HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thành Duy

ỨNG DỤNG BLOCKCHAIN TRONG BẢO MẬT IOT

Chuyên ngành : KỸ THUẬT VIỄN THÔNG
Mã số: 8.52.02.08

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

TS.VŨ THỊ THÚY HÀ

Phản biện 1: PGS.TS. Nguyễn Hữu Trung

Phản biện 2: TS. Hồ Văn Canh

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông:

Vào lúc: 08 giờ 30 ngày 20 tháng 06 năm 2020

Có thể tìm hiểu luận văn tại:

1. Thư viện Học viện Công nghệ Bưu chính Viễn thông

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.

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 cần các dịch vụ đám mây 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. Đã có rất nhiều công ty lớn làm việc về vấn đề này, chẳng hạn như IBM Watson của IBM, Nền tảng Google Cloud của Google, Azure và Oracle Cloud Oracle, v.v…ARM Mbed cũng đang phát triển đám mây của riêng mình, nhưng hiện tại nó chỉ dành cho đối tượng là các nhóm các công ty công nghiệp đi đầu được chọn.

1.3 Mô hình kiến trúc của IoT

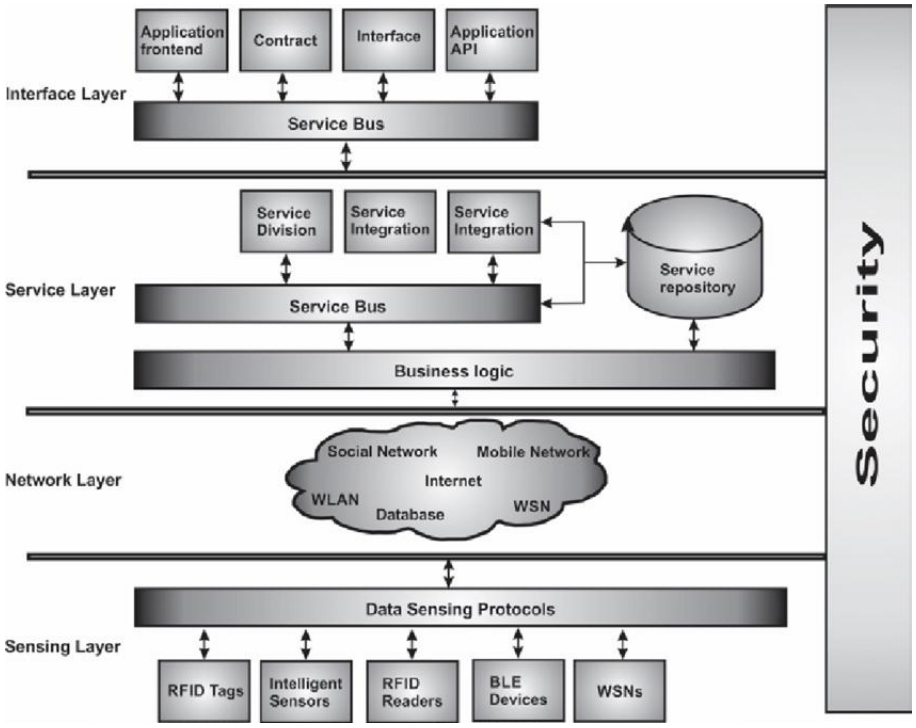
Kiến trúc hệ thống phải cung cấp đảm bảo hoạt động cho IoT, nó là cầu nối khoảng cách giữa các thiết bị vật lý và thế giới ảo. Khi thiết kế, kiến trúc IoT cần xem xét các yếu tố sau: (1) Các yếu tố kỹ thuật, như kỹ thuật cảm biến, phương thức truyền thông, công nghệ mạng, v.v.; (2) Đảm bảo an ninh, như 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.

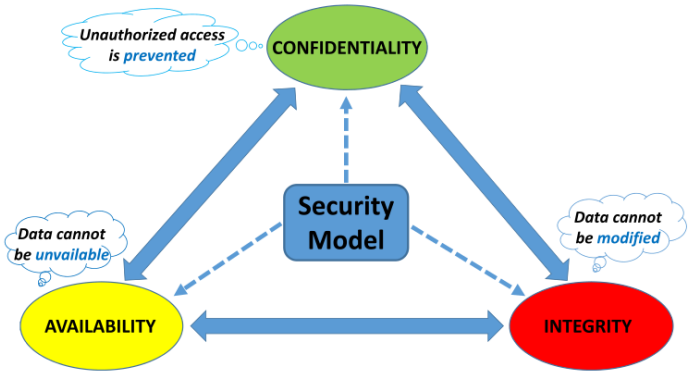
Lớp ứng dụng – giao diện bao gồm các phương thức tương tác với người dùng hoặc ứng dụng.



*Hình 1.*1: SoA cho IoT

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 1.2: 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.

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.

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.

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.

2.2 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.

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.

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.

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 khắn 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.

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

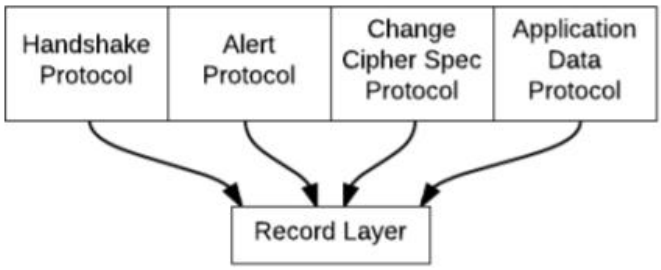
Lý do TLS không thể được sử dụng trong môi trường datagram chỉ đơn giản là các gói có thể bị mất hoặc sắp xếp lại. TLS không có khả năng xử lý loại không đáng tin cậy này; do đó, việc triển khai TLS gặp khó khăn.

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).



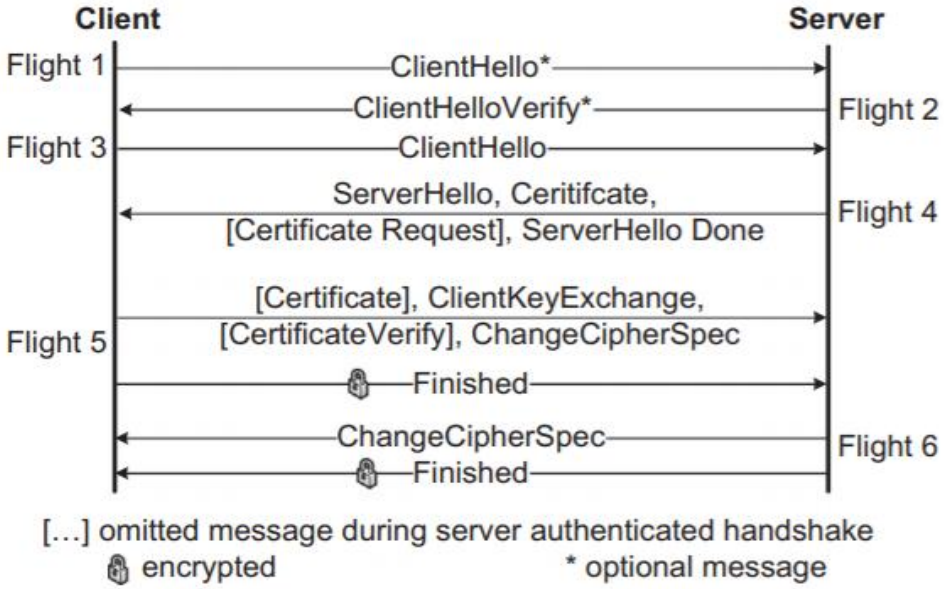
Hình 2. 1: Các giao thức con của DTLS

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. 2*:* Cấu trúc lớp bản ghi DTLS

2.4.1.2 Giao thức bắt tay DTLS



Hình 2. 3: Giao thức bắt tay DTLS được xác thực đầy đủ

Hình 2.10 cho thấy bắt tay DTLS được xác thực đầy đủ

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. 4:*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

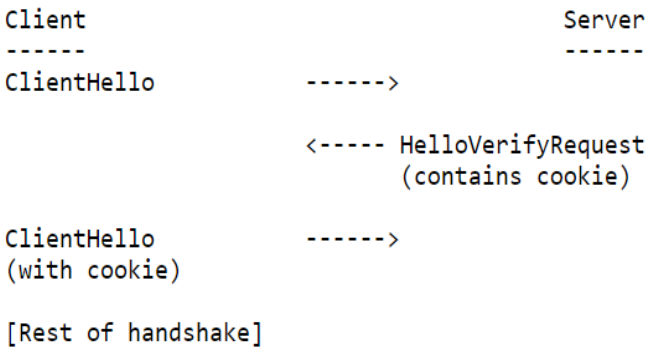
- Fragment: giống với bản ghi TLS

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. 5: 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. 6: 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. 7: Cấu trúc của bản tin HelloVerifyRequest

2.4.2 Ứng dụng bảo mật bằng Blockchain

2.4.2.1 Công nghệ Blockchain

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.

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

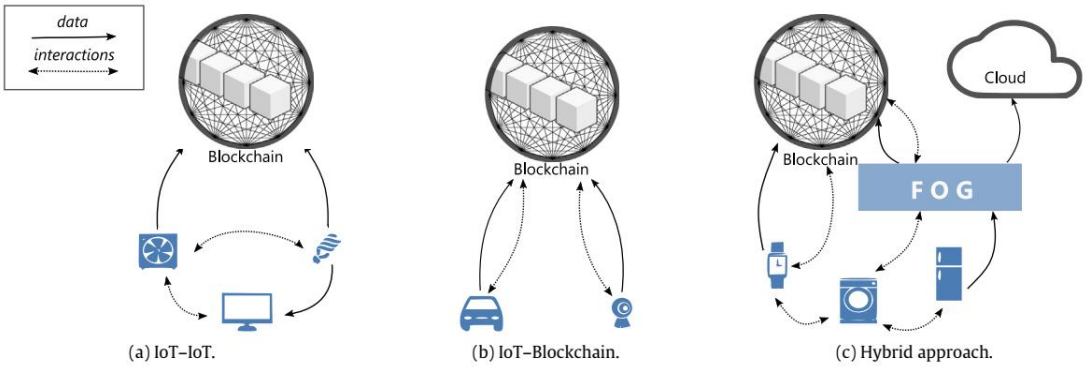
cách mở ra một cuộc cách mạng thanh toán điện tử, nền tảng công nghệ cơ bản này là nhân tố đứng đằng sau sự thành công và gia tăng của tiền điện tử.

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. Theo cách tiếp cận này điện toán đám mây sẽ phát triển mạnh mẽ để bổ sung cho những hạn chế của Blockchain và IoT (hình 2.22c).



Hình 2. 8: 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.

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

"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.

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.

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.

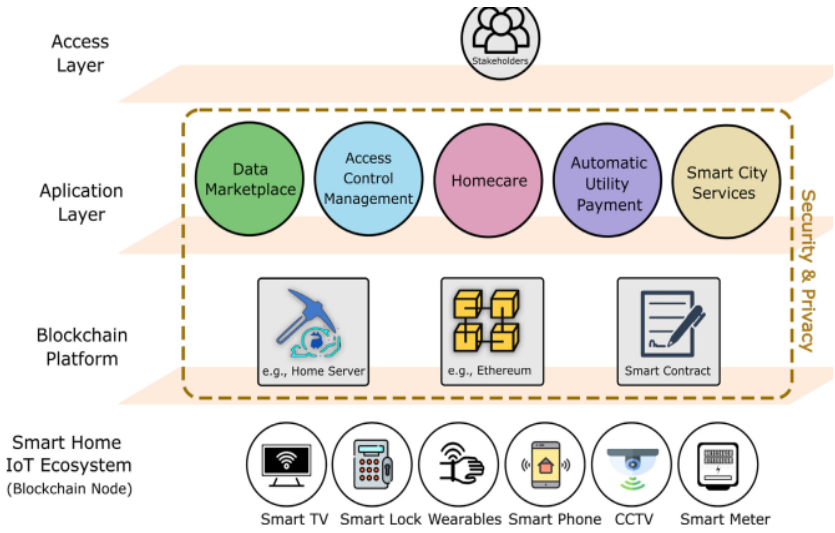
Tính sẵn sàng và độ tin cậy: Tính động và thích ứng được yêu cầu để quản lý và giám sát cơ sở hạ tầng IoT trong chế độ tự quản lý. Điều này sẽ cho phép một giải pháp bền vững cho tính khả dụng và độ tin cậy cho kết nối động và mạnh mẽ.

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.

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.

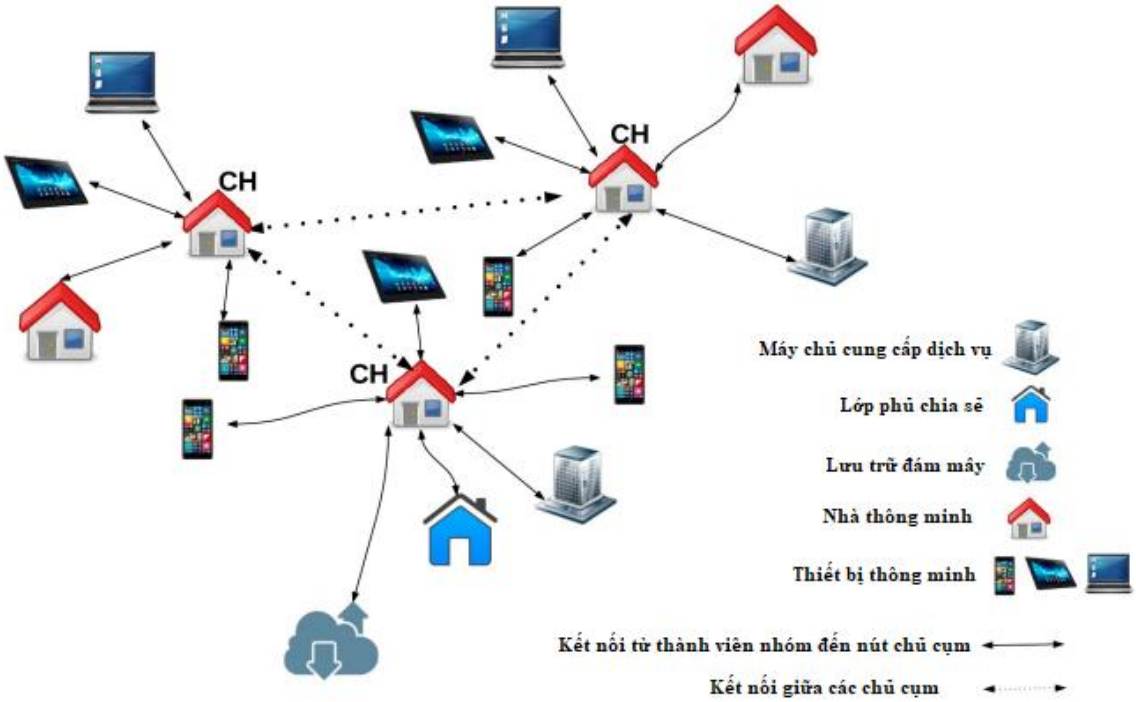


Hình 3. 1: Mô hình phân lớp Blockchain –Smarthome [6]

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. 2: 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.

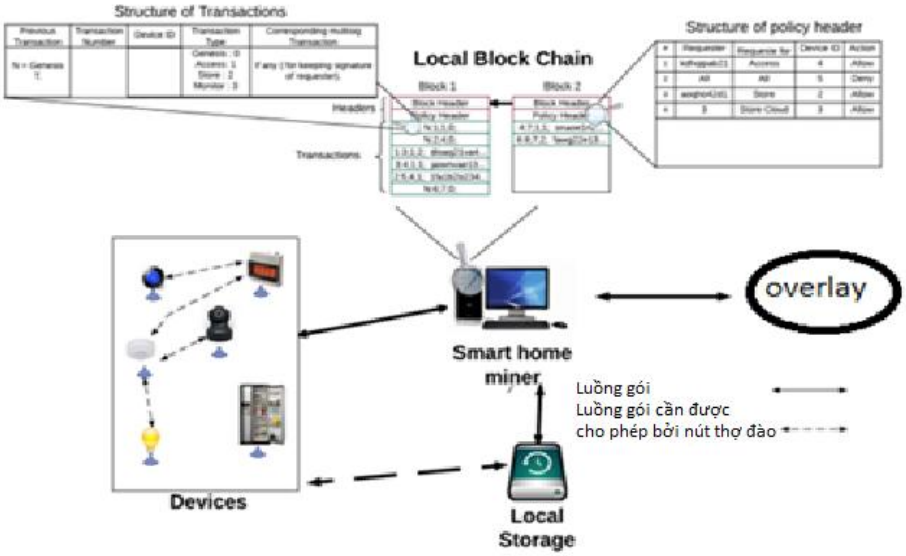
Pha 3: Sáp nhập các cụm có hệ số kết nối cao

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.

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

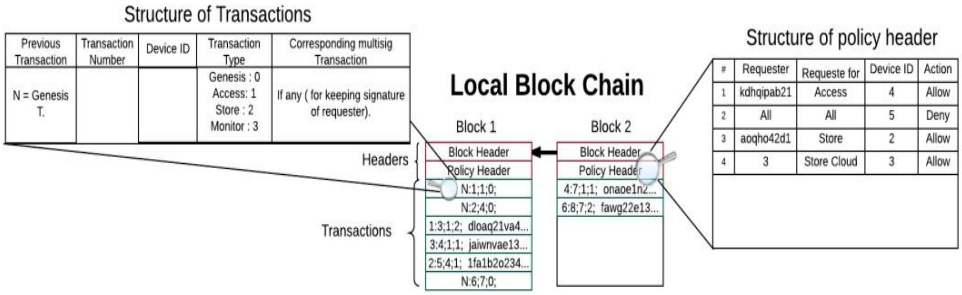


Hình 3. 3: Mô hình nhà thông minh tích hợp Blockchain

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.

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.

) 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. 4: 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.

3.3.4 Phân tích hiệu năng

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.

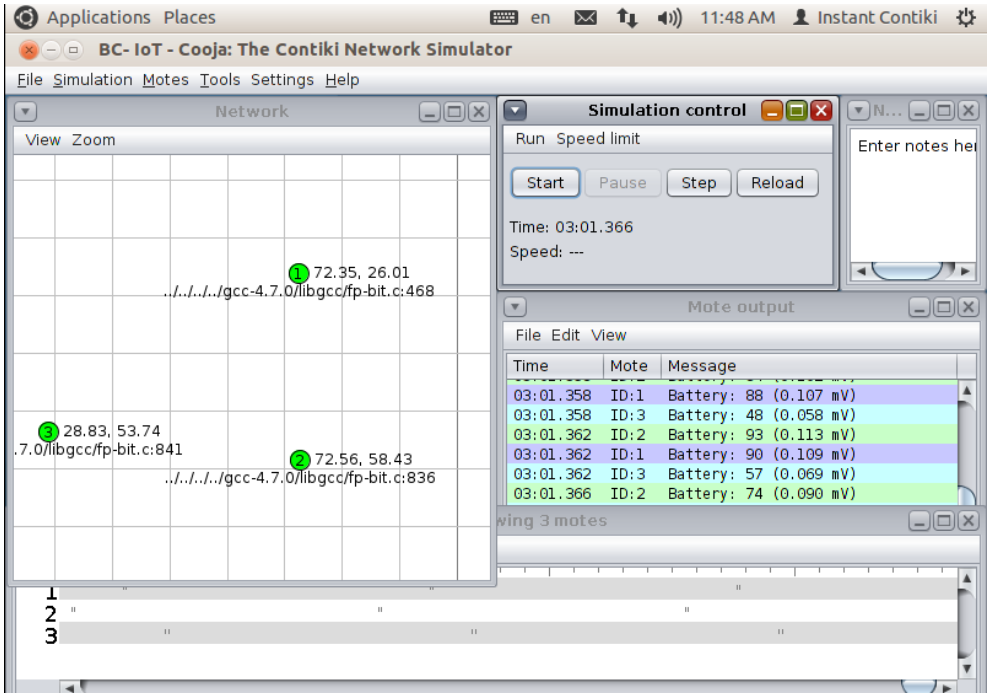
Ngoài ra mô hình đề xuất còn giảm thiểu tấn công DDOS và tấn công liên kết. Tấn công từ chối dịch vụ (DoS) là một hành động độc hại khiến máy chủ hoặc tài nguyên mạng không khả dụng với người dùng, thông thường bằng cách gián đoạn tạm thời dịch vụ của một trạm kết nối Internet. Tấn công từ chối dịch 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 thức 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.

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.



Hình 3. 5: 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:

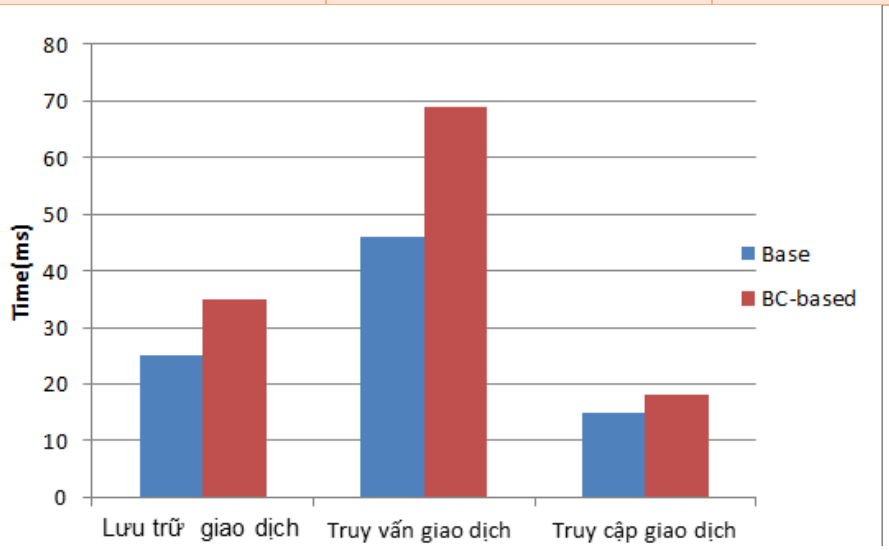
- Tiêu đề gói tin: Đề cập đến độ dài gói truyền.
- Chi phí thời gian: Đề cập đến thời gian xử lý cho mỗi giao dịch tại nút đào và được đo từ khi nhận giao dịch tại nút đào cho đến khi phản hồi thích hợp được gửi đến người yêu cầu.
- Tiêu thụ năng lượng: Đề cập đến năng lượng tiêu thụ bởi nút đào để xử 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

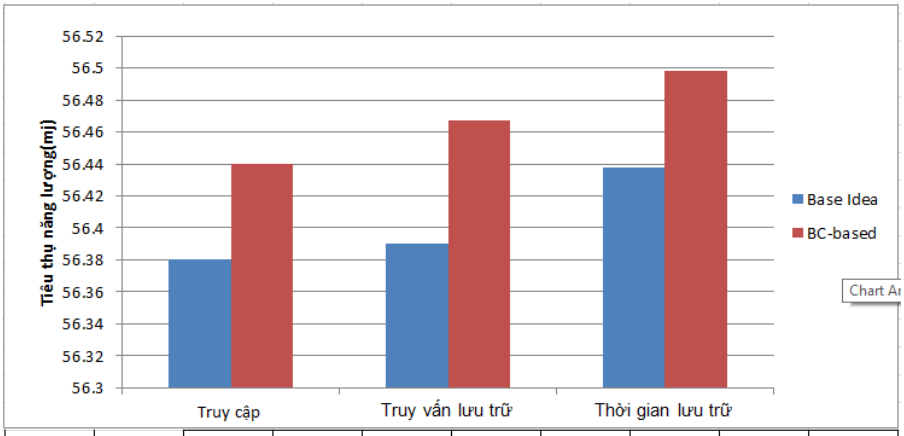
Bảng 3.2 Tiêu đề gói tin mô hình dựa trên BC - Smart home

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. 6: 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. 7: 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.

IV. 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