BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Huỳnh Thanh Tâm

NỀN TẢNG ĐẢM BẢO AN TOÀN BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO LIÊN MẠNG VẠN VẬT

Chuyên ngành: Hệ thống thông tin

Mã số: 9.48.01.04

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

Hà Nội – 2022

Công trình được hoàn thành tại:

Học viện Công nghệ Bưu chính Viễn thông

Người hướng dẫn khoa học: **1. PGS.TS. Nguyễn Đình Thúc**

2. TS. Tân Hạnh

Phản biện 1: .....

Phản biện 2: .....

Phản biện 3: .....

Luận án được bảo vệ trước Hội đồng chấm luận án cấp Học viện tại:

Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: …….giờ..... ngày..... tháng…… năm…….

Có thể tìm hiểu luận án tại thư viện:.....

MỞ ĐẦU

1. Giới thiệu

Liên mạng vạn vật còn được gọi là Internet vạn vật (từ này viết là IoT) là một mạng gồm nhiều thiết bị vật lý tham gia vào Internet nhằm mục đích kết nối và trao đổi dữ liệu với các thiết bị và hệ thống khác. Đi kèm với sự phát triển nhanh chóng về số lượng và chủng loại thiết bị IoT kết nối vào hệ thống mạng, nhu cầu về truy cập tài nguyên, lưu trữ và chia sẻ dữ liệu ngày càng gia tăng. Điều này đặt ra các thách thức cho các nền tảng bảo mật của IoT như: (1) tốc độ xử lý dữ liệu phải nhanh chóng và chính xác; (2) cần cung cấp các chức năng bảo mật cần thiết cho người dùng, chẳng hạn như: kiểm soát truy cập, lưu trữ và chia sẻ dữ liệu; và (3) cần đảm bảo tính sẵn sàng và khả năng mở rộng của hệ thống.

Với thực tế như vậy, luận án nghiên cứu và đề xuất một nền tảng bảo mật dựa trên công nghệ Blockchain cho IoT. So với các nền tảng bảo mật tương tự, nền tảng bảo mật được đề xuất trong luận án đảm bảo tối ưu hiệu năng của các nút (Node) nắm giữ sổ cái (từ này viết là Miner) trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Đồng thời cung cấp nhiều chức năng bảo mật hơn, như: lưu trữ dữ liệu an toàn, chia sẻ dữ liệu đảm bảo tính riêng tư, và kiểm soát truy cập cho các thiết bị IoT theo thời gian được cấp phép bởi chủ sở hữu thiết bị.

Các Miner trong nền tảng bảo mật được đề xuất đóng vai trò quan trọng trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái. Bảo vệ các Miner này trước các nguy cơ tấn công từ chối dịch vụ từ các Node tiềm tàng độc hại, gọi là Hot-

IP, trong mạng sẽ góp phần nâng cao tính ổn định của nền tảng. Do đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất.

2. Lý do chọn đề tài

Hầu hết các thiết bị IoT đều bị hạn chế về khả năng tính toán và dung lượng lưu trữ, làm cho việc triển khai giải pháp bảo mật trên từng thiết bị trong mạng gặp nhiều khó khăn và đôi khi không khả thi. Xây dựng một nền tảng bảo mật cho IoT là giải pháp khả thi hơn.

Các nền tảng bảo mật dựa trên kiến trúc tập trung với các ưu điểm là dễ dàng triển khai, độ trễ thấp và chí phí triển khai thấp. Tuy nhiên, các nền tảng bảo mật thuộc nhóm này có một số hạn chế liên quan đến bảo mật dữ liệu, tính sẵn sàng và khả năng mở rộng của hệ thống.

Trong khi đó, các nền tảng bảo mật dựa trên kiến trúc phi tập trung có ưu điểm là đảm bảo được tính sẵn sàng của hệ thống và có khả năng mở rộng cao. Đặc điểm chung của những nền tảng bảo mật thuộc nhóm này là sử dụng công nghệ Blockchain làm thành phần trung tâm.

Hiện tại, hầu hết các nền tảng bảo mật dựa trên Blockchain cho IoT chỉ chủ yếu tập trung vào việc cung cấp một trong các chức năng bảo mật. Trong khi cơ chế xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain của các Miner vẫn chưa được tối ưu. Do đó, luận án sẽ đề xuất một nền tảng bảo mật mới với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái đảm bảo tối ưu hiệu năng cho các Miner. Bên cạnh đó, nền tảng bảo mật được đề xuất sẽ cung cấp các chức năng bảo mật: chức năng kiểm soát truy cập dựa trên thời gian

được cấp phép, chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư.

3. Mục tiêu nghiên cứu

3.1. Mục tiêu tổng quát

Mục tiêu của luận án là đề xuất một nền tảng đảm bảo an toàn bảo mật dựa trên Blockchain cho IoT; sử dụng một số công nghệ và công cụ toán học kết hợp để đề xuất chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng; đề xuất chức năng kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu thiết bị cho nền tảng. Chức năng kiểm soát truy cập được đề xuất có thể áp dụng triển khai đối với các hệ thống Camera trong các khu vực công cộng của hệ thống nhà thông minh/thành phố thông minh. Bên cạnh đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng. Nền tảng bảo mật được đề xuất có thể áp dụng cho một mạng IoT với các thiết bị có đặc tính kết nối thông qua công nghệ IP, tầng ứng dụng trong kiến trúc IoT sẽ được dùng để xây dựng các ứng dụng phục vụ tương tác với các chức năng bảo mật được cung cấp trong nền tảng.

3.2. Các mục tiêu cụ thể

- Nghiên cứu lý thuyết về công nghệ Blockchain, các loại mạng Blockchain và các giao thức đồng thuận. Tìm hiểu các nền tảng bảo mật dựa trên Blockchain cho IoT, phân tích các ưu và nhược điểm của chúng. Từ đó đề xuất một nền tảng bảo mật tốt hơn cho IoT.
- Nghiên cứu lý thuyết về hệ thống lưu trữ phi tập trung IPFS, phương thức chữ ký nhóm. Từ đó đề xuất phương

thức lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất.

- Đề xuất giải pháp kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu thiết bị, giải pháp này là một chức năng của nền tảng bảo mật được đề xuất. Áp dụng giải pháp này để kiểm soát truy cập cho hệ thống Camera công cộng trong hệ thống nhà thông minh/thành phố thông minh để đánh giá tính hiệu quả và an toàn bảo mật của giải pháp.
- Đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất, nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng.

4. Đối tượng, phạm vi nghiên cứu

Nghiên cứu về công nghệ Blockchain, các giao thức đồng thuận, các loại mạng Blockchain, phương thức chữ ký nhóm và IPFS. Từ đó đề xuất một nền tảng bảo mật mới cho IoT; đề xuất chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng bảo mật; đề xuất chức năng kiểm soát truy cập dựa trên thời gian được cấp phép cho nền tảng bảo mật.

5. Phương pháp nghiên cứu

Luận án sử dụng phương pháp nghiên cứu phân tích, đánh giá và tổng hợp trên các kết quả nghiên cứu đã có. Từ đó đề xuất hướng giải quyết và cách tiếp cận của luận án, sau đó thực hiện so sánh, thử nghiệm và đánh giá kết quả. Cụ thể như sau:

- Phân tích và đánh giá các nền tảng bảo mật dựa trên Blockchain cho IoT.

- Phân tích và đánh giá các công trình nghiên cứu liên quan đến phương thức lưu trữ, chia sẻ dữ liệu, và kiểm soát truy cập dựa trên Blockchain cho IoT.
- Tổng hợp các phân tích và đánh giá từ các nghiên cứu đã khảo sát, từ đó đề xuất một nền tảng bảo mật mới tối ưu hơn so với các nền tảng bảo mật đã khảo sát.
- Thực hiện so sánh, thử nghiệm và đánh giá nền tảng bảo mật được đề xuất.

6. Những đóng góp chính của luận án

(i) Đề xuất một nền tảng bảo mật dựa trên Blockchain cho IoT. Trong đó, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain dựa trên hai trường hợp về các Miner trong một mạng Blockchain: trường hợp 1, tất các Miner trong một mạng Blockchain đều hoàn toàn tin cậy; trường hợp 2, trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất bao gồm hai giai đoạn: giai đoạn xác minh và giai đoạn tạo khối. Trong giai đoạn xác minh, các giao dịch được xác minh bởi một số lượng Miner nhất định tùy thuộc vào từng trường hợp nêu trên. Trong giai đoạn tạo khối, một Miner được lựa chọn sẽ đặt các giao dịch hợp lệ vào một khối mới, sau đó tạo chữ ký số trên khối mới này. Chữ ký số cùng với khối này sẽ được quảng bá đến các Miner khác trong mạng. Nếu khối mới này và chữ ký số hợp lệ, các Miner sẽ lưu khối này vào trong sổ cái của chúng. Nền tảng này mang lại sự

tối ưu về mặt hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain, đồng thời có tính mở để có thể dễ dàng tích hợp thêm nhiều chức năng bảo mật vào trong nền tảng. Ngoài ra, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất, giải pháp này nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng. Từ đó sẽ có cơ chế phù hợp để hạn chế ảnh hưởng xấu của chúng.

(ii) Đề xuất phương thức lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất. Trong phương thức lưu trữ dữ liệu, sau khi dữ liệu thô được số hóa và cấp chứng chỉ bởi một tổ chức uy tín để trở thành một dữ liệu số có giá trị. Người sở hữu có thể lưu trữ các dữ liệu có giá trị lên một hệ thống lưu trữ an toàn. Trong giải pháp này, luận án sử dụng IPFS để lưu các dữ liệu số có giá trị. Trong khi các thông tin về địa chỉ truy cập của dữ liệu trên IPFS, chứng chỉ của dữ liệu và một số thông tin khác sẽ được lưu trên sổ cái Blockchain của nền tảng bảo mật được đề xuất. Trong phương thức chia sẻ dữ liệu, từ các thông tin được công bố trên Blockchain từ người sở hữu dữ liệu, mọi người trên hệ thống đều có thể kiểm chứng được tính tin cậy và tính chính xác của dữ liệu nhưng không thể hiểu được nội dung của dữ liệu chia sẻ. Quá trình chia sẻ dữ liệu sẽ được thực hiện một cách chủ động, chính xác, minh bạch và công bằng thông qua một hợp đồng thông minh được triển khai trên Blockchain. Hai phương thức này đạt

được các tính chất bảo mật: tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ và tính ẩn danh.

(iii) Đề xuất giải pháp kiểm soát truy cập dựa trên thời gian được cấp phép cho IoT. Giải pháp này là một chức năng của nền tảng bảo mật được đề xuất. Điểm khác biệt của giải pháp này so với các giải pháp kiểm soát truy cập dựa trên Blockchain khác đó là: khi nhận được một giao dịch yêu cầu truy cập đến một thiết bị IoT, người sở hữu có thể cấp phép một khoảng thời gian truy xuất nhất định cho người yêu cầu truy cập. Khi hết khoảng thời gian được cấp phép kết nối sẽ tự động bị loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào.

7. Giới thiệu tổng quan về nội dung luận án

Luận án được tổ chức thành 4 chương và phần kết luận. Chương 1 trình bày tổng quan về nền tảng bảo mật cho IoT, một số khái niệm, tổng quan về công nghệ Blockchain, khảo sát các nghiên cứu liên quan đến các nền tảng bảo mật dựa trên Blockchain cho IoT. Khảo sát các giải pháp kiểm soát truy cập, giải pháp lưu trữ và chia sẻ dữ liệu dựa trên Blockchain. Trên cơ sở đó, luận án đề xuất một nền tảng đảm bảo an toàn bảo mật mới đảm bảo tối ưu hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Nền tảng được đề xuất cung cấp các chức năng như: kiểm soát truy cập, lưu trữ dữ liệu và chia sẻ dữ liệu.

Chương 2 trình bày kiến trúc, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất. Trong đó, quá trình xác minh giao dịch

và đồng thuận dữ liệu trên sổ cái dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Luận án so sánh tốc độ xác minh giao dịch và thời gian mining trung bình một khối mới của nền tảng bảo mật được đề xuất với các nền tảng bảo mật tương tự đã khảo sát dựa trên thuật toán và thực nghiệm. Để phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner của nền tảng bảo mật được đề xuất.

Chương 3 trình bày hai chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư của nền tảng bảo mật được đề xuất. Trong đó, luận án sử dụng phương thức chữ ký nhóm, nền tảng bảo mật được đề xuất ở Chương 2 và IPFS để thiết kế hai chức năng này. Luận án trình bày mô hình hệ thống, các tính năng bảo mật, chi tiết về phương thức lưu trữ và chia sẻ dữ liệu, tiến hành phân tích và đánh giá các ưu điểm và các tính chất bảo mật đạt được của hai chức năng được đề xuất.

Chương 4 trình bày chức năng kiểm soát truy cập dựa trên thời gian được cấp phép của nền tảng bảo mật được đề xuất. Chức năng này được áp dụng trong ngữ cảnh kiểm soát truy cập cho hệ thống Camera công cộng của hệ thống nhà thông minh/thành phố thông minh. Trong đó, quy trình đăng ký thiết bị, đăng ký truy cập và cấp phép truy cập vào thiết bị được thực hiện thông qua các giao dịch Blockchain của nền tảng bảo mật được đề xuất ở Chương 2. Các kết nối sẽ tự động bị loại bỏ khi hết thời gian được cấp phép mà không cần người sở hữu thiết bị thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào.

Trong phần kết luận, luận án trình bày những kết quả đạt được và định hướng phát triển cho nghiên cứu tương lai khi áp dụng kết quả luận án vào thực tiễn.

CHƯƠNG 1. TỔNG QUAN VỀ NỀN TẢNG BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO IoT

1.1. Giới thiệu

Với xu thế phát triển của IoT như hiện nay, việc sử dụng các một nền tảng bảo mật dựa trên kiến trúc phi tập trung cho các mạng IoT có kích thước lớn với nhu cầu mở rộng cao là một giải pháp phù hợp. Do đó, luận án sẽ đề xuất một nền tảng bảo mật dựa trên kiến trúc phi tập trung cho IoT với công nghệ Blockchain làm thành phần trung tâm.

Hiện tại, các nền tảng bảo mật dựa trên Blockchain cho IoT có hai hạn chế: (1) các Miner trong nền tảng chưa tối ưu hiệu năng trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain; và (2) hạn chế về số lượng chức năng bảo mật được cung cấp.

Về mô hình quản lý của một mạng IoT, thông thường một mạng IoT được quản lý bởi một hoặc một vài tổ chức. Trong trường hợp một mạng IoT được quản lý bởi một tổ chức, tổ chức này có thể xây dựng một Private Blockchain cho nền tảng bảo mật. Trong trường hợp mạng IoT được quản lý bởi một vài tổ chức, có thể sử dụng một Consortium Blockchain cho nền tảng bảo mật.

Xuất phát từ các hạn chế đã trình bày ở trên và mô hình quản lý của một mạng IoT, luận án nghiên cứu đề xuất một nền tảng bảo mật mới cho IoT đảm bảo tối ưu hiệu năng cho các

Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Đồng thời nền tảng cũng sẽ cung cấp các chức năng bảo mật như: kiểm soát truy cập, lưu trữ dữ liệu, chia sẻ dữ liệu. Nền tảng được đề xuất sử dụng công nghệ Blockchain làm thành phần trung tâm; kết hợp với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả các Miner trong một mạng Blockchain là hoàn toàn tin cậy, trường hợp này có thể được áp dụng đối với các mạng IoT được quản lý bởi một tổ chức. Trường hợp 2, một mạng Blockchain có tồn tại một số Miner không tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Trường hợp này có thể được áp dụng đối với các mạng IoT được quản lý bởi một vài tổ chức và số lượng Miner bên ngoài được phép tham gia vào mạng sẽ ít hơn 1/3 trong tổng số các Miner trong mạng.

Luận án cũng đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng.

1.2. Một số khái niệm

Khái niệm 1: ***Một nền tảng bảo mật*** *là một tập hợp gồm các chính sách, quy trình, công nghệ được xây dựng nhằm đảm bảo an toàn bảo mật cho hệ thống sử dụng nó.*

Khái niệm 2: ***Liên mạng vạn vật*** *(còn được gọi là IoT) là một mạng gồm nhiều thiết bị vật lý tham gia vào nhằm mục đích kết nối và trao đổi dữ liệu với các thiết bị và hệ thống khác thông qua Internet.*

Khái niệm 3: ***Node*** *là một máy tính, một server, hoặc một thiết bị IoT có thể kết nối vào Internet.*

Khái niệm 4: ***Miner*** *là một Node có khả năng tạo ra các khối mới trong sổ cái của một mạng Blockchain.*

Khái niệm 5: ***Sổ cái*** *trong công nghệ Blockchain là một cơ sở dữ liệu của một mạng Blockchain, lưu một chuỗi các khối đã được đồng thuận bởi các Miner trong một mạng Blockchain.*

Khái niệm 6: ***Giao thức đồng thuận*** *là một cơ chế mà tất cả các Miner tin cậy đều có cùng một quyết định (từ chối hoặc chấp nhận) một khối mới.*

Khái niệm 7: ***Mining*** *là quá trình các Miner sử dụng một giao thức đồng thuận để tạo một khối mới và lưu nó lên sổ cái Blockchain của chúng.*

Khái niệm 8: ***Giao dịch trong mạng Blockchain*** *là một cấu trúc dữ liệu bao gồm địa chỉ người gửi, địa chỉ người nhận, và nội dung giao dịch. Mỗi giao dịch được ký bằng phương thức chữ ký số của người thực hiện giao dịch.*

Khái niệm 9: ***Pool*** *là nơi chứa các giao dịch chưa được xác minh.*

Khái niệm 10: ***Hợp đồng thông minh*** *trong Blockchain là các mã lệnh được lưu trữ trên Blockchain và được tự động thực thi khi các điều khoản và điều kiện đã định trước được đáp ứng.*

1.3. Công nghệ Blockchain

Blockchain là một công nghệ chuỗi khối trong đó các khối được kết nối với nhau tạo thành một chuỗi dưới dạng một danh sách liên kết. Mỗi khối bao gồm phần Header lưu các thông tin quản lý của khối và chuỗi, phần Body chứa danh sách các giao dịch. Các khối liên kết với nhau thông qua một con trỏ băm

chứa giá trị băm của khối trước đó được liên kết đến, giá trị băm này cũng được sử dụng để xác định tính toàn vẹn của khối.

1.3.1. Một số giao thức đồng thuận

Một số giao thức đồng thuận thường được sử dụng trong một mạng Blockchain: *Proof-of-Work, Proof-of-Stake, Proof-of-Activity, Proof-of-Authentication, Delegated Proof of Stake, Practical Byzantine Fault Tolerance, Tendermint*.

1.3.2. Các loại mạng Blockchain

Có 3 loại mạng Blockchain: Public Blockchain, Private Blockchain, và Consortium Blockchain.

1.3.3. Các hình thức tấn công bảo mật trên Blockchain

Các hình thức tấn công có thể xảy ra trên một mạng Blockchain bao gồm: Tấn công 51 phần trăm, tấn công Double Spending, tấn công Eclipse, tấn công Selfish Mining, tấn công từ chối dịch vụ.

1.4. Khảo sát các nền tảng bảo mật cho IoT

Qua khảo sát một số nghiên cứu điển hình về nền tảng bảo mật dựa trên Blockchain cho IoT, các giải pháp này có hai hạn chế như sau:

(1) Hạn chế về các tính năng bảo mật được cung cấp.

(2) Các Miner chưa đạt được sự tối ưu trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain.

Do đó, luận án sẽ đề xuất xây dựng một nền tảng bảo mật mới cho IoT với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain đảm bảo tối ưu hiệu năng cho các Miner. Đồng thời nền tảng được đề xuất cung cấp các tính năng bảo mật như: kiểm soát truy cập cho IoT dựa trên thời gian

được cấp phép bởi chủ sở hữu thiết bị, lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư.

1.5. Các nghiên cứu về lưu trữ và chia sẻ dữ liệu

Qua khảo sát các nghiên cứu điển hình về lưu trữ và chia sẻ dữ liệu dựa trên Blockchain, các giải pháp này chưa đáp ứng được tất cả các yêu cầu sau đây:

(1) Dữ liệu lưu trữ cần phải đảm bảo tính bí mật, tính toàn vẹn.

(2) Quá trình chia sẻ dữ liệu cần phải chủ động giữa người sở hữu và người yêu cầu chia sẻ.

(3) Cần cung cấp phương thức để mọi người trên hệ thống có thể kiểm chứng được tính chính xác và tính tin cậy của dữ liệu chia sẻ trước khi gửi yêu cầu chia sẻ đến chủ sở hữu dữ liệu.

Trong luận án sẽ đề xuất phương thức lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo các yêu cầu nêu trên. Đồng thời các phương thức đề xuất cũng sẽ đạt được tính riêng tư, tính chống chối bỏ, và tính ẩn danh. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất.

1.6. Các nghiên cứu về kiểm soát truy cập cho IoT

Trong các giải pháp kiểm soát truy cập đã khảo sát, chưa có giải pháp nào cấp quyền truy cập vào tài nguyên IoT theo thời gian được cấp phép bởi chủ sở hữu tài nguyên; và việc thu hồi quyền truy cập chưa được tự động hóa, nghĩa là sau khi hết khoảng thời gian được cấp phép, kết nối sẽ tự động bị loại bỏ.

Do đó, luận án sẽ đề xuất giải pháp kiểm soát truy cập dựa trên thời gian được cấp phép bởi chủ sở hữu. Trong đó, người sở hữu thiết bị IoT có thể cấp phép một khoảng thời gian truy

xuất nhất định cho người yêu cầu truy cập. Sau khi hết thời gian được cấp phép, kết nối sẽ tự động bị loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào. Giải pháp này là một chức năng trong nền tảng bảo mật được đề xuất.

1.7. Hướng nghiên cứu của luận án

Luận án đưa ra các hướng nghiên cứu như sau:

(1) Đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain được xây dựng dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả Miner trong mạng là hoàn toàn tin cậy. Trường hợp 2, trong một mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Bên cạnh đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner để phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, từ đó sẽ có phương thức bảo mật phù hợp để ngăn chặn chúng. Hướng nghiên cứu này sẽ được luận án trình bày ở Chương 2.

(2) Đề xuất chức năng lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng bảo mật được đề xuất. Hướng nghiên cứu này sẽ được trình bày ở Chương 3.

(3) Đề xuất chức năng kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu cho nền tảng bảo mật được đề xuất. Hướng nghiên cứu này sẽ được trình bày ở Chương 4.

CHƯƠNG 2: NỀN TẢNG BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO IoT

2.1. Giới thiệu

Hai thành phần quan trọng trong một mạng Blockchain chính là các Miner và phương thức đồng thuận được sử dụng. Các Miner cần có hiệu năng tính toán cao và dung lượng lưu trữ đủ lớn để xác minh giao dịch và lưu trữ dữ liệu cho toàn mạng. Phương thức đồng thuận dữ liệu trên sổ cái của một mạng Blockchain có thể ảnh hưởng đến hiệu năng của các Miner, tốc độ xác minh giao dịch và tạo khối trên sổ cái.

2.2. Vấn đề về hiệu năng của Miner

Các nền tảng bảo mật được khảo sát ở Chương 1 chưa đảm bảo tối ưu hiệu năng của các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái trong hai trường hợp sau đây:

a. Trường hợp 1: Tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy, nghĩa là các Miner này không thể bị thỏa hiệp bởi kẻ tấn công và cũng không thực hiện bất kỳ hoạt động gian lận nào trên mạng Blockchain. Nhược điểm của những nền tảng bảo mật đã khảo sát là tốc độ xác minh các giao dịch và tốc độ tạo khối trên sổ cái của các Miner không thay đổi khi bổ sung thêm các Miner vào trong mạng Blockchain

b. Trường hợp 2: Trong mạng Blockchain có tồn tại một số Miner không tin cậy nhưng số lượng ít hơn 1/3 trong tổng số Miner trong mạng. Khi một Miner không tin cậy được lựa chọn để đề xuất khối mới tại một vòng mining, các giao dịch hợp lệ trong khối được đề xuất có thể sẽ phải xác minh tại vòng mining tiếp theo.

2.3. Nền tảng đề xuất

Gọi WL là một danh sách chứa các giao dịch chưa được xác minh nhận được từ các thiết bị IoT trong mạng. Gọi VL là một danh sách chứa các giao dịch đã được xác minh là hợp lệ bởi các Miner. Gọi l là số lượng giao dịch tối đa trong một khối.

Các luật được thiết lập cho WL và VL như sau:

- Các giao dịch chưa được xác minh được lưu vào WL.
- Chỉ các Miner mới có thể xác minh các giao dịch trong WL.
- Các giao dịch được xác minh là hợp lệ sẽ được di chuyển từ WL sang VL. Ngược lại, chúng sẽ bị xóa khỏi WL bởi một ứng dụng của hệ thống.
- Các giao dịch trong VL sau khi được lưu vào sổ cái thành công sẽ được xóa khỏi VL bởi một ứng dụng của hệ thống.

Quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất dựa trên hai trường hợp về các Miner trong một mạng Blockchain như sau:

- Trường hợp 1: Các Miner hoàn toàn tin cậy. Mỗi giao dịch chỉ cần được xác minh bởi một Miner, giao dịch hợp lệ sẽ được lưu vào VL. Tại mỗi vòng Mining, một Miner được lựa chọn để đặt l giao dịch trong VL vào một khối mới, tạo chữ ký số trên khối mới này và quảng bá chúng đến các Miner khác. Các Miner khác chỉ cần xác minh chữ ký số trên khối mới này. Nếu chữ ký số hợp lệ sẽ thêm khối mới này vào sổ cái của chúng.

- Trường hợp 2: Trong mạng có tồn tại một số Miner không tin cậy nhưng số lượng ít hơn 1/3 trong tổng số Miner. Một giao dịch sẽ được lưu vào VL khi đã được sự xác minh là hợp lệ của ít nhất 2/3 trong tổng số các Miner. Tại mỗi vòng mining, một Miner được lựa chọn để đặt l giao dịch trong VL vào một khối mới, tạo chữ ký số trên khối mới này và quảng bá chúng đến các Miner khác. Các Miner khác cần xác minh chữ ký số trên khối mới này có hợp lệ hay không và xác minh các giao dịch trong khối có thuộc VL hay không. Nếu hai điều kiện này đáp ứng thì các Miner sẽ thêm khối mới này vào sổ cái của chúng.

2.4. Đánh giá hiệu năng

2.4.1. Đánh giá nền tảng đề xuất với trường hợp 1

Gọi $A1$ là thuật toán được khái quát từ các giao thức đồng thuận: PoW, PoS, PoA, PoAh, PBFT, Tendermint.

Kết quả đánh giá bằng lý thuyết và thực nghiệm cho thấy rằng, so với thuật toán $A1$ nền tảng được đề của luận án ở trường hợp 1 đã đạt được các ưu điểm như sau:

(1) Tăng số lượng giao dịch được xác minh khi tăng số lượng Miner trong nền tảng.

(2) Giảm thời gian Mining khi tăng số lượng Miner trong nền tảng.

(3) Tăng số lượng giao dịch được xác minh khi thời gian Mining một khối tăng lên trong khi số lượng Miner không thay đổi.

2.4.2. Đánh giá nền tảng đề xuất với trường hợp 2

Gọi $A2$ là thuật toán được khái quát từ các giao thức đồng thuận: PBFT, Tendermint.

Ưu điểm của cơ chế xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng trong trường hợp này đó là các giao dịch chỉ cần xác minh một lần ngay cả khi một Miner không tin cậy được lựa chọn tại một vòng Mining.

2.5. Đánh giá về tính chính xác

Tính chính xác là đảm bảo các dữ liệu lưu trữ trên sổ cái đều là các dữ liệu hợp lệ. Phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng được đề xuất ở hai trường hợp đều đảm bảo được tính hợp lệ của dữ liệu trên sổ cái. Các Miner trong mạng Blockchain sẽ có trách nhiệm xác minh tính hợp lệ của dữ liệu trước khi lưu trữ chúng trên sổ cái.

2.6. Đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP

Các thiết bị IoT trong một mạng IoT có đặc tính và mức độ bảo mật khác nhau. Trong trường hợp một hoặc một vài thiết bị IoT bị nhiễm mã độc hoặc bị thỏa hiệp bởi kẻ tấn công, khi đó thiết bị này có thể thực hiện tấn công từ chối dịch vụ đến các Miner trong nền tảng.

Nhằm phát hiện nhanh các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, luận án đề xuất áp dụng giải pháp hiện nhanh các Hot-IP trên các Miner trong nền tảng được đề xuất. Hot-IP là những IP có tần suất xuất hiện cao trong mạng trong một khoảng thời gian rất ngắn. Các Hot-IP này có khả năng là tấn công từ chối dịch vụ đang xảy ra trong mạng. Phương pháp phát hiện nhanh các Hot-IP trên mạng dựa vào phương pháp thử nhóm bất ứng biến và thuật toán được triển

khai trên các Miner cho kết quả tốt khi xử lý dữ liệu trong thời gian thực.

CHƯƠNG 3: LƯU TRỮ VÀ CHIA SẺ DỮ LIỆU ĐẢM BẢO TÍNH RIÊNG TƯ

3.1. Giới thiệu

Dữ liệu số được cấp chứng chỉ bởi những tổ chức có uy tín được xem là dữ liệu số có giá trị hoặc dữ liệu số đáng tin cậy. Các dữ liệu này được xem là một trong những tài sản có giá trị của các cá nhân và tổ chức, chúng có thể được lưu trữ hoặc chia sẻ/mua bán trên Internet. Luận án đề xuất phương thức tạo dữ liệu, phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu đảm bảo tính riêng tư.

Luận án sử dụng nền tảng lưu trữ phi tập trung IPFS để lưu các dữ liệu số có giá trị. Trong khi đó, địa chỉ truy cập của dữ liệu trên IPFS, chứng chỉ của dữ liệu và các thông tin khác sẽ được lưu trong một giao dịch Blockchain.

3.2. Nền tảng lưu trữ IPFS

IPFS là một nền tảng lưu trữ phi tập trung, mỗi tệp tin lưu trữ trên IPFS sẽ được định danh thông qua giá trị băm của nội dung tệp. Do đó, IPFS đảm bảo được tính toàn vẹn, tính sẵn sàng và khả năng mở rộng.

3.2.1. Các tầng giao thức của IPFS

Các tầng giao thức của IPFS bao gồm: Application, Naming, Merkle Dag, Exchange, Routing, Network.

3.2.2. Các dịch vụ trong IPFS

Các dịch vụ được cung cấp bởi IPFS bao gồm: IPFS Pinning và IPFS Clustering.

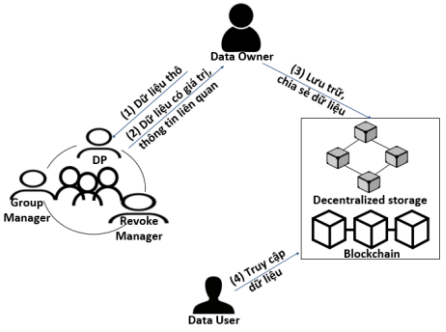
3.3. Chữ ký nhóm

Phương thức chữ ký nhóm cho phép một thành viên trong nhóm đại diện cho nhóm ký ẩn danh lên các thông điệp. Người xác minh chữ ký chỉ kiểm tra được tính hợp lệ của chữ ký nhóm nhưng không thể biết chính xác thành viên nào trong nhóm đã ký. Các thành phần tham gia trong một phương thức chữ ký nhóm bao gồm: các thành viên của nhóm, người quản lý nhóm, người quản lý thu hồi. Người quản lý nhóm có trách nhiệm thiết lập chữ ký và thêm thành viên trong nhóm. Trong khi đó, người quản lý thu hồi có khả năng thu hồi tính ẩn danh của chữ ký.

3.4. Các phương thức đề xuất

3.4.1. Mô hình hệ thống

Hệ thống bao gồm 5 thành phần: (i) Data Owner, người sở hữu dữ liệu được ký hiệu là DO; (ii) Một nhóm các Data Provider, mỗi Data Provider được ký hiệu là DP; (iii) Data User, người dùng dữ liệu được ký hiệu là DU; (iv) Decentralized Storage, hệ thống lưu trữ phi tập trung được ký hiệu là DS, luận án sử dụng IPFS làm DS; và (v) Blockchain, chính là nền tảng bảo mật được đề xuất ở Chương 2.



Hình 3.6: Mô hình hệ thống lưu trữ và chia sẻ dữ liệu

Hệ thống cung cấp ba phương thức: phương thức tạo dữ liệu, phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu.

3.4.2. Xác định các mối đe dọa

Luận án xem xét các mối đe dọa của từng phương thức như sau:

- Phương thức tạo dữ liệu: Phương thức này bao gồm DO và DP tham gia vào. Luận án giả định DO và DP là hoàn toàn tin cậy.
- Phương thức lưu trữ dữ liệu: Phương thức bao gồm các thành phần DO, IPFS và hệ thống Blockchain tham gia vào. Luận án giả định DO là hoàn toàn tin cậy, các Node của hệ thống IPFS và hệ thống Blockchain sẽ thực hiện theo đúng giao thức đã được định nghĩa nhưng chúng có thể truy cập nội dung của dữ liệu được lưu trữ trên chúng. Mục tiêu của những Node này là thỏa hiệp tính bí mật của dữ liệu lưu trữ.
- Phương thức chia sẻ dữ liệu: Phương thức bao gồm các thành phần DO, DU, IPFS và hệ thống Blockchain tham gia vào. Luận án giả định DO và DU là không tin cậy.

3.4.3. Các chức năng bảo mật

Hệ thống cung cấp các chức năng bảo mật như sau:

- *Tính bí mật:* Chỉ những người có thẩm quyền mới có thể đọc được nội dung của dữ liệu có nghĩa đã mã hóa (ký hiệu là EMD) trên IPFS và có được khóa giải mã được lưu trữ trên sổ cái Blockchain.
- *Tính toàn vẹn:* DO không thể giả mạo dữ liệu nhận được từ DP.

- *Tính riêng tư:* Từ các dữ liệu lưu trữ trên Blockchain, mọi người trên hệ thống không thể biết được DO đã sử dụng dịch vụ của DP nào.
- *Tính không chối bỏ:* Các đối tượng không thể chối bỏ các giao dịch mà họ đã thực hiện trong phương thức chia sẻ dữ liệu.
- *Tính ẩn danh:* Tất cả mọi người trong hệ thống không thể biết được danh tính thực sự của các bên tham gia trong phương thức lưu trữ và chia sẻ dữ liệu, và cũng không thể phân biệt được DP nào đã tạo ra dữ liệu có nghĩa (ký hiệu là MD).

3.4.4. Thiết lập hệ thống

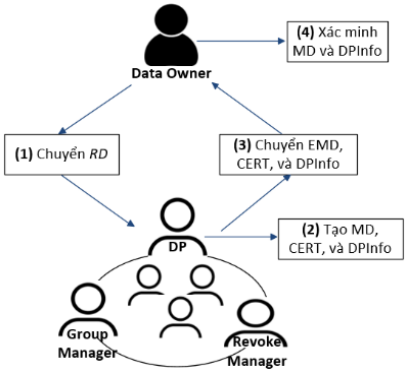
Thiết lập một nhóm các DP: Người quản lý nhóm chọn một tham số bảo mật λ và một phương thức chữ ký nhóm để khởi tạo các khóa cho n thành viên nhóm và một người quản lý thu hồi.

Hệ thống Blockchain: Mỗi DO, DU và người người quản lý nhóm thiết lập một tài khoản trên Blockchain.

3.4.5. Phương thức tạo dữ liệu

Trong phương thức này, DO chuyển dữ liệu thô (ký hiệu là RD) đến một DP cụ thể trong nhóm. Sau khi nhận được RD, DP thực hiện thuật toán Produce để tạo MD, chứng chỉ CERT, và thông tin của DP DPInfo. Để đảm bảo tính bí mật của MD cho phương thức lưu trữ và chia sẻ dữ liệu, DP sẽ mã hóa MD để tạo thành EMD và sau đó cấp CERT trên EMD. Sau đó, DP gửi EMD, CERT, DPInfo đến DO. Sau khi nhận được dữ liệu từ DP, DO xác minh tính chính xác của MD và DPInfo. Việc truyền dữ liệu giữa DO và DP được thực hiện thông qua một

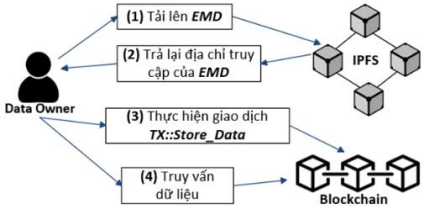
kênh an toàn. Trong phương thức này, DO và DP được xem như là biết nhau. Do đó không cần thiết phải bảo mật danh tính của nhau.



Hình 3.7: Phương thức tạo dữ liệu

3.4.6. Phương thức lưu trữ dữ liệu

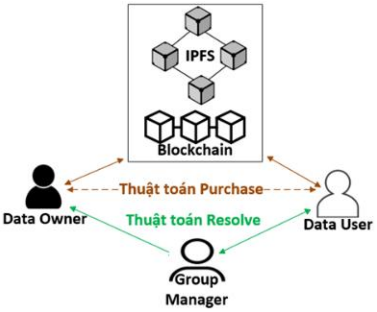
Sau khi nhận được dữ liệu từ DP, DO có thể sử dụng phương thức lưu trữ dữ liệu để lưu chúng trên một hệ thống lưu trữ an toàn. Trong phương thức này, DO lưu trữ EMD trên IPFS, sau đó lưu địa chỉ truy cập của EMD trên IPFS và các thông tin liên quan trong một giao dịch Blockchain. Các thông tin lưu trữ trong giao dịch này cũng sẽ phục vụ cho phương thức chia sẻ dữ liệu.



Hình 3.9: Phương thức lưu trữ dữ liệu

3.4.7. Phương thức chia sẻ dữ liệu

Trong phương thức này, quá trình chia sẻ dữ liệu giữa DO và DU được thực hiện thông qua thuật toán Purchase, và sử dụng thuật toán Resolve để giải quyết tranh chấp khi nhận được yêu cầu giải quyết tránh chấp.



Hình 3.10: Phương thức chia sẻ dữ liệu

Trong phương thức này, EMD được xem như dữ liệu được chia sẻ và Blockchain giống như là một chợ mua bán dữ liệu. Mọi người trên hệ thống có thể tìm và mua các dữ liệu mà họ cần.

3.5. Phân tích và đánh giá

3.5.1. Ưu điểm

Các phương thức đề xuất có các ưu điểm sau: Tính chủ động, tính minh bạch và công bằng trong chia sẻ dữ liệu.

3.5.2. Tính năng bảo mật

Cá tính năng bảo mật đạt được của các phương thức, bao gồm: Tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ và tính ẩn danh.

3.5.3. Tính năng hệ thống

Trong hệ thống đề xuất, hệ thống giao dịch Blockchain và hệ thống lưu trữ IPFS đạt được các tính chất như sau: Tính sẵn sàng, tính toàn vẹn, khả năng mở rộng.

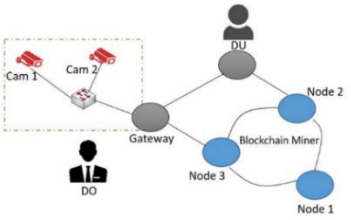
CHƯƠNG 4: GIẢI PHÁP KIỂM SOÁT TRUY CẬP DỰA TRÊN THỜI GIAN ĐƯỢC CẤP PHÉP CHO IoT

4.1. Giới thiệu

Kiểm soát truy cập là phương thức bảo mật để giám sát, cấp quyền hoặc từ chối quyền truy cập vào tài nguyên từ người sở hữu đến người yêu cầu truy cập tài nguyên. Chương này sẽ trình bày giải pháp kiểm soát truy cập cho các thiết bị IoT, giải pháp này là một chức năng trong nền tảng bảo mật được đề xuất ở Chương 2.

4.2. Mô hình hệ thống

Mô hình tổng quan của hệ thống kiểm soát truy cập bao gồm các thành phần như sau: (i) nền tảng bảo mật được đề xuất ở Chương 2, hay còn được gọi là Blockchain; (ii) người dùng; (iii) các thiết bị Camera; (iv) thiết bị gateway, thiết bị này có thể là máy trạm hoặc máy chủ; và (v) chủ sở hữu thiết bị.



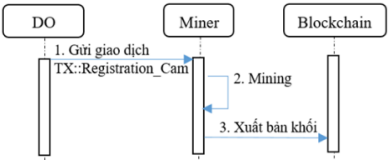
Hình 4.1: Mô hình hệ thống kiểm soát truy cập

4.3. Các quy trình

4.3.1. Quy trình đăng ký thiết bị

Quy trình đăng ký thiết bị được sử dụng bởi DO để công bố thông tin về các thiết bị Camera trong hệ thống đến người dùng, quy trình này và được thể hiện ở Hình 4.3, chi tiết các bước như sau:

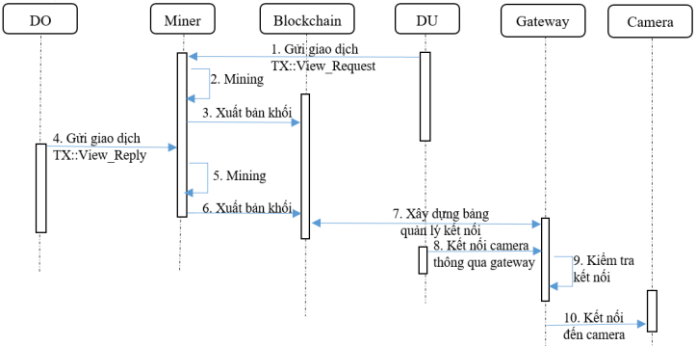
- Bước 1: DO thực hiện một giao dịch đăng ký thiết bị.
- Bước 2: Các Miner xác minh tính hợp lệ của giao dịch bằng cách kiểm tra chữ ký số của người thực hiện giao dịch.
- Bước 3: Nếu giao dịch này hợp lệ, nó sẽ được lưu vào sổ cái Blockchain của các Miner trong mạng.



Hình 4.3: Quy trình đăng ký thiết bị

4.3.2. Quy trình quản lý truy cập

Khi DU có nhu cầu truy cập một Camera, DU sẽ gửi yêu cầu truy cập đến DO, sau đó DO sẽ cấp quyền truy cập cho DU. Các kết nối đến Camera sẽ được thiết bị Gateway kiểm tra quyền truy cập, giám sát và thu hồi quyền truy cập một cách tự động. Trình tự các bước của quy trình quản lý truy cập thiết bị được thể hiện ở Hình 4.5.



Hình 4.5: Quy trình quản lý truy cập

4.4. Đánh giá bảo mật

Bên cạnh các tính chất bảo mật của Blockchain được trình bày ở Chương 3 như tính sẵn sàng, tính toàn vẹn, và khả năng mở rộng. Giải pháp kiểm soát truy cập cho IoT này cũng đạt được tính bí mật khi thông tin thiết bị Camera được lưu trữ trên sổ cái ở dạng mã hóa. Các kết nối từ người dùng đến thiết bị Camera cũng có thể được bảo vệ bằng cách sử dụng giao thức HTTPS.

KẾT LUẬN

Luận án đề xuất một nền tảng bảo mật dựa trên Blockchain cho IoT. Mục tiêu chính của luận án là xây dựng phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain đảm bảo tối ưu về hiệu năng cho các Miner trong mạng, xây dựng chức năng lưu trữ dữ liệu, chia sẻ dữ liệu và kiểm soát truy cập theo thời gian được cấp phép cho nền tảng bảo mật được đề xuất.

Nền tảng bảo mật được đề xuất có ý nghĩa quan trọng trong việc đáp ứng các nhu cầu sử dụng hiện nay trong khi vẫn đảm bảo các yêu cầu bảo mật. So với các nền tảng bảo mật tương tự đã khảo sát, nền tảng bảo mật được luận án đề xuất đạt hiệu quả cao hơn trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain trong cả hai trường hợp về các Miner trong mạng, đặc biệt đối với trường hợp 1. Đồng thời, nền tảng bảo mật được đề xuất cung cấp nhiều tính năng bảo mật hơn và có thể dễ dàng tích hợp thêm nhiều chức năng bảo mật mới. Đây là nền tảng có thể áp dụng vào thực tiễn với các mạng IoT của hệ thống nhà thông minh/thành phố thông minh.

1. Các kết quả đạt được

(1) Luận án đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT. Trong đó, đề xuất phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng được đề xuất dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1: tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy. Trường hợp 2: trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Kết quả đánh giá cho thấy rằng hiệu năng của các Miner trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain trong nền tảng bảo mật được đề xuất tối ưu hơn so với các nền tảng bảo mật tương tự đã khảo sát. Đối với trường hợp 1, càng nhiều Miner tham gia vào mạng, số lượng các giao dịch được xác minh càng lớn và thời gian mining khối mới càng giảm. Tăng số lượng giao dịch được xác minh khi thời gian Mining một khối tăng lên trong khi số lượng Miner không thay đổi. Đối với trường hợp 2, các giao dịch chỉ phải xác minh một lần.

(2) Luận án đề xuất chức năng lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư trong nền tảng bảo mật được đề xuất. Trong chức năng lưu trữ dữ liệu, dữ liệu số được lưu trữ an toàn trên IPFS và Blockchain. Trong chức năng chia sẻ dữ liệu, thông tin của dữ liệu chia sẻ được công khai trên Blockchain sao cho mọi người trên hệ thống đều có thể kiểm chứng tính chính xác và tin cậy của dữ liệu chia sẻ những vẫn đảm bảo tính bí mật của dữ liệu. Quá trình chia sẻ dữ liệu đảm bảo tính chính xác, tính minh bạch và công bằng. Hai chức năng này đạt được

các tính chất bảo mật như: tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ và tính ẩn danh.

(3) Luận án đề xuất chức năng kiểm soát truy cập trong nền tảng bảo mật được đề xuất. Trong đó, chủ sở hữu thiết bị có thể cấp phép một khoảng thời gian truy cập nhất định trên một thiết bị IoT của họ cho những người có nhu cầu truy cập. Việc cấp phép truy cập sẽ được thực hiện thông qua một giao dịch Blockchain. Khi hết thời gian được phép truy cập, kết nối sẽ tự động loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền nào.

2. Hướng phát triển

Luận án đã trình bày nền tảng bảo mật cùng các chức năng tích hợp trong nền tảng. Để có thể áp dụng hiệu quả nền tảng này vào thực tiễn, cần phải nghiên cứu sâu hơn các vấn đề như sau:

(1) Nghiên cứu cách tối ưu trong việc tổ chức WL và VL trong kiến trúc của nền tảng bảo mật được đề xuất cho từng ứng dụng cụ thể.

(2) Nghiên cứu chi tiết cách thức xây dựng và triển khai các hợp đồng thông minh trong chức năng chia sẻ dữ liệu trong nền tảng bảo mật được đề xuất.

(3) Nghiên cứu tối ưu phương thức chữ ký nhóm để nâng cao hiệu quả tính toán trong chức năng chia sẻ dữ liệu trong nền tảng bảo mật được đề xuất.

(4) Nghiên cứu các hạn chế của mạng IPFS, nghiên cứu cách xây dựng và triển khai các thuật toán đề xuất và xây dựng quy trình cài đặt và thực nghiệm nền tảng. Từ đó, thực hiện

đánh giá có tính định lượng hiệu năng bảo mật của các giải pháp đề xuất ở Chương 3, 4.

CÁC CÔNG TRÌNH NGHIÊN CỨU CỦA TÁC GIẢ

TẠP CHÍ KHOA HỌC

[CT1] **Huynh Thanh Tam**, Dang Hai Van, and Nguyen Dinh Thuc (2020). A Solution for Privacy-Preserving Data Sharing on Peer-To-Peer Networks. Tạp chí Khoa học Trường Đại học Sư phạm Thành phố Hồ Chí Minh, tập 17, số 9, trang 1713-1724.

[CT2] **Huynh Thanh Tam**, Nguyen Dinh Thuc, Tan Hanh (2020). A Blockchain-Based Access Control Solution for IoT. Tạp chí Khoa học Công nghệ Thông tin và Truyền thông, số 03(CS.01), trang 15-23.

[CT3] **Huynh Thanh Tam**, Nguyen Dinh Thuc, Dang Hai Van, Huynh Nguyen Chinh. A Novel Security Framework Based On Blockchain for IoT Networks. Tạp chí Phát triển Khoa học và Công nghệ. (đã chấp nhận đăng).

[CT4] **Tam T. Huynh**, Thuc D. Nguyen, Thang Hoang, Lam Tran, Deokjai Choi (2021). A Reliability Guaranteed Solution for Data Storing and Sharing. IEEE Access, vol. 9, pp. 108318-108328. (ISI, IF 3.367).

HỘI NGHỊ KHOA HỌC QUỐC TẾ

[CT5] **Huynh, Tam T.**, Thuc D. Nguyen, and Hanh Tan (2019). A Survey on Security and Privacy Issues of Blockchain Technology. In 2019 International Conference on System Science and Engineering (ICSSE). IEEE, pp. 362-367.

[CT6] **Huynh, Tam T.**, Thuc D. Nguyen, and Hanh Tan (2019). A decentralized solution for web hosting. In 2019 6th NAFOSTED Conference on Information and Computer Science (NICS). IEEE, pp. 82-87.

[CT7] **Huynh, Tam T.**, Chinh N. Huynh, and Thuc D. Nguyen (2020). A Novel Security Solution for Decentralized Web Systems with Real Time Hot-IPs Detection. In International Conference on Green Technology and Sustainable Development. Springer, Cham, pp. 39-48.

[CT8] **Huynh, Tam T.**, Thuc D. Nguyen, Nguyen, Nhung T. H., and Hanh Tan. (2020). Privacy-Preserving for Web Hosting. In International Conference on Industrial Networks and Intelligent Systems. Springer, Cham, pp. 314-323.