống dữ liệu, chụp màn hình, chạy các tập tin thực thi tùy ý và chiếm quyền quản lý hệ thống. Với một mạng Internet kết nối trên diện rộng, một lỗ hổng bảo mật nào đó xuất hiện trên hệ thống đều có thể ảnh hưởng đến toàn bộ hệ thống an ninh của IoT.

Theo thống kê của Cục an toàn thông tin trên thị trường Việt Nam cũng như thể giới có nhiều thiệt bị trôi nổi không đảm bảo an toàn thông tin, các lỗ hổng bị khai thác, tấn công. Có tới 70% thiết bị IoT có nguy cơ bị tấn công mạng. Trong 316.00 camera giám sát được kết nối và công khai trên mạng Internet thì có hơn 147.000 thiết bị có lỗ hổng, chiếm 65%; Thiết bị Router ở Việt Nam có khoảng 28.000 địa chỉ bị tấn công bằng mã độc Mirai và các biến thể Mirai và là nguy cơ mất an toàn rất lớn. Một nghiên cứu của Bkav cho thấy có tới 76% camera IP tại Việt Nam vẫn dùng tài khoản và mật khẩu được nhà sản xuất cài đặt sẵn. Việc cập nhật bản vá cho lỗ hổng trên thiết bị IoT cũng khó khăn hơn việc cập nhật cho phần mềm, đòi hỏi sự can thiệp trực tiếp từ phía con người với kiến thức về an toàn mạng máy tính.



Rank	OWASP Top 10 for IoT
I1	Insecure Web Interface
I2	Insufficient Authentication/ Authorization
I3	Insecure Network Services
I4	Lack of Transport Encryption/ Integrity Verification
I5	Privacy Concerns
I6	Insecure Cloud Interface
I7	Insecure Mobile Interface
I8	Insufficient Security Configurability
I9	Insecure Software/Firmware
I10	Poor Physical Security

Source: OWASP IoT Project

Hình 2. 6: Các lỗ hổng bảo mật với các thiết bị IoT

2.3 Các yêu cầu bảo mật trong môi trường IoT

2.3.1 Yêu cầu bảo mật cho lớp cảm biến

Bảo mật là mối quan tâm hàng đầu trong lớp cảm biến. IoT có thể được kết nối với mạng công nghiệp để cung cấp cho người dùng các dịch vụ thông minh. Tuy nhiên, điều này có thể gây ra mối lo ngại mới trong việc kiểm soát các thiết bị, chẳng hạn như ai đó có thể xâm nhập thông tin xác thực hoặc quyết định xem ứng dụng có đáng tin cậy hay không. Mô hình bảo mật trong IoT phải có khả năng đưa ra phán quyết và quyết định của riêng mình về việc có nên chấp nhận lệnh hay thực thi một nhiệm vụ hay không. Ở lớp cảm biến, các thiết bị được thiết kế để tiêu thụ điện năng thấp với các tài nguyên hạn chế và thường có sự kết nối hạn chế. Sự đa dạng không ngừng của các ứng dụng IoT đặt ra một loạt các thách thức bảo mật như:

- Xác thực thiết bị
- Thiết bị đáng tin cậy
- Tận dụng các kiểm soát bảo mật và tính sẵn có của cơ sở hạ tầng trong lớp cảm biến
- Thuật toán mã hóa có vòng đời ngắn hơn so với các thiết bị IoT
- Bảo mật vật lý
- Kỹ thuật phát hiện giả mạo

Trong lớp này, các mối quan tâm bảo mật có thể được phân ra thành 2 loại chính

- Các yêu cầu bảo mật tại nút cuối IoT: bảo mật an ninh vật lý, kiểm soát truy nhập, xác thực, không từ chối, bảo mật, tính toàn vẹn, tính sẵn sàng và quyền riêng tư
- Các yêu cầu bảo mật trong lớp cảm biến: bảo mật, xác thực nguồn dữ liệu, xác thực thiết bị, tính toàn vẹn và tính sẵn có.

Bảng 2.1 tóm tắt các mối đe dọa bảo mật tiềm ẩn và các lỗ hổng bảo mật tại nút cuối IoT. Như đã đề cập ở trên, trong lớp này, hầu hết các thiết bị thường có kích thước nhỏ, rẻ tiền và tính bảo mật vật lý không cao. Các thiết bị này có thể không hỗ trợ các thuật toán bảo mật phức tạp và đang được phát triển do tài nguyên hạn chế. Tại các nút này, các phương thức bảo mật phải được thực hiện để đảm bảo tính xác thực của dữ liệu hoặc người dùng, kiểm soát truy cập của các thiết bị và các tham số xác thực kết nối giữa cấu hình ban đầu và trong suốt thời gian chạy trong môi trường IoT không thể bị tác động.

Bảng 2.1 Các mối đe dọa bảo mật tại nút cuối IoT

Mối đe dọa bảo mật	Mô tả
Truy nhập trái phép	Do bị tấn công vật lý hoặc tấn công logic, thông tin nhạy cảm ở các nút cuối bị kẻ tấn công thu được
Tính khả dụng	Nút cuối dừng hoạt động khi bị lấy cắp thông tin vật lý hoặc tấn công logic.
Tấn công giả mạo	Với nút chứa phần mềm độc hại, kẻ tấn công đã giả mạo thành công như một thiết bị đầu cuối IoT, nút cuối hoặc cổng cuối bằng cách làm sai lệch dữ liệu.
Mối đe dọa chủ quan	Một số nút cuối IoT ngừng hoạt động để tiết kiệm tài nguyên hoặc băng thông gây ra lỗi mạng.
Mã độc	Virus, Trojan và tin nhắn rác có thể gây ra lỗi phần mềm
Tấn công DoS	Một nỗ lực để làm cho tài nguyên nút cuối IoT không

	có sẵn cho người dùng nó
Các mối đe dọa truyền tài	Các mối đe dọa trong truyền tải, chẳng hạn như gián đoạn, chặn, điều khiển dữ liệu, giả mạo, v.v.
Tấn công định tuyến	Tấn công vào một đường dẫn định tuyến

Để bảo mật các thiết bị trong lớp này trước khi người dùng gặp rủi ro, cần thực hiện các yêu cầu sau:

- Thực thi các tiêu chuẩn bảo mật cho IoT và đảm bảo tất cả các thiết bị được sản xuất bằng cách đáp ứng các tiêu chuẩn bảo mật cụ thể
- Xây dựng hệ thống cảm biến dữ liệu đáng tin cậy và xem xét tính bảo mật của tất cả các thiết bị/thành phần.
- Xác định và theo dõi nguồn gốc của người dùng

2.3.2 Yêu cầu bảo mật cho lớp mạng

IoT kết nối nhiều mạng khác nhau, có thể gây ra nhiều khó khăn về các vấn đề mạng, vấn đề bảo mật và các vấn đề giao tiếp. Việc triển khai, quản lý và lập lịch cho các mạng là điều cần thiết cho lớp mạng trong IoT. Điều này cho phép các thiết bị thực hiện các nhiêm vụ công tác. Trong lớp mạng, cần giải quyết các vấn đề sau:

- Công nghệ quản lý mạng bao gồm quản lý mạng cố định, không dây, di động.
- Sử dụng tài nguyên mạng hiệu quả
- Yêu cầu QoS
- Công nghệ khai thác và tìm kiếm
- Bảo mật và quyền riêng tư
- Bảo mật thông tin

Trong số các vấn đề này, bảo mật thông tin và bảo mật quyền riêng tư của con người là rất quan trọng vì tính triển khai, tính di động và độ phức tạp của nó. Các công nghệ bảo mật hiện tại có thể cung cấp cơ sở cho bảo vệ quyền riêng tư và bảo mật trong IoT, nhưng vẫn còn nhiều vấn đề cần giải quyết. Các yêu cầu bảo mật trong lớp mạng liên quan đến:

- *Yêu cầu bảo mật tổng thể*, bao gồm bảo mật, tính toàn vẹn, bảo vệ quyền riêng tư, xác thực, tính khả dụng, v.v…

- *Rò rỉ quyền riêng tư*. Vì một số thiết bị IoT được đặt ở những nơi không đáng tin cậy, điều này gây ra rủi ro tiềm ẩn cho nhưng kẻ tấn công tìm thấy thông tin riêng tư như nhận dạng người dùng, v.v…
- *An ninh truyền thông*. Nó liên quan đến tính toàn vẹn và bảo mật của tín hiệu trong truyền thông IoT.
- *Quá tải kết nối*. IoT được kết nối một cách quá mức có thể có nguy cơ mất quyền kiểm soát của người dùng. Hai mối lo ngại về bảo mật là:
  - Tấn công DoS, băng thông được yêu cầu bằng cách xác thực tín hiệu có thể gây tắc nghẽn mạng
  - Bảo mật khóa, đối với mạng được kết nối quá mức, các thao tác khóa có thể gây ra tiêu thụ tài nguyên mạng lớn.
- *Tấn công MITM*, kẻ tấn công tạo ra các kết nối độc lập với các nạn nhân và chuyển tiếp tin nhắn giữa họ, khiến họ tin rằng họ đang nói chuyện trực tiếp với nhau qua một kết nối riêng tư, trong khi thực tế, kẻ tấn công kiểm soát toàn bộ cuộc trò chuyện
- *Tin nhắn mạng giả*, kẻ tấn công có thể tạo ra các tín hiệu giả để cách ly/xử lý sai các thiết bị khỏi IoT
- *Thỏa hiệp bí mật*, dữ liệu trọng mạng đang được chuyển tiếp và có thể bị kẻ tấn công thay đổi
- *Tấn công chuyển tiếp*, dự liệu hợp lệ có thể được truyền lại hoặc trì hoãn bởi kẻ tấn công để có quyền truy cập vào một kết nối đã được thiết lập bằng cách mạo danh danh tính của chính họ.

Bảng 2.2 Các mối đe dọa bảo mật trong lớp mạng

Các mối đe dọa bảo mật	**Mô tả**
Vi phạm dữ liệu	Phát hành thông tin bảo mật đến một môi trường không tin cậy
DoS	Một nỗ lực để làm cho tài nguyên nút cuối IoT không có sẵn cho người dùng của nó

Khóa công khai và khóa bí mật	Sự thỏa hiệp của các khóa trong mạng
Mã độc	Virus, Trojan và tin nhắn rác có thể gây lỗi phần mềm
Truyền tải không an toàn	Chẳng hạn như gián đoạn, chặn, điều khiển dữ liệu, giả mạo, v.v.
Tấn công định tuyến	Tấn công vào một đường dẫn định tuyến

Cơ sở hạ tầng mạng và các giao thức được phát triển cho IoT khác với mạng IP hiện có. Cần có những nỗ lực cần thiết cho các mối quan tâm bảo mật sau:

- Xác thực/Ủy quyền, liên quan đến các lỗ hổng như mật khẩu, kiểm soát truy cập, v.v.
- Mã hóa cho việc truyền tải an toàn, điều quan trọng là phải mã hóa đường truyền cho lớp này.

2.3.3 Yêu cầu bảo mật cho lớp dịch vụ

Các yêu cầu bảo mật trọng lớp dịch vụ bao gồm:

- Yêu cầu bảo mật tổng thể, bao gồm bảo mật, tính toàn vẹn, bảo vệ quyền riêng tư, xác thực, bảo vệ khóa, tính khả dụng, v.v.
- Rò rỉ quyền riêng tư. Do một số thiết bị IoT được đặt ở những nơi không đáng tin cậy, điều này gây ra rủi ro tiền tang cho những kẻ tấn công tìm thấy thông tin riêng tư như nhận dạng người dụng, v.v.
- Dịch vụ trái phép, trong IoT, cuộc tấn công lạm dụng dịch vụ bao gồm: (1) lạm dụng dịch vụ bất hợp pháp; (2) lạm dụng dịch vụ chưa đăng ký.
- Nút xác thực giả danh
- Tấn công DoS
- Tấn công phát lại, kẻ tấn công gửi lại dữ liệu
- Từ chối trong lớp dịch vụ bao gồm từ chối truyền thông và từ chối dịch vụ

Giải pháp bảo mật sẽ có thể bảo vệ các hoạt động trên lớp này khỏi các mối đe dọa tiềm ẩn. Bảo mật dữ liệu trong lớp dịch vụ là rất quan trọng và phức tạp. Nó liên quan đến phân mảnh, đầy đủ các tiêu chuẩn cạnh tranh và giải pháp độc quyền. SoA rất hữu ích để cải thiện tính bảo mật cho lớp này, nhưng vẫn phải đối mặt với những thách thức khi xây dựng một dịch vụ hoặc ứng dụng IoT: (1) bảo mật truyền dữ liệu giữa dịch vụ và các lớp; (2) quản lý dịch vụ an toàn, như nhận dạng dịch vụ, kiểm soát truy cập, dịch vụ tổng hợp, v.v.

Bảng 2.3 Các mối đe dọa bảo mật trong lớp dịch vụ

Các mối đe dọa bảo mật	**Mô tả**
Các mối đe dọa quyền riêng tư	Rò rỉ quyền riêng tư hoặc theo dõi vị trí bất hợp pháp
Dịch vụ trái phép	Người dùng trái phép truy cập dịch vụ hoặc người dùng được ủy quyền truy cập dịch vụ chưa đăng ký
Nhận dạng giả mạo	Thiết bị cuối, nút hoặc cổng IoT bị kẻ tấn công giả mạo
Điều khiển thông tin dịch vụ	Thong tin của các dịch vụ bị kẻ tấn công điều khiển
Từ chối	Từ chối các hoạt động đã được thực hiện
DoS	Một nỗ lực để làm cho nút cuối IoT không có sẵn cho người dùng
Tấn công phát lại	Cuộc tấn công gửi lại thông tin để giả danh người nhận
Tấn công định tuyến	Tấn công trên một đường dẫn định tuyến

2.3.4 Các yêu cầu bảo mật lớp ứng dụng – giao diện

Các yêu cầu bảo mật trong lớp ứng dụng – giao diện phụ thuộc rất nhiều vào các ứng dụng. Đối với việc bảo trì ứng dụng, các yêu cầu bảo mật sẽ bao gồm:

- Cấu hình an toàn từ xa, tái xuống và cập nhật phần mềm, bản vá bảo mật, xác thực quản trị viên, nền tảng bảo mật hợp nhất, v.v.
- Tính toàn vẹn và bảo mật để truyền giữa các lớp, xác thực và ủy quyền lớp chéo, cách ly thông tin nhạy cảm, v.v. Trong thiết kế IoT cho các giải pháp bảo mật, các quy tắc sau nên được thực hiện:
    - ✓ Do hầu hết các nút cuối IoT bị ràng buộc hoạt động theo cách không giám sát, người thiết kế nên chú ý nhiều hơn đến sự an toàn của các nút này
    - ✓ Do IoT liên quan đến hàng tỉ các nút phân cụm, các giải pháp bảo mật nên được thiết kế dựa trên các sơ đồ sử dụng năng lượng hiệu quả
    - ✓ Sơ đồ bảo mật tại các nút cuối IoT có thể khác với các giải pháp bảo mật mạng hiện có; tuy nhiên, chúng ta nên thiết kế các giải pháp bảo mật trong phạm vi đủ lớn cho tất cả các thành phần trong IoT.

Bảng 2.4 Các mối đe dọa bảo mật lớp ứng dụng – giao diện

Các mối đe dọa bảo mật	**Mô tả**
Cấu hình từ xa	Không thể cấu hình tại các giao diện
Cấu hình sai	Cấu hình sai ở nút cuối IoT từ xa, thiết bị cuối hoặc cổng cuối kết nối từ xa
Quản lý bảo mật	Thông tin đăng nhập và khóa bị rò rỉ
Hệ thống quản lý	Lỗi hệ thống quản lý

Lớp ứng dụng – giao diện kết nối hệ thống IoT với các ứng dụng người dùng, có thể đảm bảo rằng sự tương tác của các hệ thông IoT với các ứng dụng hoặc người dùng khác là hợp pháp và có thể tin cậy được.

2.4 Khảo sát một số giải pháp bảo mật trong môi trường IoT

2.4.1 Bảo mật dựa trên DTLS và xác thực hai chiều

TLS là giao thức được triển khai rộng rãi nhất để đảm bảo lưu lượng mạng. Nó được sử dụng rộng rãi để bảo vệ lưu lượng truy nhập Web và cho các giao thức email như IMAP và POP. Ưu điểm chính của TLS là nó cung cấp một kênh định hướng kết nốt trong suốt. Vì vậy, nó dễ dàng để bảo mật giao thức ứng dụng bằng cách chèn TLS giữa lớp ứng dụng và lớp vận chuyển. Tuy nhiên TLS phải chạy trên kênh truyền tải đáng tin cậy – thường là TCP. Do đó, nó không thể được sử dụng đẻ bảo mật lưu lượng datagram không đáng tin cậy.

Ngày càng có nhiều giao thức lớp ứng dụng được thiết kế sử dụng truyền tải UDP. Đặc biệt, các giao thức như giao thức khởi tạo phiên SIP và giao thức trò chơi điện tử trực tuyến ngày càng phổ biến. Hiện tại, các nhà thiết kế của các ứng dụng này phải đối mặt với một số lựa chọn không thích hợp. Đầu tiên, họ có thể sử dụng IPsec. Tuy nhiên, vì một số lý do IPsec chỉ phù hợp với một số ứng dụng. Thứ hai, họ có thể thiết kế một giao thức bảo mật lớp ứng dụng tùy biến. Thật không may, mặc dù các giao thức bảo mật lớp ứng dụng thường cung cấp các thuộc tính bảo mật ưu việt, chúng thường đòi hỏi một nỗ lực lớn để thiết kế - ngược lại sẽ dễ dàng hơn khi sử dụng giao thức TLS.

Trong nhiều trường hợp, cách nhanh nhất để bảo mật các ứng dụng máy khách/máy chủ là sử dụng TLS. Tuy nhiên, TLS có một số hạn chế. Bảo mật lớp vận chuyển dữ liệu (DTLS) được thiết kế có chủ ý giống với TLS nhất có thể, vừa giảm thiết kế phương pháp bảo mật mới vừa để vừa để tối đa hóa lượng mã và tái sử dụng cơ sở hạ tầng.

Vận chuyển datagram không yêu cầu dữ liệu đáng tin cậy hoặc theo thứ tự. Giao thức DTLS bảo tồn thuộc tính này cho dữ liệu tải trọng. Các ứng dụng như truyền phát phương tiện, điện thoại internet và chơi game trực tuyến sử dụng truyền tải datagram để truyền thông do tính chất nhạy cảm của dữ liệu được vận chuyển. Các tính chất của các ứng dụng như vậy không thay đổi khi giao thức DTLS được sử dụng để bảo mật truyền thông, vì giao thức DTLS không bù cho lượng dữ liệu đã mất hoặc truyền lại.

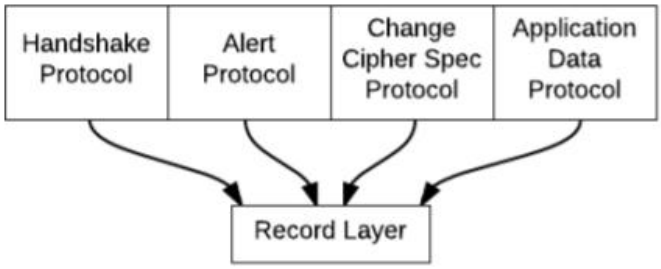
Lý do TLS không thể được sử dụng trong môi trường datagram chỉ đơn giản là các gói có thể bị mất hoặc sắp xếp lại. TLS không có khả năng xử lý loại không đáng tin cậy này; do đó, việc triển khai TLS gặp khó khăn.

Không đáng tin cậy tạo ra vấn đề cho TLS ở hai cấp độ:

- TLS không cho phép giải mã độc lập các bản ghi riêng lẻ. Bởi vì kiểm tra tính toàn vẹn phụ thuộc vào số thứ tự, nếu không nhận được bản ghi N, thì kiểm tra tính toàn vẹn trên bản ghi N+1 sẽ dựa trên số thứ tự sai và do đó sẽ bị lỗi.
- Lớp bắt tay TLS giả định rằng các tin nhắn bắt tay được gửi một cách đáng tin cậy và phá vỡ nếu những tin nhắn đó bị mất.

2.4.1.1 Cấu trúc của DTLS

DTLS bao gồm 4 giao thức con: bắt tay (Handshake), dữ liệu ứng dụng (Application Data), thông báo (Alert) và thay đổi thông số mật mã (Change Cipher Spec).

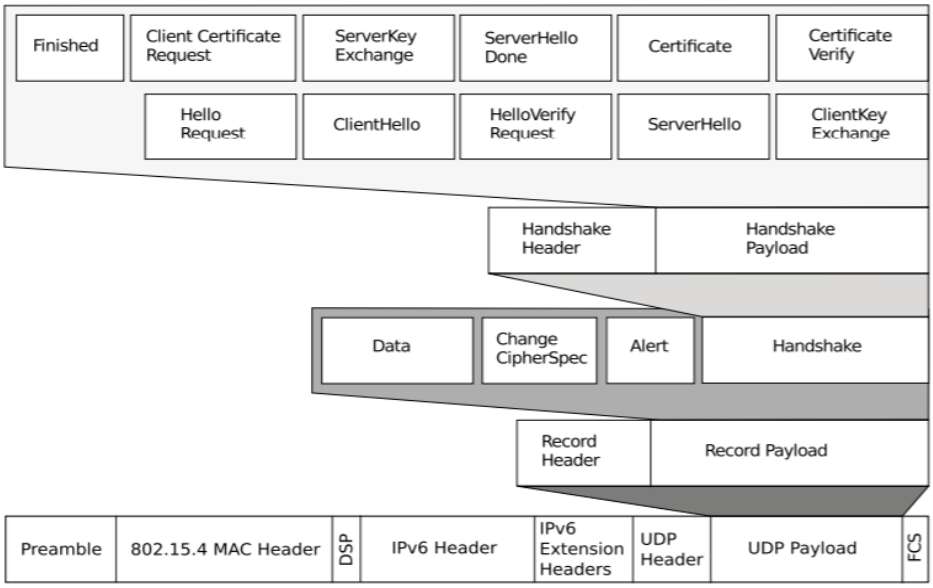


Hình 2. 7: Các giao thức con của DTLS

Lớp bản ghi là một phần của DTLS, phân đoạn, nén và mã hóa các bản tin, đính kèm chúng trong các bản ghi và chuyển chúng xuống dưới ngăn xếp truyền thông để truyền. Các giao thức bắt tay, thông báo, thay đổi mật mã và dữ liệu ứng dụng tạo ra các bản tin và chuyển chúng đến lớp bản ghi. Cấu trúc lớp bản ghi như trong Hình 2.8

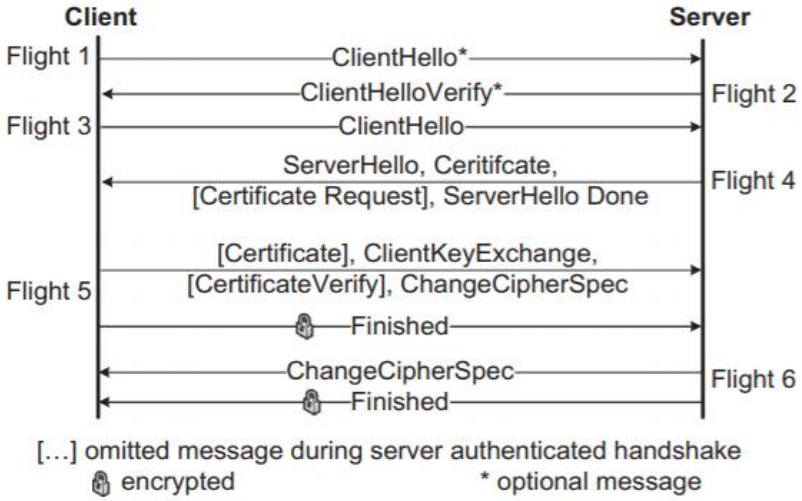
```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 epoch;
    uint48 sequence_number;
    uint16 length;
    opaque fragment[DTLSPlaintext.length];
} DTLSPlaintext;
```

Hình 2. 8*:* Cấu trúc lớp bản ghi DTLS



Hình 2. 9: Bố cục của gói được bảo mật bằng DTLS

2.4.1.2 Giao thức bắt tay DTLS



Hình 2. 10: Giao thức bắt tay DTLS được xác thực đầy đủ

Hình 2.10 cho thấy bắt tay DTLS được xác thực đầy đủ. Các tin nhắn riêng lẻ được nhóm lại thành "các chuyến bay tin nhắn" theo hướng và thứ tự xuất hiện của chúng. Chuyến bay 1 và 2 là một tính năng tùy chọn để bảo vệ máy chủ chống lại các cuộc tấn công từ chối dịch vụ (DoS). Máy khách phải chứng minh rằng nó có thể nhận dữ liệu cũng như gửi dữ liệu bằng cách gửi lại bản tin *ClientHello* của mình với cookie được gửi trong bản tin *ClientHelloVerify* của máy chủ. Bản tin *ClientHello* chứa phiên bản giao thức được hỗ tợ bởi máy khách cũng như các bộ mật mã mà nó hỗ trợ. Máy chủ trả lời với thông báo *ServerHello* chứa bộ mật mã được chọn từ danh sách do máy khách cung cấp. Máy chủ cũng gửi chứng chỉ X.509 để sác thực chính nó theo sau là bản tin *CertificateRequest* nếu máy chủ mong muốn máy khách xác thực. Bản tin *ServerHelloDone* chỉ cho biết kết thúc chuyến bay 4. Nếu được yêu cầu và hỗ trợ, máy khách sẽ gửi bản tin chứng chỉ của riêng mình vào đầu chuyến bay 5. Bản tin *ClientKeyExchange* chứa một nửa chuỗi byte ngẫu nhiên được mã hóa bằng khóa công khai RSA của máy chủ từ chứng chỉ máy chủ. Nửa còn lại của chuỗi byte ngẫu nhiên được truyền không được bảo vệ trong bản tin *ServerHello*. Các khóa sau đó được lấy từ chuỗi byte ngẫu nhiên này. Vì một nửa chuỗi byte ngẫu nhiên được mã hóa bằng khóa công khai của máy chủ, nó chỉ có thể hoàn thành bắt tay nếu nó sở hữu hóa riêng khớp với khóa công khai trong chứng chỉ máy chủ. Theo đó, trong bản tin *CertificateVerify*, máy khách tự xác thực bằng cách chứng minh rằng nó đang sở hữu khóa riêng khớp với khóa công khai của máy khách. Nó thực hiện điều này bằng cách ký một bản tóm tắt được băm của tất cả các bản tin bắt tay trước đó với khóa tiêng của nó. Máy chủ có thể xác minh điều này thông qua khóa công khai của máy khách. Bản tin *ChangeCodesSpec* chỉ ra rằng tất các các bản tin sau đó của khách hàng sẽ được mã hóa với bộ mật mã và bộ khóa đã được đàm phán. Bản tin *Finish* chứa bản tin mã hóa tất cả các bản tin bắt tay trước đó để đám bảo cả hai bên thực sự hoạt động dựa trên cùng một dữ liệu bắt tay. Máy chủ trả lời với thông báo *ChangeCiperSpec* và *Finish* của riêng mình để hoàn thành bắt tay.

2.4.1.3 Lớp bản ghi

Lớp bản ghi DTLS rất giống với TLS. Sự thay đổi duy nhất là nó có bao gồm Sequence number trong bản ghi. Sequence number cho phép bên nhận xác thực chính xác khung MAC TLS. Khuôn dạng bản ghi DTLS được mô tả như sau:

```
struct {
     ContentType type;
     ProtocolVersion version;
     uint16 epoch;                                    // New field
     uint48 sequence_number;                          // New field
     uint16 length;
     opaque fragment[DTLSPlaintext.length];
   } DTLSPlaintext;
```

*Hình 2. 11:*Cấu trúc lớp bản ghi DTLS

- Type: tương đương với kiểu thuộc tính trong TLS
- Version: phiên bản giao thức đang được sử dụng
- Epoch: một giá trị biến đếm tăng lên mỗi khi trạng thái mật mã được thay đổi
- Sequence number: sequence number của bản ghi này
- Fragment: giống với bản ghi TLS

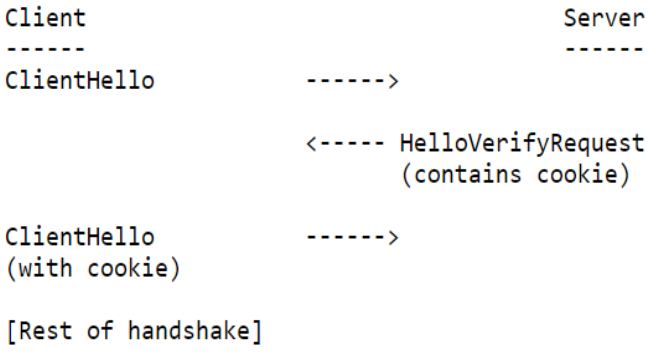
DTLS sử dụng sequence number tường minh thay vì ngầm đinh. Được gắn trong trường sequence numer của bản ghi. Sequence number được duy trì riêng cho từng epoch, với mỗi sequence number được khỏi tạo ban đầu bằng 0 cho mỗi epoch. Chẳng hạn, nếu một bản tin bắt tay từ epoch 0 được truyền lại, nó có sequence number ngay sau một bản tin từ epoch 1, ngay cả khi bản tin từ epoch 1 được truyền trước. Nếu một số bắt tay được thực hiện liên tiếp, có thể có nhiều bản ghi được truyền có cùng sequence number nhưng có các trạng thái mật mã khác nhau. Trường epoch cho phép người nhận phân biệt các gói như vậy. Số epoch ban đầu bằng 0 và được tăng lên mỗi khi bản tin ChangeCodesSpec được gửi. Để đảm bảo rằng bất kỳ cặp sequence-epoch là duy nhất, quá trình thực hiện không cho phép giá trị epoch giống nhau được sử dụng hai lần trong thời gian tồn tại của một phân đoạn.

2.4.1.4 Chống tấn công DoS

Các giao thức bảo mật datagram cực kỳ dễ bị tấn công DoS. Hai cuộc tấn công được đặc biệt quan tâm:

- Tấn công có thể tiêu thụ tài nguyên quá mức trên máy chủ bằng cách truyền một loạt các yêu cầu bắt tay, khiến máy chủ phân bổ trạng thái và có khả năng thực hiên các hoạt động mã hóa tốn kém.
- Kẻ tấn công có thể sử dụng máy chủ làm bộ khuếch đại bằng cách gửi bản tin khởi tạo kết nối với nguồn giả mạo của nạn nhân. Sau đó, máy chủ sẽ gửi bản tin tiếp theo (trong DTLS, bản tin chứng thực có thể khá lớn) đến máy nạn nhân, do đó làm quá tải nó.

Để chống lại cả hai cách tấn công này, DTLS mượn kỹ thuật cookie không trạng thái được sử dụng là Photuris và IKE. Khi máy khách gửi bản tin ClientHello của mình đến máy chủ, máy chủ có thể trả lời bằng tin nhắn HelloVerifyRequest. Bản tin này chứa cookie không trạng thái được tạo bằng kỹ thuật Photuris. Máy khách phải truyền lại ClientHello với cookie được thêm vào. Sau đó máy chủ sẽ xác minh cookie và chỉ tiến hành bắt tay nếu nó hợp lệ. Cơ chế này buộc kẻ tấn công/ máy chủ nhận cookie, điều này khiến cho các cuộc tấn công DoS với địa chỉ IP giả mạo trở nên khó khăn. Cơ chế này không cung cấp bất kỳ sự bảo vệ nào chống lại các cuộc tấn công DoS từ các địa chải IP hợp lệ.



Hình 2. 12: Trao đổi cookie giữa client và server

DTLS sẽ sửa đổi thông điệp ClientHello để thêm giá trị cookie

```
struct {
  ProtocolVersion client_version;
  Random random;
  SessionID session_id;
  opaque cookie<0..2^8-1>;                              // New field
  CipherSuite cipher_suites<2..2^16-1>;
        CompressionMethod compression_methods<1..2^8-1>;
} ClientHello;
```

Hình 2. 13: Cấu trúc bản tin ClientHello

Khi gửi ClientHello đầu tiên, máy khách chưa có cookie; trong trường hợp này, trường cookie được để trống.

```
struct {
  ProtocolVersion server_version;
  opaque cookie<0..2^8-1>;
} HelloVerifyRequest;

The HelloVerifyRequest message type is hello_verify_request(3).
```

Hình 2. 14: Cấu trúc của bản tin HelloVerifyRequest

Khi trả lời HelloVerifyRequest, máy khách phải sử dụng cùng các giá trị tham số (phiên bản, session_id, Codes_suites, compression_menthod) như trong ClientHello ban đầu. Máy chủ nên sử dụng các giá trị đó để tạo cookie của nó và xác minh rằng chúng là chính xác khi nhận cookie. Máy chủ phải sử dụng cùng số phiên bản trong HelloVerifyRequest mà nó sẽ sử dụng khi gửi ServerHello. Khi nhận được ServerHello, máy khách phải xác minh rằng các giá trị phiên bản máy chủ khớp với nhau. Để tránh sự trùng lặp số thứ tự trong trường hợp có nhiều HelloVerifyRequest, máy chủ phải sử dụng số thứ tự bản ghi trong ClientHello làm số thứ tự bản ghi trong HelloVerifyRequest.

Máy chủ DTLS nên tạo cookie theo cách mà chúng có thể được xác minh mà không giữ lại bất kỳ trạng thái trên mỗi máy khách nào trên máy chủ. Một kỹ thuật được sử dụng là tạo một giá trị bí mật và tạo cookie ngẫu nhiên như sau:

Cookie = HMAC (Secrect, Client-IP, Client-Paremeters)

Một cuộc tấn công có thể xảy ra là kẻ tấn công thu thập một số cookie từ các địa chỉ khác nhau và sau đó sử dụng lại chúng để tấn công máy chủ. Máy chủ có thể bảo vệ chống lại cuộc tấn công này bằng cách thay đổi giá trị bí mật thường xuyên,

do đó làm mất hiệu lực của các cookie đó. Nếu máy chủ muốn các máy khách hợp pháp có thể bắt tay trong quá trình chuyển đổi (ví dụ: họ đã nhận được cookie với gái trị bí mật 1 và sau đó gửi ClientHello thứ hai sau khi máy chủ đổi thành giá trị bí mật 2), máy chủ có thể có một cửa sổ giới hạn trong đó chấp nhận cả hai giá trị bí mật. IKEv2 đề nghị thêm số phiên bản vào cookie để phát hiện trường hợp này. Một cách tiếp cận khác chỉ đơn giản là thử xcas minh bằng cả hai giá tị bí mật.

Máy chủ DTLS nên thực hiện trao đổi cookie bất cứ khi nào bắt tay mới được thực hiện. Nếu máy chủ đang được vận hành trong môi trường mà sự khuếch đại không phải là vấn đề, thì máy chủ có thể được cấu hình để không thực hiện trao đổi cookie. Tuy nhiên, nên mặc định là việc trao đổi được thực hiện. Ngoài ra, máy chủ có thể chọn không thực hiện trao đổi cookie khi phiên được nối lại. Máy khách phải được chuẩn bị để thực hiện trao đổi cookie với mỗi phiên bắt tay.

2.4.1.5 Định dạng bản tin bắt tay

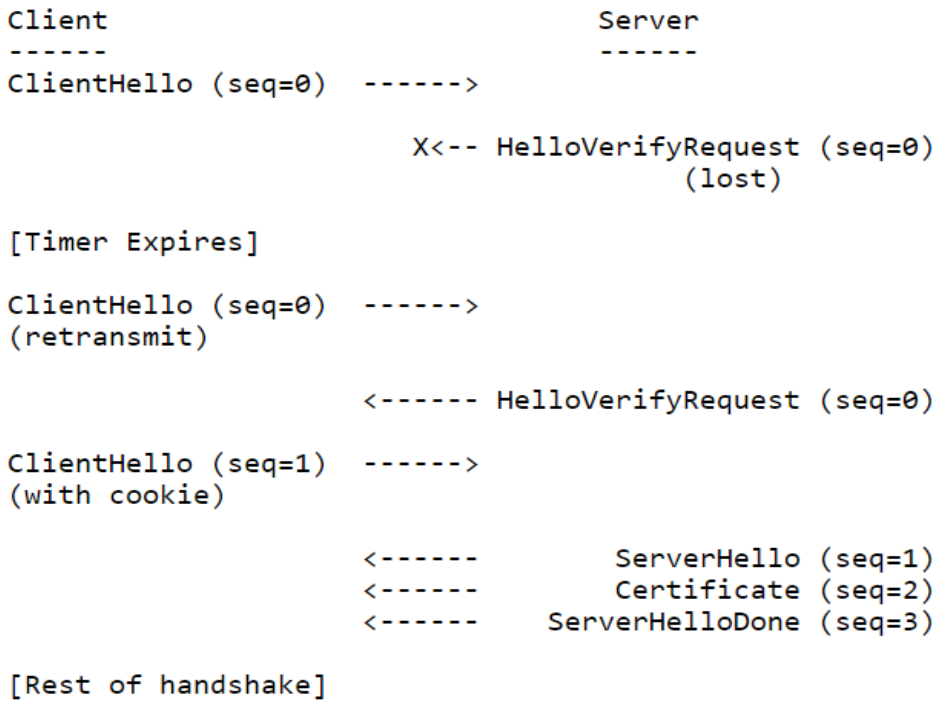
Để hỗ trợ mất bản tin, sắp xếp lại và phân mảnh bản tin, DTLS sửa đổi tiêu để bắt tay TLS v1.2.

```
struct {
  HandshakeType msg_type;
  uint24 length;
  uint16 message_seq;                                  // New field
  uint24 fragment_offset;                              // New field
  uint24 fragment_length;                              // New field
  select (HandshakeType) {
    case hello_request: HelloRequest;
    case client_hello:  ClientHello;
    case hello_verify_request: HelloVerifyRequest;     // New type
    case server_hello:  ServerHello;
    case certificate:Certificate;
    case server_key_exchange: ServerKeyExchange;
    case certificate_request: CertificateRequest;
    case server_hello_done:ServerHelloDone;
    case certificate_verify:  CertificateVerify;
    case client_key_exchange: ClientKeyExchange;
    case finished: Finished;
  } body;
} Handshake;
```

*Hình 2. 15:*Cấu trúc tiêu đề bắt tay

Thông điệp đầu tiên mà mỗi bên truyền trong mỗi lần bắt tay luôn có message_seq=0. Mỗi khi bản tin mới được tạo, giá tri message-seq được tăng thêm một. Lưu ý rằng trong trường hợp bắt tay lại, HelloRequest sẽ có message_seq = 0

và ServerHello sẽ có message_seq = 1. Khi một bản tin được truyền lại, cùng một giá tị message_seq được sử dụng. Ví dụ:



Hình 2. 16: Sử dụng SEQ trong bắt tay DTLS

Việc triển khai DTLS duy trì một bộ đếm next_receive_seq. Bộ đếm này ban đầu được đặt thành không. Khi nhận được tin nhắn, nếu số thứ tự của nó khớp với next_receive_seq, next_receive_seq sẽ tăng lên và tin nhắn được xử lý. Nếu số thứ tự nhỏ hơn next_receive_seq, bản tin phải bị loại bỏ. Nếu số thứ tự lớn hơn next_receive_seq, việc triển khai nên xếp hàng bản tin nhưng có thể loại bỏ nó.

2.4.1.6 Phân chia bản tin bắt tay và tái tạo

Mỗi bản tin DTLS phải vừa trong một datagram lớp vận chuyển duy nhất. Tuy nhiên, bản tin bắt tay có khả năng lớn hơn kích thước bản ghi tối đa. Do đó, DTLS cung cấp một cơ chế đê phân đoạn một bản tin bắt tay qua một số bản ghi, mỗi bản ghi có thể được truyền riêng, do đó tránh phân mảnh IP.

Khi gửi bản tin bắt tay, người gửi chia bản tin thành một chuỗi N phạm vi dữ liệu liên kề. Các phạm vi này phải không lớn hơn kích thước phân đoạn bắt tay tối đa và phải cùng chứa toàn bộ bản tin bắt tay. Các phạm vị không nên chồng chéo. Người gửi sau đó tạo N bản tin bắt tay, tất cả đều có cùng giá trị message_seq như

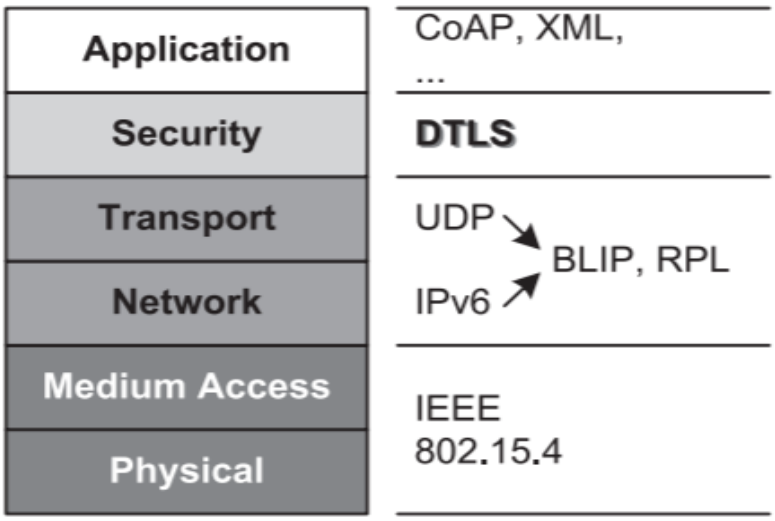
bản tin bắt tay ban đầu. Mỗi bản tin mới được gắn nhãn với Fragment_offet (số byte được chứa trong các fragment trước đó) và Fragment_length (độ dài của đoạn này). Trường độ dài trong tất cả các bản tin giống trường độ dài của bản tin gốc. Một bản tin không phân mảnh là một trường hợp đặc biệt với Fragment_offet = 0 và Fragment_length = length.

Như với TLS, nhiều tin nhắn bắt tay có thẻ được đặt trong cùng một bản ghi DTLS, miễn là có chỗ và chúng là một phần của cùng một chuyến bay. Do đó, có hai cách có thể chấp nhận để đóng gói hai thông điệp DTLS vào dùng một datagram: trong cùng một bản ghi hoặc trong các bản ghi riêng biệt

2.4.1.7 Kiến trúc bảo mật đầu cuối dựa trên tiêu chuẩn.

Tương tự như nhu cầu bảo mật trong mạng truyền thống như internet, chúng ta xem xét ba mục tiêu bảo mật:

- Tính xác thực: Người nhận bản tin có thể xác định đối tác liên lạc của hộ và có thể phát hiện nếu thông tin người gửi đã bị giả mạo
- Tính toàn vẹn: Đối tác truyền thông có thể phát hiện các thay đổi đối với bản tin trong khi truyền
- Bảo mật: Kẻ tấn công không thể có được thông tin về nội dung của bản tin được bảo mật



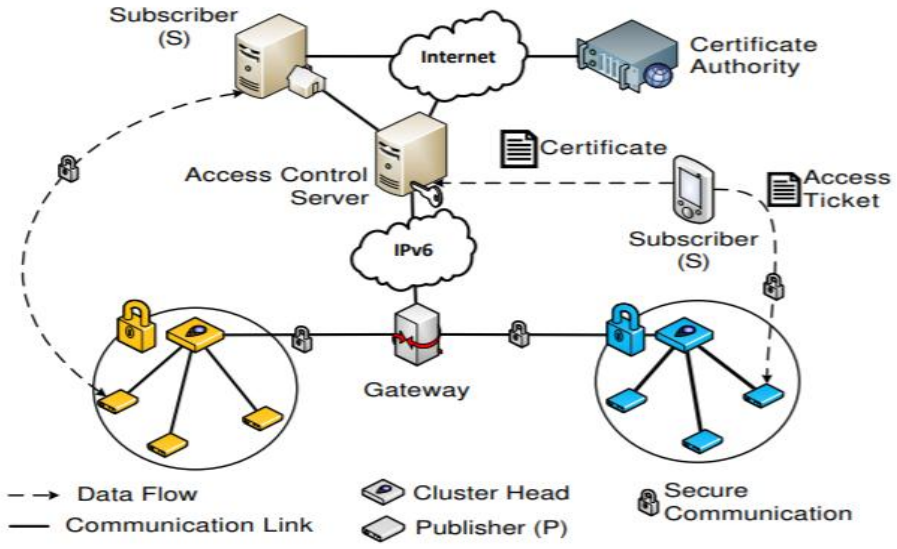
Hình 2. 17: Giao thức ngăn xếp được sử dụng trong kiến trúc bảo mật đề xuất

Bằng cách chọn DTLS làm giao thức bảo mật, chúng ta có thể đạt được các mục tiêu này. DTLS là một phiên bản sửa đổi của TLS cho UDP không đáng tin cậy và kế thừa các thuộc tính bảo mật của nó. Sử dụng giao thức bảo mật lớp ứng dụng như DTLS trái ngược với các giao thức bảo mật lớp mạng hay lớp liên kết như MiniSec có một số ưu điểm nhưng cũng có một số nhược điểm. Các giao thức bảo mật lớp thấp hơn không cung cấp bảo mật thông tin đầu cuối. Trên mỗi hop trong một mạng multi-hop, dữ liệu được giải mã khi nhận và mã hóa lại để chuyển tiếp. Do đó, kẻ tấn công có thể có quyền truy cập vào tất cả dữ liệu văn bản rõ rằng đi qua một nút bị xâm nhập. Khả năng mở rộng cũng thường là một vấn đề đối với các giao thức này vì chúng cần thiết lập kết nối bảo mật với mỗi hàng xóm của chúng để tạo thành một mạng lưới và chi phí mã hóa xảy ra trên mỗi bước nhảy. Mặt khác, trong một giao thức bảo mật đầu cuối, chỉ có phí mã hóa xảy ra đối với người gửi và người nhận. Các nút thỏa hiệp cung cấp cho kẻ tấn công quyền truy cập vào dữ liệu đo lường từ các nút cục bộ. Các thuật toán định tuyến cũng không rõ ràng về bảo vệ tải trọng, do đó, ngay cả các nút chưa thiết lập kết nốt an toàn cũng có thể được sử dụng để chuyển tiếp các gói đến một thuê bao/đích. Một kịch bản như vậy có thể là trong một tòa nhà văn phòng được chia sẻ bởi nhiều người (nhiều bên): mỗi bên chỉ đăng ký một phần của cảm biến và muốn giữ liệu họ đăng ký riêng tư từ các bên khác, nhưng họ vẫn có thể chia sẻ một liên lạc chung mạng để giảm chi phí.

Tuy nhiên, một giao thức bảo mật lớp ứng dụng không bảo vệ thông tin định tuyến. Do đó, đối thủ có thể phân tích các mẫu lưu lượng của một mạng bằng văn bản rõ ràng. Họ thậm chí có thể khởi chạy một DoS hoặc tấn công tiêu thụ tài nguyên làm giảm tính khả dụng của mạng.

Các tình huống như ở trên nêu lên nhu cầu xác thực hợp lệ các thiết bị xuất bản dữ liệu và kiểm soát truy cập trên toàn mạng. Do đó, chúng tôi giới thiệu máy chủ Kiểm soát truy cập (AC) vào kiến trúc của chúng tôi. AC là một thực thể đáng tin cậy và một máy chủ giàu tài nguyên hơn, trên đó các quyền truy cập cho các nhà xuất bản của mạng được bảo mật được lưu trữ. Danh tính của một thuê bao mặc định thường được cấu hình sẵn trên một nhà xuất bản trước khi nó được triển khai. Nếu bất kỳ thuê bao bổ sung nào muốn khởi tạo kết nối với nhà xuất bản, trước tiên

họ phải có được vé truy cập từ AC. AC xác minh rằng thuê bao có quyền truy cập thông tin có sẵn từ nhà xuất bản. Nhà xuất bản sau đó chỉ phải đánh giá danh tính của người đăng ký và xác minh vé mà họ đã nhận được từ AC. Điều này đòi hỏi một danh tính duy nhất cho một nhà xuất bản trong mạng. Trong Internet, các danh tính thường được thiết lập thông qua PKC và các danh tính được cung cấp thông qua các chứng chỉ X.509. Chứng chỉ X.509 chứa, trong số các thông tin khác, khóa công khai của một thực thể và tên chung của nó (ví dụ: mybank.com). Chứng chỉ được ký bởi một bên thứ ba đáng tin cậy, được gọi là Tổ chức chứng nhận (CA), phục vụ hai mục đích: Thứ nhất, chữ ký cho phép người nhận phát hiện các sửa đổi đối với chứng chỉ. Thứ hai, nó cũng nói rằng CA đã xác minh danh tính của thực thể yêu cầu chứng chỉ. Một CA có thể được điều hành bởi quản trị viên của mạng hoặc một trong những cơ quan chứng nhận Internet được thiết lập có thể được sử dụng. Thuật toán khóa công khai RSA được sử dụng phổ biến nhất trên Internet, có thể được sử dụng trong các mạng cảm biến với sự hỗ trợ của Mô-đun nền tảng đáng tin cậy (TPM). TPM là một con chip nhúng cung cấp khả năng tạo và lưu trữ bằng chứng giả mạo các khóa RSA cũng như hỗ trợ phần cứng cho thuật toán RSA. Chứng chỉ của nhà xuất bản được trang bị TPM và chứng chỉ của CA đáng tin cậy phải được lưu trữ trên nhà xuất bản trước khi triển khai. Đối với các nhà xuất bản không được trang bị chip TPM, chúng tôi đề xuất xác thực thông qua bộ mật mã khóa chia sẻ trước (PSK) DTLS, yêu cầu một số lượng nhỏ byte ngẫu nhiên, từ đó khóa thực tế được lấy, được tải trước cho nhà xuất bản trước khi triển khai. Bí mật này cũng phải được cung cấp cho máy chủ AC sẽ tiết lộ khóa cho các thiết bị có đủ quyền. Hình 2.18 cung cấp tổng quan về kiến trúc được đề xuất.



Hình 2. 18*:* Tổng quan kiến trúc hệ thống

Thiết lập truyền thông

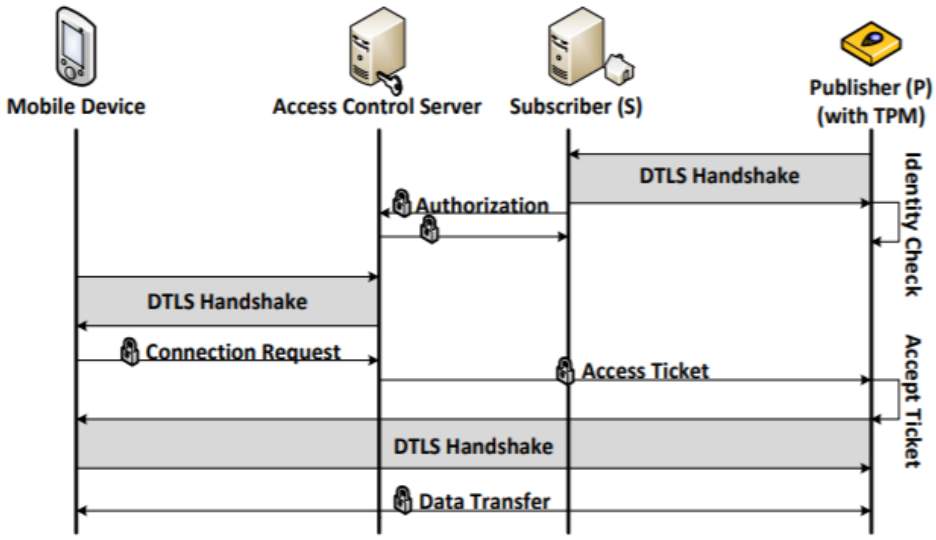
Các nhà xuất bản dữ liệu muốn tham gia vào mạng trước tiên kết nối an toàn với một thuê bao được cấu hình sẵn. Tùy thuộc vào khả năng của nút, nó có thể chọn bộ mật mã DTLS thích hợp:

Các nhà xuất bản hỗ trợ TPM có thể thực hiện bắt tay được xác thực đầy đủ với thuê bao, đóng vai trò là máy chủ DTLS trong phiên bắt tay này. Cả người đăng ký và nhà xuất bản đều truyền chứng chỉ RSA ở định dạng X.509. Các chứng chỉ này đã được ký bởi 1 CA đáng tin cậy bằng khóa riêng của nó, đảm bảo rằng chứng chỉ không bị thay đổi. Miễn là cả hai bên giữ bí mật khóa riêng RSA của mình, họ có thể chắc chắn về danh tính của nhau. Các nhà xuất bản (tức các nút cảm biến) được coi là dễ bị giả mạo vật lý trong đó người ta cho rằng kẻ tấn công có thể có quyền truy cập vào tất cả thông tin được lưu trữ trên các nút cảm biến. Nó sẽ là thảm họa trong trường hợp khóa riêng RSA vì nó sẽ cho phép kẻ tấn công mạo danh bất kỳ nút bị xâm phạm nào. Do đó, khóa riêng RSA cần được lưu trữ bên trong chip TPM chống giả mạo và không bao giờ được chuyển ra bên ngoài. Do đó, tất cả các hoạt động mã hóa khóa riêng phải được thực hiện trong TPM. Vì TPM được coi là chống lại sự giả mạo vật lý, kịch bản nói trên rất khó đối với kẻ tấn công và tính xác thực mạnh trong quá trình bắt tay được đảm bảo. Nhà xuất bản kiểm tra thông

tin nhận dạng của chứng chỉ thuê bao đối với nhận dạng được cấu hình sẵn. Thuê bao có thể tùy chọn kiểm tra với máy chủ AC nếu nhà xuất bản được phép thiết lập kết nối, dựa trên thông tin nhận dạng trong chứng chỉ của nhà xuất bản.

Các nhà xuất bản bị ràng buộc thực hiện một biến thể của bộ mật mã khóa chia sẻ trước TLS (PSK). Nhà xuất bản có một số byte ngẫu nhiên được cài đặt sẵn trước khi triển khai. Chúng được gọi là protokey và được sử dụng để lấy PSK cho một phiên. Nhà xuất bản gửi danh tính của mình (ví dụ: địa chỉ IPv6) trong bản tin ClientKeyExchange của phiên bắt tay. Nó cũng nối thêm một vài byte được tạo ngẫu nhiên vào danh tính PSK của nó để tạo thành nhận dạng phiên. Sau đó, nhà xuất bản lấy PSK bằng cách áp dụng hàm HMAC cho danh tính phiên với khóa protokey làm khóa. Thuê bao xác thực với máy chủ AC và yêu cầu PSK cho danh tính phiên của nhà xuất bản. Máy chủ AC là thực thể đáng tin cậy duy nhất trong kiến trúc, vì vậy protokey có thể được lưu trữ an toàn ở đó. Máy chủ AC tạo PSK cho thuê bao từ danh tính phiên và protokey và gửi nó đến thuê bao thông qua kết nối an toàn. Kịch bản này sử dụng một chuỗi tin cậy. PSK vẫn là cơ sở để xác thực như với bộ mật mã TLS PSK truyền thống, nhưng bằng cách sử dụng protokey và danh tính phiên tương ứng của nhà xuất bản.

Giao tiếp ngang hàng chỉ có thể bắt đầu sau khi thuê bao (S) được xác thực với máy chủ AC. Khi S muốn bắt đầu liên lạc với nhà xuất bản (P) trong mạng, trước tiên, nó phải có được một vé truy cập từ máy chủ AC. S chỉ định ngang hàng mà nó dự định kết nối và loại kết nối (đọc, ghi, đọc/ghi) mà nó muốn thiết lập. Máy chủ AC kiểm tra quyền truy cập của thuê bao cung cấp cho nhà xuất bản và nếu đủ, sẽ gửi yêu cầu kết nối tới P. Bây giờ, P có thể quyết định liệu nó có đủ tài nguyên để chấp nhận kết nối mới hay không. Nếu có, P sẽ bắt đầu bắt tay DTLS với S để thiết lập kết nối ăn toàn. Quá trình này được hiển thị trong Hình 2.19



Hình 2. 19: Thiết lập kết nối ngang hàng

Truyền dữ liệu

Khi kết nối an toàn với khóa đối xứng đã được thiết lập, lớp bảo mật sẽ trong suốt đối với mọi ứng dụng trên nhà xuất bản. Tuy nhiên, bất kỳ ứng dụng nào trước tiên phải chờ bắt tay hoàn thành trước khi dữ liệu có thể được trao đổi, điều này không xảy ra thường xuyên. Nó xảy ra khi một nút nhà xuất bản ban đầu tham gia vào mạng và sau đó trong quá trình re-keying. Re-keying thường xảy ra định kỳ và có thể được thực hiện bằng một phiên bắt tay hoàn chỉnh hoặc một cái bắt tay rút gọn sử dụng lại các khóa bí mật đã trao đổi trước đó.

2.4.2 Ứng dụng bảo mật bằng Blockchain

2.4.2.1 Công nghệ Blockchain

Gần đây, vấn đề đồng tiền kỹ thuật số Bitcoin được rất nhiều người quan tâm. Bitcoin là một loại tiền điện tử thường được sử dụng cho giaodịch trên internet, được Satoshi Nakamoto sang tạo ra. Đặc điểm của đồng tiền Bitcoin là tính ẩn danh, thanh toán không cần bên trung gian, khi đó người gửi và người nhận không biết danh tính của nhau. Điều này khiến Bitcoin có thể được sử dụng để thanh toán quốc tế mà không bị kiểm soát bởi hệ thống ngân hàng, các chính phủ. Công nghệ nền tảng đằng sau đồng tiền ảo bitcoin chính là công nghệ Blockchain. Hộ thống công nghệ hỗ trợ tiền ảo Bitcoin được cho rằng có khả năng ứng dụng cho

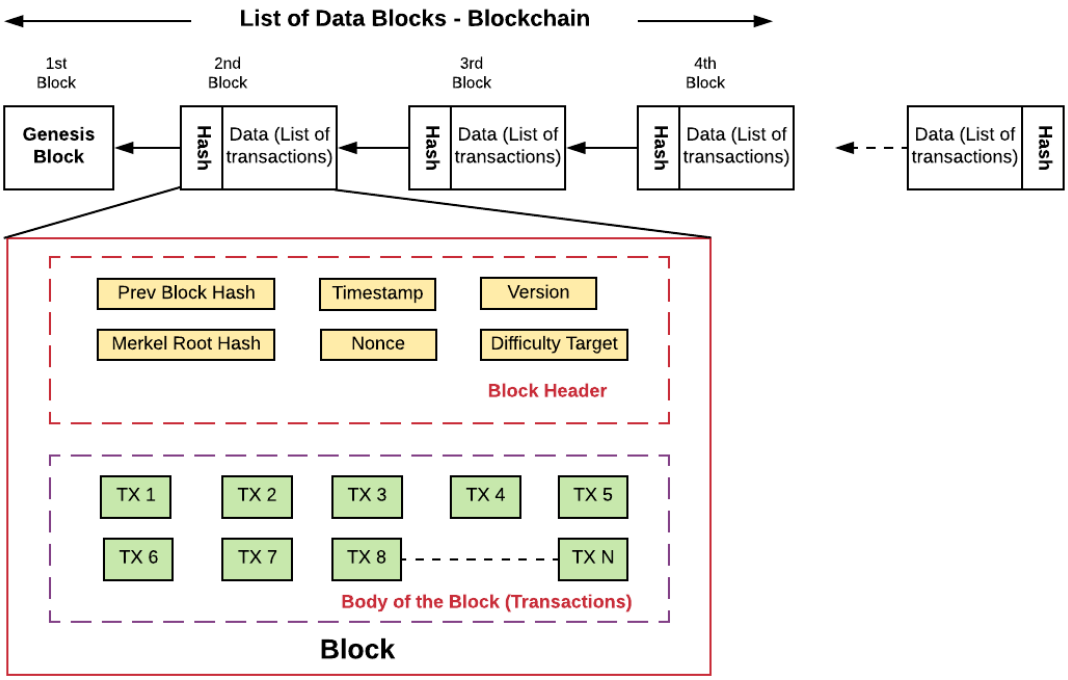
các mục đích khác nhau, không chỉ trong lĩnh vực tiền tệ, làm cho Blockchain trở thành một công nghệ chuyển đổi số tiềm năng (transformational technology).

Blockchain (Chuỗi khối) là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại việc thay đổi dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó

Theo khía cạnh chức năng có thể coi Blockchain là một sổ cái kỹ thuật số (digital ledger) phân tán: sổ cái này là một "chuỗi" (chain) của các "khối" (block) theo thời gian, trong đó mỗi "khối" chứa một bản ghi về hoạt động mạng hợp lệ kể từ khi "khối" cuois cùng được thêm vào chuỗi.

Theo Marr Bernard, công nghệ Blockchain sử dụng cơ sở dữ liệu phân tán (các thiết bị không kết nối đến một bộ xử lý chung) mà nó tổ chức dữ liệu thành các khối có xác thực mã hóa, được đánh dấu thời gian và được liên kết với các bản ghi trước đó để chúng chỉ có thể được thay đổi bởi những người sở hữu khóa mã hóa để ghi tệp. Mỗi khối (block) bao gồm dữ liệu (data), băm (hash) và băm của khối trước đó (hash of previous block).

- Data: dữ liệu được lưu trữ trong block, nó phụ thuộc vào loại block. Ví dụ: trọng Bitcoin thì dữ liệu lưu trữ là thông tin chi tiết về một giao dịch như: người gửi, người nhận và tiền (coin).
- Hash (băm): Mỗi block có một hash. Hash có thể được so sánh như vân tay. Nó giúp cho việc xác thực một block và tất cả các nội dung của block đó. Một hash là duy nhất cũng như vân tay của mỗi người là duy nhất. Khi một block được tạo ra thì hash bắt đầu được tính toán. Bất kỳ thay đổi nào bên trong block sẽ dẫn đến sự thay đổi của hash. Nói cách khác, nó giúp phát hiện sự thay đổi của block.
- Hash of previous block (băm của khối đằng trước): Giúp tạo ra chuỗi các khối (chain of block) và đó chính là công nghệ tạo ra một Blockchain.

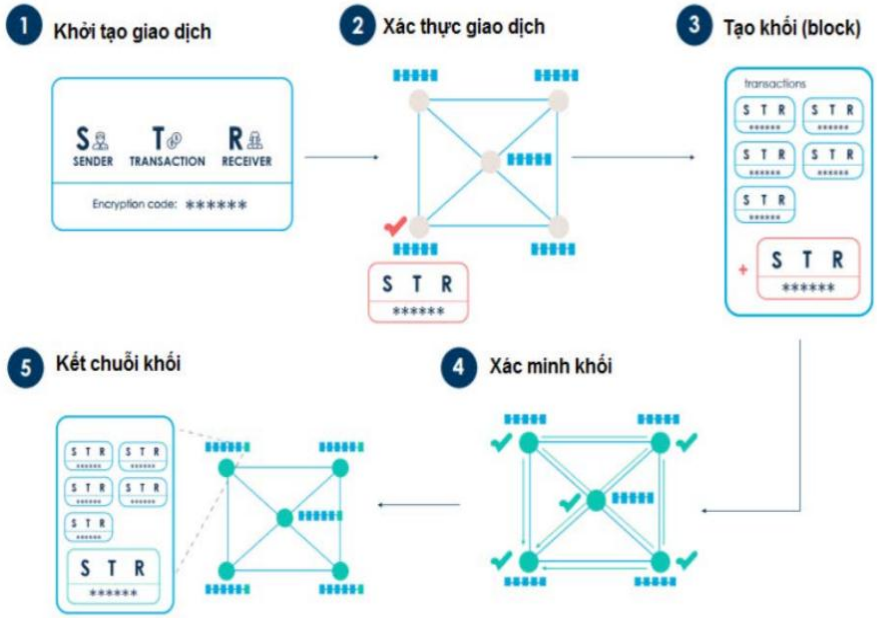


Hình 2. 20: Chuỗi các Block mà Blockchain lưu trữ

Về khái quát, có thể hình dung những bước cơ bản của công nghệ Blockchain bao gồm các bước:

- Khởi tạo giao dịch/Gửi yêu cầu: Người dùng gửi đi/tạo ra một giao dịch và chuyển nó lên mạng (thông điệp giaodịch bao gồm chi tiết địa chỉ công khai của người nhận, giá trị của giao dịch và chữ ký số để chứng minh tính xác thực của giao dịch);
- Xác thực giao dịch: Các nút mạng (máy tính/người dùng) nhận thông điệp; xác thực tính đúng đắn của thông điệp bằng cách giải mã chữ ký số. Giao dịch được xác thực được đặt vào cùng chứa các giao dịch chờ.
- Tạo khối (Block): Các giao dịch chờ này được đưa vào cùng với nhau trong một phiên bản cập nhật của sổ cái, được gọi là khối (block) bởi một trong những nút trong mạng. Tại một thời điểm xác định, nút mạng sẽ gửi khối này vào mạng để xác minh.
- Xác minh khối: Những nút xác minh của mạng nhận được khối gửi đến cần xác minh và thực hiện việc xác minh thông qua một quy trình lặp mà yêu cầu tính đồng thuận cảu đa số trên mạng.

- Kết chuỗi khối: Nếu tất cả các giaodịch được xác minh, khối mới được xâu chuỗi vào Blockchain và trang thái hiện thời của sổ cái được phát (broadcast) gửi vào mạng



Hình 2. 21: Sơ đồ các bước cơ bản của công nghệ Blockchain

Về tổng thể, công nghệ Blockchain là sự kết hợp giữa 3 loại công nghệ và thuật toán: (i) Mật mã học (sử dụng Khóa công khai (Public key) và hàm băm (Hash function)) để đảm bảo tính minh bạch, toàn vẹn và riêng tư; (ii) mạng ngang hàng (peer-to-peer): mỗi nút mạng được coi là một client đồng thời là một server để lưu trữ bản sao ứng dụng; (iii) Lý thuyết trò chơi: mọi nút tham gia vào hệ thống phải tuân thủ luật chơi trên nguyên tắc đồng thuận và được thúc đẩy bởi động lực kinh tế. Đặc trưng cơ bản của công nghệ Blockchain bao gồm:

- Cơ sở dữ liệu phân tán: Mỗi bên trên một Blockchain có quyền truy cập vào toàn bộ cơ sở dữ liệu toàn bộ lịch sử của nó; không một bên duy nhất kiểm soát dữ liệu hoặc thông tin. Mỗi bên có thể xác minh trực tiếp hồ sơ của dối tác giao dịch của mình mà không có bên trung gian.

- Truyền tải ngang hàng: Truyền thông giao tiếp xảy ra trực tiếp giữa các hệ thống ngang hàng hay qua điểm nút trung tâm. Mỗi điểm nút lưu trữ và chuyển tiếp thông tin đến tất cả các nút khác.
- Minh bạch: Mỗi giao dịch và giá trị liên quan được hiển thị cho bất cứ ai có quyền truy cập vào hệ thống. Mỗi điểm nút hoặc người dùng trên một Blockchain có một địa chỉ 30 ký tự chữ số đặc biệt duy nhất nhận dạng nó. Người dùng có thể chọn ẩn anh cung cấp bằng chứng nhận dạng của họ cho người khác. Giao dịch xảy ra giữa các địa chỉ Blockchain.
- Tính không thể đảo ngược: Khi một giao dịch được nhập vào cơ sở dữ liệu và các tài khoản được cập nhật, hồ sơ không thể bị thay đổi bởi vì chúng được liên kết đến tất cả các bản ghi giao dịch đã xuất hiện trước đó. Các thuật toán phương pháp tiếp cận tính toán khác nhau được triển khai để đảm bảo việc ghi vào cơ sở dữ liệu là vĩnh viễn, theo thứ tự thời gian, và có sẵn cho tất cả các người dùng trên mạng.
- Logic tính toán: Bản chất kỹ thuật số của sổ cái (ledger) có nghĩa là các giao dịch Blockchain có thể được gắn với logic tính toán và trong bản chất được lập trình. Vì vậy, người dùng có thể thiết lập các thuật toán và quy tắc tự động kích hoạt các giao dịch giữa các điểm nút

Nhìn từ góc độ kinh doanh, Blockchain có thể được coi như là một sổ cái kế toán, hay một cơ sở dữ liệu chứa đựng tài sản, hay một cấu trúc dữ liệu, mà dùng để ghi chép lại lịch sử của tài san giữa các thành viên trong hệ thống mạng ngang hàng. Theo khía cạnh kỹ thuật, đây là một phương thức để lưu trữ lịch sử các giao dịch tài sản mà không thay đổi được. Nếu xét trên góc độ xã hội đó là một hiện tượng, niềm tin được thiết lập bằng quy tắc đồng thuận giữa các thành viên trong một hệ thống phân cấp.

2.4.2.2 BlockChanin trong bảo mật IoT

Công nghệ Blockchain là một công nghệ mới nổi cùng với IoT sẽ mang lại nhiều hứa hẹn trong việc giúp các thiết bị được kết nối an toàn [1-2-5-6]. Trong khi công nghệ Blockchain đã trở nên nổi bật trong thế giới tài chính công nghệ bằng cách mở ra một cuộc cách mạng thanh toán điện tử, nền tảng công nghệ cơ bản này

là nhân tố đứng đằng sau sự thành công và gia tăng của tiền điện tử. Nó có thể đóng một vai trò quan trọng trong an ninh mạng, đặc biệt là trong không gian IoT. Nền tảng an ninh mạng dựa trên Blockchain có thể bảo mật các thiết bị kết nối bằng cách sử dụng chữ ký điện tử để nhận diện và xác thực các thiết bị này. Sau đó các thiết bị sẽ đóng vai trò là những đối tượng tham gia được ủy quyền trong mạng Blockchain. Mỗi thiết bị được xác thực tham gia mạng IoT bảo mật dựa trên Blockchain sẽ được coi là một thực thể tham gia, giống như trong mạng Blockchain thông thường. Tất cả thông tin liên lạc giữa những người tham gia đã được xác minh (thiết bị IoT) sẽ được bảo mật bằng mật mã và lưu trữ trong nhật ký chống giả mạo. Mọi thiết bị mới được thêm vào mạng đều được đăng ký bằng cách gán ID kỹ thuật số duy nhất trên hệ thống Blockchain. Nền tảng này sẽ cung cấp các kênh bảo mật để liên lạc giữa các thiết bị và đồng thời tất cả các thiết bị kết nối sẽ có quyền truy cập an toàn vào hệ thống chủ hay cơ sở hạ tầng.

Giải pháp an ninh mạng dựa trên Blockchain cũng có thể tận dụng kiến trúc Software-defined perimeter (SDP) và sử dụng mô hình Zero-Trust để làm cho tất cả các thiết bị đã được xác thực vô hình trước kẻ tấn công [5]. Điều này có nghĩa là chỉ những thiết bị được xác minh mới có thể "nhìn thấy" hoặc biết về sự tồn tại của các thiết bị kết nối khác và từ đó tạo thêm một lớp bảo mật bổ sung cho cơ sở hạ tầng IoT. Một nền tảng được vận hành bởi Blockchain sử dụng một mô hình mang phân tán và phân cấp (decentralized), khiến hacker gần như không thể tấn công vào hệ thống bằng cách đánh gục một mục tiêu. Kiểm soát dựa trên sự đồng thuận phân bố trách nhiệm bảo mật trên các nút trong mạng Blockchain khiến các hackers không thể giả mạo vào mạng đó và cũng đồng thời bảo vệ mạng IoT không bị phá hủy bởi các cuộc tấn công DDoS.

Việc phân cấp cũng làm cho một giải pháp như vậy có khả năng mở rộng cao hơn. Đó là một trong những mối quan tâm lớn nhất của việc triển khai hệ thống an ninh mạng trên một mạng lưới ngày càng phát triển như trong trường hợp các thiết bị được kết nối. Với mọi thiết bị mới được thêm vào hay xóa đi, thay đổi sẽ được thông báo ngay lập tức cho tất cả người tham gia. Điều này sẽ cho phép hệ thống có thể thích ứng và linh hoạt để mở rộng và phát triển theo thời gian mà không cần

nâng cấp toàn bộ nền tảng. Một hệ thống như vậy có thể được sử dụng để bảo đảm nhà thông minh, phương tiện tự vận hành được kết nối, cơ sở hạ tầng IIoT và thậm chí cả một thành phố thông minh. Giải pháp an ninh mạng dựa trên công nghệ Blockchain được tăng cường bằng kiến trúc SDP có thể cung cấp cho các thế hệ sau một cách thức về bảo mật các thiết bị, mạng và truyền thông IoT. Giải pháp này không chỉ giúp bảo vệ doanh nghiệp trước các lỗ hổng và rủi ro mạng hiện nay mà còn hiệu quả trong việc dự đoán các lỗ hổng mới. Cả Blockchain và IoT đều là những công nghệ đang phát triển với hầu hết các đổi mới trong lĩnh vực này đều ở giai đoạn khởi đầu. Tuy nhiên, việc kết hợp các thế mạnh của công nghệ Blockchain với tiềm năng của IoT có thể nhanh chóng và hiệu quả thúc đẩy toàn bộ các ngành công nghiệp, thành phố và quốc gia vào không gian "thông minh" bằng cách giảm bớt gánh nặng trong việc bảo vệ vành đai đang ngày một lớn dần của cơ sở hạ tầng và các thiết bị khác với thông thường mà không cản trở tốc độ đổi mới.

Một số mô hình lý thuyết bảo mật kết hợp IoT và BC [7]

IoT – IoT : phương pháp này có thể là phương pháp nhanh nhất về độ trễ và bảo mật vì nó có thể hoạt động ngoại tuyến. Các thiết bị IoT phải có khả năng giao tiếp với nhau, thường liên quan đến các cơ chế khám phá và định tuyến. Chỉ một phần dữ liệu IoT được lưu trữ trong Blockchain trong khi các giao dịch IoT diễn ra mà không sử dụng Blockchain. Cách tiếp cận này sẽ hữu ích trong các tình huống với dữ liệu IoT đáng tin cậy nơi các tương tác IoT đang diễn ra với độ trễ thấp (hình 2.22a)

IoT – Blockchain : theo cách tiếp cận này, tất cả các tương tác đều đi qua Blockchain, cho phép một bản ghi bất biến về các tương tác. Cách tiếp cận này đảm bảo rằng tất cả các hành động tương tác được chọn đều có thể theo dõi được vì các chi tiết của chúng có thể truy vấn trong Blockchain, và hơn nữa nó làm tăng tính tự chủ của các thiết bị IoT. Các ứng dụng IoT có ý định giao dịch hoặc cho thuê như Slock.it có thể tận dụng phương pháp này để cung cấp dịch vụ của họ. Tuy nhiên, ghi lại tất cả các tương tác trong Blockchain sẽ liên quan đến việc tăng băng thông và dữ liệu. Đây là một trong các thách thức lớn của Blockchain. Mặt khác, tất cả dữ

liệu IoT được liên kết với các giao dịch này cũng nên được lưu trữ trong Blockchain (hình 2.22b).

Các tiếp cận kết hợp : thiết kế kết hợp trong đó chỉ một phần các tương tác và dữ liệu diễn ra trong Blockchain và phần còn lại được chia sẻ trực tiếp giữa các thiết bị IoT. Một trong những thách thức trong cách tiếp cận này chọn những tương tác nào sẽ đi qua Blockchain và cung cấp cách để quyết định điều này trong quá trình vận hành. Một sự phối hợp hoàn hảo của phương pháp này sẽ là cách tốt nhất để tích hợp cả hai công nghệ IoT và Blockchain vì nó tận dụng lợi ích của Blockchain và lợi ích của các tương tác IoT thời gian thực (hình 2.22c). Theo cách tiếp cận này điện toán sương mù sẽ phát triển mạnh mẽ để bổ sung cho những hạn chế của Blockchain và IoT

Các thiết bị biên và đám mây lưu trữ tạo thành hệ thống mạng sương mù. Trong mạng sương mù, các edge device sẽ phối hợp với nhau và với dịch vụ cloud để quản lý, cấu hình và điều khiển tại chỗ một số lượng lớn end device. Hệ thống mạng sương mù có các ưu điểm sau:

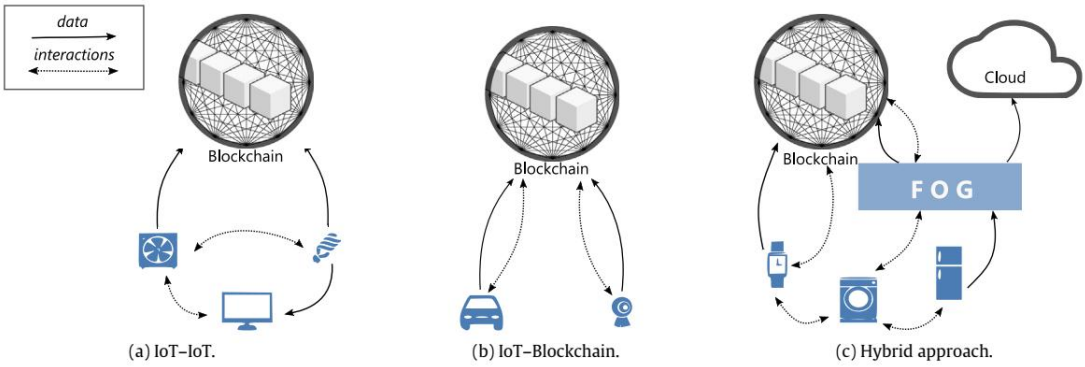
Giảm sự phụ thuộc vào dịch vụ bên ngoài: Điện toán sương mù cho phép giải pháp IoT của người dùng kiểm soát và quản trị nút biên tại chỗ mà không phụ thuộc vào nhà cung cấp dịch vụ điện toán đám mây

Các nút biên và IoT gateway sẽ hình thành mạng lưới điện toán phân tán (distributed networks) có khả năng lưu trữ dữ liệu tạm thời và ra quyết định tại chỗ. Vì vậy, ngay cả khi không có dịch vụ đám mây hoặc dịch vụ bị gián đoạn, ứng dụng IoT vẫn có thể hoạt động dù có thể gặp một vài hạn chế.

Tối ưu sử dụng băng thông mạng: trong mạng sương mù, các nút biên sẽ xử lí dữ liệu thô thu được từ thiết bị cuối và định kì gửi dữ liệu đã qua xử lí lên các máy chủ hoặc dịch vụ đám mây để lưu trữ hoặc thực hiện các xử lí khác. Do đó băng thông mạng được sử dụng hiệu quả hơn.

Vận hành theo thời gian thực và độ trễ thấp: mạng sương mù đảm bảo các dữ liệu quan trọng luôn được xử lí tại chỗ mà không cần sự can thiệp của máy chủ. Do đó độ trễ tính toán thấp và đảm bảo được các yêu cầu về thời gian trong các hệ thống thời gian thực.

Tối ưu sử dụng tài nguyên của các nút biên: các nút biên được thiết kế và tính toán cấu hình vừa đủ để giải quyết bài toán cụ thể trong ứng dụng IoT nên hạn chế được sự lãng phí tài nguyên và tối ưu băng thông mạng.



Hình 2. 22: Mô hình lý thuyết bảo mật kết hợp IoT và BC [7]

2.5 Kết luận chương II

Sự thành công của các ứng dụng IoT và cơ sở hạ tầng IoT phụ thuộc đáng kể vào sự đảm bảo về tính bảo mật và lỗ hổng trong IoT. Nội dung chương 2 đưa ra một số các ứng dụng của IoT và các yêu cầu bảo mật trong môi trường IoT. Vấn đề bảo mật là một thách thức lớn với mạng IoT do khối lượng dữ liệu, thiết bị lớn cùng số lượng thành phần vật lý khổng lồ. Trong chương còn khảo sát hai giải pháp bảo mật trong môi trường IoT đó là DTLS và xác thực hai chiều, kết hợp BC và IoT. Qua phân tích các mô hình kết hợp IoT và BC cho thấy những ưu điểm vượt trội của giải pháp bảo mật BC và IoT.

CHƯƠNG 3: XÂY DỰNG MÔ HÌNH BẢO MẬT BC CHO THIẾT BỊ IoT SMARTHOME

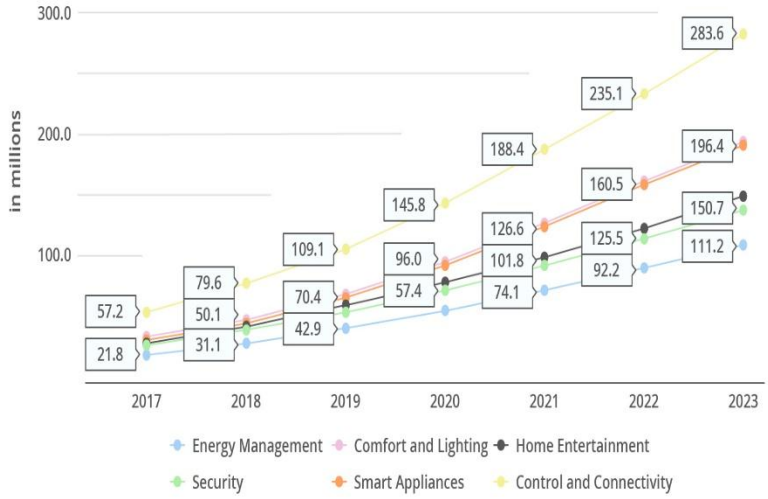
3.1 Thách thức trong bảo mật IoT.

Theo báo cáo của Juniper Research, có tới 83 tỷ thiết bị có kết nối internet (IoT devices) dự kiến sẽ được kết nối vào năm 2024 [1-11]. Trong khi đó, chi phí tích lũy của các vụ vi phạm dữ liệu từ năm 2017 đến 2022 dự kiến sẽ chạm mốc 8 nghìn tỷ đô la. Dưới áp lực của tội phạm mạng tăng cao, bảo mật IoT sẽ là một thách thức lớn đối với bất kì doanh nghiệp phát hành và sử dụng thiết bị IoT nào. Từ nhà và văn phòng thông minh cho đến ô tô được kết nối, máy bay không người lái, xe tải tự lái và thậm chí đến cơ sở hạ tầng quan trọng như hệ thống điều khiển công nghiệp. Hệ thống này đang là một phần của Internet công nghiệp (IIoT). Tất cả các mạng IoT hiện tại và mạng IoT mới đều phải đối mặt với nguy cơ đe dọa mạng rất cao.

3.2 Ứng dụng Blockchain bảo mật thiết bị IoT Smarthome

3.2.1 Tổng quan Smarthome

Nhu cầu ngày càng cao của người tiêu dùng đối với vấn đề giám sát an ninh tự động từ xa, tiết kiệm năng lượng thông qua hệ thống bật tắt đèn thông minh, nâng cao chất lượng cuộc sống bằng việc sử dụng công nghệ điều khiển bằng cử chỉ, bằng giọng nói… chính là đòn bẩy cho sự phát triển của thị trường nhà thông minh. **"Smarthome"**, hiểu đơn giản, là một ngôi nhà có các thiết bị gia dụng như: hệ thống chiếu sáng, sưởi ấm, máy lạnh, TV, máy tính, âm thanh, camera an ninh,… có khả năng tự động hóa và "giao tiếp" với nhau theo một lịch trình định sẵn. Chúng có thể được điều khiển ở bất cứ đâu, từ trong chính ngôi nhà thông minh đó đến bất kỳ nơi nào trên thế giới thông qua điện thoại hoặc internet.

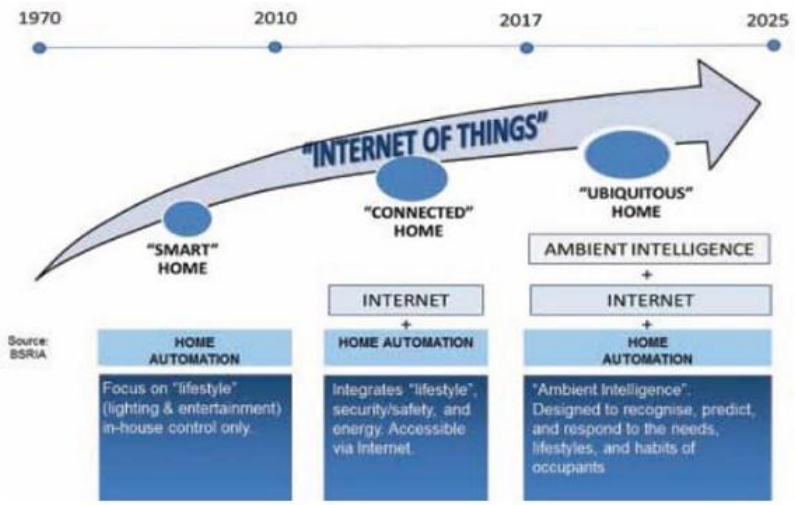


Hình 3. 1 Dự báo nguồn tài chính đầu tư vào Smarthome [11]

Công nghệ tiên tiến đã cho phép tất cả các thiết bị như đèn chiếu sáng, camera giám sát, smart TV, máy giặt, tủ lạnh… có thể được kết nối và điều khiển chỉ bởi một thiết bị như smartphone hay máy tính bảng thậm chí bằng giọng nói của gia chủ và hoàn toàn có thể điều khiển từ xa qua Internet. Các chủ nhà có thể hưởng thụ sự tiện nghi, an toàn và hiện đại từ những giải pháp giám sát an ninh toàn diện, báo cháy, tự động điều khiển mành rèm, điều khiển từ xa các thiết bị gia dụng, các hệ thống đèn chiếu sáng, điều hoà nhiệt độ, hệ thống tưới cây, hệ thống giải trí… trong ngôi nhà thông minh.

Trước đây nhiều người hình dung nhà thông minh là cái gì đó cao siêu, sợ công nghệ phức tạp nên không dám trang bị, nhưng trên thực tế SmartHome cực kỳ dễ sử dụng ngay cả với người già và trẻ em, hơn nữa hầu như các thao tác đã hoàn toàn tự động, người dùng không cần phải can thiệp gì cả. Có thể đơn cử một vài tiện ích của nhà thông minh: Nhà có người già, trẻ nhỏ có thể đi lại trong đêm tối vì khi có hoạt động di chuyển thì hệ thống đèn sẽ tự bật sáng, trẻ tự nhiên đi lại không cần bố mẹ dẫn đi vì sợ bóng tối, người già không sợ bị ngã. Khi đi vắng về tới trước cửa nhà, hệ thống đèn tự sáng, không phải mở khoá. Một số nhà lắp cổng tự động rất tiện cho việc khi về tới nhà hệ thống cửa tự mở ra, trời mưa không phải xuống xe để

mở cửa. Điều hòa nhiệt độ có thể được bật từ trước qua smartphone, khi về đến nhà thì phòng đã mát.



Hình 3. 2 Dự báo phát triển smarthome [8]

3.2.2 Thách thức bảo mật IoT Smarthome

Bảo mật và tính riêng tư: Truyền thông thực tế giữa các đối tượng tạo ra những thách thức lớn về độ tin cậy, an ninh và riêng tư. IoT đã phải đối mặt với nhiều mối đe dọa bảo mật và các cuộc tấn công. Do truyền dữ liệu khổng lồ, việc truyền dữ liệu quan trọng trong mạng có thể bị tấn công bởi một số đối thủ như MitM và DoS / DDoS. IoT gây ra nhiều thách thức độc đáo đối với quyền riêng tư chẳng hạn như các vấn đề riêng tư dữ liệu và thiết bị theo dõi cho điện thoại và xe hơi. Ngoài ra, nhận dạng giọng nói đang được được tích hợp để lắng nghe cuộc trò chuyện để chủ động truyền dữ liệu lên bộ lưu trữ đám mây để xử lý.

Khả năng mở rộng và kiểm soát truy cập: Vì IoT hỗ trợ số lượng lớn các thiết bị kết nối và giao tiếp với nhau, khả năng mở rộng được coi là một trong những thách thức lớn mà phần mềm trung gian phải đối mặt tiếp cận. Do đó, một phần mềm trung gian đáng tin cậy là cần thiết để quản lý số lượng thiết bị xử lý hiệu quả các vấn đề về khả năng mở rộng để hoạt động tốt trong môi trường IoT lớn. Điều khiển truy cập cho phép người dùng truy cập tài nguyên của hệ thống IoT. Do tăng số lượng thiết bị cũng như nhu cầu tài nguyên và băng thông thấp giữa các thiết bị và Internet, hệ thống phải đối mặt với những thách thức kiểm soát truy cập.

Tính sẵn sàng và độ tin cậy: Tính động và thích ứng được yêu cầu để quản lý và giám sát cơ sở hạ tầng IoT trong chế độ tự quản lý. Điều này sẽ cho phép một giải pháp bền vững cho tính khả dụng và độ tin cậy cho kết nối động và mạnh mẽ.

Tính toàn vẹn và bảo mật: Bảo mật là bảo vệ thông tin đặc biệt là khi chia sẻ trong mạng công cộng. Nó đảm bảo quyền riêng tư của người dùng và giữ an toàn thông tin cá nhân của người dùng. Bảo mật yêu cầu một mật mã hiệu quả và quản lý khóa theo thứ tự để đạt được tính ẩn danh cao. Mặc dù có một số giải pháp, vẫn có những cuộc tấn công chống lại sự bí mật lộ thông tin định tuyến và trao đổi dữ liệu. Tính toàn vẹn đảm bảo rằng không có sửa đổi dữ liệu trong một môi trường nhà thông minh phải đối mặt với vấn đề toàn vẹn. Kẻ tấn công có thể sửa đổi dữ liệu được cảm nhận sẽ được lưu trữ trong nút hoặc trong khi nó di chuyển trong mạng.

3.2.3 Phân loại Blockchain

Hệ thống Blockchain chia thành 3 loại chính:

Public: Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phi khá cao. Ví dụ: Bitcoin, Ethereum…

Private: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Tổ chức này có thể hoặc không cho phép người dùng đọc dữ liệu trong một số trường hợp. Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.

Permissioned: Hay còn gọi là Consortium, một dạng của Private nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa "niềm tin" khi tham gia vào Public và "niềm tin tuyệt đối" khi tham gia vào Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

3.2.4 Blockchain ứng dụng Smarthome [4]

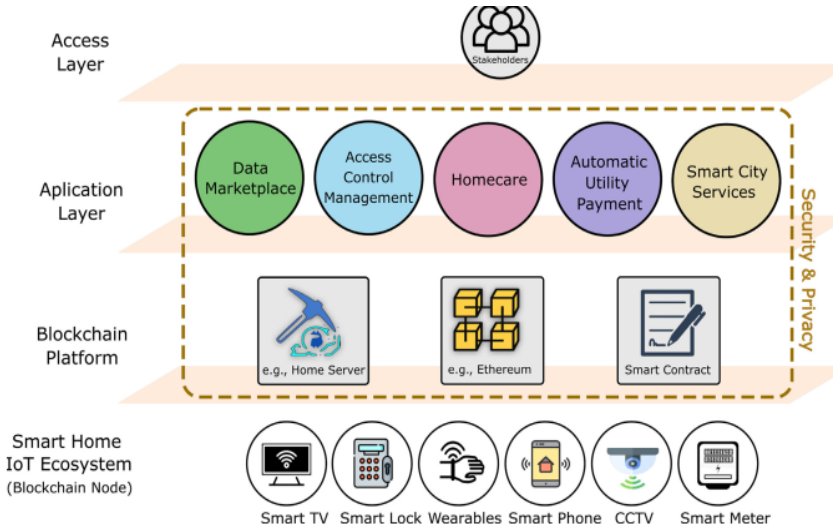
Công nghệ chuỗi khối đang nhanh chóng định hình hệ sinh thái nhà thông minh vì nó có tính linh hoạt và khả năng thích ứng dễ dàng tích hợp với các thiết bị IoT nhà thông minh không đồng nhất. Nền tảng hệ sinh thái ngôi nhà thông minh dựa trên Blockchain bao gồm 4 lớp: Lớp nguồn dữ liệu IoT, lớp Blockchain, lớp ứng dụng nhà thông minh và lớp khách hàng.

Lớp nguồn dữ liệu IoT tạo dữ liệu từ các thiết bị đóng vai trò quan trọng trong việc đánh giá trạng thái, môi trường và con người của ngôi nhà thông minh. Các thiết bị này được phân thành ba loại chính: cảm biến, đa phương tiện và chăm sóc sức khỏe.

Công nghệ Blockchain nằm trên đỉnh của hệ sinh thái IoT và bao gồm hai thành phần chính: cấu trúc dữ liệu Blockchain và hợp đồng thông minh. Giá trị băm mật mã kết nối các khối. Một máy tính ở nhà có thể được coi là một công cụ khai thác chịu trách nhiệm xác minh và thêm các giao dịch mới vào các khối mới, trong khi hợp đồng thông minh tuân theo các quy tắc được xác định trước và tạo điều kiện cho các giao dịch phi tập trung. Có nhiều cách khác nhau để triển khai Blockchain bao gồm Blockchain công khai, Blockchain riêng tư và Blockchain liên kết, nhưng nói chung Blockchain riêng tư (Private) được sử dụng trong mạng gia đình thông minh để giảm chi phí mào đầu.

Lớp ứng dụng được tạo điều kiện cho các ứng dụng nhà thông minh khác nhau và sự tích hợp của chúng với nền tảng Blockchain hiện có. Lớp này bao gồm các ứng dụng nhà thông minh như thị trường dữ liệu, quản lý truy cập, khả năng tương tác tại nhà, chăm sóc sức khỏe, thanh toán tiện ích tự động và dịch vụ thành phố thông minh. Qua khảo sát nghiên cứu một trong số các ứng dụng đang sử dụng nền tảng Blockchain và một số vẫn đang được nghiên cứu [6].

Lớp máy khách, cho phép các bên liên quan của bên thứ ba được hưởng lợi từ các ứng dụng nhà thông minh dựa trên Blockchain như microgrid, cửa hàng bán lẻ, nhà cung cấp dịch vụ, người chăm sóc, v.v.

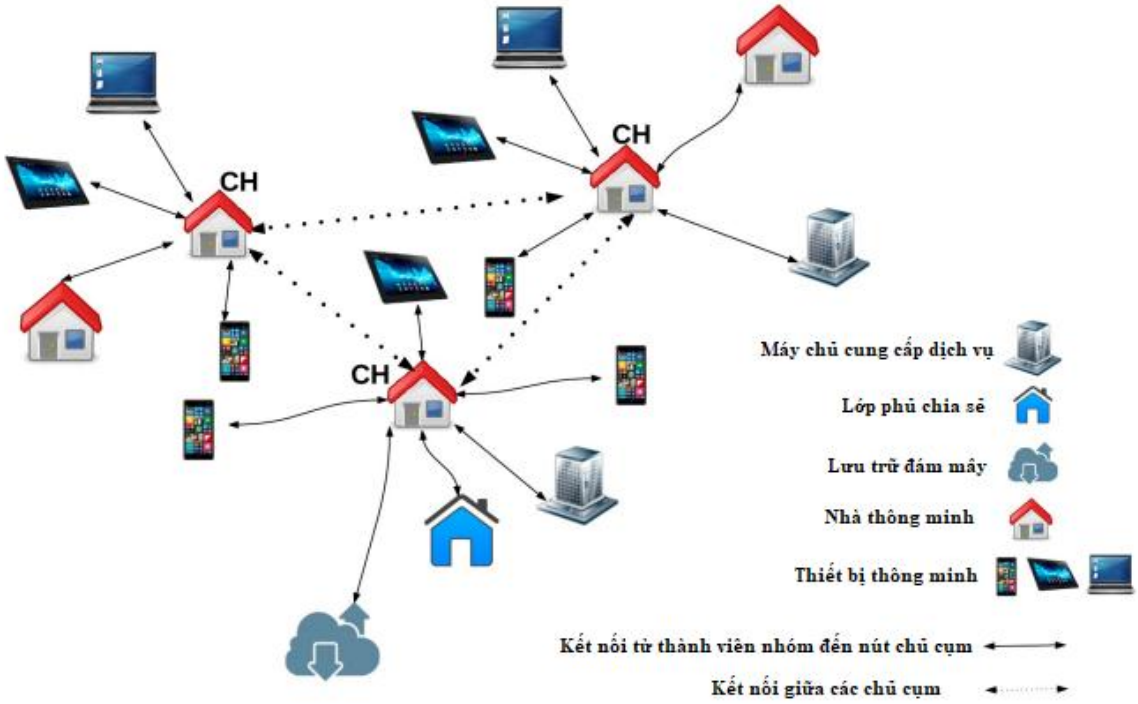


Hình 3. 3: Mô hình phân lớp Blockchain –Smarthome [6]

3.3 Xây dựng mô hình bảo mật Blockchain - Smarthome

3.3.1 Mô hình bảo mật Blockchain - Smarthome

Mô hình nhà thông minh kết hợp Blockchain thiết kế bao gồm gồm ba tầng cốt lõi là: nhà thông minh, lưu trữ đám mây và lớp phủ. Các thiết bị thông minh được đặt bên trong tầng nhà thông minh và được quản lý tập trung bởi một người khai thác. Nhà thông minh tạo thành mạng lớp phủ cùng với nhà cung cấp dịch vụ , đám mây kho lưu trữ và người dùng điện thoại thông minh hoặc máy tính cá nhân như hình 3.4



Hình 3. 4: Mô hình kiến trúc ứng dụng Blockchain cơ bản trong smarthome

Mạng lớp phủ là mạng ngang hàng P2P phân cấp. Để giảm chi phí và trễ mạng, các nút trong lớp phủ được nhóm thành các cụm và mỗi cụm bầu ra một nút chủ cụm (CH). Các lớp phủ CHs duy trì Blockchain public kết hợp với hai danh sách chính. Những danh sách chính là: danh sách khóa của người yêu cầu là danh sách khóa công khai PK (public key) của người dùng lớp mạng P2P được phép truy cập dữ liệu trong các ngôi nhà thông minh được kết nối với cụm này; danh sách khóa yêu cầu là danh sách PK của nhà thông minh kết nối với cụm này được phép truy cập.

Thuật toán chọn nút chủ cụm gồm ba pha:

Pha 1: Hình thành các cụm ban đầu với người đứng đầu và các thành viên trong cụm.

Trong giai đoạn đầu tiên, tập hợp các cụm ban đầu được hình thành dựa trên tham số mức độ (degree) D_i theo thuật toán:

- *Tìm kiếm các nút hàng xóm*

- *Tính toán D_i;*
- *Quảng bá D_i cho các nút khác.*
- *Thu thập $D_{i,j}$ từ tất cả các nút hàng xóm.*
- *Chọn nút H_i, nút có giá trị lớn nhất trong khi so sánh ($D_{i,j}$,D_i)*
- *Nếu nút i là là nút đầu của nhóm không có thành viên thì nút sẽ tham gia vào cụm của cụm hàng xóm có giá trị đầu k, D_k*

Nút đầu không phải là nút thành viên của bất kỳ cụm nào khác và mỗi thành viên chỉ được phân bổ cho một đầu / cụm. Mỗi nút thành viên lưu trữ mức độ và ID của đầu của nó, trong khi người đứng đầu biết số lượng nút thành viên cấu thành cụm và ID của họ. Khi kết thúc giai đoạn này, các cụm ban đầu được hình thành, bao gồm người đứng đầu và các thành viên.

Pha 2: Mở rộng các cụm có hệ số phân cụm cao

Mục tiêu của pha hai là mở rộng các cụm có hệ số phân cụm cao. Do đó, các khu vực của đồ thị với mô-đun cao sẽ được xác định. Đối với bước này, nút đầu cụm và các nút thành viên tham gia, thực hiện các nhiệm vụ khác nhau,

Đầu tiên, mỗi nút đầu cụm H_k tính toán số lượng các nút thành viên hiện có của nó, ký hiệu là M_k, và quảng bá thông tin đi h bước nhảy. Giá trị ban đầu của h là một (h = 1). Sau đó, nút chủ chờ một khoảng thời gian T_k để hoàn thành pha chuyển tiếp của gói tin quảng bá và phân bổ lại các nút thành viên thành cụm. Giai đoạn phân bổ lại diễn ra như sau: Mỗi thành viên nhận được một thông điệp quảng bá và chuyển tiếp nó đến một nút lân cận nếu thỏa mãn các điều kiện sau:

- h -1≠0
- Nó thuộc cùng một cụm với nút đầu tạo thông điệp quảng cáo. Nút đầu không chuyển tiếp các thông điệp quảng bá của nút đầu khác. Mục tiêu của những điều kiện này là để tránh tạo các khu vực cụm bị ngắt kết nối.

Mỗi nút thành viên thu thập tất cả các thông điệp quảng cáo trong h bước nhảy tối đa. Sử dụng những thông điệp này, mỗi thành viên tính toán hệ số ảnh hưởng của mỗi người đứng đầu. Ảnh hưởng IF_j^k của đầu H_k đến nút thành viên i, được tính như sau:

$$IF_j^k = \begin{cases} M_k & \text{Nếu TTL= 1} \\ S_{j,k} & \text{Nếu TTL >1} \end{cases} \quad (1)$$

Trong đó M_k là số lượng thành viên của nút đầu k. $S_{j,k}$ biểu thị số lượng tin nhắn quảng bá mà thành viên nút i đã nhận được từ H_k thông qua các đường dẫn khác nhau kết nối nút k và nút j. Mỗi nút thành viên chọn đầu (tức là cụm để tham gia) với giá trị IF lớn nhất. Do đó, các nút thành viên, theo mô hình ưu tiên, tham gia cụm gần nhất với ảnh hưởng lớn hơn vào nó.

Pha 3: Sáp nhập các cụm có hệ số kết nối cao

Sau khi hoàn thành giai đoạn quảng bá, số lượng các cụm đã hình thành và do đó số lượng cụm đầu có đã được giảm. Phép đo liên kết nối R_k được tính bởi mọi nút đầu k là tỷ lệ cạnh liên cụm và nội cụm của nó:

$$R_k = \frac{I_k^e}{I_k^a} \quad (2)$$

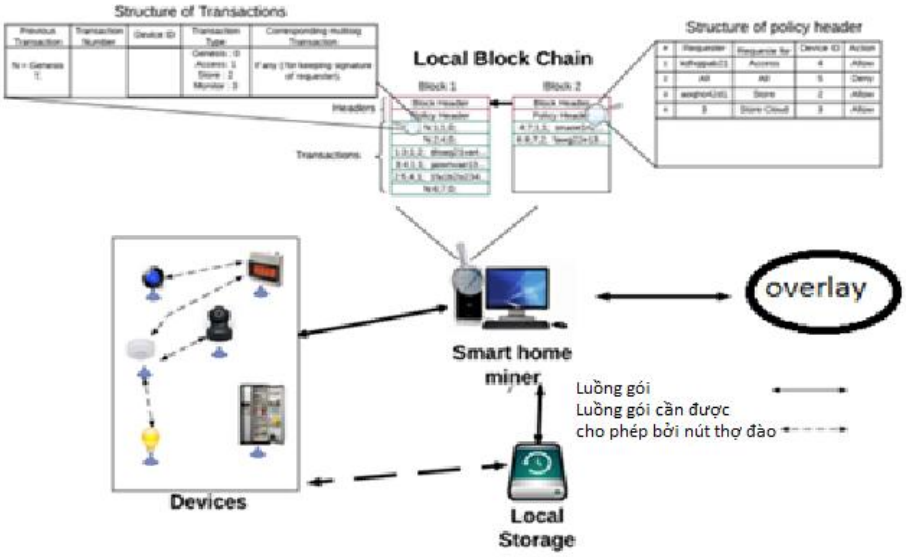
I_k^a biểu thị tổng số cạnh trong cụm của cụm k, Nếu $R_k > R_{thr}$ thì cụm k kích hoạt việc hợp nhất với cụm lân cận có giá trị DF tối đa. Lý do của giai đoạn hợp nhất này là để tránh hình thành các cụm không phải là mô-đun và các nút thành viên không độc lập rõ ràng về mặt tương tác từ các cụm lân cận. Việc hợp nhất sẽ dẫn đến việc giảm các cụm (tức là, các nút cụm chủ được bầu) và do đó làm tăng các nút thành viên được phân bổ trên mỗi cụm. Sau khi kết thúc pha sáp nhập, các cụm đã được hình thành và người đứng đầu của mỗi cụm đã được bầu. Cuối cùng, mỗi nút chủ cụm nhận thức được các nút thành viên tạo thành cụm của nó, trong khi mỗi nút thành viên nhận thức được cụm chủ được gán và khoảng cách của nó theo các bước nhảy.

Lưu trữ đám mây được sử dụng bởi các thiết bị nhà thông minh để lưu trữ và chia sẻ dữ liệu.

Mô hình smarthome tích hợp với Blockchain nội bộ và private để cung cấp kiểm soát truy cập an toàn cho IoT và dữ liệu của họ. Bên cạnh đó, Blockchain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã

thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó. Thiết kế bảo mật đến từ các tính năng đa dạng bao gồm: (1) các thiết bị có thể truy cập gián tiếp; và (2) các cấu trúc giao dịch khác nhau trong nhà thông minh và lớp phủ. Để đạt được bảo mật , mã hóa đối xứng được sử dụng cho các thiết bị nhà thông minh. Trong chương 3 học viên phân tích định tính để chứng minh rằng lớp nhà thông minh đạt được tính bảo mật, tính toàn vẹn, tính sẵn sàng và phòng ngừa các cuộc tấn công bảo mật quan trọng như tấn công liên kết, tấn công từ chối dịch vụ phân tán (DDOS). Phần kết quả mô phỏng chỉ ra chi phí để đạt được các kết quả bảo mật là tương đối nhỏ.

3.3.2 Các thành phần cốt lõi của mô hình Blockchain-Smarthome bảo mật

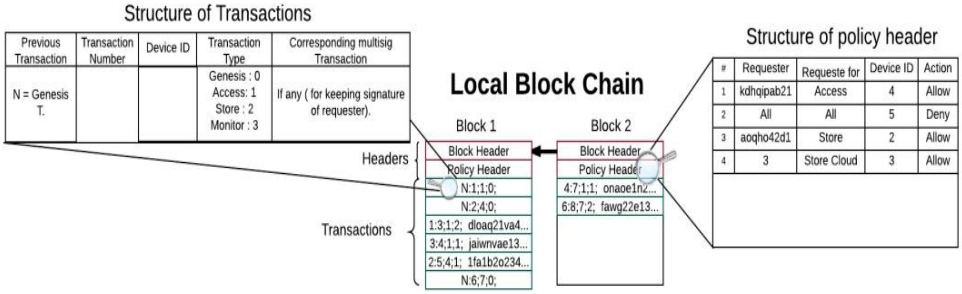


Hình 3. 5: Mô hình nhà thông minh tích hợp Blockchain

Giao dịch: Truyền thông giữa các thiết bị cục bộ hoặc các nút trong lớp phủ được gọi là giao dịch (transactions). Có nhiều giao dịch khác nhau trong nhà thông minh dựa trên BC thiết kế cho một chức năng cụ thể. *Giao dịch lưu trữ* được tạo ra bởi các thiết bị để lưu trữ dữ liệu. *Giao dịch truy cập* được tạo bởi nhà cung cấp dịch vụ hoặc chủ sở hữu nhà để truy cập vào lưu trữ đám mây. *Một giao dịch giám sát* được tạo ra bởi chủ sở hữu nhà hoặc nhà cung cấp dịch vụ để theo dõi định kỳ thông tin thiết bị. Thêm một thiết bị mới vào nhà thông minh thông qua một *giao*

dịch genesis và một thiết bị được loại bỏ thông qua một *giao dịch xóa*. Tất cả các giao dịch nói trên sử dụng khóa công khai để bảo mật thông tin liên lạc. Hàm băm được sử dụng để phát hiện bất kỳ thay đổi nào của nội dung giao dịch trong quá trình truyền tải. Tất cả các giao dịch đến hoặc từ nhà thông minh được lưu trữ trong một *BC private*.

BC riêng (Private Blockchains) : Là mạng Blockchain được kiểm soát, một người chỉ có thể tham gia nếu được mời/cho phép tham gia, việc truy cập của người tham gia và người thẩm định là có những hạn chế. Đây là loại Blockchain cho các công ty muốn ứng dụng công nghệ Blockchain nhưng không muốn có sự kiểm soát lỏng lẻo kiểu công cộng như với mạng công cộng. Họ có thể áp dụng Blockchain vào thủ tục kế toán và lưu trữ hồ sơ màvẫn được tính tự chủ, không lo bị lộ thông tin nhạy cảm cho Internet công cộng. Trong mỗi ngôi nhà thông minh, có một BC private lưu giữ theo dõi các giao dịch và có một tiêu đề chính sách để thực thi chính sách người dùng cho các giao dịch đến và đi. Bắt đầu từ *giao dịch genesis*, mỗi giao dịch của thiết bị trên mạng được kết nối chuỗi với nhau như một sổ cái bất biến trong BC. Sổ cái này là một "chuỗi" (chain) của các "khối" (block) theo thời gian, trong đó mỗi "khối" chứa một bản ghi về hoạt động mạng hợp lệ kể từ khi "khối" cuối cùng được thêm vào chuỗi. Tổ chức dữ liệu thành các bản ghi (gọi là khối - Block) có có xác thực mã hóa, được đánh dấu thời gian và được liên kết với các bản ghi trước (Chuỗi - Chain) đó để chúng chỉ có thể được thay đổi bởi những người sở hữu khóa mã hóa để ghi tệp. Mỗi khối trong BC chứa hai tiêu đề: tiêu đề khối và tiêu đề chính sách khối. Tiêu đề khối có giá tri băm của khối trước để giữ cho BC bất biến. Các tiêu đề chính sách được sử dụng để xác thực các thiết bị và thi hành chính sách kiểm soát của chủ sở hữu trong nhà của mình.



Hình 3. 6: Cấu trúc Block trong mô hình tích hợp Smarthome và BC

Thợ đào (Home miner): Thợ đào là một nút trong nhà thông minh xử lý tập trung giao dịch đến và đi từ hoặc đến nhà thông minh. *Home miner* có thể tích hợp với cổng *Gateway Internet* gia đình hoặc là một thiết bị hoạt động độc lập. Ngoài ra *Home miner* cũng thực hiện các chức năng bổ sung sau: tạo giao dịch *genesis*

, phân phối và cập nhật khóa, thay đổi cấu trúc giao dịch, hình thành và quản lý cụm. Nút người đào nhận được và xác thực các giao dịch thêm chúng vào vùng bộ nhớ và và bắt đầu xắp xếp chúng thành một khối nhiều giao dịch.

Lưu trữ cục bộ: Bộ nhớ cục bộ là một thiết bị lưu trữ, ví dụ: ổ đĩa sao lưu được sử dụng bởi các thiết bị để lưu trữ dữ liệu cục bộ. Bộ lưu trữ này có thể được tích hợp với công cụ khai thác hoặc nó có thể là một thiết bị riêng biệt. Bộ lưu trữ sử làm việc theo nguyên tắc FIFO để lưu trữ dữ liệu và lưu trữ dữ liệu của từng thiết bị, cũng như một sổ cái được nối vào điểm bắt đầu của thiết bị.

3.3.3 Hoạt động của mô hình Smarthome tích hợp BC bảo mật

(1)Khởi tạo: Quá trình thêm thiết bị và tiêu đề chính sách cho *Blockchain Private* . Để thêm một thiết bị vào nhà thông minh, thợ đào tạo ra một giao dịch *genesis* bằng cách chia sẻ một khóa với thiết bị sử dụng Diffie-Hellman. Các khóa được chia sẻ giữa thợ đào và thiết bị được lưu trữ trong giao dịch *genesis*. Đối với việc xác định tiêu đề chính sách, chủ sở hữu nhà tạo chính sách riêng của mình và thêm tiêu đề chính sách vào khối đầu tiên. Thợ đào sử dụng tiêu đề chính sách trong khối mới nhất của BC; do đó, để cập nhật chính sách, chủ sở hữu cập nhật tiêu đề chính sách của khối mới nhất.

(2)Xử lý giao dịch: Các thiết bị thông minh có thể giao tiếp trực tiếp với nhau hoặc với các thực thể bên ngoài nhà thông minh. Mỗi thiết bị trong nhà có thể yêu cầu dữ liệu từ một thiết bị nội bộ khác để cung cấp một số dịch vụ nhất định, ví dụ: bóng đèn yêu cầu dữ liệu từ cảm biến chuyển động để bật đèn tự động khi có người vào nhà. Để đạt được sự kiểm soát của người dùng đối với giao dịch nhà thông minh, một khóa công khai được phân bổ bởi thợ đào đến các thiết bị cần liên lạc trực tiếp với nhau. Để phân bổ khóa, thợ đào kiểm tra tiêu đề chính sách hoặc xin phép chủ sở hữu và sau đó phân phối khóa giữa các thiết bị. Sau khi nhận được

khóa, thiết bị giao tiếp trực tiếp miễn là khóa của họ hợp lệ. Để từ chối cấp phép, thợ đào đánh dấu phân phối khóa là không hợp lệ bằng cách gửi tin nhắn điều khiển đến các thiết bị. Lợi ích của phương pháp này là: Thợ đào có một danh sách các thiết bị chia sẻ dữ liệu, thông tin liên lạc giữa các thiết bị được bảo mật với một khóa được chia sẻ.

Thuật toán xác minh giao dịch:

1. **Input**: Overlay transaction (X)
2. **Output:** True or False
3. Requester verification
4. **If** (hash (X.Requester – PK) $\neq X_{-1}.output[2]$) **Then**
5. **Return** False;
6. **Else**
7. **If** (X.Requester – PK redeem x. requester-signature) **Then**
8. **Return** True;
9. **End if**
10. **End if**
11. Output validation
12. **If** (X.output[0] $- X_{-1}.output[0] + (X.output[1] - X_{-1}.output[1]) > 1)$ **Then**
13. **Return** False;
14. **End if**
15. Requester verification
16. **If** (X.Requester – PK redeem x. requester-signature) **Then**
17. **Return** True;

(3)Lưu trữ dữ liệu trên bộ nhớ cục bộ của thiết bị là giao dịch có thể có trong nhà. Lưu trữ dữ liệu cục bộ mỗi thiết bị cần được xác thực với bộ lưu trữ thực hiện bằng cách sử dụng khóa chia sẻ. Để cấp khóa, thiết bị cần phải gửi yêu cầu cho thợ đào và nếu nó có quyền lưu trữ, thợ đào tạo khóa chia sẻ và gửi khóa cho thiết bị và lưu trữ. Bằng cách nhận khóa, bộ nhớ cục bộ tạo một điểm bắt đầu có chứa khóa chia sẻ. Đang có khóa dùng chung, thiết bị có thể lưu trữ dữ liệu trực tiếp tại lưu trữ cục bộ. Các thiết bị có thể yêu cầu lưu trữ dữ liệu trên bộ lưu trữ đám mây được gọi là *giao dịch lưu trữ*. Lưu trữ dữ liệu trên đám mây là một quá trình ẩn

danh. Để lưu trữ dữ liệu người yêu cầu cần một điểm bắt đầu có chứa một số khối và hàm băm được sử dụng để xác thực ẩn danh.

Khi một thiết bị cần lưu trữ dữ liệu trên bộ lưu trữ đám mây, nó sẽ gửi dữ liệu và yêu cầu đến thợ đào. Bằng cách nhận yêu cầu, thợ đào ủy quyền cho thiết bị lưu trữ dữ liệu trên lưu trữ đám mây. Nếu thiết bị đã được ủy quyền, thợ đào trích xuất số khối và hàm băm cuối cùng từ BC cục bộ và tạo một giao dịch lưu trữ và gửi nó cùng với dữ liệu tới lưu trữ. Sau khi lưu trữ dữ liệu, bộ lưu trữ đám mây trả về số khối mới cho thợ đạo được sử dụng để lưu trữ thêm giao dịch. Các giao dịch khác có thể là truy cập và theo dõi giao dịch. Các giao dịch này chủ yếu được tạo ra bởi chủ nhà để giám sát nhà khi anh ta ở ngoài hoặc bởi nhà cung cấp dịch vụ để xử lý dữ liệu thiết bị của các dịch vụ được cá nhân sử dụng. Bằng việc nhận một giao dịch truy cập từ các nút trong lớp phủ, thợ đào kiểm tra xem dữ liệu được yêu cầu có ở nơi lưu trữ cục bộ hay lưu trữ đám mây. Nếu dữ liệu được lưu trữ trong bộ nhớ cục bộ, thợ đào yêu cầu dữ liệu từ bộ nhớ cục bộ và gửi nó đến người yêu cầu. Mặt khác, nếu dữ liệu được lưu trữ trong đám mây, người khai thác yêu cầu dữ liệu từ bộ lưu trữ đám mây và gửi nó cho người yêu cầu, hoặc gửi chỉ số khối cuối cùng và băm cho người yêu cầu. Người yêu cầu đọc toàn bộ dữ liệu được lưu trữ bởi thiết bị trên đám mây và là người duy nhất. Nếu không, quyền riêng tư của người dùng có thể bị đe dọa bởi cuộc tấn công liên kết. Bằng cách nhận một giao dịch giám sát, thợ đào sẽ gửi dữ liệu hiện tại của thiết bị được yêu cầu cho người yêu cầu. Nếu một người yêu cầu được phép nhận dữ liệu trong một khoảng thời gian sau đó thì thợ đào gửi dữ liệu định kỳ cho đến khi người yêu cầu gửi kết thúc yêu cầu đến thợ đào và xóa giao dịch. Giao dịch giám sát cho phép chủ sở hữu nhà để xem camera hoặc các thiết bị khác trong quá trình gửi dữ liệu định kỳ. Để tránh chi phí hoặc các cuộc tấn công có thể xảy ra, chủ sở hữu nên xác định ngưỡng thời gian cho quá trình gửi dữ liệu định kỳ. Nếu thời gian thợ đào đang gửi dữ liệu cho người yêu cầu đạt đến ngưỡng, kết nối bị chấm dứt bởi thợ đào.

(4) Lớp phủ chia sẻ : Khi một cá nhân có nhiều hơn một nhà, anh ta cần khai thác riêng và lưu trữ cho mỗi ngôi nhà. Giảm chi phí và quản lý mào đầu trong trường hợp này, mạng phủ chia sẻ được xác định. Lớp phủ được chia sẻ bao gồm ít

nhất hai ngôi nhà thông minh được quản lý tập trung như một nhà của một thợ mỏ chia sẻ. Lớp phủ được chia sẻ tương tự như nhà thông minh, tuy nhiên, cấu trúc của BC được chia sẻ là khác với nhà thông minh. Trong BC được chia sẻ mỗi nhà có một *giao dịch genesis* và *giao dịch genesis* của tất cả các thiết bị được kết nối với *giao dịch genesis* nhà của họ bởi sự chia sẻ thợ đào lớp phủ. Một sự khác biệt trong lớp phủ chia sẻ liên quan đến thông tin liên lạc giữa các ngôi nhà với thợ đào. Các thiết bị ở cùng nhà với thợ đào không thay đổi, trong khi đối với các thiết bị ở nhà khác kết nối mạng riêng ảo (VPN) được thiết lập giữa cổng Internet ở mỗi nhà và thợ đào của mạng phủ chia sẻ định tuyến các gói đến thợ đào chia sẻ.

Quản lý điều khiển truy nhập cho Smarthome tích hợp BC:

(1) Khách truy cập được yêu cầu liệt kê cấp độ truy cập của mình và khởi tạo yêu cầu đến máy tính phục vụ tại nhà. Ví dụ, người quản lý được sự cho phép ở cấp cao nhất (quản trị viên) trong khi thanh thiếu niên, trẻ em, thăm gia đình và người giữ trẻ ở mức trung bình. Hàng xóm hoặc người lạ có quyền truy cập cấp thấp (mức zezo).

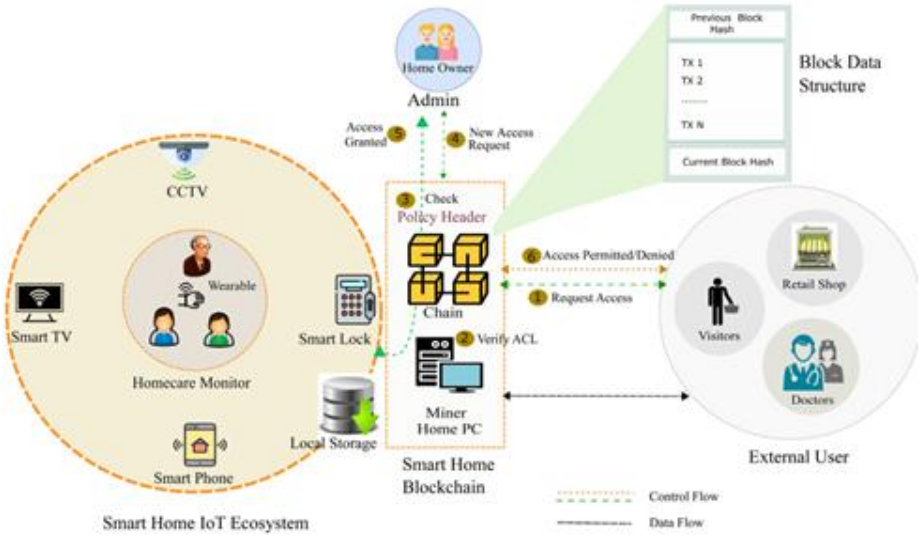
(2) Khi nhận được yêu cầu của khách truy cập, máy chủ gia đình sẽ xác minh danh sách kiểm soát truy cập (ACL). Sau đó, máy chủ chuyển tiếp yêu cầu này đến Blockchain để xác minh chính sách của người dùng cụ thể đó.

(3) Tiêu đề chính sách của một Blockchain lưu trữ ACL cho những người dùng và thiết bị khác nhau. Tiêu đề chính sách là một phần của dữ liệu khối được sử dụng để thực hiện chính sách kiểm soát và xác thực các thiết bị .

(4) Yêu cầu nhận được từ người dùng mới được chuyển đến quản trị viên có thể xác thực hoặc từ chối mọi yêu cầu truy cập.

(5) Sau khi quản trị viên cấp quyền truy cập, nút đào Blockchain sẽ chèn thông tin vào tiêu đề chính sách và thực hiện các hành động.

(6) Khách truy cập được phép truy cập và thực hiện các hành động theo các quy tắc được triển khai trong ACL.



Hình 3. 7: Mô hình cơ bản cho truy cập người dùng BC

3.3.4 Yêu cầu bảo mật đối với mô hình Blockchain-Smarthome

Yêu cầu đối với một hệ thống an toàn là phải nhận dạng, xác thực chính xác người sử dụng. Xác thực là một trong ba yêu cầu bảo vệ: 3A (*Authentication - Authorization - Authentication*). Các phương thức xác thực chính gồm: mật khẩu (*Password*), CHAP, Kerberos, 2 yếu tố (2FA- *Two factor Authentication*), mật khẩu dùng một lần (OTP-*One Time Password*), thẻ từ (*Tokens*), sinh trắc học (*Biometrics*), xác thực đa nhân tố (MultiFactor Authentication), xác thực lẫn nhau (*Mutual Authentication*).

Tính bảo mật (*Confidentiality*): Tính bảo mật là đặc tính thông tin không bị tiết lộ cho các thực thể hay quá trình không được ủy quyền biết hoặc không để cho các đối tượng đó lợi dụng. Dữ liệu được phân thành các cấp độ bảo mật khác nhau để bảo đảm rằng chỉ người dùng được cấp phép mới có thể truy cập vào thông tin nhằm ngăn chặn truy nhập bất hợp pháp và thông tin được tiết lộ dựa trên sự phân loại, mã hóa thông tin. Mô hình đề xuất sử dụng mật mã đối xứng để đạt được yêu cầu này.

Tính toàn vẹn (*Integrity*): Dữ liệu và thông tin cần được đảm bảo không bị sửa chữa bởi những người dùng trái phép khi chưa được ủy quyền. Dữ liệu phải đảm bảo tính nhất quán, xác thực và không bị giả mạo. Mỗi người dùng chỉ thấy được sự thay đổi của mình và những cam kết của những người dùng khác thông qua

xác thực các dữ liệu cảm biến. Mô hình đề xuất sử dụng hàm băm để đạt được yêu cầu này.

Tính xác thực (*Authentication/Authorization*): Kiểm tra tính xác thực của một thực thể giao tiếp trong thành phố thông minh. Một thực thể có thể là một người dùng, một chương trình máy tính, hoặc một thiết bị phần cứng. Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật. Hệ thống luôn sẵn sàng sử dụng cho người được uỷ quyền và chứng thực. Mô hình đề xuất sử dụng tiêu đề chính sách và khóa chia sẻ để đạt được yêu cầu này.

Bảng 3.1: Hiệu năng của mô hình đề xuất

Yêu cầu	Cách đánh giá
Bảo mật	Đạt được bằng cách sử dụng mã hóa đối xứng
Độ khả dụng	Hạn chế thành công các giao dịch được chấp nhận bởi các thiết bị và người khai thác
Tính toàn vẹn	Xác thực phân mảnh để kiểm tra tính toàn vẹn
Kiểm soát người dùng	Đạt được bằng cách giao dịch trong BC nội bộ
Ủy quyền	Đạt được bằng cách sử dụng khóa chia sẻ và tiêu đề chính sách.

Trong mô hình đề xuất để tăng tính sẵn sàng của thiết bị nhà thông minh được bảo vệ khỏi các yêu cầu độc hại, điều này đạt được bằng cách giới hạn các giao dịch được chấp nhận cho những giao dịch đó các thực thể mà mỗi thiết bị đã thiết lập một khóa chung. Giao dịch nhận được từ lớp phủ được xác thực bởi thợ đào trước khi chuyển tiếp chúng vào thiết bị. Hơn nữa, qua kết quả mô phỏng cho thấy nền tảng smarthome dựa trên BC đề xuất chỉ tăng một khoảng *delay* nhỏ do quá trình xử lý giao dịch và quá trình khởi tạo để tạo và phân phối khóa chia sẻ.

Ngoài ra mô hình đề xuất còn giảm thiểu tấn công DDOS và tấn công liên kết. Tấn công từ chối dịch vụ (DoS) là một hành động độc hại khiến máy chủ hoặc

tài nguyên mạng không khả dụng với người dùng, thông thường bằng cách gián đoạn tạm thời dịch vụ của một trạm kết nối Internet. Tấn công từ chối dịch vụ phân tán (DDoS), sử dụng rất nhiều thiết bị và kết nối Internet, thường phân tán toàn cầu. Do đó tấn công DDoS thường khó đối phó hơn, nạn nhân sẽ bị tấn công bởi yêu cầu từ hàng trăm đến hàng ngàn nguồn khác nhau. Chống tấn công từ chối dịch vụ: Nhanh chóng phát hiện và ứng cứu có thể ngăn chặn tấn công DoS. Thách thưc đầu tiên dành cho cơ chế bảo vệ DoS là phát hiện hiệu quả và nhanh chóng những lưu lượng đầu vào độc hại. Khi lưu lượng tấn công DoS đã được xác định, việc ứng cứu hiệu quả thường liên quan đến thiết lập một cơ sở hạ tầng mở rộng xử lý cuộc tấn công, đến khi nguồn tấn công được xác định và ngăn chặn. Tấn công DDoS không thể đề phòng từ trước, nhưng có rất nhiều công cụ tuyệt vời và hiệu quả giúp giảm thiểu tối đa ảnh hưởng của những cuộc tấn công như vậy.

Mô hình đề xuất có hệ thống phân cấp phòng thủ chống lại cuộc tấn công này. Cấp độ phòng thủ đầu tiên có thể được quy cho thực tế là không thể có kẻ tấn công trực tiếp cài đặt phần mềm độc hại trên các thiết bị nhà thông minh vì các thiết bị này là không thể truy cập trực tiếp. Tất cả các giao dịch phải được kiểm tra bởi thợ đào. Chúng ta hãy giả sử rằng kẻ tấn công bằng cách nào đó vẫn quản lý để lây nhiễm các thiết bị. Cấp độ thứ hai xuất phát từ thực tế là tất cả lưu lượng đi được xác thực bởi thợ đào bằng cách kiểm tra tiêu đề chính sách. Vì vậy các yêu cầu cấu thành lưu lượng tấn công DDoS sẽ không được xác thực, nó sẽ bị chặn. Hai lớp phòng thủ tiếp theo được thiết kế đặc biệt và được quản lý bởi mục tiêu tấn công DDOS có thể là bất kỳ người dùng nào trong lớp phủ. Các lớp phòng thủ, được cấp phép bằng cách sử dụng danh sách khóa CH và thay đổi PK trong danh sách khóa CH.

Tấn công liên kết: Để bảo vệ chống lại cuộc tấn công này, mỗi dữ liệu của thiết bị được chia sẻ và lưu trữ bởi một khóa duy nhất. Thợ đào tạo ra sổ cái duy nhất của dữ liệu trong bộ lưu trữ đám mây cho mỗi thiết bị sử dụng PK khác. Từ quan điểm lớp phủ, thợ đào sử dụng một khóa duy nhất cho mỗi giao dịch.

3.4 Mô phỏng đánh giá hiệu năng mô hình bảo mật Blockchain-Smarthome

3.4.1 Lựa chọn ngôn ngữ mô phỏng

Học viên dùng phần mềm mô phỏng Cooja chạy trên hệ điều hành Contiki 2.7 để đánh giá hiệu năng của mô hình Blockchain kết hợp Smarthome.

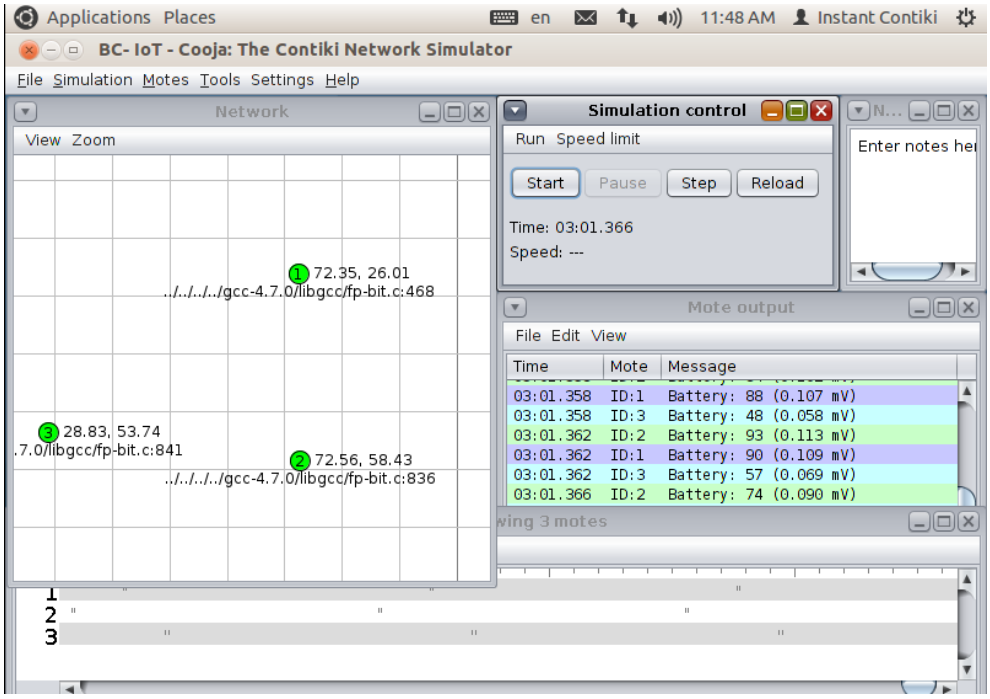
Hệ điều hành contiki là hệ điều hành mã nguồn mở, được nghiên cứu, thiết kế và phát triển bởi một nhóm các nhà phát triển từ viện khoa học máy tính Thụy Điển, người đứng đầu là Adam Dunkels. Nhóm phát triển Contiki gồm nhiều thành viên đến từ SICS, CISCO, cùng nhiều tổ chức và các trường đại học khác trên thế giới. Hệ điều hành Contiki được thiết kế cho các vi điều khiển có bộ nhớ nhỏ, với thông số 2KB RAM và 40KB ROM. Nhờ đó, Contiki được sử dụng cho các hệ thống nhúng và các ứng dụng trong mạng cảm biến không dây. Phiên bản hiện nay của Contiki là 2.4, với nhiều thay đổi, bổ sung và phát triển vượt bậc. Trong thực tế, Contiki đã được ứng dụng trong nhiều dự án như giám sát đường hầm xe lửa, theo dõi nước trong biển Baltic… Nhiều cơ chế, ý tưởng trong Contiki đã được ứng dụng rộng rãi trong công nghiệp. Điển hình như mô hình uIP được phát hành năm 2001 đã được sử dụng trong hệ thống ứng dụng của hàng trăm công ty trong các lĩnh vực hàng hải, thông tin vệ tinh, khai thác dầu mỏ,…; mô hình Protothreads được công bố lần đầu tiên năm 2005, đến nay đã được sử dụng trong nhiều ứng dụng như bộ giải mã kỹ thuật số và thiết bị cảm biến rung không dây. Hệ điều hành Contiki được lập trình bằng ngôn ngữ C, hoạt động dựa trên cơ chế event - driven và có những đặc điểm phù hợp với các hệ thống nhúng và mạng cảm biến không dây:

- Contiki được chia thành nhiều modul hoạt động độc lập. Nhờ đó các ứng dụng có thể sử dụng các modul một cách linh động và chỉ load những modul cần thiết.
- Cơ chế hoạt động điều khiển sự kiện làm giảm năng lượng tiêu hao và hạn chế dung lượng bộ nhớ cần sử dụng.
- Có thể sử dụng IP trong mạng cảm biến thông qua uIP stack được xây dựng dựa trên nền TCP/IP.

- Có những modul cho phép ước lượng và quản lý năng lượng một cách hiệu quả.
- Các giao thức tương tác giữa các lớp và các node trong mạng dễ dàng hơn.
- Sử dụng RIME stack phục vụ các giao thức dành cho mạng năng lượng thấp một cách hiệu quả.

Bên cạnh đó, Contiki còn cung cấp những công cụ hỗ trợ mô phỏng với giao diện đơn giản, dễ sử dụng và hỗ trợ tốt những thiết bị trong thực tế, phục vụ những mục đích nghiên cứu, mô phỏng và triển khai những giao thức mới.

Cooja là phần mềm mô phỏng hệ thống mạng được tích hợp trong hệ điều hành Contiki. Công cụ này cho phép người sử dụng thay đổi các thông số như vị trí, phạm vi kết nối, tỉ lệ truyền gói thành công… Nhờ đó người sử dụng có thể mô phỏng và đánh giá kết quả một cách hiệu quả hơn. Giao diện của chương trình thân thiện và dễ sử dụng, với một màn hình cho phép hiển thị các quá trình hoạt động của nút, có khả năng thay đổi vị trí, phạm vi phủ sóng của mỗi nút. Bên cạnh đó Cooja cung cấp một số các cửa sổ theo dõi sự kiện như Log listener, Radio listener cho phép người sử dụng tìm kiếm những sự kiện theo một số thông số nhất định, theo dõi sự giao tiếp giữa một số node cụ thể, ….Có thể nói, đây là một công cụ mô phỏng khá trực quan và dễ sử dụng, phục vụ tốt cho quá trình nghiên cứu, mô phỏng, đánh giá.



Hình 3. 8: sử dụng Cooja mô phỏng hệ thống với 3 nút cảm biến

3.4.2 Kịch bản mô phỏng

Qua phân tích lý thuyết cho thấy mô hình đề xuất cải thiện bảo mật và tính riêng tư tuy nhiên chi phí tính toán và mào đầu gói tin trên các thiết bị nhà thông minh và nút đào cũng là vấn đề cần quan tâm. Tuy nhiên qua mô phỏng sử dụng Cooja cho thấy chi phí cũng không đáng kể so với các hệ thống *Smarthome* đang triển khai. Để so sánh chi phí hoạt động của kiến trúc kết hợp Blockchain, học viên đã mô phỏng một kịch bản khác xử lý các giao dịch mà không cần mã hóa, băm (base method) và BC. Mô phỏng sử dụng IPv6 LoWPAN là giao thức truyền thông cơ bản.

Mô phỏng ba cảm biến z1 (bắt chước thiết bị thông minh gia đình) gửi dữ liệu trực tiếp đến nút đào tại nhà cứ sau 10 giây, mỗi mô phỏng kéo dài trong 3 phút. Lưu trữ đám mây được kết nối trực tiếp với nút đào để lưu trữ dữ liệu và trả về số khối. Để cung cấp một cách toàn diện đánh giá học viên mô phỏng *giao dịch truy cập và giao dịch lưu trữ*. Đối với *giao dịch lưu trữ* mô phỏng hai lưu lượng khác nhau:

- Định kỳ: Trong cài đặt này, các thiết bị định kỳ gửi dữ liệu vào bộ lưu trữ đám mây.

- Dựa trên truy vấn: Ở đây, thiết bị sẽ gửi dữ liệu theo yêu cầu và để đáp lại một truy vấn nhận được từ người khai thác.

Các tham số đánh giá:

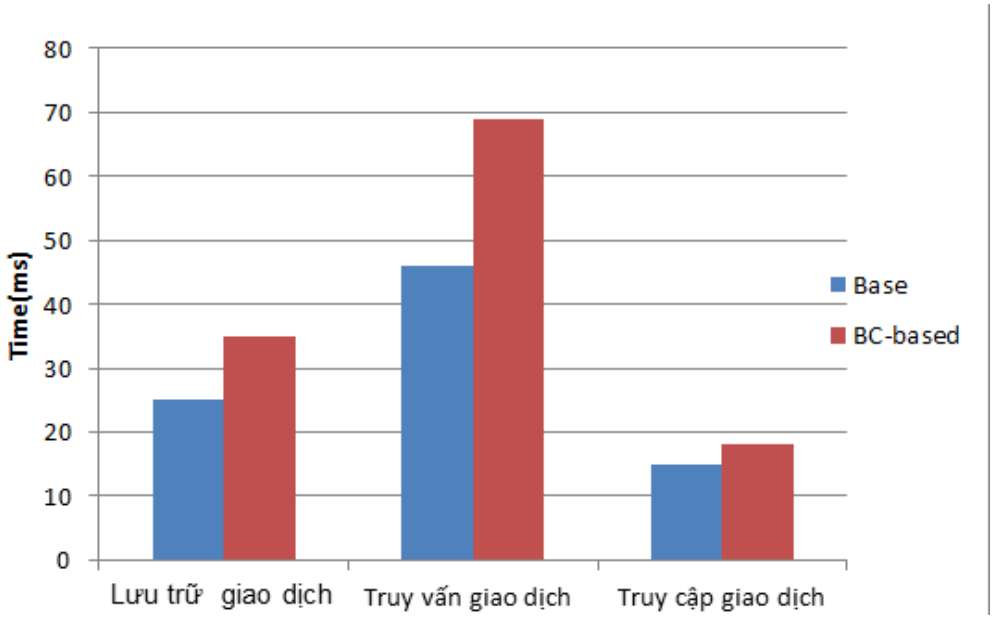
- Tiêu đề gói tin: Đề cập đến độ dài gói truyền.
- Chi phí thời gian: Đề cập đến thời gian xử lý cho mỗi giao dịch tại nút đào và được đo từ khi nhận giao dịch tại nút đào cho đến khi phản hồi thích hợp được gửi đến người yêu cầu.
- Tiêu thụ năng lượng: Đề cập đến năng lượng tiêu thụ bởi nút đào để xử lý các giao dịch. Nút đào là thiết bị tiêu thụ năng lượng cao nhất trong nhà thông minh kể từ khi nó xử lý tất cả các giao dịch và thực hiện hàm băm và mã hóa. Tiêu thụ năng lượng của các thiết bị khác được giới hạn mã hóa cho các giao dịch của riêng họ.

3.4.3 Đánh giá kết quả

Kết quả mô phỏng cho thấy chi phí phải trả cho phần tiêu đề gói từ thiết bị đến thợ đào, từ thợ đào đến đám mây và từ đám mây đến thợ đào tăng không đáng kể so với mô hình Base

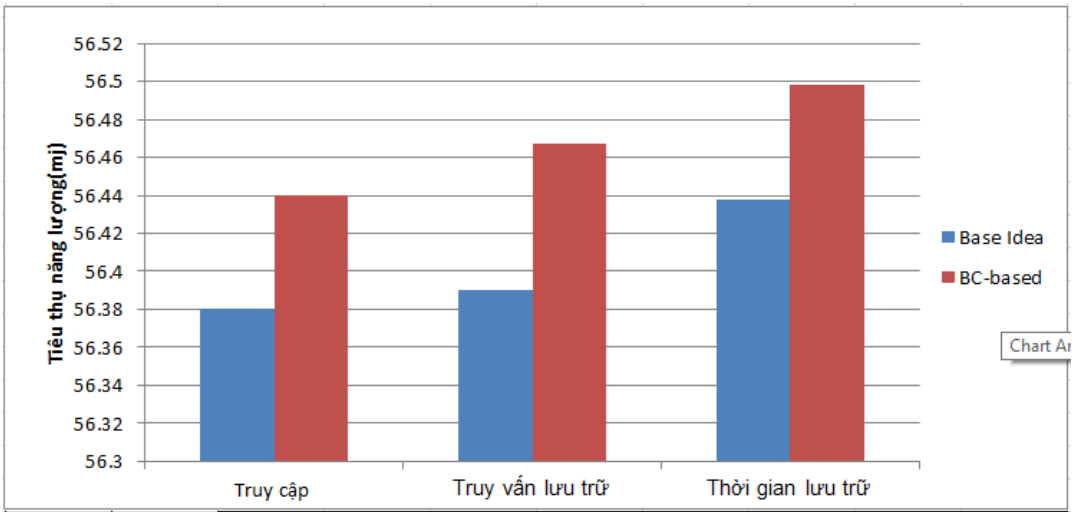
Bảng 3.2 Tiêu đề gói tin mô hình dựa trên BC - Smart home

Lưu lượng gói	Mô hình cơ bản Base (Bytes)	Kết hợp BC (Bytes)
Từ thiết bị đến thợ đào	5	16
Từ thợ đào đến đám mây	5	36
Từ đám mây đến thợ đào	5	16



Hình 3. 9: Thời gian xử lý các giao dịch mô hình BC – Smart home

Kết quả hình 3.9 cho thấy chi phí thời gian xử lý các giao dịch lưu trữ và truy nhập của BC so với mô hình Base tăng tương đối nhỏ.



	CPU	Tx	Lx	CPU	Tx	Lx	CPU	Tx	Lx
Base Idea	0.0103	0.0102	56.3489	0.0117	0.0357	56.3393	0.0121	0.0549	56.3645
BC-based	0.0127	0.0834	56.3496	0.0132	0.1106	56.3379	0.0133	0.1166	56.3657

Hình 3. 10: Đánh giá độ tiêu thụ năng lượng mô hình BC – Smart home

Kết quả hình 3.10 cho thấy tiêu thụ năng lượng của mô hình dựa trên BC tăng rất ít, phương pháp BC làm tăng tiêu thụ năng lượng bằng 0,07 (mj).

3.5 Kết luận chương III

Nội dung chương 3 đề xuất kiến trúc IoT smart home kết hợp BC bao gồm 4 lớp: Lớp smart home, Lớp mạng BC, Lớp cloud computing và lớp dịch vụ. Mô hình

đề xuất hạn chế thành công các giao dịch được chấp nhận bởi các thiết bị và người khai thác để tăng độ khả dụng của hệ thống. Ngoài ra mô hình sử dụng mã hóa đối xứng, hàm băm, chữ ký số để đạt được tính năng bảo mật. Để mở rộng hệ thống mô hình đề xuất đã đưa vào giải thuật bầu chọn chủ cụm cho mạng ngang hàng phân cấp. Chi phí phải trả là trễ, năng lượng tiêu thụ, mào đầu gói tin cũng được phân tích chi tiết qua phần mềm giả lập Cooja, tuy nhiên chi phí phải trả cũng không đáng kể so với mô hình Smarthome hiện đang triển khai.

KẾT LUẬN

Kết quả đạt được

Luận Văn nghiên cứu về công nghệ IoT thông quá các khái niệm, các ứng dụng của IoT cùng với việc phân tích cấu trúc từng lớp trong IoT để đưa ra một cái nhìn toàn diện nhất về IoT.

Bên cạnh đó luận văn cũng phân tích và chỉ ra các thách thức trong bảo mật IoT, các lỗ hổng bảo mật của từng lớp trong cấu trúc phân lớp IoT và các cách thức tấn công bảo mật cụ thể. Thông qua đó đưa ra các giải pháp bảo mật hiệu quả.

Luận văn đã ứng dụng lý thuyết về IoT và Blockchain xây dựng mô hình phân lớp ứng dụng BC trong bảo mật IoT smart home, nhà thông minh trong mô hình đề xuất đạt được tính bảo mật, tính toàn vẹn, tính sẵn sàng và phòng ngừa các cuộc tấn công bảo mật quan trọng như tấn công liên kết, tấn công từ chối dịch vụ phân tán (DDOS). Phần kết quả mô phỏng chỉ ra chi phí để đạt được các kết quả bảo mật là tương đối nhỏ.

Hướng phát triển của đề tài

Tuy nhiên khi kết hợp BC vào IoT còn có một số các vấn đề cần quan tâm nghiên cứu: mào đầu gói tin khi kết nối một khối vào chuỗi khối, thời gian trễ khi xử lý của các giải thuật đồng thuận, mã hóa, hàm băm, năng lượng tiêu tốn của các

nút. Đây cũng là các hướng nghiên cứu tiếp theo để cải thiện hiệu năng của mô hình bảo mật liên kết BC và IoT smarthome.

DANH MỤC TÀI LIỆU THAM KHẢO

[1]Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G.,... & Zanichelli, F. (2018, April). IoTChain: A Blockchain security architecture for the Internet of Things. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE.

[2]Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A Blockchain future for internet of things security: A position paper. *Digital Communications and Networks*, *4*(3), 149-160.

[3]Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized Blockchain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 173-178). ACM.

[4]Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

[5]Khan, M. A., & Salah, K. (2018). IoT security: Review, Blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

[6]Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of Blockchain systems. *Future Generation Computer Systems*.

[7]Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173-190.

[8]Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650-655.

[9] Stogner, L. (2015, June). An Introduction to the Internet of Things from the perspective of the IEEE Internet of Things initiative. In 2015 International Conference on Collaboration Technologies and Systems (CTS) (pp. 506-506). IEEE.

[10] Gil, D., Ferrández, A., Mora-Mora, H., & Peral, J. (2016). Internet of things: A review of surveys based on context aware intelligent services. Sensors, 16(7), 1069.

[11]https://www.juniperresearch.com/researchstore/devices-technologies/the-internet-of-things

Các website tham khảo:

1. https://tools.ietf.org/html/rfc6347
2. https://www.marketsandmarkets.com/internet-of-things-and-m2m-market-research-262.html