# Chap 5: Quản lý thiết bị và An toàn thông tin IoT

# 1. Quản lý thiết bị

- Quản lý thiết bị IoT là quá trình theo dõi và quản lý vòng đời của các thiết bị IoT trong một hệ sinh thái.

- Việc quản lý một mạng lưới cảm biến và thiết bị ngày càng lớn có thể trở nên phức tạp.

- Quản lý Thiết bị IoT giải quyết thách thức này bằng cách cung cấp một trung tâm điều khiển để giám sát toàn bộ hệ thống

- Tóm lại, Quản lý Thiết bị IoT đóng vai trò như hệ thần kinh trung ương cho các thiết bị kết nối của bạn, đảm bảo chúng hoạt động an toàn, hiệu quả và cung cấp dữ liệu giá trị để hỗ trợ việc ra quyết định.

# 1. Quản lý thiết bị


[*] https://www.softwareag.com/en_corporate/resources/iot/article/iot-device-management.html

# 1. Quản lý thiết bị

- **Các chức năng chính của khối quản lý thiết bị:**
  - **Kết nối thiết bị** - Kết nối an toàn các thiết bị mới, cung cấp cho chúng thông tin đăng nhập và cấu hình cần thiết để kết nối và hoạt động liền mạch trong hệ thống.

  - **Xem thiết bị** - Cung cấp giao diện xem thiết bị tập trung.

  - **Cấu hình thiết bị** - Cấu hình thiết bị cho phép bạn quản lý các cài đặt và thông số trên tất cả các thiết bị mà không cần tương tác trực tiếp với chúng.

# 1. Quản lý thiết bị

- **Các chức năng chính của khối quản lý thiết bị:**
  - **Nhóm thiết bị** - Nhóm thiết bị cho phép bạn tổ chức các thiết bị một cách logic theo chức năng (ví dụ: tất cả các bộ điều chỉnh nhiệt), vị trí (ví dụ: cảm biến tòa nhà), hoặc bất kỳ tiêu chí nào khác.

  - **Chẩn đoán** - Chẩn đoán giám sát liên tục hiệu suất thiết bị và phát hiện các vấn đề tiềm ẩn như cảnh báo pin yếu, thông báo lỗi, hoặc lỗi cảm biến.

  - **Giám sát trạng thái** - Cung cấp dữ liệu theo thời gian thực về tình trạng sức khỏe của từng thiết bị.

# 1. Quản lý thiết bị

- **Các chức năng chính của khối quản lý thiết bị:**
  - **Bảo mật thiết bị** - Liên tục theo dõi các lỗ hổng, nhận diện hoạt động đáng ngờ, và cho phép cập nhật từ xa để giữ thiết bị được bảo vệ khỏi các mối đe dọa an ninh mạng.

  - **Cập nhật thiết bị** - Quản lý Thiết bị IoT giữ cho các thiết bị được cập nhật bằng cách triển khai từ xa các bản cập nhật phần mềm hoặc firmware mới trên toàn bộ mạng lưới hoặc nhóm thiết bị cụ thể.

# 1. Quản lý thiết bị

- **Các chức năng chính của khối quản lý thiết bị:**
  - **Tích hợp dữ liệu** - Thu thập thông tin từ tất cả các thiết bị của bạn, chuyển đổi nó thành một định dạng thống nhất.

  - **Ngưng hoạt động thiết bị** - Quản lý Thiết bị IoT giúp bạn dễ dàng ngưng hoạt động thiết bị khi cần.

# 1. Quản lý thiết bị

- **Lợi ích của quản lý thiết bị IoT:**
  - Đơn giản hóa quy trình cho việc thay đổi và cập nhật thiết bị
  - Tăng cường bảo mật
  - Cải thiện độ tin cậy và ổn định của thiết bị IoT
  - Thích ứng với các mô hình kinh doanh thay đổi nhanh chóng
  - Đăng ký thiết bị nhanh hơn
  - Tổ chức thiết bị tốt hơn
  - Quản lý thiết bị từ xa dễ dàng hơn.

# 1. Quản lý thiết bị

- **Thách thức trong quản lý thiết bị IoT:**
  - Dữ liệu phân tán
  - Kiểm soát truy cập
  - Sự gia tăng của thiết bị
  - Quy mô và độ phức tạp của hệ sinh thái thiết bị IoT
  - Hiệu suất mạng và khả năng tương tác
  - Cập nhật firmware và software

# 1. Quản lý thiết bị

- **Thực hành tốt nhất cho Quản lý Thiết bị IoT:**

| Implement device monitoring & control mechanisms | Maintain security throughout the device lifecycle | Establish effective asset tracking & management |
|---|---|---|
| Remote monitoring tools | Authentication & access control | Device inventory & identification |
| Alert systems | Encryption & data protection | Asset tracking systems |
| Control mechanisms | Regular security updates | Lifecycle management |

[*]https://www.kaaiot.com/blog/understanding-iot-device-management

# 1. Quản lý thiết bị

- **Thực hành tốt nhất (Best practice) cho Quản lý Thiết bị IoT:**
  - **Triển khai các cơ chế giám sát và kiểm soát thiết bị:**
    - Công cụ giám sát từ xa.
    - Hệ thống cảnh báo.
    - Cơ chế kiểm soát.
  - **Duy trì bảo mật trong suốt vòng đời của thiết bị:**
    - Xác thực và kiểm soát truy cập
    - Mã hóa và bảo vệ dữ liệu.
    - Cập nhật bảo mật thường xuyên.
  - **Thiết lập hệ thống theo dõi và quản lý tài sản hiệu quả:**
    - Kiểm kê và nhận dạng thiết bị.
    - Hệ thống theo dõi tài sản.
    - Quản lý vòng đời.

# 1. Quản lý thiết bị

- **Các Thành Phần của Quản Lý Thiết Bị IoT:**
  - Cảm biến và bộ điều khiển - thiết bị
  - Cloud
  - Kết nối
  - Phân tích dữ liệu
  - Giao diện người dùng

# 1. Quản lý thiết bị

- **Nền tảng quản lý thiết bị IoT:** Nền tảng Quản lý Thiết bị IoT là trung tâm chỉ huy chính cho toàn bộ mạng lưới IoT của bạn. Các hệ thống này đơn giản hóa mọi khía cạnh của việc quản lý thiết bị, từ thiết lập ban đầu và cấu hình đến giám sát và bảo trì liên tục. Chúng giúp đơn giản hóa việc đăng ký và cập nhật hàng trăm thiết bị đồng thời, sau đó liên tục giám sát tình trạng thiết bị, xác định các vấn đề tiềm ẩn và thậm chí cho phép khắc phục sự cố từ xa.

# 1. Quản lý thiết bị

- **Nền tảng quản lý thiết bị IoT.**
  - **Các tính năng chính của nền tảng quản lý thiết bị IoT:**
    - Khắc phục sự cố từ xa
    - Tự động hóa
    - Giám sát mạng
    - Báo cáo và phân tích
    - Tích hợp mạnh mẽ
    - Bảo mật nghiêm ngặt

| Nhà cung cấp | Khả năng mở rộng | Kết nối | Bảo mật | Phân tích dữ liệu | Học Máy | Quản lý từ xa | Dễ sử dụng | Giá thành | Ưu điểm | Nhược điểm |
|---|---|---|---|---|---|---|---|---|---|---|
| **AWS IoT Device Management** | Highly scalable | Supports various protocols (MQTT, HTTP, etc.) | Robust security features (IAM, encryption) | Integrates with AWS analytics services | Integrates with AWS machine learning services | Enables remote device monitoring and control | User-friendly interface with a learning curve | Pay-as-you-go model | Highly scalable, robust security, extensive integrations | Complex setup for beginners, can be expensive |
| **Azure IoT Hub** | Highly scalable | Supports various protocols (MQTT, HTTP, etc.) | Multi-layered security (authentication, encryption) | Integrates with Azure analytics services | Integrates with Azure machine learning services | Enables remote device monitoring and control | User-friendly interface | Pay-as-you-go model | Highly scalable, secure, integrates with Azure services | Complex setup for beginners, can be expensive |
| **Oracle Internet of Things Asset Monitoring Cloud Service** | Scalable | Cellular, Wi-Fi, LoRaWAN | Secure data storage and access controls | Limited data analytics features | Limited machine learning capabilities | Remote monitoring and diagnostics | User-friendly interface | Subscription-based pricing | Easy to use, cellular connectivity, asset monitoring focus | Limited data analytics and machine learning |
| **Bosch IoT Suite** | Scalable | Cellular, Wi-Fi, Bluetooth | Multi-layered security | Advanced data analytics capabilities | Integrates with Bosch machine learning services | Remote device management and provisioning | Customizable interface | Subscription-based pricing | Customizable, advanced data analytics, Bosch expertise | Vendor lock-in, higher cost |
| **Google Cloud IoT Core** | Scalable | Supports various protocols (MQTT, HTTP, etc.) | Robust security features (IAM, encryption) | Integrates with Google Cloud analytics services | Integrates with Google Cloud machine learning services | Enables remote device monitoring and control | User-friendly interface | Pay-as-you-go model | Scalable, secure, integrates with Google Cloud services | Can be complex for simple use cases |
| **Hologram** | Scalable | Cellular | Cellular network security | Limited data analytics features | Limited machine learning capabilities | Remote SIM management | Straightforward setup | Per SIM card pricing | Cellular connectivity, simple setup | Limited features compared to others |
| **IBM Watson IoT Platform** | Highly scalable | Supports various protocols (MQTT, HTTP, etc.) | Multi-layered security framework | Advanced data analytics capabilities | Integrates with IBM machine learning services | Enables remote device monitoring and control | User-friendly interface | Subscription-based pricing | Advanced data analytics, machine learning capabilities | Steeper learning curve compared to some |

# 2. An Toàn Thông Tin IoT

- **Tổng quan về bảo mật IoT**
  - **Các vấn đề trong bảo mật IoT:**
    - Thiết kế ban đầu cho mạng truyền thông riêng, sau đó được chuyển sang mạng IP (internet)
    - Cập nhật firmware cho thiết bị IoT khó khăn
    - Xuất phát từ những yêu cầu bảo mật cơ bản, sau đó qua thời gian xuất hiện các lỗi bảo mật kèm theo các yêu cầu bảo mật cao hơn.
    - Các thiết bị bảo mật kém từ thiết kế ban đầu đã được sử dụng trong thực tế

# 2. An Toàn Thông Tin IoT

- **Tổng quan về bảo mật IoT**
  - **Phân loại nguy cơ trong bảo mật IoT:**
    - Capture: Các nguy cơ liên quan đến “bắt” (thu thập, nghe lén) thông tin dữ liệu từ hệ thống
    - Disrupt: Các nguy cơ liên quan đến tấn công từ chối dịch vụ (DoS), phá hủy (destroy), ngắt/dừng (interrupt) hệ thống
    - Manipulate: Các nguy cơ liên quan đến can thiệp/thay đổi (manipulate) dữ liệu, định danh.

# 2. An Toàn Thông Tin IoT

- **Tổng quan về bảo mật IoT**
  - **Các yêu cầu bảo mật IoT:**
    - Confidentiality: Tính tin cẩn - dữ liệu truyền đi chỉ có thể được đọc bởi bên nhận.
    - Availability: Tính sẵn sàng - Việc truyền thông giữa các thiết bị truyền và nhận luôn luôn sẵn sàng.
    - Integrity: Tính toàn vẹn - Dữ liệu nhận không bị nhiễu trong quá trình truyền, đảm bảo tính chính xác, vẹn toàn của dữ liệu.
    - Authenticity: Tính xác thực - Bên gửi luôn luôn có thể xác thực dữ liệu được gửi đi. Dữ liệu chỉ có thể được truy cập bởi bên nhận được cho phép.

# 2. An Toàn Thông Tin IoT

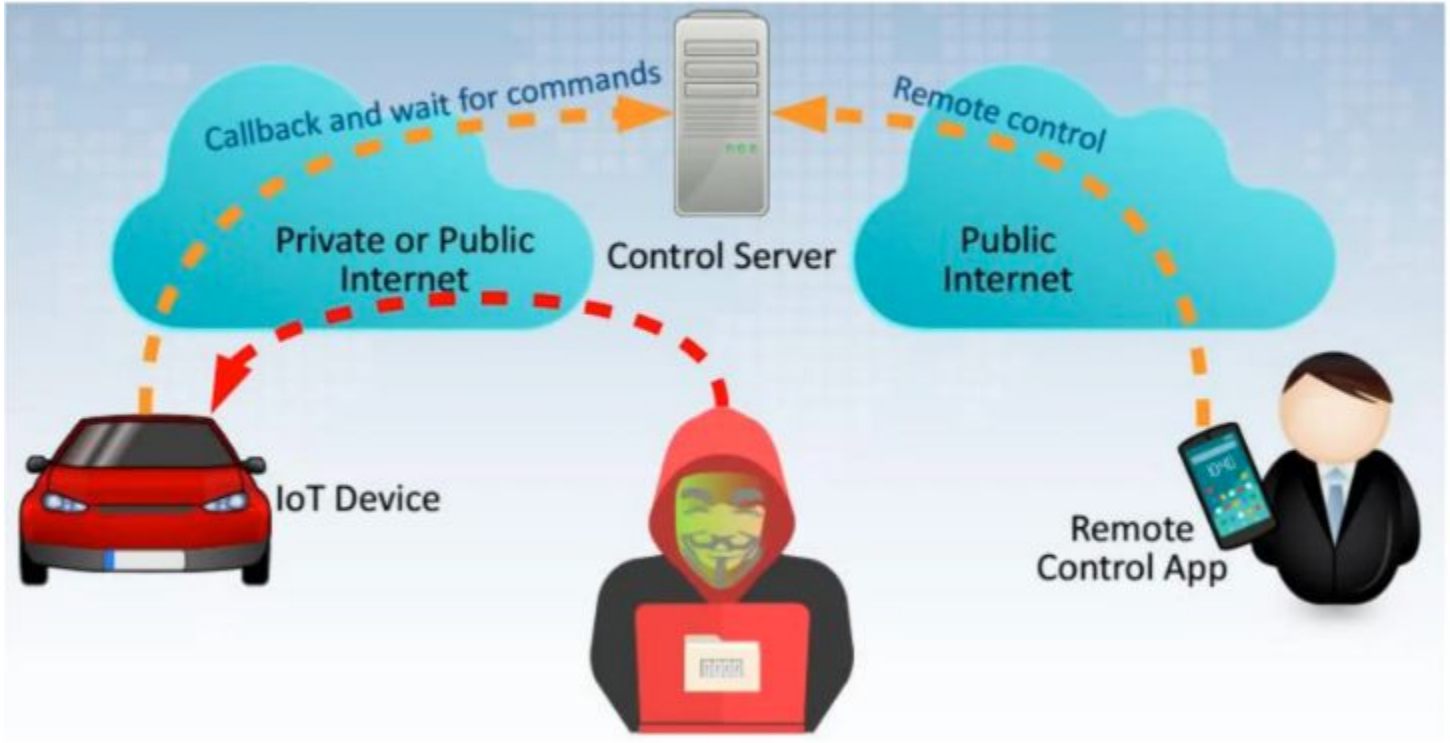
- **Các dạng tấn công hạ tầng IoT**

# 2. An Toàn Thông Tin IoT

- **Fake control Server**

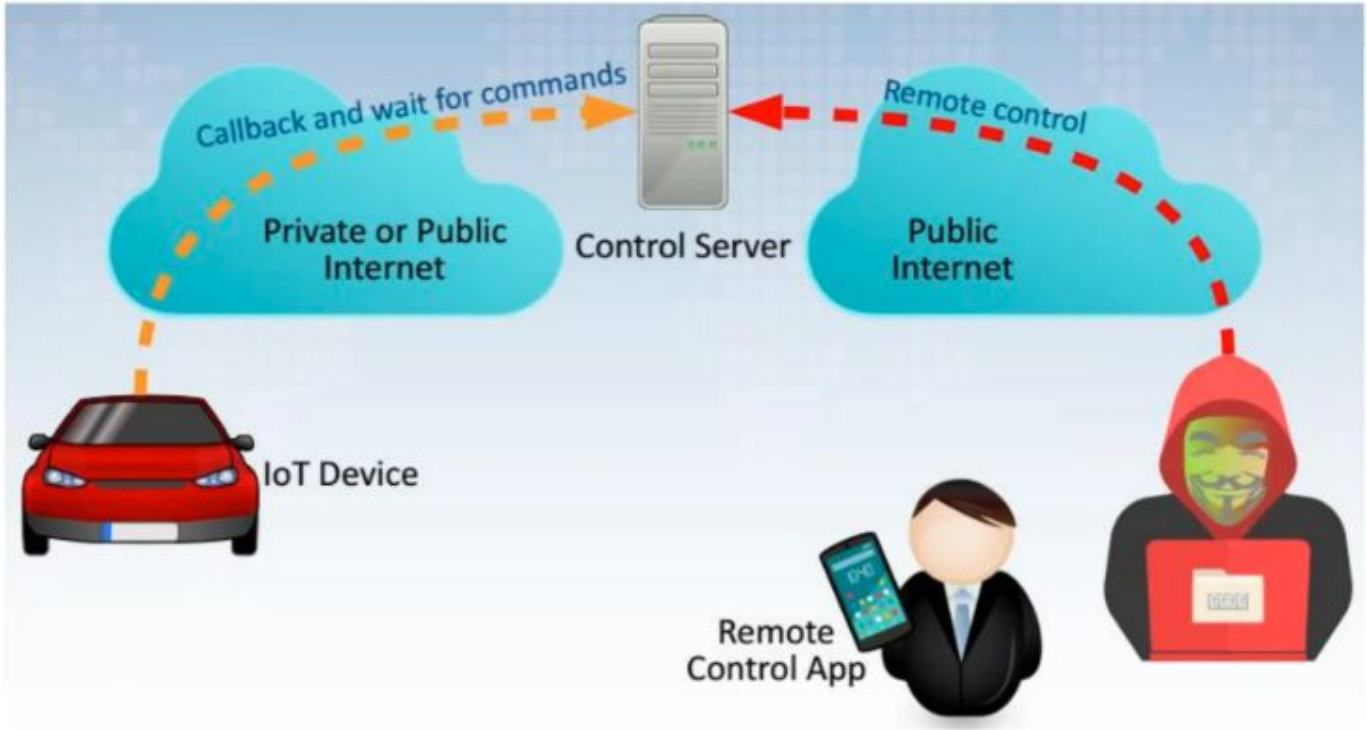
# 2. An Toàn Thông Tin IoT

- **Attack on device's open port**



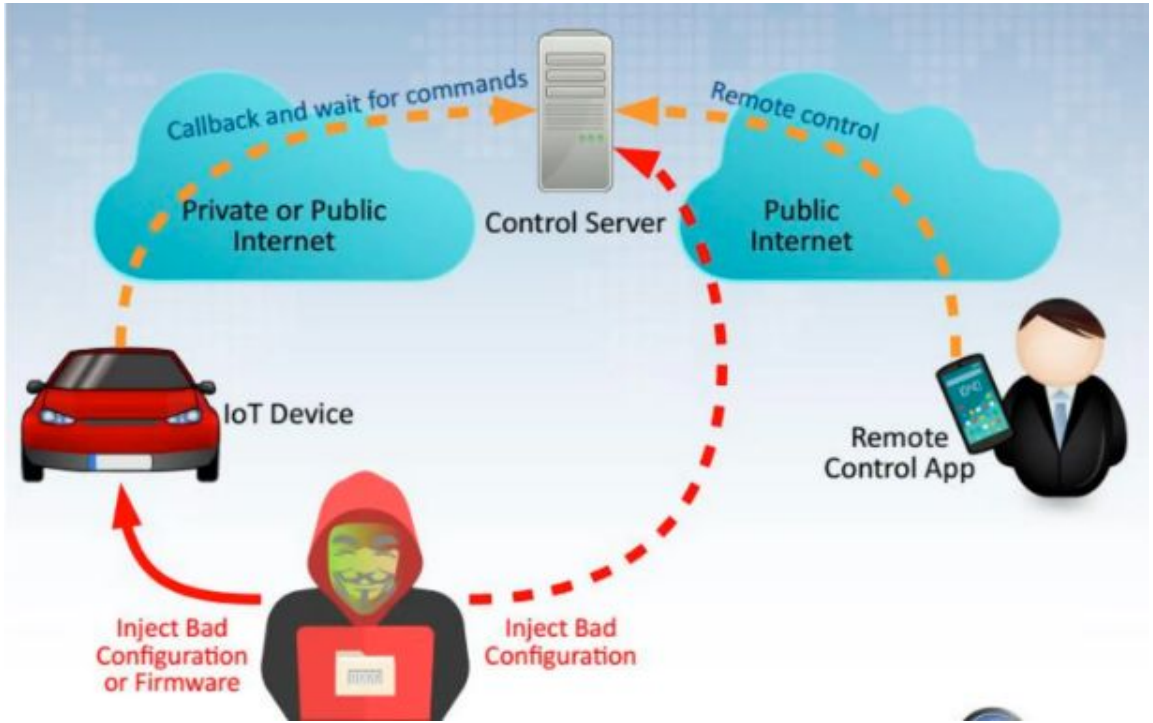
# 2. An Toàn Thông Tin IoT

- **Steal Credential**



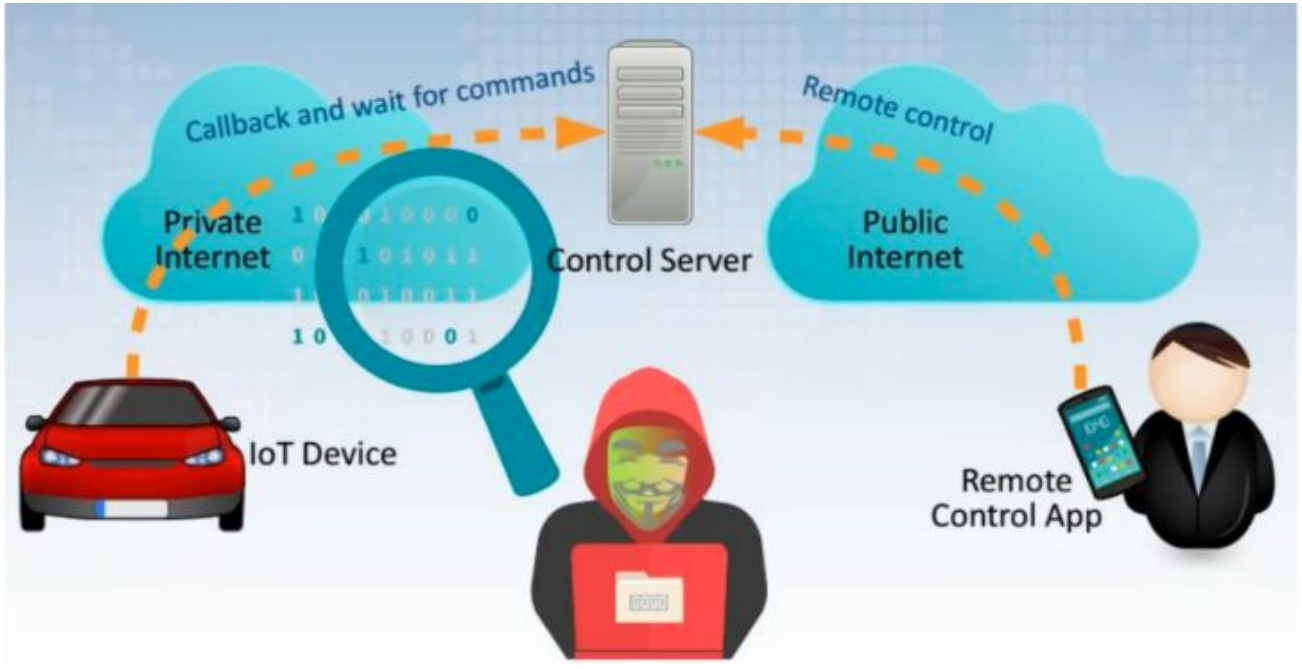
# 2. An Toàn Thông Tin IoT

- **Configuration/Malware Injection**



# 2. An Toàn Thông Tin IoT

- **Sniffing data on private network**



# 2. An Toàn Thông Tin IoT

- **Các điểm yếu bảo mật IoT**
  - Giao diện quản trị không an toàn
    - Default Usernames và password
    - SQL injection
  - Xác thực không đủ an toàn
    - Password yếu
    - Cơ chế khôi phục password thiếu an toàn
    - Thiếu 2-FA
  - Các dịch vụ mạng thiếu bảo mật
    - Mở thừa port
    - Lộ thông tin port
    - Thiếu cơ chế chống DDoS

# 2. An Toàn Thông Tin IoT

- **Các điểm yếu bảo mật IoT**
  - Thiếu mã hóa dữ liệu.
    - Dữ liệu nhạy cảm không được mã hóa
    - Cấu hình SSL/TLS không được sử dụng hoặc cấu hình không phù hợp
  - Các vấn đề liên quan đến quyền riêng tư
    - Thu tập quá nhiều dữ liệu riêng tư
    - Dữ liệu thu thập được không được bảo vệ đúng, dẫn đến lọt lộ thông tin
    - Người dùng không được thông báo hay lựa chọn khi bị/được thu thập thông tin

# 2. An Toàn Thông Tin IoT

- **Các điểm yếu bảo mật IoT**
  - Cấu hình bảo mật không đầy đủ
    - Không có cơ chế bảo vệ password
    - Không có tùy chọn mã hóa
    - Thiếu các cơ chế cảnh báo bảo mật
  - Phần mềm không an toàn
    - Phần mềm của các thành phần IoT có thể bị nhiễm mã độc.
  - Thiếu bảo mật tầng vật lý
    - Tín hiệu truyền đi không được mã hóa bảo vệ ở tầng vật lý.

# Tài Liệu Đọc Thêm


[1]https://www.softwareag.com/en_corporate/resources/iot/article/iot-device-management.html

[2]https://arxiv.org/html/2312.06689v2

[3]https://www.servicenow.com/products/field-service-management/what-is-iot-device-management.html

[4]https://arxiv.org/pdf/2307.13952

[5]https://arxiv.org/pdf/2204.05921

[5]https://arxiv.org/pdf/2405.08528