ỨNG DỤNG BLOCKCHAIN TRONG BẢO MẬT IOT

Vũ Thị Thúy Hà
Học Viện Công Nghệ Bưu chính Viễn thông

Tóm tắt – Bảo mật và quyền riêng tư của Internet of Things (IoT) vẫn là một thách thức lớn, chủ yếu là do quy mô lớn và bản chất phân tán của mạng IoT. Các thiết bị IoT thường có thể can thiệp trực tiếp vào hoạt động, môi trường sống của con người , 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. Công nghệ Blockchain (BC) ra đời nhằm tăng cường cho các nền tảng an ninh mạng để nâng cao tính bảo mật và an toàn cho các hệ thống truy cập IoT [1-6].

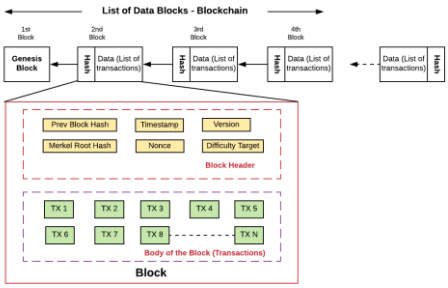
Bài báo ứng dụng lý thuyết về IoT và BC xây dựng mô hình kết hợp BC trong bảo mật Smart home, nhà thông minh trong mô hình đưa ra đạt được tính bảo mật, tính toàn vẹn, tính sẵn sàng, khả năng mở rộng và phòng ngừa các cuộc tấn công bảo mật quan trọng như tấn công liên kết, tấn công từ chối dịch vụ phân tán. Phần kết quả mô phỏng chỉ ra chi phí để đạt được các kết quả bảo mật là tương đối nhỏ.

Từ khóa – Kiểm soát truy cập (ACL), chuỗi khối (BC), nút chủ cụm (CH), từ chối dịch vụ phân tán (DDOS), vào trước ra trước (FIFO), khóa công khai (PK), ngang hàng (P2P), internet vạn vật (IoT), định danh (ID).

I. ĐẶT VẤN ĐỀ

Cách mạng công nghiệp 4.0 mà nền tảng là IoT dựa trên sự phát triển vượt bậc của công nghệ thông tin truyền thông, đang mang đến xu thế phát triển như vũ bão cho nhiều ngành, lĩnh vực trong đời sống xã hội hiện nay và tương lai. 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. 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 [1]. 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. 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.

Tất cả các mạng IoT hiện tại và mạng IoT mới đều phải đối mặt với nguy cơ đe dọa mạng rất cao. 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. Qua phân tích các hướng nghiên cứu về bảo mật IoT đều cho thấy giải pháp kết hợp BC và IoT có những ưu điểm vượt trội [1-8]. 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 BC. Vì thế, càng có nhiều đối tượng tham gia, thì hệ thống BC càng mạnh, tính bảo mật càng cao. Tuy nhiên do BC có một số các đặc tính không phù hợp với các thiết bị IoT có mức năng lượng và khả năng xử lý thấp. Trong lĩnh vực IoT, rất nhiều ứng dụng nhạy cảm với thời gian. Dù chỉ một chút chậm trễ cũng có thể dẫn đến kết quả vô cùng tồi tệ. Ví dụ như các giải thuật đồng thuận phức tạp, thời gian xác nhận một giao dịch và số lượng giao dịch bị hạn chế được thực hiện trong 1 giây. Nên khi triển khai kết hợp BC vào IoT cũng cần phải điều chỉnh một số các đặc tính của BC để phù hợp với đặc tính của IoT [3].



Hình 1. Cấu trúc chuỗi khối BC

Nôi dung tiếp theo của bài báo phân tích mô hình lý thuyết IoT và BC, phân tích đánh giá hiệu năng mô hình bảo mật BC – Smarthome.

II. KHẢO SÁT CÁC MÔ HÌNH LÝ THUYẾT KẾT HỢP IOT VÀ BC

Công nghệ BC là một công nghệ mới cùng với IoT sẽ mang lại nhiều hứa hẹn trong việc giúp các thiết bị được kết nối an toàn [1-2]. 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 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 BC. Mỗi thiết bị được xác thực tham gia mạng IoT bảo mật dựa trên BC sẽ được coi là một thực thể tham gia, giống như trong mạng BC 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 đinh danh ID duy nhất trên hệ thống BC. 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.

Contact author: Vũ Thị Thúy Hà
Email: havvt@ptit.edu.vn
Manuscript received: 26/11/2021, revised: 9/12/2021, accepted: 30/3/2022.

Giải pháp an ninh mạng dựa trên BC 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 [1]. 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 BC 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 BC 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.

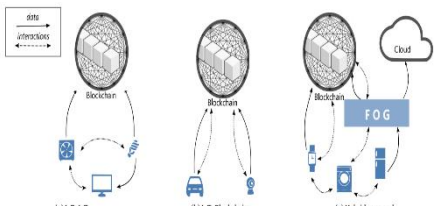
Cả BC và IoT đều là những công nghệ đang phát triển với hầu hết các đổi mới trong lĩnh vực này đều ở giai đoạn khởi đầu. Tuy nhiên, việc kết hợp các thế mạnh của công nghệ BC với tiềm năng của IoT có thể nhanh chóng và hiệu quả thúc đẩy toàn bộ các ngành công nghiệp, thành phố và quốc gia vào không gian "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 mà không cản trở tốc độ đổi mới.

Một số mô hình lý thuyết kết hợp IoT và BC

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 BC trong khi các giao dịch IoT diễn ra mà không sử dụng BC. 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

IoT – BC : Theo cách tiếp cận này, tất cả các tương tác đều đi qua BC, 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 BC, và hơn nữa nó làm tăng tính tự chủ của các thiết bị IoT. Tuy nhiên, ghi lại tất cả các tương tác trong BC sẽ liên quan đến việc tăng băng thông và dữ liệu. Đây là một trong các thách thức lớn của BC. Mặt khác, tất cả dữ liệu IoT được liên kết với các giao dịch này cũng được lưu trữ trong BC.

Các tiếp cận kết hợp: Thiết kế kết hợp trong đó chỉ một phần các tương tác và dữ liệu diễn ra trong BC 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 BC 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 BC vì nó tận dụng lợi ích của BC 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 BC và IoT

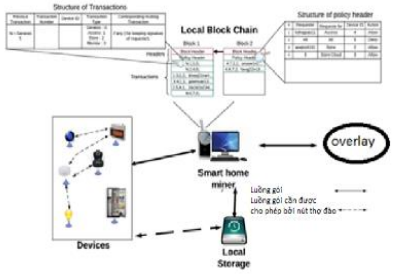


Hình 2. Mô hình lý thuyết bảo mật kết hợp IoT và BC [1]

III.XÂY DỰNG MÔ HÌNH BẢO MẬT BC - SMARTHOME

Mô hình bảo mật BC-Smarthome được phát triển dựa trên nghiên cứu [11], nó được xây dựng dựa trên cách tiếp cận kết hợp [1]. Để tăng khả năng mở rộng của mô hình, mạng chồng phủ ngang hàng được thiết kế phân cấp dựa trên nghiên cứu [12].

Mô hình nhà thông minh kết hợp BC bao gồm các thành phần chính: Nhà thông minh, lưu trữ đám mây và lớp phủ. Các thiết bị thông minh được đặt bên trong nhà thông minh và được quản lý tập trung bởi một "miner". Nhà thông minh tạo thành mạng lớp phủ cùng với nhà cung cấp dịch vụ, đám mây lưu trữ và người dùng điện thoại thông minh hoặc máy tính cá nhân



Hình 3. Mô hình bảo mật BC – Smarthome [11]

Lớp phủ là mạng ngang hàng P2P phân cấp [12]: 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 Public BC kết hợp với hai danh sách chính. Danh sách khóa của người yêu cầu là danh sách khóa công khai PK (Public key) của người dùng lớp mạng ngang hàng 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. Một nút với khả năng vượt trội sẽ được chọn để trở thành một nút chủ cụm CH. Các tham số đánh giá khả năng của nút bao gồm: Khả năng xử lý, thời gian online.

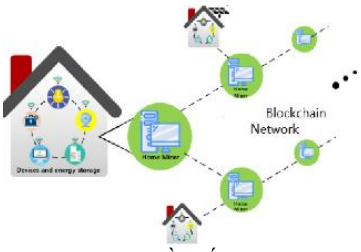
$$G = \sqrt{\frac{t_{on(p)}}{t_{on(CH)}} \frac{P_{(p)}}{P_{(CH)}}} \quad (1)$$

Trong đó $t_{on(p)}$, $P_{(p)}$ lần lượt là thời gian hoạt động trung bình của nút, khả năng xử lý CPU (MIPS Million Instruction Per Second) ; $t_{on(CH)}$, $P_{(CH)}$ lần lượt là các giá trị yêu cầu tối thiểu của các tham số đối với một nút CH, giá trị tham số được chọn tùy theo mục tiêu của từng dịch vụ triển khai.

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 Private BC để cung cấp kiểm soát truy cập an toàn cho thiết bị IoT và dữ liệu. Thiết kế bảo mật đến từ các tính năng bao gồm: (1) các thiết bị có thể

truy cập gián tiếp; (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.

Các thành phần cốt lõi của Smarthome



Hình 4. Các thành phần cốt lõi của Smarthome

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 bảo mật nhẹ được sử dụng để phát hiện bất kỳ thay đổi nào của nội dung giao dịch trong quá trình truyền tải [13]. Tất cả các giao dịch đến hoặc từ nhà thông minh được lưu trữ trong một *Private BC.*

Private BC: BC 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 có những hạn chế. Trong mỗi ngôi nhà thông minh, có một *Private BC* 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. 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.

Home miner: *"Miner"* là một nút trong nhà thông minh xử lý tập trung giao dịch đến và đi từ 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. *"Miner"* 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 "*miner"* hoặc nó có thể là một thiết bị riêng biệt. Bộ lưu trữ 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.

Hoạt động của mô hình BC - Smarthome

(1)Khởi tạo: Quá trình thêm thiết bị và tiêu đề chính sách cho *Private BC***.** Để thêm một thiết bị vào nhà thông minh, "*miner*" tạo ra một giao dịch *genesis* bằng cách chia sẻ một khóa với thiết bị sử dụng. Các khóa được chia sẻ giữa "*miner*" 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. "*Miner*" 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 "*miner*" đến các thiết bị cần liên lạc trực tiếp với nhau. Để phân bổ khóa, "*miner*" 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, "*miner*" 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: "*miner*" 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.

(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 "*miner*" và nếu nó có quyền lưu trữ, "*miner*" 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 "*miner*". Bằng cách nhận yêu cầu, "*miner*" ủy quyền cho thiết bị lưu trữ dữ liệu trên đám mây. Nếu thiết bị đã được ủy quyền, "*miner*" trích xuất số khối và hàm băm cuối cùng từ *Private BC* 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 "*miner*" 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 chủ nhà 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, "*miner*" 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, *"miner"* 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, "*miner*" 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, "*miner*" 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 "*miner*" gửi dữ liệu định kỳ cho đến khi người yêu cầu gửi kết thúc yêu cầu đến "*miner*" 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 "*miner*" đang gửi dữ liệu cho người yêu cầu đạt đến ngưỡng, kết nối bị chấm dứt bởi "*miner*".

Quản lý điều khiển truy nhập cho mô hình bảo mật BC - Smarthome :

(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, khách và người giữ trẻ ở mức trung bình. Hàng xóm hoặc người lạ có quyền truy cập cấp thấp (mức zezo).

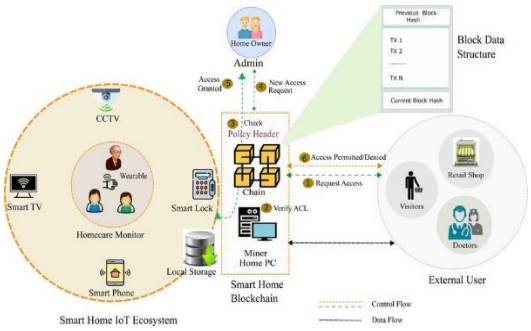
(2) Khi nhận được yêu cầu của khách truy cập, máy chủ gia đình sẽ xác minh danh sách kiểm soát truy cập (ACL). Sau đó, máy chủ chuyển tiếp yêu cầu này đến BC để xác minh chính sách của người dùng cụ thể đó.

(3) Tiêu đề chính sách của một BC 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, "*miner*" BC 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 5. Điều khiển truy nhập mô hình bảo mật BC - Smarthome

IV. PHÂN TÍCH, MÔ PHỎNG ĐÁNH GIÁ HIỆU NĂNG

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*). Phân tích mô hình bảo mật BC - Smarthome cho thấy mô hình đạt được một số các yêu cầu về hiệu năng.

Bảng 1: Hiệu năng của mô hình bảo mật BC - Smarthome

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.

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 Smarthome - BC sử dụng mật mã đối xứng để đạt được yêu cầu này.

Khả năng mở rộng: Do mạng phủ có cấu trúc phân cấp, các nút trong lớp phủ được nhóm thành các cụm và mỗi cụm bầu ra một nút chủ cụm (CH).

Tính toàn vẹn (*Integrity*): Dữ liệu và thông tin cần được đảm bảo không bị sửa chữa bởi những người dùng không 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 Smarthome - BC sử dụng hàm băm SHA3-256 để đạt được yêu cầu này [13].

Tính xác thực (*Authentication/Authorization*): Kiểm tra tính xác thực của một thực thể giao tiếp. 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 Smarthome – BC sử dụng tiêu đề chính sách và khóa chia sẻ để đạt được yêu cầu này.

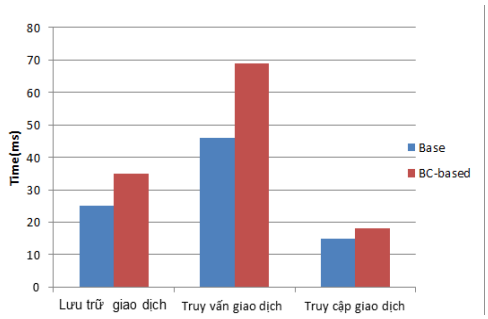
Tính khả dụng: Trong mô hình Smarthome - BC để tăng tính sẵn sàng của thiết bị nhà thông minh được bảo vệ khỏi các yêu cầu độc hại, điều này đạt được bằng cách giới hạn các giao dịch được chấp nhận cho những giao dịch đó các thực thể mà mỗi thiết bị đã thiết lập một khóa chung. Giao dịch nhận được từ lớp phủ được xác thực bởi *"miner"* trước khi chuyển tiếp chúng vào thiết bị.

Tấn công DDOS. Mô hình Smarthome - BC 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 *"miner"*. 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 *"miner"* 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. "Miner" 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,*"miner"* sử dụng một khóa duy nhất cho mỗi giao dịch.

Để so sánh chi phí hoạt động của mô hình bảo mật BC-Smarthome, mô phỏng sử dụng phần mềm Cooja chạy trên hệ điều hành Contiki OS, hệ điều hành chuyên để mô phỏng các thiết bị nhúng không dây [14]. Mô phỏng xây dựng kịch bản so sánh xử lý các giao dịch của mô hình không sử dụng mã hóa, hàm băm (base) và BC. Mô phỏng sử dụng IPv6 LoWPAN là giao thức truyền thông cơ bản. Mô phỏng 10 nút cảm biến, các nút sử dụng là Tmote Sky. Tham số được đánh giá thời gian xử lý cho mỗi giao dịch tại nút *"miner"* và được đo từ khi nhận giao dịch tại nút *"miner"* cho đến khi phản hồi thích hợp được gửi đến người yêu cầu. Kết quả mô phỏng cho thấy chi phí thời gian xử lý các giao dịch lưu trữ và truy nhập của BC so với mô hình không sử dụng BC, hàm băm, mã hóa (Base) tăng tương đối nhỏ.



Hình 4. Thời gian xử lý các giao dịch mô hình bảo mật BC - Smarthome

V. KẾT LUẬN

Bài báo phân tích và chỉ ra những thách thức trong bảo mật IoT, các lỗ hổng bảo mật và giải pháp kết hợp BC để tăng cường bảo mật cho IoT. Thông qua đó đưa ra các giải pháp bảo mật hiệu quả. Mô hình nhà thông minh kết hợp BC bao gồm các thành phần chính: Nhà thông minh, lưu trữ đám mây và lớp phủ. Mô hình kết hợp Smart home – BC hạn chế thành công các giao dịch được chấp nhận bởi các thiết bị và *"miner"* 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, tính toàn vẹn và phòng ngừa các cuộc tấn công bảo mật DDOS. Để tăng khả năng mở rộng, mô hình đã đưa vào giải thuật bầu chọn chủ cụm cho mạng ngang hàng phân cấp [12]. Chi phí phải trả cho các giao dịch BC cũng được phân tích chi tiết qua phần mềm giả lập Cooja [14], trễ tăng không đáng kể so với mô hình base.

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.

TÀI LIỆU THAM KHẢO

[1] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G.,... and Zanichelli, F. (2018, April). IoTChain: A BC 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., and Choo, K. K. R. (2018). A BC future for the internet of things security: A position paper. *Digital Communications and Networks*, *4*(3), 149-160.

[3] Dorri, A., Kanhere, S. S., and Jurdak, R. (2017, April). Towards an optimized BC 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., and Gauravaram, P. (2017, March). BC 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., and Salah, K. (2018). IoT security: Review, BC solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

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

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

[8] Sharma, P. K., and Park, J. H. (2018). BC-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., and Peral, J. (2016). Internet of things: A review of surveys based on context-aware intelligent services. Sensors, 16(7), 1069.

[11] Dorri, A., Kanhere, S. S., and Jurdak, R. (2016). BC is the internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

[12] Hà, V. T. T., San, V. V., and Đức, N. H. (2017). Optimal supernode selection for large-scale P2P networks. Journal of Science and Technology on Information and Communications, 1(1), 40-44.

[13] Hammad, B. T., Jamil, N., Rusli, M. E., and Reza, M. (2017). A survey of the lightweight cryptographic hash function. Inter. J. Sci. Eng. Res, 8, 806-814.

[14] https://anrg.usc.edu/contiki/index.php/Cooja_Simulator

BLOCKCHAIN FOR IOT SECURITY

Abstract- Internet of Things (IoT) security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. IoT devices can often directly enter people's activities and living environments, so in the event of a hacker attack, check and install malware, the IoT devices could become a tool, so that crooks can search for information and directly target people. Blockchain technology was born to strengthen the

network security platform to improve security and safety for IoT system access.

The article applies the theory of IoT and Blockchain to build a model combining BC in Smart home security, the Smart home in the proposed model achieves security, integrity, availability, scalability and prevents important security attacks such as linking attacks and Distributed Denial of Service (DDOS). The simulation results section shows that the cost to achieve security results is relatively small.

Keywords - Access Control List, Blockchain, Cluster Head, Distributed Denial-of-Service, First-in-First-out, Peer to Peer, Identification.

Vũ Thị Thúy Hà, tốt nghiệp khoa Toán-Tin Đại học Tổng hợp Hà Nội năm 1993, nhận bằng Thạc sỹ CNTT năm 2001 tại Đại học Quốc gia Hà Nội. Năm 2017, nhận bằng Tiến sĩ chuyên ngành kỹ thuật Viễn thông tại Học viện công nghệ Bưu chính Viễn thông. Hiện là Giảng viên khoa Viễn thông. Lĩnh vực quan tâm: Phân tích đánh giá hiệu năng mạng, mạng chồng phủ ngang hàng, nén và xử lý dữ liệu truyền thông đa phương tiện.