

THIẾT BỊ ĐIỀU KHIỂN NHÀ THÔNG MINH CÓ TÍNH BẢO MẬT CAO DỰA TRÊN CƠ SỞ PHẦN CỨNG IOT VÀ HOME ASSISTANT

TS. Lê Trung Dũng^{1*}, ThS. Huỳnh Hoàng Tân²

¹Trường Đại học Thủy Lợi

²Trường Đại học Công nghệ Đồng Nai

*Tác giả liên hệ: Lê Trung Dũng, dung_lt@tlu.edu.vn

THÔNG TIN CHUNG

Ngày nhận bài: 21/07/2023

Ngày nhận bài sửa: 07/09/2023

Ngày duyệt đăng: 21/09/2023

TỪ KHOÁ

Internet of Things;

Virtual Private Network;

Edge Computing;

Smart Home.

TÓM TẮT

Ngày nay, các thiết bị Internet of Things (IoT) đã được phát triển và phổ cập tới từng gia đình, từ các hãng sản xuất phần mềm đến phần cứng, trong và ngoài nước như Amazon, Alphabet, Apple, BKAV, CMC,... Tuy nhiên xu hướng chung là sử dụng dịch vụ lưu trữ dữ liệu trên nền tảng điện toán đám mây của các hãng cung cấp. Do vậy, có nguy cơ rò rỉ dữ liệu qua các trung tâm lưu trữ dữ liệu. Ngoài ra một nguy cơ nữa là các camera thông minh có thể hoạt động như một cửa hậu để xâm phạm mạng của công ty hoặc các cơ sở hạ tầng quan trọng. Thêm nữa, tin tặc có thể tấn công các thiết bị quan trọng và tạo ra rủi ro đáng kể đối với an toàn cá nhân. Nhiều nghiên cứu cũng cho thấy những nguy cơ tiềm tàng đối với các thiết bị IoT. Do vậy, mục tiêu của bài báo là nghiên cứu, nâng cao tính bảo mật dựa trên mạng riêng ảo VPN và tiến tới cá nhân hóa việc điều khiển giám sát nhà thông minh dựa trên nền tảng thiết bị IoT. Dữ liệu hoàn toàn được lưu trữ trực tiếp trên thiết bị của người dùng, không phụ thuộc vào dịch vụ lưu trữ trên nền tảng điện toán đám mây, đảm bảo tính riêng tư và bảo mật.

ABSTRACT

Internet of Things (IoT) devices have become ubiquitous in every household, thanks to the efforts of software and hardware manufacturers such as Amazon, Alphabet, Apple, BKAV, CMC, etc. However, the trend is to use cloud-based data storage services provided by these companies, which poses a risk of data leakage through data storage centers. Additionally, smart cameras could act as a backdoor to compromise corporate networks or critical infrastructure. Hackers can also attack critical devices and pose a significant risk to personal safety.

Many researches highlight potential dangers for IoT devices. Therefore, the goal of the article is to research and improve security based on a virtual private network (VPN) and proceed to personalize smart home monitoring controls based on IoT device platform. Data is completely stored directly on the user's device, independent of cloud storage services, ensuring privacy and security.

1. GIỚI THIỆU

Ngày nay, các thiết bị IoT đã được phát triển và phổ cập tới từng gia đình. Các hãng sản xuất phần cứng lớn đều đã có những sản phẩm mang tính thương mại và phổ cập tới từng nhu cầu của cá nhân lẫn tổ chức lớn. Cụ thể là các sản phẩm của các hãng lớn về dịch vụ Internet như Amazon (Amazon, 2023), Alphabet (Alphabet, 2023), Apple (Apple, 2023)... Tuy nhiên, khi sử dụng, người dùng có một nỗi lo rất lớn về bảo mật. Những thông tin nhạy cảm như âm thanh, hình ảnh đều được lưu trữ, phân tích trên nền tảng điện toán đám mây.

Với những hãng công nghệ lớn trong nước như BKAV (BKAV, 2023), CMC (CMC, 2023),... các sản phẩm điều khiển giám sát nhà thông minh cũng đã được nghiên cứu và thương mại hóa. Tuy nhiên xu hướng chung là sử dụng nền tảng công nghệ được tích hợp từ dịch vụ điện toán đám mây của nhà cung cấp. Do vậy có nguy cơ rò rỉ dữ liệu thông qua trung tâm dữ liệu.

Ngoài ra, hệ thống điều khiển nhà thông minh có nguy cơ từ các camera thông minh (Security Week, 2016), khi hệ thống camera có thể hoạt động như cửa hậu để xâm phạm mạng của công ty hoặc cơ sở hạ tầng quan trọng. Tin tặc cũng có thể tấn công các thiết bị quan trọng và tạo ra rủi ro đáng kể đối với an toàn cá nhân (Basu, 2013). Thêm nữa, bài báo (Westling, 2016) cũng cho thấy những nguy cơ tiềm tàng đối với các thiết bị IoT.

Ngay cả khi có những lựa chọn lưu trữ dữ liệu trên thẻ nhớ của các camera thông minh của các

hãng phổ biến (TP-Link Tapo, Ezviz) thì người dùng vẫn phải tạo tài khoản trên nền tảng điện toán đám mây của hãng để điều khiển và giám sát. Do vậy việc cô lập dữ liệu nhạy cảm như hình ảnh, âm thanh cá nhân khỏi điện toán đám mây là rất khó khăn.

Một trong những xu hướng nghiên cứu là hướng áp dụng mã nguồn mở trong lĩnh vực nhà thông minh như (Thinger.io, 2023) (openHAB, 2023) và (Home Assistant, 2023). Soteris (Soteris Constantinou, 2021) là ứng dụng hệ thống tự động hoá nhà thông minh dựa trên mã nguồn mở OpenHAB và thiết bị phần cứng Raspberry Pi (Raspberry Pi, 2023).

Thêm nữa, hệ thống điều khiển và giám sát nhà thông minh cần tích hợp thêm chức năng của mạng riêng ảo (Virtual Private Network) để không phụ thuộc vào nền tảng điện toán đám mây. Có rất nhiều dịch vụ mạng riêng ảo như OpenVPN (OpenVPN, 2023), Tailscale (Tailscale, 2023), Hamachi (Hamachi, 2023)... Chọn công cụ VPN phù hợp với công cụ mã nguồn mở trong lĩnh vực nhà thông minh cũng là một vấn đề khi mà các công cụ phát triển nhà thông minh dựa trên mã nguồn mở không thể hỗ trợ tất cả các công cụ VPN có trên thị trường.

Trên cơ sở những đánh giá trên, mục tiêu đặt ra của bài báo là phát triển một hệ thống điều khiển giám sát nhà thông minh trên nền tảng thiết bị IoT, công cụ mã nguồn mở trong lĩnh vực nhà thông minh và công cụ VPN phù hợp nhằm đảm bảo tính bảo mật, riêng tư của dữ liệu và không phụ thuộc

vào khả năng lưu trữ của điện toán đám mây. Bài toán đặt ra khả năng lưu trữ dữ liệu tại chính ngôi nhà của chủ nhân. Người sử dụng hoàn toàn có thể điều khiển, giám sát từ xa các thiết bị bên trong ngôi nhà của mình từ bất cứ nơi nào có Internet. Dữ liệu được truyền trực tiếp từ thiết bị IoT tới thiết bị của người dùng thông qua công cụ VPN, đảm bảo tính bảo mật và riêng tư trên môi trường Internet..

2. HỆ THỐNG NHÀ THÔNG MINH MÃ NGUỒN MỞ

Nội dung của phần này sẽ giới thiệu một số hệ thống mã nguồn mở chuyên dùng dành cho hệ thống IoT.

2.1. Thingier.io

Thingier.io là một nền tảng mã nguồn mở dành cho thiết bị Internet Vạn Vật (Internet of Things - IoT). Nền tảng này cung cấp các công cụ cần thiết để nghiên cứu, phát triển từ các nguyên mẫu cho tới các sản phẩm công nghiệp dựa trên nền tảng điện toán đám mây. Hệ thống giúp cho người dùng có thể truy cập tới dữ liệu của các thiết bị IoT từ bất cứ đâu, phát triển nhanh những hệ thống thiết bị IoT với số lượng lớn.

- Nền tảng IoT miễn phí: Thingier.io cung cấp tài khoản miễn phí cho phép người dùng trong quá trình học tập, nghiên cứu với tính năng giới hạn. Khi sản phẩm đã hoàn thiện, người dùng có thể nâng cấp tài khoản Premium Server với đầy đủ tính năng một cách nhanh chóng.

- Hệ thống đơn giản nhưng mạnh mẽ: Chỉ cần một vài dòng lệnh, hệ thống đã có thể kết nối thiết bị IoT, truy xuất dữ liệu hoặc kiểm soát các chức năng bằng bảng điều khiển tích hợp trên nền tảng Web của hệ thống. Hệ thống cung cấp khả năng kết nối tới hàng ngàn thiết bị với cách thức đơn giản như vậy.

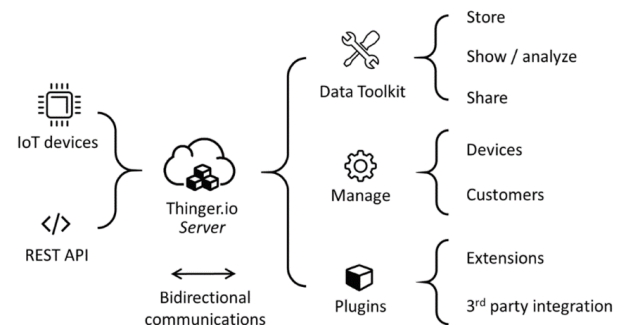
- Hỗ trợ phần cứng: Mọi thiết bị từ bất kỳ nhà sản xuất nào đều có thể dễ dàng tích hợp với cơ sở hạ tầng của Thingier.io.

- Cơ sở hạ tầng hiệu quả và khả năng mở rộng: nhờ vào mô hình giao tiếp độc đáo, máy chủ IoT tương ứng với phần cứng chỉ truy xuất dữ liệu khi cần thiết. Tài khoản Thingier.io duy nhất có thể quản lý hàng nghìn thiết bị IoT với băng thông, tải tính toán và độ trễ thấp.

- Mã nguồn mở: Hầu hết các mô đun, thư viện và mã nguồn đều được đăng tải công khai trên Github (Github Thingier.io, 2023). Người dùng có thể tải về và chỉnh sửa theo bản quyền của MIT (The MIT license, 2023)

Tính năng chính của Thingier.io

Thingier.io được hình thành dựa trên hai sản phẩm chính: Backend (IoT server) và Frontend đơn giản có thể được thực hiện tất cả các tính năng trên bất kỳ máy tính hay điện thoại thông minh nào. Hình 2.1 mô tả các thành phần chính của nền tảng với các dự án IoT.



Hình 1. Nền tảng Thingier.io (Thingier.io, 2023)

- Thiết bị kết nối (IoT devices): Hệ thống hỗ trợ nhiều loại thiết bị, vi xử lý, mạng và các nhà cung cấp thiết bị khác nhau. Hệ thống cho phép tạo kết nối hai chiều với các thiết bị chạy trên nền tảng hệ điều hành Linux, Arduino, Raspberry Pi, hoặc MQTT hay thậm chí cả những công nghệ hỗ trợ Edge computing (Pérez, 2022) như Sigfox, LoRaWan hay nguồn dữ liệu trên Internet từ các hàm API nào.

- Dữ liệu: Chỉ cần kích vào mục tạo Data Bucket để lưu dữ liệu của thiết bị IoT, hệ thống đã có thể lưu dữ liệu một cách hiệu quả. Hệ thống cho

phép khả năng mở rộng, giá thành hợp lý và cho phép tổng hợp dữ liệu theo thời gian thực.

- Hiện thị thời gian thực và lưu trữ dữ liệu bằng nhiều công cụ như time series, donut charts, gauges hoặc công cụ cá nhân hoá theo nhu cầu người dùng một cách nhanh chóng.

- Cơ chế sự kiện và giá trị dữ liệu được nhúng trong hệ thống Node-RED (Node-RED, 2023).

- Có thể mở rộng hệ thống theo tính năng do người dùng tích hợp thêm theo dự án IoT, hệ thống phần mềm hay bất cứ dịch vụ Internet nào.

- Tùy chỉnh theo giao diện, và tên miền web tùy ý của người dùng.

2.2. OpenHAB

Nền tảng open Home Automation Bus (openHAB) là một dự án mã nguồn mở. Nền tảng phát triển với mục tiêu trở thành trung tâm điều khiển của một ngôi nhà thông minh.

Điểm mạnh của openHAB

- Nền tảng cho phép tích hợp nhiều thiết bị và hệ thống khác nhau như các hệ thống tự động hoá nhà thông minh, thiết bị thông minh hay các công nghệ khác.

- Cho phép giao diện người dùng trong việc điều khiển giám sát, tự động hoá toàn bộ ngôi nhà thông minh với các nhà cung cấp thiết bị khác nhau.

- Cung cấp các công cụ có thể thực hiện được hầu hết các công việc, nhiệm vụ khác nhau trong ngôi nhà thông minh.

Các thành phần cơ bản của openHAB

- Thing: Thành phần đại diện cho thiết bị ở lớp vật lý trong phần mềm openHAB.

- Item: Thành phần đại diện cho thông tin của thiết bị (lớp ảo). Item thể hiện chức năng được sử dụng trong giao diện người dùng. Item có khả

năng thể hiện trạng thái và có thể nhận lệnh điều khiển từ giao diện.

- Binding: Thành phần phần mềm cho phép Thing được sẵn sàng trong hệ thống và cung cấp kết nối giữa Item và thiết bị vật lý.

- Channel: Thing cung cấp các chức năng khác nhau và có thể coi mỗi Channel là một hàm từ thông tin của Thing. Ví dụ, Thing có thể là thông tin thời tiết từ một dịch vụ web và các Channel khác nhau có thể là nhiệt độ, áp suất và độ ẩm. Channel cũng chính là liên kết với Item, đó là liên kết giữa lớp ảo và lớp vật lý.

- Rule: Là các quy tắc, luật hay các hàm được thực thi tự động trong ngôi nhà thông minh.

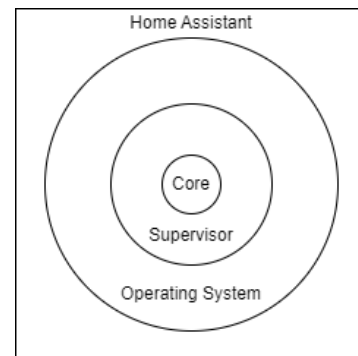
- Page: Giao diện cho phép trao đổi thông tin và giao tiếp giữa người dùng và thiết bị.

2.3. Home Assistant

Home Assistant là hệ thống mã nguồn mở có khả năng quản lý các thiết bị trong ngôi nhà thông minh, đảm bảo tính riêng tư và bảo mật cao.

Tổng quan cấu trúc của hệ thống

Hệ thống cung cấp nền tảng cho điều khiển và tự động hoá ngôi nhà. Hệ thống không chỉ là một phần mềm, đó còn là hệ thống nhúng có khả năng cấu hình, nâng cấp, và giám sát trên giao diện người dùng một cách đơn giản.



Hình 2. Các thành phần của Home Assistant (Home Assistant, 2023)

- Operating system: cung cấp môi trường hệ điều hành Linux để chạy Supervisor và Core.

- Supervisor: quản lý hệ điều hành

- Core: giao tiếp với người dùng, supervisor, và dịch vụ của thiết bị IoT.

Các tính năng quan trọng:

Phần cứng: Home Assistant hỗ trợ cài đặt trên nhiều nền tảng phần cứng khác nhau như Hardkernel ODROID, Raspberry Pi, Asus Tinkerboard, Intel NUC; nhiều hệ điều hành khác nhau như Windows, macOS, Linux.

Điều khiển: Giao diện điều khiển Home Assistant được xây dựng trên giao diện Front-end tên là Lovelace. Giao diện này cho phép hiển thị và điều khiển trên các thẻ khác nhau. Người dùng có thể cá nhân hóa các thẻ này thông qua các đoạn mã dựa trên hệ thống tệp tin YAML.

Tự động hóa: Home Assistant hoạt động như một thiết bị điều khiển thông minh có thể giao tiếp với nhiều loại thiết bị thông minh (như Amazon, Apple, ...) trên cùng mạng nội bộ. Hệ thống có thể tạo ra các kịch bản tự động hóa khác nhau dựa trên các sự kiện mà Home Assistant có thể giám sát. Ví dụ như tự động bật hệ thống bảo mật khi chủ nhân đi vắng và tự động tắt khi chủ nhân ở nhà.

Bảo mật: Hệ thống cho phép tạo nhiều tài khoản điều khiển và giám sát khác nhau. Các tài khoản đều có cơ chế đăng nhập theo mật khẩu tương ứng.

3. MẠNG RIÊNG ẢO

Phần này sẽ trình bày một số giải pháp mạng riêng ảo, và khả năng ứng dụng vào các nền tảng phát triển nhà thông minh.

3.1. LogMeIn Hamachi

LogMeIn Hamachi là một dịch vụ VPN. Hệ thống cho phép người dùng mở rộng mạng lưới nhóm máy tính, điện thoại phân tán cùng làm việc với nhau giống như trên cùng một mạng LAN cục bộ.

Hệ thống cho phép quản lý thông qua website:

- Yêu cầu tạo và quản lý mạng ảo theo yêu cầu người dùng.

- Quản lý và khôi phục mạng ảo cho người dùng cuối từ bất kỳ đâu thông qua giao diện web.

- Nhanh chóng và dễ dàng cung cấp phần mềm máy khách mạng ảo cho các máy tính mới mà không cần phải đến tận nơi.

- Truy cập không giám sát: phần mềm được chạy trên đa nền tảng hệ điều hành, luôn nối mạng để người dùng có quyền truy cập mạng ảo ngay cả khi chúng không được giám sát.

Với bản miễn phí, người dùng có thể tạo không giới hạn số mạng riêng ảo. Mỗi mạng riêng ảo có tối đa 5 thiết bị.

3.2. OpenVPN

OpenVPN là một dự án mã nguồn mở được giới thiệu năm 2001. Dự án giới thiệu cách tạo giao thức VPN miễn phí, bảo mật, nhanh, có thể làm việc với các giao thức TCP (L. Wood, 2007) và UDP (H. Li, 2021) thông qua Internet. Với OpenVPN, người dùng có thể tạo ra mạng ảo, giúp cho các máy tính có thể mã hoá dữ liệu và kết nối với nhau thông qua môi trường Internet. Điều này giúp cho dữ liệu có thể truyền qua mạng Internet công cộng một cách an toàn.

Khi cần tạo mạng riêng ảo, hệ thống cần phải tạo ra:

- OpenVPN Access Server: cho phép điều khiển, vận hành hệ thống OpenVPN trên server. Access Server được xây dựng trên mã nguồn mở OpenVPN có thể được xây dựng một cách nhanh chóng thông qua giao diện Web, kể cả với người không có kiến thức về hệ điều hành Linux. Access Server được triển khai một cách miễn phí. Nếu không có sẵn server, người dùng có thể thuê phần cứng và triển khai ngay trên đám mây của Amazon AWS (AWS, 2023).

- OpenVPN Connect: các máy tính kết nối với OpenVPN Access Server có thể chạy hệ điều hành Windows, macOS, Android, iOS, và hầu hết các hệ điều hành Linux.

Có nhiều phiên bản dựa trên mã nguồn của OpenVPN. Trong đó PiVPN được phát triển nhằm tạo một máy chủ VPN dựa trên giao thức của OpenVPN và phần cứng Raspberry.

3.3. Tailscale

Tailscale là một dịch vụ VPN cho phép các thiết bị có thể được truy cập mọi nơi một cách an toàn và hiệu quả. Hệ thống cho phép mã hoá dữ liệu thông qua giao thức WireGuard (WireGuard, 2023).

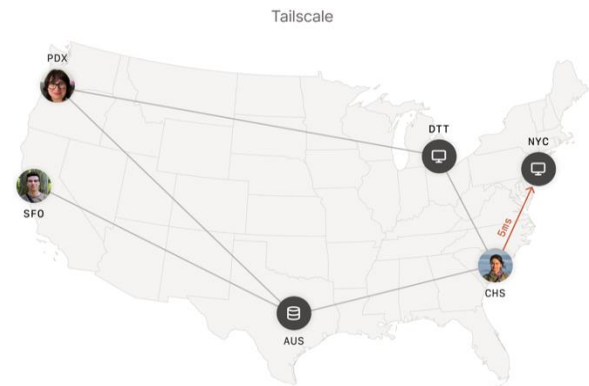
Được xây dựng dựa trên kết cấu mạng an toàn, Tailscale cung cấp tốc độ, độ ổn định và tính đơn giản so với các VPN truyền thống.

Tailscale nhanh và đáng tin cậy. Không giống như các VPN truyền thống tạo đường hầm cho tất cả lưu lượng truy cập mạng thông qua một máy chủ cổng trung tâm, Tailscale tạo ra một mạng lưới ngang hàng (được gọi là Tailnet).

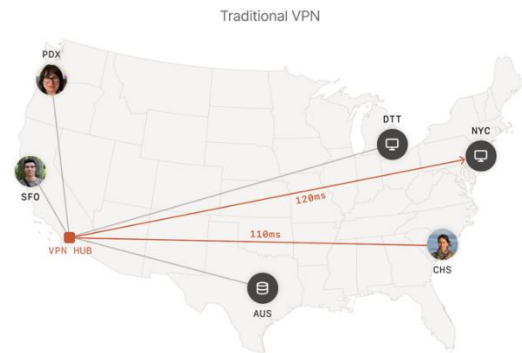
Phương pháp Tailscale tránh tập trung hóa nên có thể, dẫn đến cả thông lượng cao hơn và độ trễ thấp hơn vì lưu lượng mạng có thể truyền trực tiếp giữa các máy. Ngoài ra, phân cấp cải thiện tính ổn định và độ tin cậy bằng cách giảm các điểm lỗi đơn lẻ.

Cài đặt và sử dụng Tailscale rất đơn giản và dễ dàng. Dịch vụ có thể xử lý cấu hình mạng phức tạp. Tailscale có thể tạo kết nối mạng giữa các thiết bị xuyên qua tường lửa và bộ định tuyến, cho phép kết nối trực tiếp mà không cần định cấu hình chuyển tiếp cổng theo cách thủ công. Tailscale cho phép di chuyển kết nối để các kết nối hiện tại vẫn hoạt động ngay cả khi chuyển đổi giữa các mạng khác nhau (ví dụ: có dây, di động, Wi-Fi, v.v.). Với Tailscale, người dùng không phải xử lý các địa chỉ IP, người dùng vẫn có thể SSH hoặc FTP vào thiết bị của mình, truyền tệp giữa các thiết bị hoặc truy

cập máy chủ web hoặc cơ sở dữ liệu chỉ bằng cách sử dụng một tên máy chủ dễ nhớ.



VPN truyền thống



Tailscale

Hình 3. So sánh VPN truyền thống và Tailscale (Tailscale, 2023)

Hình 3 thể hiện sự so sánh giữa giải pháp của Tailscale và công cụ VPN truyền thống. Hình vẽ cho thấy dữ liệu được truyền với tốc độ cao và độ trễ thấp giữa các máy trong mạng khi sử dụng Tailscale. Do vậy việc sử dụng Tailscale là phù hợp với hệ thống điều khiển và giám sát nhà thông minh.

4. LỰA CHỌN MÃ NGUỒN MỞ VÀ MẠNG RIÊNG ẢO

4.1. Lựa chọn mã nguồn mở

Do hệ thống Thinger.io tập trung vào kết nối với các thiết bị IoT, nên nếu hệ thống chỉ cần tập trung vào việc thu thập dữ liệu và điều khiển giám sát thì Thinger.io là phù hợp. Tuy nhiên trong lĩnh vực nhà thông minh, người dùng còn đòi hỏi các kết nối với các trợ lý ảo như Amazon Alexa, Google Assistant.

Thêm nữa, để đảm bảo tính bảo mật và lưu trữ dữ liệu không phụ thuộc vào lưu trữ trên nền tảng điện toán đám mây, Thinger.io là không phù hợp.

Do vậy, bài báo không lựa chọn Thinger.io cho hệ thống điều khiển và giám sát nhà thông minh. Phần sau chỉ trình bày và so sánh giữa hai nền tảng openHAB và Home Assistant.

4.1.1. Ưu và nhược điểm của openHAB

a. Ưu điểm

- Tiện ích mở rộng được sử dụng để bổ sung và tăng khả năng của openHAB.
- Hỗ trợ hàng nghìn thiết bị, nhiều hệ thống và công nghệ.
- Chạy trên nhiều nền tảng như Linux, Mac OSx, Windows, PINE64, Raspberry Pi, Docker, Synology và nhiều nền tảng khác.
- Có thêm bảng Lovelace, các thành phần phần mềm, v.v.
- Hoạt động với Zigbee và Z-Wave.
- Có các cộng đồng tương tác được xây dựng xung quanh chính nó.
- Cài đặt tốt và hướng dẫn tổng thể.

b. Nhược điểm

- Nhiều tùy chọn hơn có nghĩa là cần nhiều thời gian hơn.
- Khó sử dụng.
- Cập nhật bằng dòng lệnh.
- Các phiên bản Raspberry Pi cũ có thể gây ra sự cố do dung lượng RAM thấp.

- Cộng đồng không hấp dẫn so với Home Assistant.

4.1.2. Ưu và nhược điểm của Home Assistant

a. Ưu điểm

- Giao diện người dùng hấp dẫn.
- Hỗ trợ cả Google Assistant và Alexa.
- Nhiều tùy chọn hữu ích.
- Tất cả các mã và bản sửa lỗi đều có sẵn trên GitHub.
- Sáng tạo và linh hoạt.
- Quy tắc tự động hóa linh hoạt để người dùng tùy chỉnh theo ý muốn.
- Nhiều tính năng được kiểm soát bởi Web-UI giúp tiết kiệm thời gian.
- Hướng dẫn từng bước trên trang web cho người dùng mới.
- Thông báo và cảnh báo ổn định hơn.
- Cộng đồng hoạt động tích cực với 500 chủ đề trong 10 danh mục mỗi tuần.

b. Nhược điểm

- Có một số lỗi chữ hoa và chữ thường có thể gây ra sự cố.
- Việc sử dụng tệp YAML có thể khó khăn đối với một số người dùng.
- Người dùng mới có thể khó khăn khi tiếp xúc ban đầu.

4.2. Lựa chọn mạng riêng ảo

Phần này bài báo sẽ so sánh khả năng cài đặt và sử dụng các công cụ VPN trên các nền tảng Linux, Thinger.io, OpenHAB, Home Assistant.

Bảng 1 thể hiện khả năng sử dụng VPN trên các nền tảng khác nhau. Trong đó nếu sử dụng nền tảng hệ điều hành Linux, các công cụ VPN đều có khả năng sử dụng. Tuy nhiên, nếu cài đặt trên hệ thống Thinger.io hoặc OpenHAB thì rất khó cài đặt trực tiếp các công cụ VPN do các hệ thống

không hỗ trợ. Nếu muốn thì hệ thống cần cài đặt bằng dòng lệnh trên hệ điều hành Linux. Điều này gây khó khăn hơn rất nhiều so với nền tảng nhà thông minh có hỗ trợ cài đặt trực tiếp.

Bảng 1. So sánh giải pháp VPN trong các nền tảng điều khiển và giám sát nhà thông minh

	LogMeIn Hamachi	OpenVPN	Tailscale
Linux	Có	Có	Có
Thinger.io	Không	Không	Không
OpenHAB	Dòng lệnh	Dòng lệnh	Dòng lệnh
Home Assistant	Không	Không	Add-on

Ở bảng trên, chỉ có Home Assistant là hỗ trợ cài đặt Tailscale dưới dạng add-on một cách trực tiếp và rất dễ thực thi.

4.3. Lựa chọn hệ thống

Như ở phần trước đã phân tích, công cụ VPN Tailscale cho tốc độ truyền cao và trễ thấp nếu so sánh với các giải pháp VPN truyền thống.

Phần 4.1 và 4.2 cũng cho thấy việc lựa chọn Home Assistant và Tailscale để thực thi hệ thống là phù hợp nhất với bài toán điều khiển và giám sát nhà thông minh đảm bảo tính mật cao và dễ sử dụng.

Phần sau sẽ trình bày thực nghiệm của hệ thống nhà thông minh sử dụng Home Assistant và mạng riêng ảo Tailscale.

5. THỰC NGHIỆM

5.1. Home Assistant

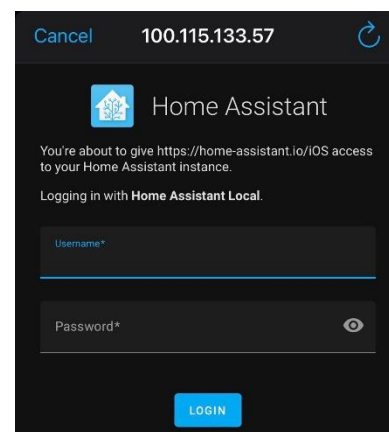
Home Assistant được cài đặt trên phần cứng IoT Raspberry pi 4B (Raspberry Pi, 2023) với cấu hình:

- Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8GHz
- 4GB LPDDR4-3200 SDRAM
- 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE
- Gigabit Ethernet
- 2 USB 3.0 ports; 2 USB 2.0 ports.
- Raspberry Pi standard 40 pin GPIO header
- 2 × micro-HDMI ports (up to 4kp60 supported)
- 2-lane MIPI DSI display port
- 2-lane MIPI CSI camera port
- 4-pole stereo audio and composite video port

Phiên bản Home Assistant

- Home Assistant 2023.5.4
- Supervisor 2023.04.1
- Operating System 10.1

Khi truy cập với địa chỉ IP của Raspberry Pi cài đặt Home Assistant, hệ thống yêu cầu đăng nhập theo tài khoản và mật khẩu của hệ thống. Điều này giúp đảm bảo tính bảo mật của hệ thống điều khiển và giám sát nhà thông minh.



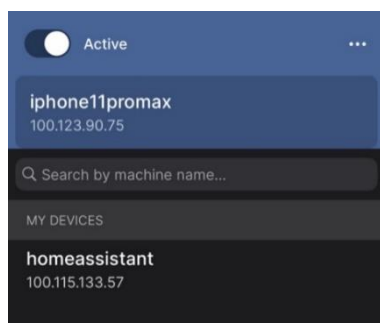
Hình 4. Màn hình đăng nhập Home Assistant

5.2. Tailscale

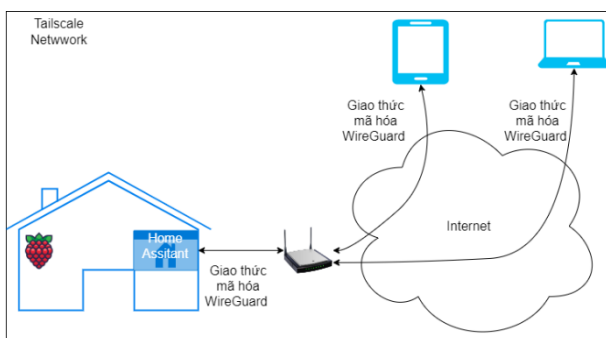
Mạng riêng ảo của hệ thống được khởi tạo:

- Dịch vụ VPN được cung cấp tại địa chỉ <https://tailscale.com/>
- Cài add-on Tailscale trên Home Assistant và đăng nhập theo tài khoản đã tạo.
- Cài phần mềm Tailscale trên thiết bị giám sát. Phần mềm hỗ trợ hầu hết các hệ điều hành thông dụng như: macOS, iOS, Windows, Linux, Android. Đăng nhập phần mềm theo tài khoản đã tạo.

Sau khi đã đăng nhập trên Home Assistant và thiết bị giám sát, hệ thống đã được thiết lập cùng một mạng VPN, dữ liệu được mã hoá đảm bảo tính năng bảo mật và an toàn trên Internet.



Hình 5. Kích hoạt mạng riêng ảo, tạo kết nối VPN với Home Assistant



Hình 6. Hệ thống điều khiển và giám sát dựa trên phần cứng Raspberry, phần mềm Home Assistant và mạng riêng ảo Tailscale

5.3. Giao diện điều khiển và giám sát nhà thông minh

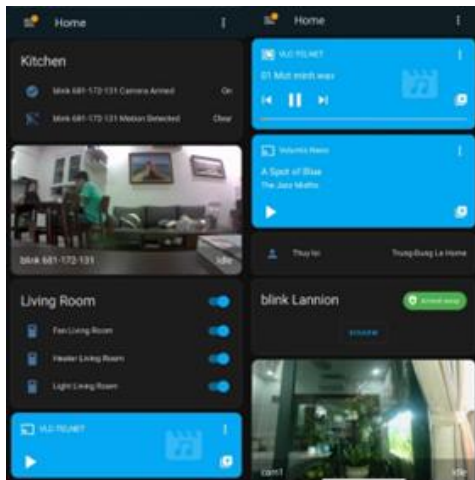
Hình 6 mô tả hệ thống thực nghiệm sau khi đã thiết lập trên các thiết bị. Hệ thống cho thấy dữ liệu đã được mã hóa trước khi truyền đi trên môi trường internet. Hệ thống cũng cho thấy các thiết bị có thể điều khiển và giám sát thông qua mạng riêng ảo Tailscale. Ngoài ra, hệ thống cũng cho thấy không sử dụng bất kì dịch vụ điện toán đám mây của nhà cung cấp dịch vụ lưu trữ dữ liệu nào. Toàn bộ dữ liệu đều được lưu trữ và giám sát trực tiếp trên thiết bị của hệ thống.

Cụ thể hệ thống đã được thực nghiệm trên nền tảng phần cứng Raspberry, camera thông minh Blink Mini, webcam, hệ thống Rơ le kết nối với Raspberry thông qua cổng GPIO, giám sát trên các thiết bị có khả năng kết nối Internet và mạng riêng ảo Tailscale.

Các thiết bị điện thông qua cổng GPIO của Raspberry Pi 4B:

- Fan Living Room
- Heater Living Room
- Light Living Room
- Điều khiển chơi nhạc bằng phần mềm VLC và phát âm thanh qua cổng audio của Raspberry Pi.
- Giám sát hình ảnh (blink 681-172-131) trên Camera thông minh Amazon Blink (dữ liệu hình ảnh được lưu trữ đường dẫn /media/camera/)
- Giám sát hình ảnh (cam1) thông qua webcam gắn trực tiếp trên cổng USB của Raspberry Pi 4B (dữ liệu hình ảnh được lưu trữ trực tiếp trên thẻ nhớ tại đường dẫn /dev/video/)

Hình 7 cho thấy giao diện điều khiển và giám sát hệ thống nhà thông minh bằng Home Assistant. Trong đó hệ thống cho phép giám sát hình ảnh qua Camera thông minh Blink Mini, web cam, điều khiển các thiết bị điện thông qua cổng GPIO, điều khiển chơi nhạc thông qua phần mềm VLC.



Hình 7. Giao diện điều khiển và giám sát nhà thông minh

Hình 7 cho thấy giao diện điều khiển và giám sát hệ thống nhà thông minh bằng Home Assistant. Trong đó hệ thống cho phép giám sát hình ảnh qua Camera thông minh Blink Mini, web cam, điều khiển các thiết bị điện thông qua cổng GPIO, điều khiển chơi nhạc thông qua phần mềm VLC.

5.4. So sánh với các giải pháp công nghệ phổ biến

Phần này sẽ đề cập tới các nhóm giải pháp của các nhà sản xuất nổi tiếng trên thế giới như Amazon, Alphabet, Apple hay giải pháp mã nguồn mở openHAB.

Đầu tiên, khi so sánh giữa các nền tảng điều khiển giám sát nhà thông minh, các giải pháp phải được so sánh ở khả năng tích hợp các thiết bị Internet vạn vật.

- + Amazon Alexa: 20 000 thiết bị.
- + Google Home: 5000 thiết bị.
- + Apple HomeKit: 200 thiết bị
- + OpenHAB: 2000 thiết bị
- + Home Assistant: 2400 thiết bị

Tiếp theo, các nền tảng thường hỗ trợ khả năng tự động hoá ngôi nhà.

- + Amazon Alexa: hệ thống cho phép tự động hoá với các thiết bị vào/ra, thời gian, cảm biến.

+ Google Home: hệ thống chỉ cho phép tự động hoá theo lệnh hoặc thời gian.

+ Apple HomeKit: hệ thống cho phép tự động hoá theo vị trí, thời gian hoặc các cảm biến thông minh.

+ OpenHAB: hệ thống cho phép tự động hoá với các thiết bị vào/ra, thời gian, vị trí, cảm biến.

+ Home Assistant: hệ thống cho phép tự động hoá với các thiết bị vào/ra, thời gian, vị trí, cảm biến.

Lưu trữ dữ liệu trên nền tảng điện toán đám mây: tất cả các nền tảng đều có khả năng lưu trữ dữ liệu trên đám mây do hãng cung cấp.

Lựa chọn lưu trữ không sử dụng điện toán đám mây: trong các nền tảng tham gia khảo sát thì Home Assistant và openHAB cho phép tự động hoá lưu trữ dữ liệu trên bộ nhớ của người dùng.

Các hệ thống tham gia khảo sát đều cho phép quản lý giao diện người dùng một cách hiệu quả.

Tăng cường hệ thống bảo mật: các hệ thống như Amazon Alexa, Google Home, Apple HomeKit đều không cho phép tạo hoặc cài đặt mạng riêng ảo VPN trên phần cứng của hãng. Hệ thống openHAB và Home Assistant đều cho phép cài đặt thêm mạng riêng ảo như Tailscale. Tuy nhiên openHAB chỉ cho phép cài đặt VPN trên hệ thống dòng lệnh gây khó khăn cho người dùng. Home Assistant cho phép cài đặt VPN dạng giao diện người dùng nên rất dễ thao tác.

Bảng 2. So sánh các nền tảng điều khiển và giám sát nhà thông minh

	Amazon Alexa	Google Home	Apple HomeKit	openHaB	Home Assistant
Khả năng kết nối	20 000+	5000+	200+	2000+	2400+
Tự động hoá	Cảm biến, thời gian	Lệnh, thời gian	Vị trí, cảm biến, thời gian	Vị trí, cảm biến, thời gian	Vị trí, cảm biến, thời gian
Đám mây	Có	Có	Có	Có	Có
Giao diện người dùng	Có	Có	Có	Có	Có
VPN	Không	Không	Không	Có Dòng lệnh	Có Giao diện

Bảng 2 tổng hợp các so sánh giữa các nền tảng điều khiển, giám sát nhà thông minh. Trong đó thể hiện khả năng phát triển hệ thống dựa trên mã nguồn mở và tăng cường tính bảo mật dựa trên mạng riêng ảo giúp người dùng bảo vệ dữ liệu cá nhân tránh rò rỉ dữ liệu trên nền tảng điện toán đám mây. Nhờ khả năng mã hoá của mạng riêng ảo, hệ thống cũng giảm khả năng rò rỉ dữ liệu trên đường truyền Internet.

6. KẾT LUẬN

6.1 Kết luận

Kết quả thực nghiệm cho thấy hệ thống Home Assistant cho phép

- Điều khiển các thiết bị điện thông thường thông qua cổng GPIO của phần cứng Raspberry pi 4B
- Giám sát hình ảnh thông qua webcam, lưu trữ trực tiếp trên bộ nhớ.
- Phát hiện chuyển động, giám sát hình ảnh thông qua Camera Blink mini và lưu trữ dữ liệu trên bộ nhớ.
- Có thể phát nhạc qua hệ thống âm thanh qua cổng audio 3.5 mm.
- Điều khiển và giám sát qua Internet thông qua công cụ mạng riêng ảo Tailscale.

Hệ thống có tính bảo mật cao:

- Hệ thống được điều khiển và giám sát thông qua tài khoản và mật khẩu trên Home Assistant.
- Hệ thống mạng riêng ảo quản lý theo tài khoản và mật khẩu riêng.
- Dữ liệu được mã hoá theo chuẩn WireGuard cho phép hệ thống truyền dữ liệu một cách an toàn và hiệu quả

Như vậy hệ thống cho thấy ngoài 2 lớp bảo mật theo tài khoản và mật khẩu của Home Assistant và Tailscale, dữ liệu của hệ thống được mã hoá, đảm bảo an toàn cho việc gửi dữ liệu qua lại giữa các thiết bị trong hệ thống. Điều này là cần

thiết nếu các thiết bị kết nối với các mạng Internet không an toàn tại nơi công cộng.

6.2 Hướng phát triển

Đối với hệ thống điều khiển và giám sát, hệ thống có thể phát triển theo hướng không phụ thuộc vào nền tảng Home Assistant hay các nền tảng có sẵn khác. Tuy nhiên với hướng đi này, hệ thống phải được xây dựng từ đầu với phần cứng đóng vai trò như một server thu thập dữ liệu và điều khiển các thiết bị trong nhà thông minh.

Đối với hệ thống mạng riêng ảo, hệ thống có thể phát triển theo hướng tự khai thác các hệ thống mã nguồn mở như OpenVPN hay WireGuard. Tuy nhiên nếu phát triển theo hướng này thì hệ thống sẽ phải biết cấu hình của Modem Internet, mở cổng và kết nối tới máy chủ mạng riêng ảo. Thêm nữa, với địa chỉ IP động thì cấu hình hệ thống mạng riêng ảo cũng thay đổi liên tục. Do vậy, hướng phát triển này không phù hợp với hệ thống có khả năng truy cập Internet nhưng không có khả năng thay đổi cấu hình của Modem Internet.

Trong trường hợp phát triển mạng riêng ảo trên nền tảng điện toán đám mây, người dùng có thể thuê máy ảo và cài đặt máy chủ mạng riêng ảo OpenVPN hoặc WireGuard. Tuy nhiên, bài toán sẽ phát sinh chi phí thuê máy chủ bên ngoài để quy trị mạng riêng ảo cho hệ thống.

TÀI LIỆU THAM KHẢO

- Alphabet. (2023). <https://home.google.com>
- Amazon. (2023). <https://www.amazon.com/SmartHome/>
- Apple. (2023). <https://www.apple.com/shop/accessories/all/homekit>
- AWS. (2023). <https://aws.amazon.com>
- Basu, E. (2013, Aug 3). Hacking Insulin Pumps and Other Medical Devices From Black Hat. Được truy lục từ FORBES: <http://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other->

- medical-devices-reality-not-fiction/#3ca2eab34327
- BKAV. (2023). <https://smarthome.com.vn/>
- CMC. (2023). <https://cmcsmarthome.com/>
- Github Thinger.io. (2023). <https://github.com/-thinger-io>
- H. Li, Y. Z. (2021). Optimal Design of UDP Protocol in Embedded Real-Time OS. 13th International Conference on Advanced Infocomm Technology (ICAIT), (trang 180-184). Yanji, China.
- Hamachi. (2023). <https://www.vpn.net/>
- Home Assistant. (2023). <https://www.home-assistant.io/>
- L. Wood, C. P. (2007). TCP's protocol radius: the distance where timers prevent communication. International Workshop on Satellite and Space Communications, (trang 163-167). Salzburg, Austria. Được truy lục từ https://en.wikipedia.org/wiki/Transmission_Control_Protocol
- Node-RED. (2023). <https://nodered.org/>
- openHAB. (2023). <https://www.openhab.org/>
- OpenVPN. (2023). <https://www.openvpn.net/>
- Pérez, J. a.-V.-P. (2022). Edge computing. Computing, 104, 2711–2747.
- Raspberry Pi. (2023). <https://www.raspberrypi.com/>
- Security Week. (2016, Jan 13). IoT Devices Easily Hacked to be Backdoors: Experiment. Security Week: <http://www.securityweek.com/iot-devices-easily-hacked-be-backdoors-experiment>
- Soteris Constantinou, A. V.-Y. (2021). IMCF: The IoT Meta-Control Firewall for Smart Buildings. EDBT, (trang 658-661).
- Tailscale. (2023). <https://www.tailscale.com/>
- The MIT license. (2023). <https://opensource.org/license/mit/>
- Thingier.io. (2023). <https://thingier.io/>
- Westling, J. (2016, November 2). Future of the Internet of Things in Mission Critical Applications. Silicon Flatirons Center. doi:<http://dx.doi.org/10.2139/ssrn.2863204>
- WireGuard. (2023). <https://www.wireguard.co-m/>