**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA VIỄN THÔNG I**

****

**BÁO CÁO BÀI TẬP LỚN**

**Môn học: Giải pháp và hệ thống IoT tiến tiến**

**ĐỀ TÀI: GIẢI PHÁP MỚI TRONG NHÀ THÔNG MINH  
CHO PHÉP KẾT NỐI ĐA HỆ SINH THÁI SỬ DỤNG  
GIAO THỨC MATTER**

|  |  |
| --- | --- |
| **Nhóm :** | **01** |
| **Tạ Văn An** | **B20DCVT009** |
| **Vi Xuân Trường** | **B20DCVT009** |
| **Hoàng Thành Long** | **B20DCVT009** |
| **Nhóm lớp học :** | **IoT1** |
| **Giảng viên :** | **TS. Ngô Thị Thu Trang** |

**LỜI MỞ ĐẦU**

Internet of Things (IoT) đã từng bước trở thành một phần không thể thiếu của cuộc sống hiện đại, mở ra nhiều cơ hội mới và thú vị trong việc kết nối các thiết bị và tự động hóa các quy trình hàng ngày. Từ thiết bị gia đình thông minh như đèn chiếu sáng và máy lạnh đến các ứng dụng công nghiệp như quản lý hệ thống sản xuất và theo dõi tài sản, IoT đã thúc đẩy sự phát triển và tiến bộ trong nhiều lĩnh vực.

Tuy nhiên, với sự phát triển nhanh chóng của IoT, đã xuất hiện nhiều tiêu chuẩn và giao thức khác nhau, dẫn đến sự phức tạp và sự không tương thích giữa các thiết bị từ các nhà sản xuất khác nhau. Khách hàng cũng đối diện với thách thức khi lựa chọn các sản phẩm tương thích với hệ sinh thái của họ và việc chuyển đổi giữa các hệ sinh thái có thể gặp rất nhiều rắc rối. Để giải quyết vấn đề này, Matter Protocol đã ra đời với mục tiêu tạo ra một tiêu chuẩn giao thức chung và mở, cho phép các thiết bị IoT từ nhiều nhà sản xuất khác nhau có thể tương thích và tương tác với nhau một cách dễ dàng và linh hoạt. Matter Protocol hứa hẹn mở ra một tương lai IoT đơn giản hơn, tiện lợi hơn và đồng nhất hơn, mang lại lợi ích to lớn cho người dùng và doanh nghiệp.

**CHƯƠNG I: TÓM TẮT VỀ GIAO THỨC TRONG HỆ THỐNG IOT**

**1.1. Đặt vấn đề**

* + 1. **IoT và các giao thức trong IoT**

Internet of Things (IOT) là công nghệ cho phép chúng ta truyền dữ liệu và lệnh tới các thiết bị thông minh trong thời gian thực. IoT là một mạng lưới các thiết bị được kết nối qua Internet, với một trung tâm có thể phân tích dữ liệu tổng hợp. Các điểm cuối IoT có thể là một người, một động vật, một ngôi nhà, một trang trại, một tòa nhà hoặc toàn bộ thành phố. Nhưng trong mọi trường hợp, những vật này có thể “nói chuyện” với nhau mà không cần bất kỳ sự can thiệp nào của con người thông qua giao thức IoT. Có nhiều giao thức khác nhau cho các lớp khác nhau trong kiến trúc IoT

Dưới đây là một số giao thức phổ biến trong IoT:

1. MQTT (Message Queuing Telemetry Transport): MQTT là một giao thức được sử dụng rộng rãi trong các ứng dụng IoT để truyền thông tin giữa các thiết bị và máy chủ. MQTT sử dụng mô hình publish-subscribe, trong đó các thiết bị có thể xuất bản (publish) dữ liệu và các thiết bị khác có thể đăng ký (subscribe) để nhận dữ liệu.

2. HTTP (Hypertext Transfer Protocol): Mặc dù HTTP không được thiết kế đặc biệt cho IoT, nhưng nó vẫn được sử dụng rộng rãi trong một số ứng dụng IoT.Các thiết bị IoT có thể sử dụng HTTP để truyền dữ liệu đến các máy chủ hoặc ứng dụng web, hoặc để nhận các chỉ thị điều khiển từ các máy chủ.

3. CoAP (Constrained Application Protocol): là một giao thức nhẹ, được thiết kế đặc biệt cho các thiết bị IoT có tài nguyên hạn chế như bộ nhớ, CPU và pin. Nó cung cấp một cách tiếp cận RESTful cho giao tiếp giữa các thiết bị IoT và máy chủ, giúp đơn giản hóa việc phát triển ứng dụng IoT.

4. Bluetooth và Bluetooth Low Energy (BLE): Bluetooth và BLE là các giao thức không dây được sử dụng phổ biến trong các ứng dụng IoT ngắn phạm vi như các thiết bị đeo thông minh, cảm biến, và các hệ thống điều khiển nhà thông minh.

6. Zigbee và Z-Wave: Zigbee và Z-Wave là hai giao thức mạng không dây được thiết kế đặc biệt cho IoT, đặc biệt là trong các ứng dụng nhà thông minh và điều khiển thiết bị.

**1.2. Giải pháp Matter**

**1.2.1. Sự ra đời của Matter**

Trong những năm gần đây, với sự bùng nổ của IoT nhà thông minh ngày càng trở nên phổ biến và được dự đoán sẽ trở thành xu hướng của tương lai. Nhà thông minh là không gian sống được lắp đặt, trang bị các thiết bị công nghệ điện tử được điều khiển tự động hóa hay bán tự động thông qua các ứng dụng quản lý trên điện thoại, trợ lý ảo thông minh hoặc bằng giọng nói với bộ điều khiển trung tâm đặt bên trong ngôi nhà. Nhờ vào việc ứng dụng kết hợp các công nghệ như hồng ngoại, cảm biến, điện thoại thông minh, công nghệ đám mây, IoT, hệ thống tự động hóa, camera giám sát,… nhà thông minh có khả năng giúp bạn hoàn thành các công việc thường ngày như: kéo rèm, tắt, mở đèn, tivi, điều hòa, loa,... chỉ với vài thao tác chạm hoặc nói thông qua thiết bị mà không cần tốn quá nhiều công sức để trực tiếp thực hiện như trước đây.

Kết quả báo cáo tổng kết của Zion Market Research công bố cho thấy thị trường smarthome trên toàn cầu đạt giá trị khoảng 24,10 tỷ USD trong năm 2016 và đã tăng gần gấp đôi sau khoảng 6 năm với mức tăng trưởng dự kiến là 53,45 tỷ USD trong năm 2022 với mức tăng trưởng trung bình hàng năm đều trên 14,5%, một con số tăng trưởng vô cùng khả quan. Thị trường Bắc Mỹ và châu Âu được xem là nơi tiên phong của nhà thông minh, trong khi khu vực châu Á - Thái Bình Dương là khu vực có tiềm năng phát triển về nhà thông minh nhiều nhất với nhu cầu khổng lồ về thiết bị điều khiển tự động, thiết bị giải trí, an ninh trong ngôi nhà.

Theo thống kê từ Statista, Mỹ là quốc gia đứng đầu thế giới về nhu cầu sử dụng nhà thông minh với doanh thu 18 tỷ USD mỗi năm. Đứng ở vị trí thứ 2 là thị trường đông dân nhất thế giới, Trung Quốc với 6,5 tỷ USD và Nhật Bản hiện xếp thứ 3. Dự kiến, số lượng người sử dụng căn hộ thông minh tại Mỹ sẽ là 700.000 đến năm 2022. Các chuyên gia dự đoán tốc độ phát triển của smarthome cùng nhu cầu của người dân sẽ càng tăng cao, smarthome hoàn toàn có thể trở thành xu hướng lựa sống trong tương lai.

Tuy nhiên, với sự phát triển nhanh chóng này đến từ các nhà sản xuất khác nhau, người tiêu dùng thường gặp phải một vấn đề lớn: sự không tương thích giữa các thiết bị từ các hãng khác nhau. Điều này dẫn đến một hệ sinh thái khó sử dụng, khi mà mỗi thiết bị thông minh đều yêu cầu ứng dụng và giao thức riêng biệt để hoạt động. Trong bối cảnh này, việc phát triển smarthome sử dụng đa hệ sinh thái đã trở thành một thách thức đáng kể. Các nhà sản xuất phải đối mặt với việc tích hợp các thiết bị từ nhiều nguồn khác nhau vào một hệ thống hoạt động một cách mượt mà và hiệu quả. Điều này không chỉ yêu cầu sự hợp tác giữa các nhà sản xuất, mà còn đòi hỏi một tiêu chuẩn chung về giao thức liên kết các thiết bị này với nhau.

* Giao thức Matter ra đời

**1.2.2. Giao thức Matter là gì?**

Matter là một giao thức mạng không dây đặc biệt được thiết kế để hoạt động trên các tầng vật lý, liên kết dữ liệu, và mạng, cũng như tích hợp với các tầng cao hơn như tầng ứng dụng để cung cấp các dịch vụ IoT, Matter không là một phần của mô hình OSI.

Matter được thiết kế để tạo ra một môi trường kết nối thông minh và tương thích cho các thiết bị trong ngôi nhà thông minh và Internet of Things (IoT). Là tiêu chuẩn thống nhất ngành được xác nhận qua Connectivity Standards Alliance với hơn 300 thành viên các công ty

**1.2.3 Đặc điểm**

Đơn giản: Matter được thiết kế để dễ sử dụng cho người tiêu dùng và dễ phát triển cho các nhà sản xuất. Với giao thức này, việc kết nối và quản lý các thiết bị trong ngôi nhà thông minh trở nên đơn giản hơn bao giờ hết.

Đáng tin cậy: cung cấp một mạng cục bộ đáng tin cậy, với các quy trình chứng nhận đảm bảo tính an toàn và tin cậy cho người dùng.

Liền mạch: Với cấu trúc thống nhất, Matter cho phép các thiết bị tương tác với nhau một cách liền mạch, không gặp sự cản trở do sự không tương thích.

Bảo mật: Matter thực hiện xác thực trước khi thiết bị tham gia mạng, và tất cả các giao tiếp giữa các thiết bị được mã hóa, đảm bảo tính bảo mật cho dữ liệu và thông tin cá nhân của người dùng.

Mở: mã nguồn mở, tạo điều kiện cho sự hợp tác và phát triển từ cộng đồng lập trình viên

**CHƯƠNG II: GIAO THỨC MATTER**

**2.1. Kiến trúc**

**2.1.1. Kiến trúc phân lớp**

Kiến trúc được chia thành các lớp giúp phân tách các nhiệm vụ khác nhau .Để phù hợp cho việc triển khai, bốn tầng cuối cùng được xử lý như một Masaging Layer và một Transport Layer.

A diagram of a pyramid

Description automatically generated

**Lớp ứng dụng (Application Layer):**

+ Tầng cao nhất trong kiến trúc Matter.

+ Bao gồm logic cấp cao của thiết bị và ứng dụng người dùng.

+ Xây dựng trên mô hình dữ liệu thống nhất để cải thiện tính tương thích và tương tác giữa các thiết bị.

**Mô hình Dữ liệu (Data Model):**

+ Quản lý cách dữ liệu và các yếu tố hành động hỗ trợ chức năng của ứng dụng.

+ Bao gồm định nghĩa của các yếu tố dữ liệu, không gian tên cho các điểm cuối, cụm và thuộc tính trong ứng dụng.

**Mô hình Tương tác (Interaction Model):**

+ Xử lý các tương tác giữa các nút trong mạng.

+ Quản lý cách dữ liệu được truyền giữa các nút.

+ Thừa kế từ tiêu chuẩn dotdot của Zigbee.

**Khung Hành động (Action Framing):**

+ Chuyển đổi các tương tác thành một gói dữ liệu.

**Khung tin nhắn và Định tuyến(Message Framing and Routing):**

+ Cập nhật gói dữ liệu với thông tin định tuyến như fabric và Node ID.

+ Đảm bảo việc định tuyến hiệu quả của các thông điệp trong mạng.

**Lớp Vận chuyển và khung IP (Transport and IP Framing):**

+ Đảm bảo việc vận chuyển dữ liệu thông qua mạng IP.

+ Bao gồm việc sử dụng TCP hoặc Matter's Message Reliability Protocol để quản lý IP của dữ liệu.2.1.2 Cấu trúc liên kết mạng

**2.1.2. Kiến trúc mạng Matter**

Matter phát triển dựa trên hai công nghệ kết nối nổi bật đó là : Thread và Wi-Fi. Thread là giao thức mạng lưới không dây công suất thấp tạo điều kiện liên lạc đáng tin cậy giữa các nút. Nó cho phép phạm vi phủ sóng mở rộng và kết nối đáng tin cậy để cải thiện hiệu suất tổng thể của hệ sinh thái IoT.

Matter cũng dựa trên IPv6 sử dụng các giao thức lớp vận chuyển như TCP/UDP để hỗ trợ việc đánh địa chỉ mạng và truyền các gói dữ liệu một cách đáng tin cậy. Do đó, Matter tương thích với nhiều tùy chọn kết nối (chẳng hạn như Thread và Wi-Fi). Tính linh hoạt này cho phép các thiết bị hỗ trợ Matter giao tiếp qua nhiều giao thức mạng khác nhau, đảm bảo khả năng tương thích và tích hợp rộng rãi với các công nghệ mạng khác nhau.

A close-up of a computer screen

Description automatically generated

Sức mạnh thực sự của Matter nằm ở khả năng tương tác. Các công ty hàng đầu trong ngành như Google, Apple, Amazon và Samsung Smart Things đã triển khai Matter trong các thiết bị IoT của họ, thúc đẩy việc áp dụng rộng rãi hơn từ các nhà sản xuất khác. Matter cũng hỗ trợ kết nối từ các công nghệ hiện có khác, chẳng hạn như Zigbee, Bluetooth® Mesh và Z-Wave. Điều này cho phép công nghệ IoT hiện có được tích hợp vào một môi trường có thể tương tác. Khả năng tương thích và tích hợp liền mạch giữa các thương hiệu tạo ra một hệ sinh thái thống nhất nơi các thiết bị thông minh của bạn hoạt động hài hòa.

Trên lý thuyết, Matter có thể hoạt động trên bất kỳ mạng chứa IPv6 nào. Tuy nhiên, trong thực tế, các thông số kỹ thuật của Matter tập trung hoàn toàn vào ba công nghệ lớp liên kết, cho phép Matter chạy trên các mạng Ethernet, Wi-Fi và Thread 802.15.4. Như đã đề cập ở trên, một trong những lợi ích lớn của Matter là tính linh hoạt của nó, đặc biệt là khi điều chỉnh cấu hình mạng.

Có hai Topology mạng cơ bản thường được sử dụng trong Matter. Đầu tiên là gọi là Topology mạng đơn, trong đó Matter chỉ chạy trên một mạng. Nghĩa là mạng Matter có thể chạy qua một mạng Thread 802.15.4 hoặc qua một mạng Wi-Fi. Trong trường hợp này, tất cả các thiết bị Matter được kết nối với cùng một mạng logic duy nhất.

A screenshot of a phone

Description automatically generatedA close-up of a network

Description automatically generated

Cấu trúc liên kết mạng khác, phổ biến hơn là mạng hình sao, bao gồm nhiều mạng ngoại vi được nối với nhau bằng mạng trung tâm. Nếu sử dụng mạng ngoại vi, mạng đó phải được kết nối trực tiếp với hub thông qua một hoặc nhiều bộ định tuyến biên. Bộ định tuyến viền (hoặc bộ định tuyến biên) là một bộ định tuyến đặc biệt có thể cung cấp dịch vụ định tuyến giữa hai mạng con IP, hoạt động hiệu quả như một cầu nối giữa hai mạng khác nhau. Điều này cho phép rất linh hoạt và khả năng tương tác giữa các mạng gia đình khác nhau mà tất cả đều có thể được kết nối với nhau.

A screenshot of a computer

Description automatically generated

**2.3. Vai trò của BLE trong Matter Network (Bluetooth Low Energy):**

* Sử dụng chủ yếu cho việc khám phá và cấu hình thiết bị : Bluetooth LE cho phép thiết bị Matter được tìm kiếm và thiết lập kết nối với nhau trong quá trình khởi đầu.
* Kết nối thiết bị vào mạng Matter: Bluetooth LE được sử dụng để kết nối một thiết bị mới vào mạng Matter thông qua một bộ điều khiển Matter.
* Không sử dụng cho việc giao tiếp thiết bị đến thiết bị hoặc thiết bị đến bộ điều khiển sau khi hoàn tất quá trình cấu hình. Sau khi quá trình cấu hình được hoàn tất, BLE không được sử dụng cho việc giao tiếp giữa các thiết bị hoặc giữa thiết bị và bộ điều khiển.

**2.4. Những thành phần trong mạng Matter (Matter Network Components)**

- Platform: Một hệ thống nhà thông minh từ một nhà cung cấp cụ thể, có khả năng kết nối và điều khiển các thiết bị Matter từ nhiều nhà cung cấp khác nhau.

- Border Router (Thread): Một Bộ định tuyến Biên. Thread cho phép các thiết bị Thread kết nối vào mạng cục bộ, để chúng có thể giao tiếp với các thiết bị khác được xây dựng trên các công nghệ dựa trên IP như Wi-Fi hoặc Ethernet

- Thread có thể được tích hợp vào các sản phẩm hiện có, như các điểm truy cập Wi-Fi, loa thông minh và nhiều hơn nữa.

- Mesh Extender (Thread): Một Mesh Extender là một thiết bị được cung cấp bằng nguồn AC, lặp lại tín hiệu và mở rộng phạm vi hoặc phạm vi của mạng Thread đến các góc xa của nhà và tòa nhà. Mạng Thread mở rộng tự động khi có thêm nhiều mesh extender được thêm vào, do đó xây dựng một mạng mạnh mẽ, đáng tin cậy hơn.

- Home Gateway (ví dụ: Bộ định tuyến Wi-Fi, Điểm truy cập): Giao diện cho phép giao tiếp IP chảy giữa mạng nhà thông minh cục bộ và Internet.

+ Kết nối các thiết bị Thread với mạng cục bộ,

các thiết bị khác được xây dựng trên công nghệ dựa trên IP như Wi-Fi hoặc Ethernet và Internet.

Nhiều nhà cung cấp nền tảng bao gồm Bộ định tuyến viền chủ đề với các thiết bị đã có mặt ở hàng triệu gia đình ngày nay, ví dụ:

- Amazon Echo (thế hệ thứ 4)

- Apple HomePod (thế hệ thứ 2) và HomePod mini

- Apple TV 4K

- Google Nest Hub Max

- Google Nest Hub (thế hệ thứ 2)

- Google Nest Wifi

- Samsung SmartThings hubs and Station…

**2.3. Mô hình hệ thống**

**2.3.1. Mô hình dữ liệu**

Mô hình dữ liệu là một cách thức tổ chức và mô tả dữ liệu trong giao thức Matter. Nó cung cấp một cấu trúc phân cấp giúp các thiết bị Matter hiểu và chia sẻ thông tin với nhau một cách hiệu quả.

Các thành phần chính của mô hình dữ liệu:

**1. Nút Matter (node):**

- Đại diện cho một **thiết bị vật lý** (Physical Device) duy nhất trong mạng Matter (mỗi thiết bị chỉ có một **Matter Node)**

- Một node có thể chứa nhiều endpoint, tương tự một device có thể có nhiều node.

- Các node trong cùng mạng có thể giao tiếp trực tiếp với nhau.

- Ví dụ: bóng đèn thông minh, ổ cắm thông minh, thermostat thông minh,vv

**2. Điểm kết nối (endpoint):**

- Một **Matter Node** có thể chứa một hoặc nhiều **Endpoint(s)**.

- Mỗi **Endpoint** đại diện cho một **loại chức năng** (Device Function) cụ thể của thiết bị.

- Ví dụ: một bóng đèn thông minh có thể có một **Endpoint** cho chức năng chiếu sáng và một **Endpoint** khác cho cảm biến chuyển động.

**3. Cụm (cluster):**

- Mỗi **Endpoint** được liên kết với một hoặc nhiều **Cluster(s)**.

**- Cluster** là một nhóm các **Attribute(s)** (Thuộc tính) và **Command(s)** (Lệnh) được thiết kế để thực hiện một chức năng cụ thể.

**- Cluster** được xác định trước trong **Device Type** (Loại thiết bị) của thiết bị.

- Ví dụ: **Cluster** On/Off được sử dụng để điều khiển bật/tắt thiết bị, **Cluster** Color Control được sử dụng để điều khiển màu sắc của đèn.

**4. Loại hình thiết bị**

**- Device Type** (Loại thiết bị) xác định cấu trúc của một **Matter Node** (Nút Matter).

- Nó bao gồm các **Cluster** bắt buộc và tùy chọn mà **Endpoint(s)** (Điểm kết nối) của thiết bị phải hỗ trợ.

- Ví dụ: **Device Type** Dimmable Light (Đèn có thể điều chỉnh độ sáng) yêu cầu **Endpoint** hỗ trợ **Cluster** On/Off và Level Control.

**5. Thuộc tính**

- Thuộc tính đại diện cho **trạng thái** (State) của một chức năng cụ thể được mô tả bởi **Cluster**.

**- Attribute** có giá trị, ví dụ: On/Off có thể có giá trị true (bật) hoặc false (tắt), Color Control có thể có giá trị là các thông số màu sắc (độ sáng, nhiệt độ màu, v.v.).

**6. Câu lệnh**

- Lệnh đại diện cho **hành động** (Action) có thể được thực hiện trên một chức năng cụ thể được mô tả bởi **Cluster**.

- Ví dụ: On/Off có thể có lệnh TurnOn và TurnOff, Color Control có thể có lệnh SetColor.

Mô hình dữ liệu trong Matter cung cấp một cách thức chuẩn hóa để các thiết bị Matter giao tiếp và chia sẻ dữ liệu với nhau. Bằng cách sử dụng các thành phần như nút, endpoint, cụm, câu lệnh, thuộc tính, các thiết bị có thể hiểu rõ chức năng của nhau và tương tác một cách hiệu quả trong hệ thống nhà thông minh.

A screenshot of a computer

Description automatically generated

**Cụm máy chủ - máy khách**: là một mô hình thiết kế quan trọng trong giao thức Matter, cho phép chia sẻ dữ liệu và chức năng giữa các thiết bị Matter một cách hiệu quả và an toàn. Mô hình này bao gồm hai thành phần chính:

* Thiết bị khách: Các thiết bị Matter có khả năng truy cập dữ liệu và chức năng từ các Server. Ví dụ: bóng đèn thông minh, ổ cắm thông minh, v.v.
* Thiết bị chủ:

+ Cung cấp dữ liệu và chức năng cho thiết bị khách.

+ Có thể là:

* **Cục bộ:** Chạy trên một thiết bị Matter trong mạng nội bộ. Ví dụ: Matter Hub.
* **Đám mây:** Cung cấp dịch vụ từ xa. Ví dụ: dịch vụ của nhà sản xuất thiết bị.

**Cách thức hoạt động:**

**- Kết nối:** Thiết bị khách kết nối với thiết bị chủ bằng cách sử dụng giao thức Matter over IP (MQTT).

**- Truy cập dữ liệu:** Thiết bị khách yêu cầu dữ liệu từ thiết bị chủ bằng cách sử dụng các lệnh Matter.

**- Cập nhật dữ liệu:** Thiết bị khách có thể cập nhật dữ liệu trên thiết bị chủ.

**Ví dụ: Điều khiển bóng đèn thông minh:**

* “Khách” (bóng đèn) kết nối với “Chủ” (Matter Hub).
* “Khách” yêu cầu “Chủ” bật đèn.
* “Chủ” gửi lệnh bật đèn đến “Khách”.

A diagram of a light switch

Description automatically generated

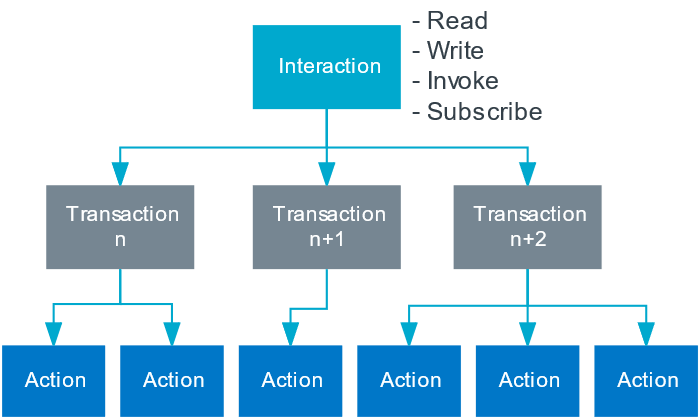
**3.2. Mô hình tương tác**

Mô hình Tương tác Matter (IM) xác định các phương pháp giao tiếp giữa các nút và đóng vai trò là ngôn ngữ chung cho việc truyền thông thông tin từ nút này sang nút khác. Các nút giao tiếp với nhau thông qua các tương tác. Các tương tác là một chuỗi các Transactions, mà trong đó mỗi Transactions lại là một chuỗi các hành động.

Ví dụ, trong một tương tác ĐỌC, một cụm Client có thể khởi tạo một Transactions Đọc, trong đó Client có thể yêu cầu đọc một thuộc tính và một cụm máy chủ có thể phản hồi bằng cách báo cáo thuộc tính. Cả yêu cầu của khách hàng và phản hồi của máy chủ đều là các hành động riêng biệt, nhưng chúng là một phần của cùng một Giao dịch Đọc

Mô hình Tương tác hỗ trợ bốn loại tương tác:

* Đọc: Đọc lấy các thuộc tính, giá trị từ máy chủ
* Ghi: Thay đổi giá trị các thuộc tính
* Kích hoạt: Gửi lệnh đến client
* Đăng ký: Nhận dữ liệu từ thiết bị định kỳ thay vì phải yêu cầu gửi dữ liệu.



Ví dụ về khóa cửa:

A close-up of a document

Description automatically generated

A close-up of a message

Description automatically generated

A close-up of a diagram

Description automatically generated

A diagram of a door lock

Description automatically generated

**CHƯƠNG III: BẢO MẬT TRONG MATTER**

**3.1. Nguyên tắc**

* Không cho phép xâm nhập lạ (No anonymous joining) : Luôn yêu cầu “bằng chứng về quyền sở hữu” (nghĩa là mật mã dành riêng cho thiết bị).
* Chứng thực thiết bị: Mỗi thiết bị đều có danh tính duy nhất được nhà sản xuất xác thực và xác minh thông qua CSA như một thiết bị được chứng nhận.
* Thông tin xác thực hoạt động: Khi được đưa vào mạng Matter, mọi thiết bị đều được cấp thông tin xác thực hoạt động duy nhất sau khi xác minh thông tin xác thực của nhà sản xuất.
* Thông tin xác thực mạng: Khóa mạng Wi-Fi hoặc khóa Thread Master không được cung cấp cho đến khi chứng chỉ của thiết bị được xác minh và xác thực chính xác.
* Tiêu chuẩn mở: Phần mềm nguồn mở được mở cho các bên thứ ba xem xét các khiếu nại bằng cách kiểm tra tiêu chuẩn và kiểm tra mã nguồn.

**3.2. Tổng quan về chứng chỉ và quy trình**

* Mỗi thiết bị Matter nhận được hai chứng chỉ.  Đầu tiên, chứng chỉ thiết bị, được nhà sản xuất lập trình trước khi thiết bị được xuất xưởng. Điều này sẽ được sử dụng sau này để chứng thực thiết bị khi cố gắng tham gia mạng.
* Chứng chỉ còn lại là chứng chỉ vận hành do ủy viên cấp trong giai đoạn vận hành thử. Chứng chỉ vốn sử dụng định dạng CHIP TLV nhưng có thể chuyển đổi sang/từ định dạng X.509. Tất cả các thiết bị đều được cấp chứng chỉ hoạt động để chứng minh quyền của chúng trên mạng Matter (kết cấu) và nhận dạng chúng một cách an toàn.
* Giao tiếp giữa các thiết bị Matter được bảo vệ bằng các khóa khác nhau ở các giai đoạn khác nhau.
* Ở giai đoạn chạy thử, khóa là kết quả của quá trình Thiết lập phiên xác thực bằng mật khẩu (PASE) trên kênh chạy thử bằng cách sử dụng mật mã từ mã QR của thiết bị làm đầu vào. Trong quá trình thiết lập ban đầu này, việc xác minh quyền sở hữu mật mã của cả người ủy quyền và thiết bị tham gia sẽ được xác nhận.
* Ở giai đoạn vận hành, khóa là kết quả của quy trình Thiết lập phiên xác thực chứng chỉ (CASE) qua kênh vận hành sử dụng chứng chỉ vận hành làm đầu vào. Các phiên này được sử dụng trong quá trình hoạt động bình thường giữa bộ điều khiển và thiết bị để xác thực rằng cả hai đều là một phần của mạng Matter.

**3.3. Bảo vệ bản tin**

Các thuật toán mã hóa khác nhau được sử dụng để đảm bảo tính bảo mật và toàn vẹn của thông tin liên lạc

* Hashing Algorithm: SHA-256
* Message Authentication: HMAC-SHA-256
* Public Key: ECC Curve NIST P-256
* Message Encryption: AES-CCM (128 bit keys)

A diagram of a computer program

Description automatically generated

Figure 1: Confidentiality: Message payload is encrypted by the encryption key (AES)

A diagram of a computer

Description automatically generated

Figure 2 :Privacy: Addresses are encrypted by the privacy key

**Commissioning Steps**: Có bốn bước liên quan đến việc vận hành thử các thiết bị để bắt đầu tham gia trên mạng Matter:

**1. Khám phá Thiết bị (Device Discovery)**: Trong giai đoạn này, thiết bị thông báo về sự sẵn có của nó để được kết nối. Ủy viên (Commissioner) sau đó tìm ra thiết bị thông qua các thông tin như Discriminator, Vendor ID, Product ID. Sau khi xác định được thiết bị, ủy viên kết nối với thiết bị để tiếp tục quá trình onboarding.

2. **Kênh An Toàn (Secure Channel):** Giai đoạn này tập trung vào việc thiết lập một kênh an toàn giữa ủy viên và thiết bị. Giao thức PASE (Password Authenticated Session Establishment) được sử dụng, dựa trên giao thức SPAKE2+. Điều này bao gồm việc sử dụng mật khẩu và verifiers để thiết lập một kết nối an toàn.

3. **Device Attestation (xác nhận)**: mỗi thiết bị được trang bị một chứng chỉ duy nhất do nhà sản xuất ký. Không có một Root Certificate Authority (CA) duy nhất áp dụng cho tất cả các thiết bị. Trong quá trình commissioning (thuê giao), thiết bị được thách thức để chứng minh sở hữu khóa riêng tư tương ứng. Chứng chỉ này có thể được xác thực thông qua Distributed Compliance Ledger (DCL) để xác minh trạng thái chứng nhận của thiết bị.

Cấu trúc của hệ thống cho phép tồn tại 3 cấp độ:

* Cấp độ đầu tiên là Product Attestation Authority (PAA).
* PAA sẽ được sử dụng để ký Product Attestation Intermediate (PAI).
* PAI sẽ được sử dụng để ký Device Attestation Certificate (DAC). DAC sẽ được chuyển đến ủy viên và được xác minh so với DCL.

A diagram of a product

Description automatically generated

Quá trình xác thực chứng chỉ tập trung vào việc xác minh tính xác thực của Thiết bị. Các bước bao gồm:

* Ủy viên xác minh các thông tin của Thiết bị như: Vendor ID (VID), Product ID (PID), trạng thái chứng nhận.
* Để thực hiện điều này, Ủy viên sử dụng:

+ Các thông tin chứng nhận Thiết bị

+ Distributed Compliance Ledger (DCL) hoặc Certification Declaration

A cell phone with a blue and green rectangle

Description automatically generated

Để trở thành một thiết bị hợp lệ, DAC được truy xuất và xác minh trước khi thiết bị tham gia mạng. Ủy viên đưa ra một thách thức cho thiết bị để chứng minh rằng nó sở hữu khóa riêng tư tương ứng.

Trước tiên, Ủy viên yêu cầu Thiết bị cung cấp CD, PAI Certificate, và DAC. Sau đó, Ủy viên trích xuất Certificate ID, PAA Certificate, và Device VID/PID từ DCL để thực hiện xác minh. Sau khi kiểm tra chuỗi chứng chỉ từ DAC đến PAI, nếu mọi thứ đều kết nối chính xác, Ủy viên so sánh certification ID từ DCL với CD ID từ chính thiết bị để đảm bảo thiết bị là một thiết bị được chứng nhận của CSA thật sự.

Bước cuối cùng là xác minh rằng khóa công khai trong DAC tương ứng với khóa riêng tư được chèn vào thiết bị trong quá trình sản xuất. Điều này được thực hiện bằng cách gửi một tin nhắn đến thiết bị trong bước cuối cùng của quá trình Attestation, và có tin nhắn được ký bởi thiết bị, sau đó chữ ký được xác minh bằng khóa công khai từ DAC.

**Node Operational Credentials** cho phép một Node xác định chính nó trong một Fabric. Một Node nhận bộ thông tin xác thực ban đầu của Node khi nó được giao cho một Fabric bởi một Ủy viên.

A diagram of a computer code

Description automatically generated with medium confidence

Các thông tin xác thực của Node bao gồm:

* Node Operational Key Pair
* Node Operational Certificate (NOC)
* Intermediate Certificate Authority (ICA) Certificate (optional)
* Trusted Root Certificate Authority (CA) Certificate(s)

**Commissioning Process** sử dụng DAC để xác định rằng Ủy viên đang nói chuyện với một Thiết bị Matter được chứng nhận và sau đó tải các định danh hoạt động cho mỗi hệ sinh thái mà nó tham gia.

A diagram of a light bulb

Description automatically generated

**3.4. Cấu hình**

Quá trình cấu hình bao gồm :

1. Tải Node Operational Credentials cho mỗi hệ sinh thái:

* ID của Fabric
* ID của Node
* Chứng chỉ Root đáng tin cậy
* Chứng chỉ ICA
* Chứng chỉ hoạt động
* Cặp khóa hoạt động của Node
* Danh sách kiểm soát truy cập (ACL)
* Mạng hoạt động
* Thời gian (tùy chọn)

2. Thiết lập kết nối với các Node khác bằng cách sử dụng CASE (Cryptography for Authenticated Session Establishment).

Sau khi những bước này hoàn tất quá trình thuê giao và hiện đã sẵn sàng hoạt động trên Mạng Matter.

**3.5. Yêu cầu bảo mật**

Yêu cầu bảo mật của Matter được quy định bởi CSA và các yêu cầu bảo mật khác như sau:

* Sản xuất: Các thiết bị Matter phải được cấp chứng chỉ/private key DAC duy nhất, Onboarding Payload (QR code), Certification Declaration (CD), và các dữ liệu tĩnh/dynamic khác trong quá trình sản xuất. (YÊU CẦU)
* Thuê giao: DAC với VID/PID phải được kiểm tra trên DCL và CD phải được xác minh để đảm bảo chỉ có các thiết bị Matter chính thức và được chứng nhận được thuê giao. (YÊU CẦU)
* Giao tiếp của Thiết bị: Giao tiếp giữa các thiết bị Matter phải được bảo mật và mã hóa bằng các khóa mật mã và PBKDF. (YÊU CẦU)
* Cập nhật Phần mềm: Thiết bị phải hỗ trợ cập nhật phần mềm qua không dây (OTA) để cho phép vá các lỗ hổng. (YÊU CẦU)

**Các yêu cầu bảo mật khác bao gồm:**

* Các khóa xác thực và mã hóa phải được tạo ra bởi một "Trình tạo số ngẫu nhiên quy định" được khởi tạo bởi NIST 800-90B TRNG.
* Giao diện gỡ lỗi và truy cập vào các thức ăn mật mã khởi đầu an toàn nên bị vô hiệu hóa chỉ cho phép truy cập được ủy quyền (fusing). (NÊN)
* Bảo mật bí mật của DAC và khóa riêng tư hoạt động nên được bảo vệ khỏi các cuộc tấn công từ xa. (NÊN)
* Các nhà cung cấp nên có chính sách công khai và cơ chế để xác định và khắc phục các lỗ hổng bảo mật kịp thời. (NÊN)
* Phần mềm nên được mã hóa khi nằm yên để ngăn chặn truy cập trái phép vào IP cốt lõi. (CÓ THỂ)
* Một số thiết bị nên được bảo vệ chống lại các cuộc tấn công vật lý để ngăn chặn can thiệp, tấn công kênh bên hoặc glitching gỡ lỗi. (CÓ THỂ)

**Giải pháp bảo mật tuân thủ Matter bao gồm:**

* Secure Vault Mid hoặc High hỗ trợ tất cả các chức năng bảo mật của Matter hiện tại và tương lai.
* Các khóa không thể bẻ được được tạo ra bởi Bộ Tạo Số Ngẫu Nhiên Thực (TRNG) cho DAC, khởi đầu an toàn, gỡ lỗi an toàn, OTA, hình ảnh phần mềm và mã hóa giao tiếp.
* Crypto Engine hỗ trợ các thuật toán đặc biệt như SPAKE2+ và CASE với bảo vệ chống lại các cuộc tấn công kênh bên.
* Lưu trữ khóa an toàn ở cấp độ PSA/SESIP Level 2 (Mid) và Level 3 (High); Các khóa riêng tư được lưu trữ bằng TEE/TZ (SV Mid) hoặc PUF Wrapped (SV High).
* Định danh Matter an toàn (DAC) được lập trình an toàn tại nhà máy của chúng tôi.
* Khởi đầu an toàn với RTSL đảm bảo mã chạy trên thiết bị được tin tưởng.
* Cập nhật phần mềm OTA an toàn phối hợp với Secure Boot ngăn chặn việc cài đặt phần mềm độc hại và cho phép vá lỗ hổng.
* Khóa/Gỡ lỗi an toàn chống lại lỗi Glitch chỉ cho phép truy cập được ủy quyền với các token bảo mật có thể bị thu hồi.

**CHƯƠNG IV: ỨNG DỤNG VÀ TRIỂN KHAI**

Hiện tại Matter đã nhận được sự hỗ trợ từ nhiều nhà phát triển, bao gồm:

* Các nhà sản xuất thiết bị: Google, Amazon, Apple, Samsung, Huawei, Xiaomi, LG, v.v.
* Các nhà sản xuất thiết bị gia dụng lớn như Whirlpool, Electrolux, Haier, v.v.
* Các nhà sản xuất thiết bị an ninh như ADT, Ring, Nest, v.v.

2. Các nhà phát triển ứng dụng:

* SmartThings, Wink, Hubitat, Home Assistant, v.v.
* Các nhà phát triển ứng dụng điều khiển nhà thông minh khác.

3. Các nhà cung cấp dịch vụ:

* Amazon Alexa, Google Assistant, Apple HomeKit, v.v.

Ngoài ra, còn có:

* Các nhà phát triển phần mềm độc lập.
* Các công ty cung cấp giải pháp nhà thông minh.
* Các nhà nghiên cứu và học giả.

Sự hỗ trợ rộng rãi này là một dấu hiệu tích cực cho thấy Matter đang được đón nhận và có tiềm năng trở thành tiêu chuẩn thống nhất cho nhà thông minh.

**Dưới đây là một số ví dụ cụ thể về sự hỗ trợ của nhà phát triển:**

* Google đã tích hợp Matter vào Android 13 và Google Home.
* Amazon đã tích hợp Matter vào Alexa và Echo.
* Apple đã cam kết hỗ trợ Matter trong iOS và HomePod.
* Samsung đã phát triển SmartThings Hub mới hỗ trợ Matter.
* Các nhà phát triển ứng dụng như SmartThings và Hubitat đã thêm hỗ trợ cho Matter vào các nền tảng của họ.