MỘT HƯỚNG TIẾP CẬN TÍNH RIÊNG TƯ TRONG NHÀ THÔNG MINH SỬ DỤNG CÔNG NGHỆ BLOCKCHAIN HYPERLEDGER FABRIC

AN APPROACH TO PRIVACY IN SMART HOME USING HYPERLEDGER FABRIC BLOCKCHAIN TECHNOLOGY

Nguyễn Thanh Nhật An, Nguyễn Minh Sơn
Đại học Công nghệ Thông tin, Đại học quốc gia TP.HCM, Việt Nam

Ngày toà soạn nhận bài 28/10/2020, ngày phản biện đánh giá 25/11/2020, ngày chấp nhận đăng 20/12/2020

TÓM TẮT

Ngày nay, nhiều ứng dụng của hệ thống Nhà thông minh (Smart Home - SH) cung cấp các khuyến nghị dịch vụ cho người dùng, bao gồm giảm công suất tiêu thụ, cảnh báo các thiết bị lỗi, chẩn đoán bệnh,... [1]. Do tính chất kết nối internet, động và bất đồng bộ của môi trường SH tạo ra các thách thức bảo mật, xác thực và tính riêng tư [2]. Trong bài báo này một hướng tiếp cận tính riêng tư dữ liệu người dùng trong SH sử dụng công nghệ blockchain, gọi là (SH based on the IoT-Blockchain - SHIB), được đề xuất. Để chứng minh kiến trúc đề xuất, một kịch bản thực nghiệm dùng Hyperledger Fabric, NodeJS và C# được xây dựng giữa người dùng, nhà cung cấp dịch vụ và SH. Dựa trên kết quả thực nghiệm, kiến trúc SHIB thể hiện các ưu điểm như tính riêng tư dữ liệu và khả năng mở rộng cao. Ngoài ra, sự so sánh giữa kiến trúc đề xuất và các mô hình tồn tại trước đó trong các thông số khác nhau như hợp đồng thông minh và tính riêng tư của dữ liệu cũng được thực hiện.

Từ khóa: *Blockchain; Hyperledger Fabric; Hợp đồng thông minh; Internet of Things; Nhà thông minh; Tính riêng tư.*

ABSTRACT

Nowadays, numerous applications of smart home (SH) systems provide recommendations for users, including reducing their energy consumption, warnings of defective devices, diagnoses, etc [1]. Due to internet-connected, dynamic and heterogeneous nature of SH environment creates new security, authentication, and privacy challenges [2]. An approach to privacy in SH using blockchain technology, which is called SH based on the IoT-Blockchain (SHIB), is proposed in this paper. In order to demonstrate the proposed architecture, an experimental scenario using Hyperledger Fabric, NodeJS and C# are built among the user, service provider (SP), and SH. Based on the experimental results, SHIB architecture brings the advantages like data privacy and high extension ability. In addition, the comparison between the proposed architecture and existing models in different parameters such as Smart contract (SC) and the privacy of data are performed.

Keywords: *Blockchain; Hyperledger Fabric; Smart Contract; Internet of Things; Smart Home; Privacy*

1. GIỚI THIỆU

Năm 2003, có xấp xỉ 6,3 tỉ người trên thế giới và 500 triệu thiết bị được kết nối đến Internet. Sự tăng trưởng bùng nổ của điện thoại thông minh và máy tính bảng đã đưa số lượng thiết bị kết nối Internet lên 12,5 tỷ trong năm 2010. Cisco IBSG dự đoán sẽ có khoảng 25 tỷ thiết bị kết nối Internet năm 2015 và lên đến 50 tỷ năm 2020 [3]. Là một phần quan trọng của Internet vạn vật (Internet of thing - IoT), SHs phục vụ người dùng hiệu quả bằng cách liên lạc với nhiều thiết bị kỹ thuật số khác nhau dựa trên IoT [1]. Trong trường hợp SH, các thiết bị IoT sẽ thu thập dữ liệu riêng tư người dùng và đưa

Doi: https://doi.org/10.54644/jte.63.2021.47

lên thiết bị lưu trữ đám mây (Cloud), khi đó, các câu hỏi về tính riêng tư người dùng nên được xem xét. Trong [4], S. Zheng và cộng sự đã tiến hành một cuộc phỏng vấn 11 chủ SH để hiểu hơn về các đánh giá tính riêng tư và mong muốn của họ. Từ kết quả những cuộc phỏng vấn, nhóm tác giả đưa ra nhận xét như sau: Đầu tiên, người sử dụng ưu tiên đến sự tiện lợi và kết nối trong ngôi nhà của họ, đánh giá này dựa trên những hành vi và ý kiến riêng của họ. Thứ hai, ý kiến người dùng về người có quyền truy cập vào dữ liệu SH của họ phụ thuộc vào khía cạnh lợi ích mang lại. Thứ ba, người dùng giả định và tin rằng tính riêng tư của họ được bảo vệ vì họ tin tưởng vào nhà sản xuất các thiết bị IoT. Dựa trên phân tích của S. Zheng và cộng sự, có thể thấy rằng người dùng vẫn ưu tiên đến tính tiện lợi, nhanh chóng và chính xác trong hệ thống SH, nhận thức về tính bảo mật và riêng tư vẫn chưa được chú trọng.

Một cuộc khảo sát các vấn đề bảo mật chính trong IoT được M.A. Khan và cộng sự thực hiện năm 2017 [5]. Họ đưa ra các yêu cầu bảo mật chung cho IoT dựa trên các vấn đề tấn công, tác nhân đe dọa và những giải pháp mới nhất. Hơn nữa, các tác giả phân loại và ánh xạ các vấn đề bảo mật IoT với những giải pháp tìm được trong cuộc khảo sát. Quan trọng hơn, họ đã đề cập đến việc làm thế nào để Blockchain, công nghệ nền tảng của Bitcoin, có thể giải quyết những yêu cầu bảo mật trong IoT. Trong cuộc khảo sát, các công việc nghiên cứu liên quan đến bảo mật IoT và Blockchain rất hạn chế, với điểm chính của những nghiên cứu là tập trung vào tận dụng công nghệ Blockchain vào lợi ích IoT nói chung. Nhóm tác giả trong [6] đã tiến hành phân loại 18 tình huống sử dụng của Blockchain, trong đó có 4 trường hợp cho IoT. 4 trường hợp này được phân loại cho IoT bao gồm: sự đăng nhập bất biến các sự kiện và quản lý điều khiển truy nhập dữ liệu [7], xây dựng mô hình kinh doanh điện tử IoT [8], [9], quản lý khóa đối xứng và bất đối xứng cho các thiết bị IoT [10], [11], và các thách thức cho nhận dạng trong IoT [12]. IBM chỉ ra các thách thức hiện tại của IoT như giá thành cao, thiếu tính riêng tư, thiếu chức năng giá trị, và các mô hình kinh doanh bị phá vỡ [13]. Ngoài ra, nghiên cứu này chỉ ra rằng blockchain là công nghệ cho phép dân chủ hóa thế giới số.

Tiếp theo sẽ xem xét công nghệ blockchain được ứng dụng cụ thể như thế nào trong IoT nói chung và SH nói riêng.

2. CÁC NGHIÊN CỨU LIÊN QUAN

Các ứng dụng của SC Blockchain cho IoT được khảo sát bởi K. Christidis và cộng sự [14]. Nghiên cứu mô tả làm thế nào để SC của blockchain có thể tạo thuận tiện và hỗ trợ sự vận hành dòng công việc và chia sẻ dịch vụ giữa các thiết bị IoT. Hơn nữa, nhóm tác giả cũng chỉ rõ bằng cách nào IoT có thể tận dụng lợi ích từ mạng Blockchain trong khía cạnh lên quan đến thanh toán hóa đơn, giao dịch điện tử, giao hàng và quản lý chuỗi cung ứng. Hơn nữa, họ đặc tả một kịch bản nơi Blockchain có thể tạo thuận tiện cho mua và bán năng lượng hoàn toàn tự động giữa thiết bị IoT như những thiết bị đo thông minh. Nhiều hợp đồng thông minh có thể được sử dụng để xây dựng một tập các tiêu chí, được người dùng định nghĩa, cho các giao dịch năng lượng.

A. Dorri và cộng sự [15] đề xuất một kiến trúc tinh gọn, riêng tư và bảo mật cho IoT dựa trên nền tảng công nghệ Blockchain. Phương pháp được xây dựng trong kịch bản SH như một tình huống nghiên cứu cụ thể để mở rộng hơn cho những ứng dụng IoT. Kiến trúc đề xuất có dạng phân cấp, bao gồm nhiều SH, một mạng phủ (overlay network) và các thiết bị lưu trữ Cloud phối hợp các dữ liệu giao dịch với Blockchain nhằm cung cấp tính riêng tư và bảo mật. Thiết kế của nhóm tác giả sử dụng nhiều dạng khác nhau của Blockchain phụ thuộc vào nơi phân cấp mạng xảy ra giao dịch và sử dụng các phương pháp tin cậy phân tán nhằm đảm bảo một cấu trúc phân quyền. Sự đánh giá chất lượng của kiến trúc dựa trên các mô hình đe dọa phổ biến làm nổi bật tính hiệu quả trong việc cung cấp bảo mật và riêng tư đến các ứng dụng IoT.

Kiến trúc SHIB dùng công nghệ blockchain công cộng Ethereum đảm bảo

tính riêng tư bằng SC được đề xuất bởi T.L.N. Dang [16]. Kiến trúc này có những hiện thực đem đến những kết quả khó chấp nhận trong nhiều trường hợp như: đòi hỏi không gian lưu trữ lớn cho sổ cái toàn cục của cả mạng blockchain (thiết bị nào muốn trở thành 1 nút của mạng phải chuẩn bị không gian lưu trữ đủ lớn mới vận hành được); phát sinh chi phí giao dịch trên mạng blockchain do bản chất phải trả phí cho những nút khai phá được khối lưu trữ mới cho các giao dịch trên mạng. Cùng với khả năng triển khai blockchain liên doanh Hyperledger Fabric lên thiết bị IoT bởi L. Hang [17], P. Tunstad [18] đã tạo tiền đề cải tiến kiến trúc SHIB này dùng công nghệ blockchain Hyperledger Fabric để cải thiện những điều trên cho những ứng dụng thực tế có không gian lưu trữ hạn chế, không muốn phát sinh chi phí giao dịch trên mạng blockchain và không cần hoạt động liên tục, giảm chi phí năng lượng.

3. NỀN TẢNG HYPERLEDGER FABRIC VÀ FRAMEWORK CHO SHIB CẢI TIẾN

3.1 Hyperledger Fabric [19] – Một blockchain liên doanh mã nguồn mở

Hyperledger Fabric (HLF) là blockchain riêng tư và có phép. Thay vì một hệ thống không phép mở cho phép các danh tính không xác định tham gia vào mạng (yêu cầu các giao thức như "bằng chứng công việc" để xác thực giao dịch và bảo mật mạng), các thành viên của mạng HLF đăng ký thông qua nhà cung cấp dịch vụ thành viên (Membership Service Provider) đáng tin cậy.

HLF có khả năng tạo kênh (channel) cho phép nhóm những thành viên tham gia tạo sổ cái giao dịch riêng. Đây là 1 đặc điểm quan trọng cho những mạng mà một số thành viên có thể là đối thủ cạnh tranh không muốn mọi giao dịch mà họ tạo (như 1 giá đặc biệt họ đề xuất cho một số thành viên mà không cho những thành viên khác) bị mọi thành viên biết. Nếu 2 thành viên thành lập 1 kênh thì chỉ các thành viên đó có bản sao sổ cái cho kênh đó.

3.2 Kiến trúc hệ thống IoT-Blockchain cho SH

Về cơ bản, kiến trúc SHIB cải tiến có mô hình giống với kiến trúc SHIB [16] (hình 2) nhưng chi tiết thành phần có thay đổi. Trung tâm vẫn là mạng ngang hàng [20] hay mạng blockchain [16] (LAN, WAN hoặc hỗn hợp), cổng IoT (IoT Gateway - IoTG), nhà cung cấp dịch vụ, nhà thông minh. Cụ thể hình 2 có các thành phần sau:

- Nhà cung cấp dịch vụ (NCCDV): là một thiết bị hoặc một tập các thiết bị có khả năng tương tác với mạng HLF và các thiết bị lưu trữ nhằm cung cấp các dịch vụ thông minh mà người dùng mong muốn. Ngoài những NCCDV thông thường như điện, nước, hệ thống có NCCDV đặc biệt đó là NCCDV dặt hàng. NCCDV này thường là NCCDV hạ tầng mạng HLF, cung cấp giải pháp và ứng dụng cho mạng HLF. Đó là 1 tổ chức khởi sự ra mạng, cấu hình mạng, quản lý việc cấu hình của mạng là chủ yếu mà không tham gia vào các giao dịch thông thường trên mạng HLF.

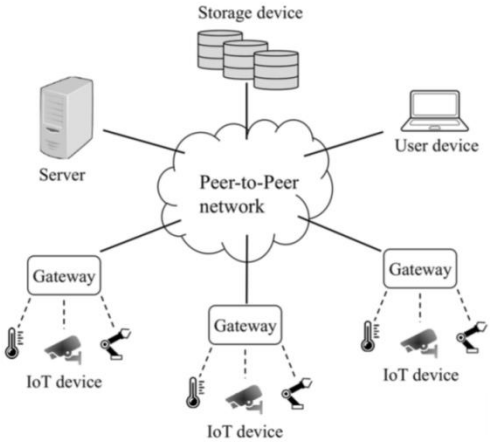
- Chủ SH (User): chủ nhân của một SH cụ thể, sử dụng các dịch vụ được cung cấp bởi NCCDV.

- IoTG: Cổng trung gian giúp kết nối thiết bị IoT và mạng HLF. Tập thiết bị IoT kết nối đến IoTG dựa trên các công nghệ truyền thông cự ly ngắn như: Wifi, Bluetooth, ZigBee. Trong trường hợp SH, IoTG có thể là một máy tính hoặc thiết bị IoT có khả năng xử lý tương đối như Raspberry Pi 4 (RP4) được đặt trong nhà.

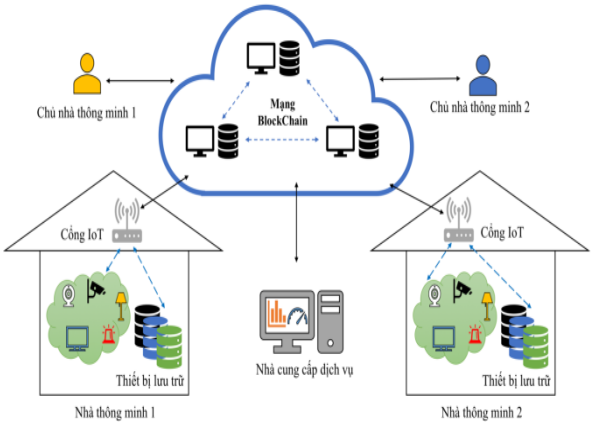
- Thiết bị IoT: thường bao gồm tập các cảm biến, thiết bị truyền động, công tắc và bóng đèn.

- Mạng blockchain dùng công nghệ HLF mã nguồn mở (IBM đóng góp chủ yếu). Ở đây mạng đảm bảo tính riêng tư bằng việc sử dụng SC và kênh, mỗi thiết bị IoT muốn được truy xuất qua mạng HLF cần có 1 hợp đồng (tương ứng là 1 SC và 1 kênh được triển khai trên mạng HLF) được ký giữa 2 bên SH và NCCDV. Trên kênh này còn có thêm NCCDV đặt hàng. Mạng HLF trên 1 nút IoTG dùng Raspberry Pi sẽ đạt được

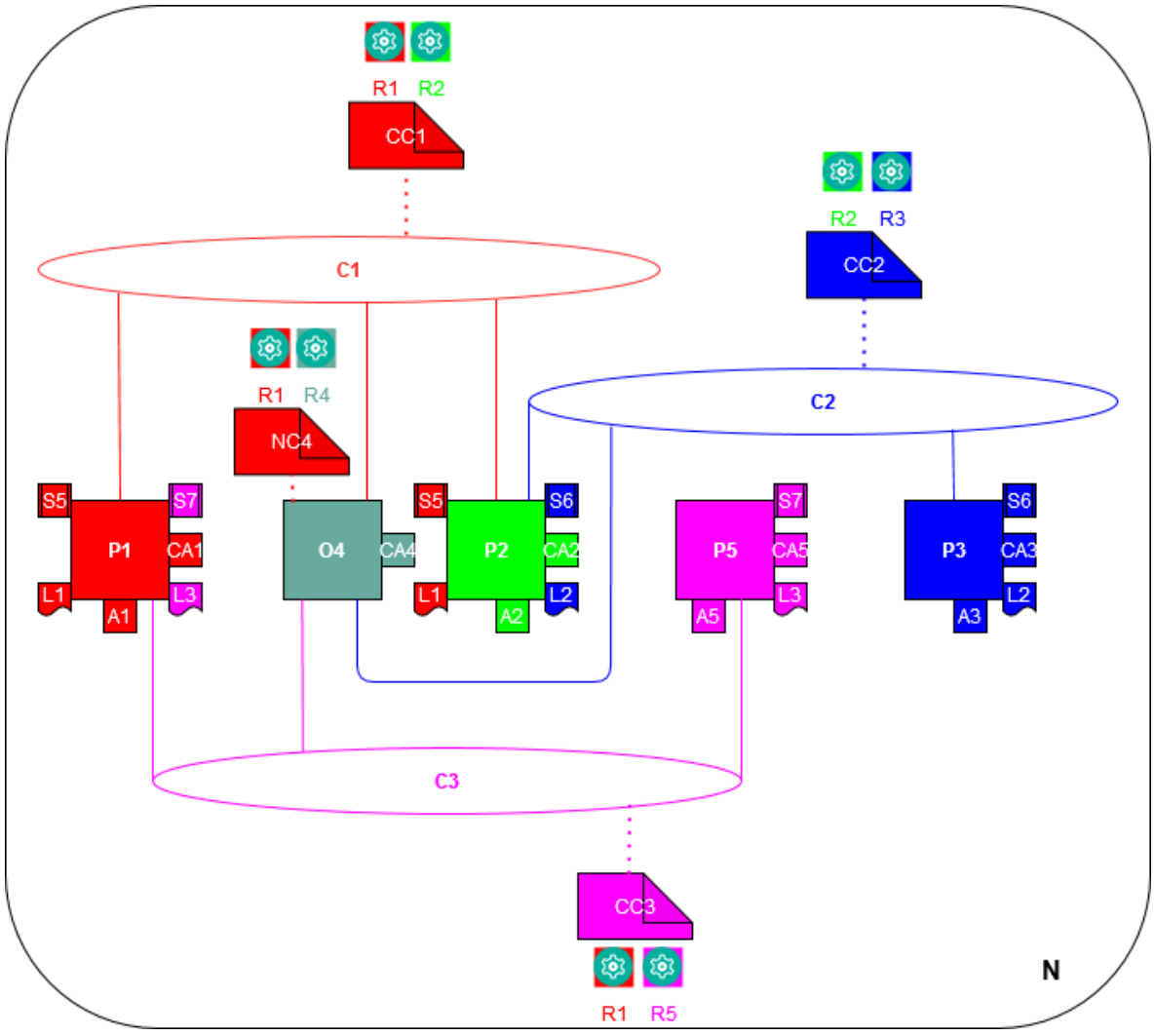
750-1500 giao dịch đơn (không bao gồm xử lý khác trên HLF) trong 1 giây theo A. David [21] và tiêu thụ khoảng 3,64W trong 10 phút theo P. Tunstad [18].



Hình 1. *Kiến trúc IoT-Blockchain [20]*



Hình 2. *Kiến trúc SHIB [16]*



Hình 3. *Mô hình IoT-Blockchain cho SH thực nghiệm*

4. MÔ HÌNH NGHIÊN CỨU ĐỀ XUẤT

Trong hình 3, điều đầu tiên xác định một mạng, N, là một dịch vụ đặt hàng, O4. Dịch vụ đặt hàng được xem như là điểm quản trị ban đầu cho mạng. Theo thỏa thuận trước, O4 ban đầu được cấu hình và bắt đầu bởi một quản trị viên trong tổ chức R4 và được lưu trữ trong R4. Cấu hình NC4 chứa các chính sách mô tả bộ khả năng quản trị bắt đầu cho mạng. Bốn tổ chức, R1 (Electricity - Tổng công ty điện lực miền Nam), R2 (Smart-home-1), R3 (Water - Thủy cục Chợ Lớn) và R4 (O4 - Cơ quan đề xuất mạng Blockchain kinh doanh và các ứng dụng trên đó) đã cùng quyết định và viết thành một thỏa thuận, rằng họ sẽ thiết lập và khai thác mạng HLF. R4 đã được chỉ định làm người khởi tạo mạng - nó đã được trao quyền để thiết lập phiên bản ban đầu của mạng. R4 không có ý định thực hiện các giao dịch nghiệp vụ trên mạng. R1 và R2 có nhu cầu liên lạc riêng trong mạng chung, cũng như R2 và R3. Tổ chức R1 có một ứng dụng khách A1 có thể thực hiện các giao dịch nghiệp vụ trong kênh C1 (electricity-channel-s5) (thông qua SC S5). Tổ chức R2 có một ứng dụng khách A2 có thể thực hiện công việc tương tự cả trong kênh C1 (thông qua SC S5) và C2 (water-channel-s6) (thông qua SC S5). Tổ chức R3 có một ứng dụng khách A3 có thể thực hiện việc này trên kênh C2 (thông qua SC S6). Nút ngang hàng P1 duy trì một bản sao của sổ cái L1 được liên kết với C1. Nút ngang hàng P2 duy trì một bản sao của sổ cái L1 được liên kết với C1 và một bản sao của sổ cái L2 được liên kết với C2. Nút ngang hàng P3 duy trì một bản sao của sổ cái L2 liên kết với C2. Mạng được điều chỉnh theo các quy tắc chính sách được chỉ định trong cấu hình mạng NC4, mạng nằm dưới sự kiểm soát của các tổ chức R1 và R4. Kênh C1 được điều chỉnh theo các quy tắc chính sách được chỉ định trong cấu hình kênh CC1; kênh nằm dưới sự kiểm soát của các tổ chức R1 và R2. Kênh C2 được điều chỉnh theo các quy tắc chính sách được chỉ định trong cấu hình kênh CC2; kênh nằm dưới sự kiểm soát của các tổ chức R2 và R3. Hệ thống có một dịch vụ đặt hàng O4 phục vụ như một điểm quản trị mạng cho N và sử dụng kênh hệ thống. Dịch vụ đặt hàng cũng hỗ trợ các kênh ứng dụng C1 và C2, cho mục đích đặt hàng giao dịch thành các khối để phân phối. Mỗi trong số bốn tổ chức có một cơ quan chứng nhận ưa thích CA1, CA2, CA3, CA4 tương ứng.

Tương tự, kênh C3 (electricity – channel - s7) được điều chỉnh theo các quy tắc chính sách được chỉ định trong cấu hình kênh CC3; kênh nằm dưới sự kiểm soát của các tổ chức R1 và R5 (Smart-home-2). Kênh C3 có nút ngang hàng P1, nút ngang hàng P5, sổ cái L3, SC S7. Tổ chức R1 có ứng dụng khách A1 bây giờ còn có thể thao tác trên kênh C3. Tổ chức R5 có ứng dụng khách A5 có thể thao tác trên kênh C3. Dịch vụ đặt hàng O4 hỗ trợ thêm kênh C3. Tổ chức R5 có cơ quan chứng nhận CA5.

Ý nghĩa của các SC có thể hiểu như sau: SC S5 cho phép nhà cung cấp điện yêu cầu SH 1 cho xem chỉ số cảm biến điện và cho phép SH 1 trả kết quả chỉ số cảm biến điện hiện thời. Tương tự, SC S6 cho phép nhà cung cấp nước yêu cầu SH 1 cho xem chỉ số cảm biến nước và cho phép SH 1 trả kết quả chỉ số cảm biến nước hiện thời. SC S7 cho phép nhà cung cấp điện yêu cầu SH 2 cho xem chỉ số cảm biến điện và cho phép SH 2 trả kết quả chỉ số cảm biến điện hiện thời.

Bảng 1. *Kịch bản xây dựng và các phân quyền truy cập*

Thiết bị IoT	**NCC Điện**	**NCC Nước**	**Thành Viên**	**Chủ nhà**
Cảm biến điện	Đọc dữ liệu		Bật, Tắt, Đọc dữ liệu (nếu được chủ nhà cho xem)	Bật, Tắt, Đọc dữ liệu
Cảm biến nước		Đọc dữ liệu	Bật, Tắt, Đọc dữ liệu (nếu được chủ nhà cho xem)	Bật, Tắt, Đọc dữ liệu

Nhìn chung mỗi kênh mới sẽ có 1 cấu hình kênh gồm 2 tổ chức tham gia chính và 1 tổ chức dịch vụ đặt hàng O4. Điều này sẽ đáp ứng được tính riêng tư tối đa. Ở đây, dịch vụ đặt hàng theo cơ chế đồng thuận Solo, tức là chỉ dùng 1 nút duy nhất.

Kịch bản xây dựng và các phân quyền truy cập được chi tiết trong bảng 1. Các phân quyền truy cập này được lưu trong cơ sở dữ liệu nội bộ trên nút ngang hàng của mỗi tổ chức.

Thực nghiệm hiện thực 4 nút ngang hàng P1, P3, O4, P5 hoạt động trên cùng 1 máy ảo và 1 nút ngang hàng P2 hoạt động trên RP4. Mạng N hiện thực trên mạng nội bộ.

5. THỰC NGHIỆM VÀ KẾT QUẢ

5.1 Phần cứng và phần mềm

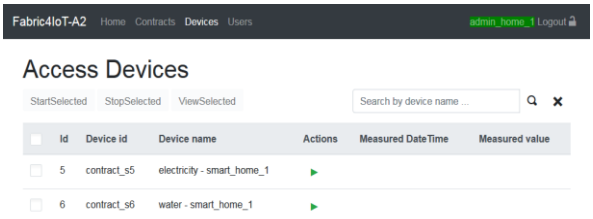
Phần cứng thực hiện dành cho kịch bản gồm 1 máy ảo Ubuntu Desktop 18.04.4 CPU 4 lõi, RAM 12GB chạy trên VMWare của máy xách tay HP 8570w CPU Intel i7-3720QM, RAM 32GB, SSD 512GB, hệ điều hành MS Windows 7; 1 thiết bị IoT RP4 RAM 4GB, uSD 64GB, hệ điều hành Ubuntu Server 18.04.4.

Phần mềm: Visual Studio Code trên Ubuntu Desktop được dùng để viết các SC bằng NodeJS, viết máy chủ Web API bằng NodeJS (vừa tương tác với giao diện Web người sử dụng, vừa tương tác với mạng HLF), thay đổi các tập tin cấu hình. Visual Studio 2019 Community trên MS Windows 10 để viết giao diện Web bằng C#. Phần mềm Docker Community để dựng nên các Docker image cần thiết cho mạng HLF và tạo ra các container vận hành nhiều máy chủ cho hệ thống thực nghiệm.

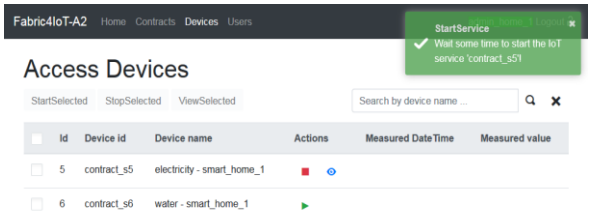
Tại mỗi tổ chức (trong 4 tổ chức gồm 2 nhà thông minh, nhà cung cấp dịch vụ điện và nhà cung cấp nước), kịch bản xây dựng 1 ứng dụng Web với dữ liệu động lấy từ cơ sở dữ liệu nội bộ có trên nút ngang hàng của tổ chức (tương ứng mỗi tổ chức, ứng dụng Web sẽ có tên A1, A2, A3, A5) giúp cho người sử dụng/vận hành tại mỗi tổ chức dễ dàng thao tác truy cập và điều khiển thiết bị IoT. Tùy theo dữ liệu được thiết lập trong cơ sở dữ liệu nội bộ và ID của người đăng nhập vào hệ thống của tổ chức mà thực đơn những trang được phép truy cập, cũng như dữ liệu và hành động tương ứng có thể thao tác với hệ thống, sẽ hiện lên trang Web.

5.2 Kịch bản nghiên cứu và kết quả

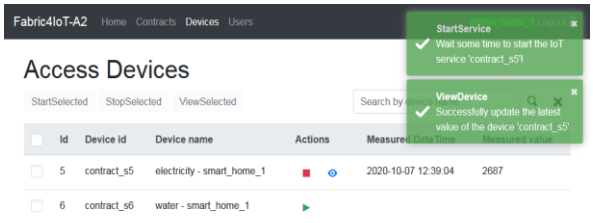
- Chủ SH 1 (admin_home_1): được phép mở (hình 4, hình 7) / tắt (hình 5) dịch vụ cho xem cảm biến điện S5 (SC S5) và cảm biến nước S6 (SC S6), cũng như xem được chỉ số của S5 (hình 6) và S6 khi dịch vụ cho xem mở.



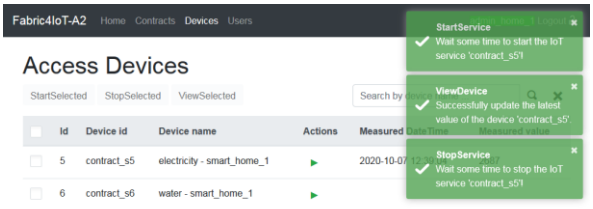
Hình 4. *Trang Devices khi vừa truy cập vào*



Hình 5. *Trang Devices sau khi khởi động dịch vụ cho xem cảm biến S5*

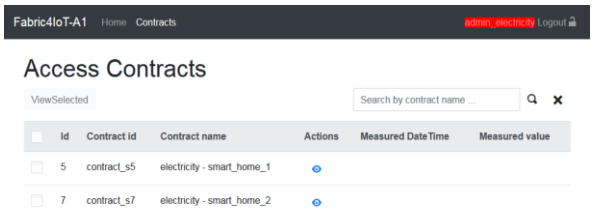


Hình 6. *Trang Devices xem được chỉ số hiện thời của S5*

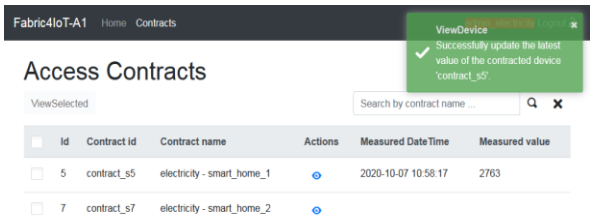


Hình 7. *Trang Devices sau khi ngừng dịch vụ cho xem cảm biến S5*

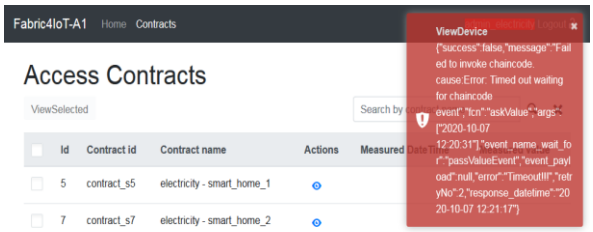
- NCCDV điện (admin_electricity): thấy được SC S5 và S7 (hình 8), cũng như xem được chỉ số của S5 và S7 khi SH tương ứng mở dịch vụ cho xem (hình 9) hoặc hiện thông báo lỗi khi tắt dịch vụ cho xem (hình 10).



Hình 8. *Trang Contracts khi vừa truy cập vào*

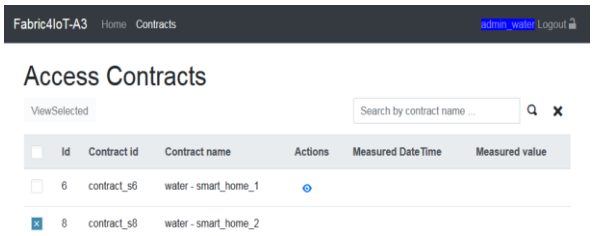


Hình 9. *Trang Contracts xem được chỉ số hiện thời của S5*



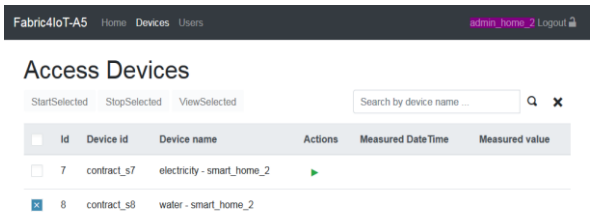
Hình 10. *Trang Contracts bị lỗi xem S5*

- NCCDV nước (admin_water): thấy được SC S6 và S8 nhưng chỉ có thể xem S6, bị vô hiệu hóa hành động với S8 vì S8 có trên thông tin quản lý nhưng chưa triển khai SC S8 (hình 11).



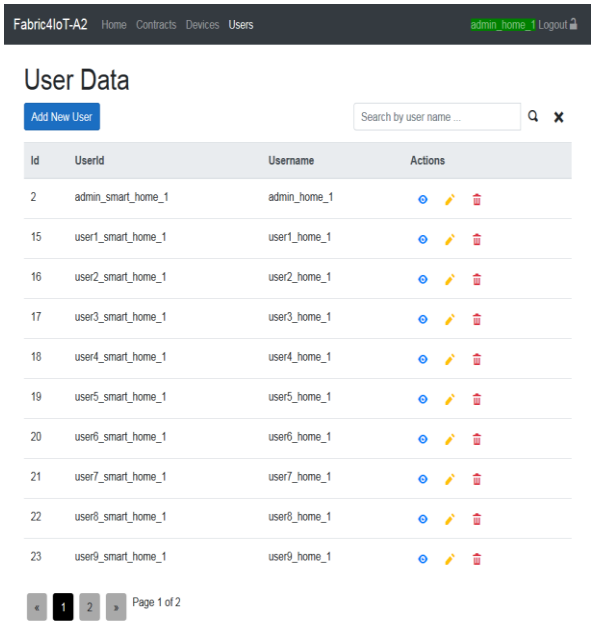
Hình 11. *NCCDV nước truy cập hợp đồng*

- Chủ SH 2 (admin_home_2): được phép mở/tắt/xem cảm biến S7, không có hành động với cảm biến S8 vì S8 có trên thông tin quản lý nhưng chưa triển khai SC S8 (hình 12).



Hình 12. *Chủ SH 2 truy cập thiết bị*

- Chủ SH có thể thêm/sửa/xóa thành viên của SH mình, cũng như giới hạn thành viên có thể truy xuất vào những thiết bị có SC của SH mình quản lý (hình 13).



Hình 13. *Trang Users khi vừa truy cập vào*

5.3 So sánh với mô hình nghiên cứu [16]

Kiến trúc SHIB cải tiến được đề xuất dựa trên kiến trúc trong nghiên cứu [16] nhưng hai kiến trúc có những khác biệt nhất định. Tính riêng tư vẫn được đảm bảo nhưng tính bảo mật được nâng lên nhờ sử dụng kênh, dữ liệu kênh (có sổ cái riêng nhỏ gọn cho mỗi kênh) chỉ chia sẻ cho 2 tổ chức chính và 1 dịch vụ đặt hàng. Trong nghiên cứu [16], sổ cái dùng chung cho cả mạng rất lớn nên nếu muốn trở thành 1 nút trên mạng Blockchain thì phải chuẩn bị không gian lưu trữ đủ lớn để lưu trọn sổ cái chung. Các thông số so sánh bao gồm: nền tảng blockchain, thiết bị lưu trữ, đối tượng, chủ thể, SC, thời gian truy cập trung bình cho 1 lần truy cập thiết bị được trình bày cụ thể trong bảng 2.

Bảng 2. *So sánh kiến trúc SHIB cải tiến và kiến trúc trong [16]*

Thông số	**Kiến trúc SHIB cải tiến**	**Kiến trúc trong [16]**
Nền tảng blockchain	Blockchain liên doanh HLF.	Blockchain công cộng Ethereum.
Thiết bị lưu trữ	Không xem xét vận hành trong mạng blockchain.	Không xem xét vận hành trong mạng blockchain.
Đối tượng	Tổ chức (SH hoặc NCCDV).	Luôn luôn là SH.
Chủ thể	Những người dùng muốn truy cập vào SH. Người vận hành của NCCDV.	Những người dùng muốn truy cập vào SH.
SC	Mỗi thiết bị cần truy cập qua blockchain có một hợp đồng.	Mỗi SH sử dụng một hợp đồng RC và JC riêng biệt.
Thời gian xử lý giao dịch trung bình	1 mili giây [21]	15 giây đến 5 phút [22]
Thời gian truy cập thiết bị IoT trung bình	8-10 giây.	15 giây.

6. KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TƯƠNG LAI

Bài báo tập trung đề xuất một hướng tiếp cận bảo mật tính riêng tư dữ liệu người dùng trong SH sử dụng các SC và kênh dựa trên nền tảng HLF, cụ thể là kiến trúc SHIB cải tiến. Một kịch bản thực nghiệm sử dụng HLF, NodeJS và C# được xây dựng để đánh giá khả năng vận hành của các SC trong SHIB cải tiến có thể hoạt động ngay trên IoTG là thiết bị IoT RP4. Qua thực nghiệm và kết quả thu được, kiến trúc SHIB cải tiến mang lại các lợi thế:

- Việc sử dụng SC và kênh cho mỗi thiết bị IoT cần truy cập qua mạng HLF khiến cho việc truy cập vào sổ cái chỉ có các đối tượng trên kênh mới thực hiện được, đảm bảo được tính riêng tư dữ liệu. Mỗi kênh có 1 sổ cái riêng nhỏ gọn, có thể lưu trữ ngay trên IoTG RP4.

- Không phát sinh chi phí giao dịch trên mạng HLF.

- Trừ các nút làm dịch vụ đặt hàng, các nút khác trên mạng chỉ cần hoạt động khi cần giao dịch với nút khác, bình thường có thể ngừng hoạt động, tắt nguồn nhằm giảm chi phí năng lượng.

- Khả năng mở rộng cao: cần thêm thiết bị IoT thì thêm SC và kênh; chủ SH dễ dàng thêm/sửa/xóa người dùng SH.

Để đánh giá kiến trúc cải tiến, sự so sánh kiến trúc SHIB cải tiến và kiến trúc SHIB [16] đã được thực hiện. Trong tương lai, chúng tôi sẽ tiến hành những việc sau:

- Tiến hành thêm nhiều thực nghiệm mở rộng kiến trúc lên nhiều loại cổng IoT không chỉ cổng IoT dùng RP4.

- Đo hiệu suất xử lý khi có rất nhiều nút trên mạng Blockchain với các yêu cầu theo lô lớn đồng thời dù chương trình đã được viết sẵn để phục vụ cho việc này. Ví dụ như 1 truy cập thiết bị mất 8-10 giây, nhưng truy cập theo lô lên đến hàng triệu thiết bị thì cũng mất chừng ấy cộng thêm ít độ trễ của mạng dù 1 gói dữ liệu gửi đi và nhận về trên mạng Blockchain khoảng 1KB cho 1 yêu cầu truy xuất thiết bị.

- Triển khai mạng Blockchain cho các nút trên mạng WAN để kiểm tra độ trễ xử lý truy cập.

- Tăng số nút ngang hàng, số nút dịch vụ đặt hàng để tăng khả năng xử lý của mạng HLF.

TÀI LIỆU THAM KHẢO

[1] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal and M.L.M. Kiah, A Review of Smart Home Applications based on Internet of Things, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2017.08.017

[2] W. Ali, G. Dustgeer, M. Awais, M. A. Shah, "IoT based Smart Home: Security Challenges, Security Requirements and Solutions", in 2017 23rd International Conference on Automation and Computing (ICAC). https://doi.org/10.23919/IConAC.2017.8082057
[3] D. Evans. The Internet of Things how the next evolution of the internet is changing everything. Technical report, 04 2011
[4] S. Zheng, M. Chetty, N. Feamster, "User Perceptions of Privacy in Smart Homes", arXiv preprint arXiv:1802.08182
[5] M.A. Khan, K. Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems (2017), https://doi.org/10.1016/j.future.2017.11.022
[6] M. Conoscenti, A. Vetrò, J.C.D. Martin, "Blockchain for the internet of things: a systematic literature review", in: The 3rd International Symposium on Internet of Things: Systems, Management, and Security (IOTSMS-2016), 2016.
[7] G. Zyskind, O. Nathan, A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy" (June 2015). URL: http://enigma.media.mit.edu/enigma full.pdf
[8] Y. Zhang, J. Wen, "An IoT electric business model based on the protocol of bitcoin", in: 2015 18th International Conference on Intelligence in Next Generation Networks, 2015, pp. 184–191. doi:10.1109/ICIN.2015.7073830.
[9] D. Wo¨rner, T. von Bomhard, "When your sensor earns money: Exchanging data for cash with bitcoin", in: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, UbiComp '14 Adjunct, ACM, New York, NY, USA, 2014, pp. 295–298. doi:10.1145/2638728.2638786. URL: http://doi.acm.org/10.1145/2638728.2638786
[10] L. Axon, "Privacy-awareness in blockchain-based pki", Tech.rep. (October 2015). URL https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b/datastreams/ATTACHMENT01
[11] C. Fromknecht, D. Velicanu, S. Yakoubov, "Certcoin: A namecoin based decentralized authentication system" (May 2014). URL https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov- certcoin.pdf
[12] I. Friese, J. Heuer, N. Kong, "Challenges from the identities of things: Introduction of the identities of things discussion group within kantara initiative", in: 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 1–4. doi:10.1109/WF- IoT.2014.6803106.
[13] Device Democracy: Saving the Future of the Internet of Things, IBM, New York, NY, USA, 2015.
[14] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", IEEE Access 4 (2016) 2292–2303. doi: 10.1109/ACCESS.2016.2566339
[15] A. Dorri, S. S. Kanhere, R. Jurdak, "Blockchain in internet of things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
[16] T.L.N. Dang, M.S. Nguyen: An approach to data privacy in smart home using blockchain technology. In: 2018 International Conference on Advanced Computing and Applications (ACOMP), pp. 58–64 (2018).
[17] L. Hang, D. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," May 2019, doi: 10.3390/s19102228
[18] P. Tunstad, A.M. Khan, P.H. Ha, "HyperProv: Decentralized Resilient Data Provenance at the Edge with Blockchains", October 2019, arXiv:1910.05779
[19] Hyperledger Fabric, URL: https://hyperledger-fabric.readthedocs.io/en/release-1.4/blockchain.html
[20] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, "Smart Contract-Based Access Control for the Internet of Things", arXiv preprint arXiv:1802.04410v1 [cs.CR]
[21] A. David, "Managing IOT Data on Hyperledger Blockchain," August 2019. URL: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=4721&context=thesesdissertations
[22] "How long does an Ethereum transaction really take?", URL: https://ethgasstation.info/blog/ethereum-transaction-how-long/

Tác giả chịu trách nhiệm bài viết:
Nguyễn Minh Sơn
Trường Đại học Công nghệ Thông tin, Đại học quốc gia TPHCM
Email: sonnm@uit.edu.vn