



ugr

Universidad
de Granada

TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA INFORMÁTICA

TFG - DASIoT

DASIoT: Desarrollo y Auditoría de Seguridad para prototipo de dispositivos IoT

Autor

Luis Aróstegui Ruiz

Directores

José Manuel Soto Hidalgo

Alberto Guillén Perales



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE
TELECOMUNICACIÓN

Granada, 26 de junio de 2022

TFG - DASIoT: Desarrollo y Auditoría de Seguridad para prototipo de dispositivos IoT

Luis Aróstegui Ruiz

Palabras clave: Internet de las Cosas, Seguridad

Resumen

En el contexto de IoT, hay un ecosistema de entornos de desarrollo específicos. En este TFG se hará uso de alguno de ellos para llevar a cabo la implementación de un dispositivo IoT y analizar los potenciales problemas de seguridad que pueden aparecer durante la etapa de implementación.

Project Title: Project Subtitle

First name, Family name (student)

Keywords: Keyword1, Keyword2, Keyword3,

Abstract

Write here the abstract in English.

Yo, **Nombre Apellido1 Apellido2**, alumno de la titulación **TITULACIÓN de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación de la Universidad de Granada**, con DNI **XXXXXXXXXX**, autorizo la ubicación de la siguiente copia de mi Trabajo Fin de Grado en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Nombre Apellido1 Apellido2

Granada a X de mes de 201 .

D. **Nombre Apellido1 Apellido2 (tutor1)**, Profesor del Área de XXXX del Departamento YYYY de la Universidad de Granada.

D. **Nombre Apellido1 Apellido2 (tutor2)**, Profesor del Área de XXXX del Departamento YYYY de la Universidad de Granada.

Informan:

Que el presente trabajo, titulado ***Título del proyecto, Subtítulo del proyecto***, ha sido realizado bajo su supervisión por **Nombre Apellido1 Apellido2 (alumno)**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a X de mes de 201 .

Los directores:

Nombre Apellido1 Apellido2 (tutor1)
(tutor2)

Nombre Apellido1 Apellido2

Agradecimientos

Poner aquí agradecimientos...

Índice general

1. Introducción	19
1.1. Descripción y contexto	19
1.2. Motivación	20
1.3. Objetivos	21
1.3.1. Objetivos específicos	21
2. Estado del arte	23
2.1. Internet de las Cosas	23
2.1.1. Arquitecturas	24
2.1.2. Tecnologías asociadas	26
2.1.3. Aplicaciones	31
2.1.4. Retos	32
2.2. Seguridad	32
2.2.1. Características de seguridad en el IoT	33
2.2.2. Aspectos legales y éticos	34
I Propuesta	37
3. Planificación	39
3.1. Planificación a priori	39
3.1.1. Diagrama de Gantt	39
3.1.2. Etapas de desarrollo	39
3.1.3. Temporización	40
3.1.4. Seguimiento del desarrollo	40
3.2. Planificación a posteriori	42
4. Presupuesto	43

5. Análisis del problema	45
5.1. Middleware	46
5.1.1. Requisitos del servicio de middleware	47
5.1.2. Requisitos de arquitectura en el middleware	48
5.2. Frameworks IoT	49
5.2.1. Requisitos para seleccionar un framework IoT	49
5.2.2. Varios framework IoT	50
5.3. Elección del framework	52
5.4. Explotación de vulnerabilidad	53
5.4.1. MQTT en profundidad	53
5.4.2. Características de MQTT	54
5.4.3. Seguridad en MQTT	55
5.4.4. Fases de un ataque	55
6. Diseño	57
6.1. Tecnologías usadas en la creación de la aplicación	57
6.1.1. Lenguaje de programación	57
6.1.2. Pycharm	58
6.1.3. Diagrama de clases	58
6.1.4. Bibliotecas usadas	60
7. Implementación	63
7.1. Conectar dispositivo	64
7.1.1. Términos y conceptos	64
7.1.2. Pasos a seguir	66
7.2. Recogida de datos de un dispositivo	69
7.2.1. Términos y conceptos	69
7.2.2. Pasos a seguir	70
7.3. Envío de comandos al dispositivo	71
7.3.1. Términos y conceptos	71
7.3.2. Pasos a seguir	71
7.4. Explotación de vulnerabilidad	72
7.4.1. Reconocimiento	72
7.4.2. Análisis de vulnerabilidades	72
7.4.3. Explotación de una vulnerabilidad	73
8. Pruebas	75
8.1. Conectar un cliente	75
8.1.1. Conexión mediante HTTP	75
8.1.2. Conexión mediante MQTT	76
8.2. Recogida de datos y ejecución de comandos de un dispositivo	78
8.2.1. Envío de datos mediante MQTT	78
8.3. Escanear red	86
8.4. Explotación de una vulnerabilidad	86

9. Conclusiones y trabajos futuros

89

Índice de figuras

2.1. Arquitectura de 3 capas. [1]	26
2.2. Arquitectura de 4 capas. [2]	27
3.1. Diagrama de Gantt. Gráfico.	40
5.1. Elementos principales de un framework en IoT. [3]	46
5.2. Modelo publicación/suscripción [4]	55
6.1. Clase de envío de metadatos del dispositivo	59
6.2. Clase de envío de datos de telemetría y ejecución de comandos	59
6.3. Conexion del led con Raspberry [5]	61
7.1. Dashboard Kaa IoT.	63
7.2. Nombre y descripción de la aplicación	66
7.3. Versiones de la aplicación	67
7.4. Endpoint creado	68
7.5. Datos del dispositivo creado	68
7.6. Habilitar opción de auto extracción de datos	70
7.7. Crear usuario para iniciar conexión	74
7.8. Identificador para el nuevo usuario	74
8.1. Metadatos una vez creada nuestra aplicación	83
8.2. Metadatos actualizados y telemetría de la temperatura de la CPU	83
8.3. Encendido y apagado del led	83
8.4. Petición de encendido del led	84
8.5. Inicio de conexión y envío de datos a la aplicación	85
8.6. Encendiendo el led	85
8.7. Apagando el led	85
8.8. Escaneo de red con nmap	87

8.9. Insertar PASS_FILE y USER_FILE	87
8.10. Insertar host y puerto para ejecución. Resultado de la explotación	87
8.11. Captura de tráfico con tcpdump. Inicio de sesión	88

Índice de tablas

3.1. Organización temporal del proyecto.	40
5.1. Características de soluciones comerciales para framework IoT. [6]	52

CAPÍTULO 1

Introducción

1.1. Descripción y contexto

El Internet de las Cosas, o IoT, es un sistema de dispositivos informáticos, máquinas mecánicas y digitales, objetos, animales o personas interrelacionados que cuentan con identificadores únicos (UID) y la capacidad de transferir datos a través de una red sin que sea necesaria la interacción entre personas o entre ordenadores. [7]

Una “cosa” en el Internet de las Cosas puede ser una persona con un implante de monitor cardíaco, un animal de granja con un chip, un automóvil que tiene sensores incorporados para alertar al conductor cuando la presión de los neumáticos es baja o cualquier otro objeto natural o artificial al que se le pueda asignar una dirección de Protocolo de Internet (IP) y que sea capaz de transferir datos a través de una red. Cada vez más, las organizaciones de diversos sectores utilizan el IoT para operar de forma más eficiente, comprender mejor a los clientes para ofrecerles un mejor servicio, mejorar la toma de decisiones y aumentar el valor del negocio.

El concepto de *Internet of Things* fue propuesto en 1999 por el laboratorio de identificación automática del Instituto Tecnológico de Massachusetts (MIT). La UIT lo dio a conocer en 2005, empezando por China. El IoT puede definirse como “*datos y dispositivos continuamente disponibles a través de Internet*”. La interconexión de “cosas” (objetos) que pueden dirigirse de forma inequívoca y las redes heterogéneas constituyen el IoT. La identificación por radiofrecuencia (RFID), los sensores, las tecnologías inteligentes y las nanotecnologías son los principales contribuyentes a al IoT para una variedad de servicios. Con la drástica

reducción del coste de sensores y con la evolución de tecnologías como el ancho de banda, el procesamiento, los teléfonos inteligentes, la migración hacia el IPv6 y el 5G se está facilitando la adopción del IoT.

El IoT también ve todo como lo mismo, sin discriminar entre humanos y máquinas. Las “cosas” incluyen a los usuarios finales, los centros de datos (DC), las unidades de procesamiento, los teléfonos inteligentes, las tabletas, el Bluetooth, el ZigBee, la Asociación de Datos por Infrarrojos (IrDA), la banda ultraancha (UWB), las redes celulares, las redes Wi-Fi, los DC de comunicación de campo cercano (NFC), la RFID y sus etiquetas, los sensores y los chips, los equipos domésticos, los relojes de pulsera, los vehículos y las puertas de las casas. [8]

1.2. Motivación

Las personas de todo el mundo están ya preparadas para disfrutar de las ventajas del Internet de las cosas (IoT). El IoT lo incorpora todo, desde el sensor corporal hasta la computación en la nube. Comprende los principales tipos de redes, como la distribuida, la de red, la ubicua y la vehicular, que han conquistado el mundo de la informática durante una década. Desde el estacionamiento de vehículos a su seguimiento, de la introducción de datos de pacientes a la observación de los pacientes a la observación de los pacientes, de la atención a los niños a la atención a los ancianos, de las tarjetas inteligentes a las tarjetas de campo cercano, los sensores están haciendo sentir su presencia. Los sensores desempeñan un papel fundamental en el IoT.

El IoT funciona en redes y estándares heterogéneos. Excepcionalmente, ninguna red está libre de amenazas y vulnerabilidades de seguridad. Cada una de las capas del IoT está expuesta a diferentes tipos de amenazas. Este proyecto se centra en las posibles amenazas que hay que abordar y mitigar para conseguir una comunicación segura en el IoT. [9]

En otras palabras, el IoT combina “lo real y lo virtual” en cualquier lugar y en cualquier momento, atrayendo la atención tanto de desarrolladores como de ciberdelicuentes. Inevitablemente, dejar los dispositivos sin intervención humana durante un largo periodo podría dar lugar a robos. La seguridad ha sido finalmente reconocida como un requisito esencial para todo tipo de sistemas informáticos, incluidos los de IoT. Sin embargo, muchos sistemas IoT son mucho menos seguros que los típicos sistemas Windows/Mac/Linux.

Los problemas de seguridad de IoT se derivan de seguridad de la IoT provienen de una serie de causas: características de seguridad inadecuadas en el hardware, software mal diseñado con una serie de vulnerabilidades, contraseñas

por defecto y otros errores de seguridad. Los nodos IoT inseguros crean problemas para la seguridad de todo el sistema IoT. Dado que los nodos suelen tener una vida útil de varios años, la gran base instalada de dispositivos inseguros creará problemas de seguridad durante algún tiempo. Los nodos IoT inseguros son ideales para los ataques de denegación de servicio. El ataque Dyn es un ejemplo de ataque basado en el IoT contra la infraestructura tradicional de Internet. Los sistemas IoT inseguros también causan problemas de seguridad al resto de Internet.

La privacidad está relacionada con la seguridad, pero requiere medidas específicas a nivel de aplicación, la red y los dispositivos. No sólo hay que proteger los datos de los usuarios contra el robo, sino que la red debe diseñarse de forma que los datos menos privados no puedan utilizarse fácilmente para inferir datos más privados. [7]

Se prevé que el Internet de las cosas crezca rápidamente debido a la proliferación de la tecnología de la comunicación, la disponibilidad de los dispositivos y los sistemas informáticos. Por lo tanto, la seguridad de IoT es un área de preocupación para proteger el hardware y las redes en el sistema del IoT. El objetivo principal de la seguridad de la IoT es preservar la privacidad, la confidencialidad, garantizar la seguridad de los usuarios, las infraestructuras, los datos y los dispositivos de la IoT, y garantizar la disponibilidad de los servicios ofrecidos por un ecosistema de IoT.

Por lo tanto, la investigación sobre la seguridad del IoT ha cobrado recientemente un gran impulso con la ayuda de las herramientas de simulación, los modeladores y las plataformas de cálculo y análisis disponibles. En la actualidad, las técnicas y los métodos de seguridad que se han propuesto se basan esencialmente en los métodos de seguridad de red convencionales. Sin embargo, la aplicación de mecanismos de seguridad en un sistema IoT es más difícil que en una red tradicional, debido a la heterogeneidad de los dispositivos y protocolos, así como a la escala o el número de nodos del sistema. [10]- [11].

1.3. Objetivos

El principal objetivo de este proyecto es hacer uso de un framework específico para llevar a cabo una implementación de un dispositivo IoT y analizar los potenciales problemas de seguridad que pueden aparecer durante la etapa de implementación.

1.3.1. Objetivos específicos

- **OE.1:** Estudiar los distintos frameworks para IoT y analizar funcionalidades y propiedades que se ajusten al proyecto.

- **OE.2:** Desarrollar un prototipo de aplicación para IoT utilizando un framework de desarrollo.
- **OE.3:** Explotación de una vulnerabilidad a nivel de dispositivo, protocolo, SO, aplicación o HW.

CAPÍTULO 2

Estado del arte

Antes de empezar a desarrollar los objetivos del proyecto es necesario conocer primero los fundamentos del Internet de las Cosas, esto engloba desde su funcionamiento, tipos de arquitecturas hasta los distintos estándares que existen.

2.1. Internet de las Cosas

El término “Internet de las Cosas” (IoT) se conoce desde hace unos años. En los últimos tiempos, está recibiendo más atención debido al avance de la tecnología inalámbrica. La idea básica se debe a la variedad de objetos, como RFID, sensores, actuadores, teléfonos móviles, que pueden interactuar entre sí teniendo una dirección distinta. El IoT permite a los objetos ver, oír, pensar y realizar trabajos haciendo que ‘hablen’ entre sí, para compartir y sincronizar información. Transforma estos objetos de convencionales a inteligentes mediante la manipulación de sus tecnologías subyacentes, como los dispositivos integrados, las tecnologías de comunicación, las redes de sensores, los protocolos y las aplicaciones. [12]

La premisa básica y el objetivo de IoT es “conectar lo que no está conectado”. Esto significa que los objetos que no están actualmente unidos a una red informática, es decir, a Internet, se conectarán para que puedan comunicarse e interactuar con personas y otros objetos. IoT es una transición tecnológica en la que los dispositivos nos permitirán sentir y controlar el mundo físico haciendo que los objetos sean más inteligentes y conectándolos a través de una red inteligente. Cuando los objetos y las máquinas pueden ser detectados y controlados a distancia a través de una red, se consigue una mayor integración entre el mundo físico y los ordenadores. Esto permite mejoras en las áreas de eficiencia, preci-

sión, automatización y habilitación de aplicaciones avanzadas.

El mundo del IoT es amplio y puede resultar algo complicado al principio debido a la abundancia de componentes y protocolos que engloba. En lugar de considerar IoT como un único tecnología, es bueno verlo como un paraguas de varios conceptos, protocolos y tecnologías, todos ellos dependientes a veces de un sector concreto. Aunque la amplia gama de elementos de IoT está diseñado para crear numerosos beneficios en las áreas de productividad y automatización, al mismo al mismo tiempo, introduce nuevos retos, como la ampliación del gran número de dispositivos y de la cantidad de datos que deben procesarse. [9]

2.1.1. Arquitecturas

En esta sección se muestran distintas arquitecturas para el IoT, que suele describirse como un proceso de cuatro etapas en el que los datos fluyen desde los sensores conectados a las cosas.^a través de una red y, finalmente, a un centro de datos corporativo o a la nube para su procesamiento, análisis y almacenamiento.

2.1.1.1. Arquitectura de tres capas

Normalmente, la arquitectura de IoT se divide en tres capas básicas: capa de aplicación, capa de red y capa de percepción, que se describen con más detalle a continuación.

- **Capa de percepción.** También conocida como capa de sensores, se implementa como la capa inferior en la arquitectura de IoT. La capa de percepción interactúa con los dispositivos y componentes físicos a través de dispositivos inteligentes (RFID, sensores, actuadores, etc.). Sus principales objetivos son conectar las cosas a la red IoT, y medir, recoger y procesar la información de estado asociada a estas cosas a través de los dispositivos inteligentes desplegados, transmitiendo la información procesada a la capa superior a través de las interfaces de la capa.
- **Capa de red.** También es conocida como la capa de transmisión, se implementa como la capa intermedia en la arquitectura de IoT. La capa de red se utiliza para recibir la información procesada proporcionada por la capa de percepción y determinar las rutas para transmitir los datos y la información al centro del IoT, los dispositivos y las aplicaciones a través de redes integradas. La capa de red es la más importante en la arquitectura de IoT, ya que varios dispositivos (hub, switching, gateway, cloud computing perform, etc.), y varias tecnologías de comunicación (Bluetooth o Wi-Fi) se integran en esta capa. La capa de red debe transmitir datos hacia o desde diferentes cosas o aplicaciones, a través de interfaces o pasarelas entre redes heterogéneas, y utilizando diversas tecnologías y protocolos de comunicación.

- **Capa de aplicación.** También conocida como la capa de negocio, se implementa como la capa superior en la arquitectura de IoT. La capa de aplicación recibe los datos transmitidos desde la capa de red y utiliza los datos para proporcionar los servicios u operaciones requeridos. Por ejemplo, la capa de aplicación puede proporcionar el servicio de almacenamiento para respaldar los datos recibidos en una base de datos, o proporcionar el servicio de análisis para evaluar los datos recibidos para predecir el estado futuro de los dispositivos físicos. Existen varias aplicaciones en esta capa, cada una con requisitos diferentes.

La arquitectura de tres capas es básica para el IoT y se ha diseñado y realizado en varios sistemas. Sin embargo, a pesar de la simplicidad de la arquitectura multicapa de IoT, las funciones y operaciones en las capas de red y aplicación son diversas y complejas. Por ejemplo, la capa de red no sólo necesita determinar rutas y transmitir datos, sino también proporcionar servicios de datos como agregación de datos, computación, etc. La capa de aplicación no sólo necesita proporcionar servicios a los clientes y dispositivos, sino que también debe proporcionar servicios de datos tales como minería de datos, análisis de datos, por ejemplo. Por lo tanto, para establecer una arquitectura multicapa genérica y flexible para la IoT, debe desarrollarse una capa de servicio entre la capa de red y la capa de aplicación para proporcionar los servicios de datos. Basándose en este concepto, recientemente se han desarrollado arquitecturas orientadas a los servicios (SoAs). [10]

2.1.1.2. Arquitectura basada en SoA

En general, SoA (Arquitectura Orientada a Servicios) es un modelo basado en componentes, que puede ser diseñado para conectar diferentes unidades funcionales, también conocidas como servicios, de una aplicación a través de interfaces y protocolos. SoA puede centrarse en el diseño del flujo de trabajo de los servicios coordinados, y permitir la reutilización de los componentes de software y hardware, mejorando la viabilidad de SoA para su uso en el diseño de la arquitectura IoT. Así, SoA puede integrarse fácilmente en la arquitectura de IoT, en la que servicios de datos proporcionados por la capa de red y la capa de aplicación en la arquitectura tradicional de tres capas pueden ser de la arquitectura tradicional de tres capas pueden extraerse y formar una nueva capa, la capa de servicios, también conocida como capa de interfaz o capa de middleware. Así, en una arquitectura de IoT basada en SoA, existen cuatro capas que interactúan entre sí, siendo éstas la capa de percepción, la capa de red, la capa de servicio y la capa de aplicación.

En la arquitectura de IoT basada en cuatro capas, la capa de percepción desempeña la función de la capa inferior de la arquitectura, y se utiliza para medir, recoger y extraer los datos asociados a los dispositivos físicos. La capa de

red se utiliza para determinar las rutas y proporcionar soporte de transmisión de datos a través de redes heterogéneas integradas. La capa de servicio se sitúa entre la capa de red y la capa de aplicación, proporcionando servicios para apoyar la capa de aplicación. La capa de servicio consiste en el descubrimiento de servicios, la composición de servicios, la gestión de servicios y las interfaces de servicios. La capa de aplicación se utiliza para dar soporte a las solicitudes de servicio de los usuarios. [10]

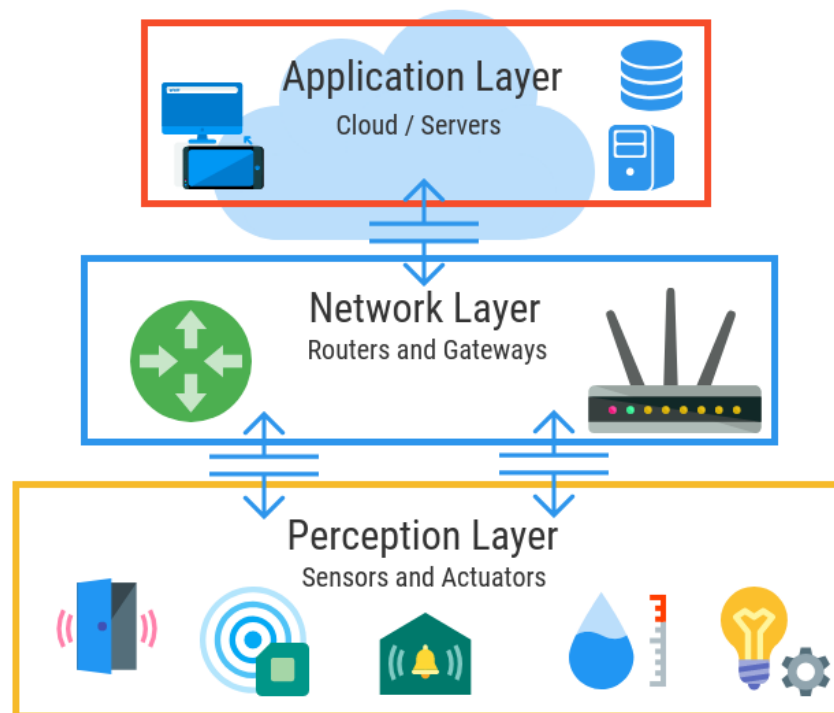


Figura 2.1: Arquitectura de 3 capas. [1]

2.1.2. Tecnologías asociadas

Teniendo en cuenta las arquitecturas mencionadas anteriormente, el IoT cuenta con varias tecnologías que hacen posible la cumplir el objetivo de cada capa de la arquitectura. A continuación se comentan sobre las tecnologías que nos encontramos en la Arquitectura basada en SoA. [10]- [13]

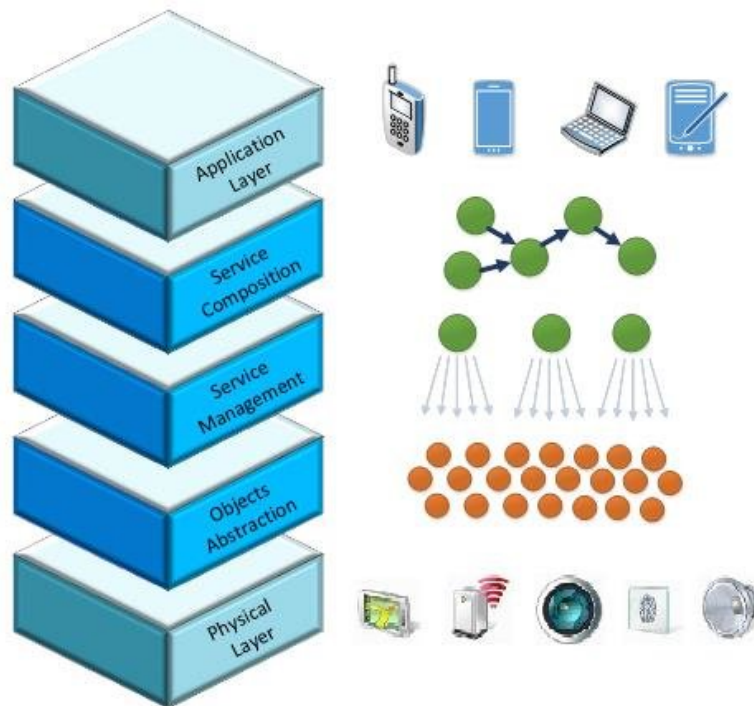


Figura 2.2: Arquitectura de 4 capas. [2]

2.1.2.1. Capa de percepción

En la capa de percepción, la función principal es identificar y rastrear objetos. Para lograr esta función, se pueden implementar las siguientes tecnologías pueden ser implementadas.

- **Radio frequency identification (RFID).** El sistema RFID se compone de uno o varios lectores y varias etiquetas RFID. Utiliza campos electromagnéticos de radiofrecuencia para enviar los datos adjuntos. Las etiquetas que se adjuntan a ella, almacenan datos electrónicamente que pueden ser leídos por RFID cuando se encuentra en la proximidad del lector. [12]
- **Redes de sensores inalámbricos (WSN).** Pueden desempeñar un papel muy importante en el IoT. Las WSN pueden monitorizar y rastrear el estado de los dispositivos, y transmitir los datos de estado al centro de control o a los nodos de enlace a través de múltiples saltos. Por lo tanto, las WSN pueden considerarse como un puente más entre el mundo real y el mundo cibernético. [10]

2.1.2.2. Capa de red

La capa de red se utiliza para determinar el enrutamiento y proporcionar soporte de transmisión de datos a través de redes heterogéneas integradas. A continuación, se presentan algunos protocolos que pueden permitir la comunicación fiable y segura en el IoT. [10]

- **IEEE 802.15.4.** Se lanzó a principios de 2003 y ha satisfecho la necesidad de dispositivos de bajo consumo. Es un protocolo diseñado para la capa física y la capa MAC en redes inalámbricas de área personal (WPAN). El objetivo de IEEE 802.15.4 es centrarse en las WPAN de baja velocidad, proporcionando las conexiones de baja velocidad de todas las cosas en un área personal con bajo consumo de energía, baja tasa de transmisión, y bajo coste. Una de las tecnologías que rompen los esquemas es el estándar de radio IEEE 802.15.4. [14]
- **6LoWPAN.** Las WPAN de baja potencia (LoWPAN) están organizadas por un gran número de dispositivos de bajo coste conectados mediante comunicaciones inalámbricas. En comparación con otros tipos de redes, las LoWPAN presentan una serie de ventajas, como el tamaño reducido de los paquetes, baja potencia, poco ancho de banda, etc. Como mejora, el protocolo 6LoWPAN fue diseñado combinando IPv6 y LoWPAN. En 6LoWPAN, los paquetes IPv6 pueden transmitirse a través de redes IEEE 802.15.4. Debido a que bajo coste y el bajo consumo de energía, 6LoWPAN es adecuado para el IoT, en el que se incluye un gran número de dispositivos de bajo coste.
- **ZigBee.** Es una tecnología de red inalámbrica, diseñada para la comunicación a corto plazo con bajo consumo de energía. En el protocolo ZigBee se incluyen cinco capas la capa física, la capa MAC, la capa de transmisión, la capa de capa de red y la capa de aplicación. Las ventajas de las redes ZigBee son el bajo consumo de energía, el bajo coste baja tasa de datos, baja complejidad, fiabilidad y seguridad.
- **Z-Wave.** Es una tecnología de comunicación inalámbrica a corto plazo con las ventajas de bajo coste, bajo consumo de energía consumo de energía y gran fiabilidad. El objetivo principal de Z-Wave es proporcionar una transmisión fiable entre una control y uno o más dispositivos finales, y Z-wave es adecuada para la red con poco ancho de banda. La red Z-wave soporta la tecnología de enrutamiento dinámico, y cada esclavo almacena una lista en su memoria, que es actualizada por el controlador. La principal diferencia entre ZigBee y Z-wave es la banda de frecuencia en la que opera la capa física.
- **Message Queue Telemetry Transport (MQTT).** Usa la técnica de publicación/suscripción, es un protocolo de mensajería, que se utiliza para

recoger datos medidos en sensores remotos y transmitir los datos a los servidores. MQTT es un protocolo simple y ligero, y soporta la red con bajo ancho de banda y alta latencia. MQTT puede implementarse en varias plataformas para conectar en Internet, y por lo tanto MQTT puede ser utilizado como un protocolo de mensajería entre sensores/actuadores y servidores, lo que hace que MQTT desempeñe un papel importante en el IoT.

- **Constrained Application Protocol (COAP).** Es un protocolo de mensajería basado en la arquitectura de transferencia de estado representativa (REST). Dado que la mayoría de los dispositivos del IoT tienen recursos limitados (es decir, poco almacenamiento y poca capacidad de cálculo), HTTP no puede utilizarse en el IoT, debido a su complejidad. Para superar este problema, se propuso CoAP para modificar algunas funciones de HTTP con el fin de satisfacer los requisitos de el IoT. En términos generales, CoAP es el protocolo de la capa de aplicación en la pila de protocolos 6LoWPAN, y tiene como objetivo permitir que los dispositivos con recursos limitados logren interacciones RESTful. La comunicación de grupo y la notificación push son compatibles con CoAP, pero la difusión no lo es. La observación de recursos, el transporte de recursos en bloque descubrimiento de recursos, interacción con HTTP, y seguridad son todas las características importantes proporcionadas por CoAP.
- **Advanced Message Queuing Protocol (AMQP).** Es un protocolo de colas de mensajes de estándar abierto que se utiliza para proporcionar servicios de mensajes (colas, enrutamiento, seguridad, fiabilidad, etc.) en la capa de aplicación. AMQP se centra en los entornos orientados a mensajes y puede considerarse como un protocolo middleware orientado a mensajes. Usando AMQP, los clientes pueden lograr una comunicación estable con los middlewares de mensajes, incluso si estos clientes y middlewares son producidos por diferentes lenguajes de programación.
- **Extensible Messaging and Presence Protocol (XMPP).** Es un protocolo de mensajería instantánea basado en protocolos de transmisión XML. XMPP hereda las características del protocolo XML, por lo que XMPP tiene una gran escalabilidad, direccionamiento y capacidades de seguridad, y puede ser utilizado para el chat multipartito, voz y vídeo, y telepresencia. En XMPP, se incluyen los siguientes tres funciones: 1) cliente; 2) servidor; y 3) pasarela, así como así como la comunicación bidireccional entre dos partes de estos tres roles.
- **Data Distribution Service (DDS).** Es un protocolo de publicación/suscripción para soportar la comunicación de dispositivo a dispositivo de alto rendimiento. DDS esta centrado en los datos, en el que se puede soportar la multidifusión para lograr una gran QoS y una alta fiabilidad. La ar-

arquitectura de publicación/suscripción sin intermediario hace que DDS sea adecuado para el IoT con restricciones de tiempo real y para la comunicación entre dispositivos. [10]

2.1.2.3. Capa de servicio

Como se ha descrito anteriormente, la capa de servicio se encuentra entre la capa de red y la capa de aplicación, y proporciona servicios eficientes y seguros a los objetos o aplicaciones. En la capa de servicio, deben incluirse las siguientes tecnologías habilitadoras para garantizar que el servicio pueda prestarse de forma eficiente: tecnología de interfaz, tecnología de gestión de servicios, tecnología de middleware y tecnología de gestión y compartición de recursos.

- **Interfaz.** Debe diseñarse en la capa de servicio para garantizar el intercambio de información eficiente y seguro para las comunicaciones entre dispositivos y aplicaciones. Además, la interfaz debe gestionar eficientemente los dispositivos interconectados, incluyendo la conexión de dispositivos, la desconexión de dispositivos, la comunicación de dispositivos y el funcionamiento de dispositivos. Para dar soporte a las aplicaciones en el IoT, un perfil de interfaz (IFP) puede ser considerado como un estándar de servicio, que puede ser utilizado para facilitar las interacciones entre los servicios proporcionados por varios dispositivos o aplicaciones. Para lograr un IFP eficiente, debe implementarse el plug and play universal. Con el desarrollo del IoT, se han realizado varios esfuerzos sobre la interfaz.
- **Gestión de servicios.** Puede descubrir eficazmente los dispositivos y aplicaciones, y programar servicios eficientes y fiables para satisfacer las solicitudes. Un servicio puede considerarse como un comportamiento, que incluye la recogida, el intercambio y el almacenamiento de datos, o una asociación de estos comportamientos para lograr un objetivo especial. En el IoT, algunos requisitos pueden ser satisfechos por un solo servicio, mientras que otros deben ser satisfechos mediante la integración de múltiples servicios.
- **Middleware.** Es un software o servicio de programación que puede proporcionar una abstracción interpuesta entre las tecnologías de IoT y las aplicaciones. En el middleware se ocultan los detalles de las diferentes tecnologías y se proporcionan las interfaces estándar para que los desarrolladores puedan centrarse en el desarrollo de aplicaciones sin tener en cuenta la compatibilidad entre las aplicaciones y las infraestructuras. Así pues, mediante el uso de middleware, los dispositivos y las aplicaciones con diferentes interfaces pueden intercambiar información y compartir recursos entre sí. [10]

2.1.3. Aplicaciones

El IoT es una tecnología emergente que reclama la tercera posición después del ordenador e Internet. En esta tecnología, las cosas se conectan a Internet de una forma u otra, lo que da lugar a una enorme cantidad de datos que deben ser procesados, almacenados y representados de forma eficiente. Las aplicaciones de el IoT varían en diferentes campos e incluyen aplicaciones personales, industriales y nacionales. En los últimos años, estas aplicaciones han aumentado constantemente y algunas de ellas ya están desplegadas y se utilizan a diferentes niveles. Las aplicaciones de IoT requieren hardware, middleware y presentación. Estas aplicaciones tienen características como la comunicación de dispositivos con el mundo real, interacción con el entorno interacción entre personas y dispositivos, tareas rutinarias automáticas con menos supervisión, infraestructura organizada y seguridad en la comunicación.

Son muchas las aplicaciones que se están desarrollando hoy en día y en los últimos años las aplicaciones de IoT han ido a más. Las aplicaciones requieren un avance RFID y tecnologías de direccionamiento, con mejor visualización y capacidad de almacenamiento. Teniendo en cuenta los requisitos de IoT se ha desarrollado una arquitectura de aplicaciones para un menor consumo de energía. Algunos ejemplos que nos encontramos de aplicaciones del IoT son: [14]- [13]

- **Casas inteligentes.** En este caso nos encontramos nuevos inventos que se conectan y controlan nuestros hogares desde nuestros teléfonos.
- **Wearable Technology.** Se han diseñado e implementado varios productos diseñados y aplicados en este ámbito, desde anillos a calzado, y desde relojes hasta mochilas. Esta tecnología puede verse en todas partes.
- **Ciudades inteligentes.** Es un área de tecnología al servicio de las personas, y esta tecnología se construye esencialmente en torno al usuario. Una ciudad no es más que una red diseñada para optimizar los recursos.
- **Red inteligente.** Desde que las instalaciones del IoT se han añadido a la red anterior de datos, se han vuelto más inteligentes, lo que significa más y más información de la red. Desde que el IoT ha ayudado a convertirse en el sistema de suministro de energía de dos maneras la información se enviará al centro principal sobre el uso y el consumo.
- **Atención sanitaria inteligente.** Es un elemento vital para nuestra salud y bienestar, ya sea para el hospital, la odontología o la residencia de ancianos. Este apunta a todos los grupos de edad de la población al mismo tiempo. Para ello se requiere eficacia y menos costes.

2.1.4. Retos

Muchas empresas se apresuran a crear aplicaciones para el IoT y gastan enormes sumas de dinero porque es la próxima gran oportunidad. Se han introducido lavadoras, sistemas de calefacción y frigoríficos inteligentes. El IoT ha traído muchos cambios y dimensiones positivas. Sin embargo, tienen una serie de riesgos y desafíos. [14]- [13]

- **Seguridad y privacidad.** Las aplicaciones del IoT y las áreas inteligentes manejan muchos datos a diario y estos datos se comparten entre dispositivos. La información sobre casas, edificios y coches se comparte entre dispositivos todo el tiempo. Toda esta información exige un mejor sistema de gestión. Los sistemas de seguridad existentes no son adecuados en muchos aspectos y pueden causar graves problemas al usuario. Un error puede hacer que la seguridad del hogar, los coches, los edificios y los datos guardados sean vulnerables.
- **Comunicación fiable.** El IoT se compone de tecnologías fijas y móviles, y se intenta conseguir una comunicación bidireccional sin pérdida de datos y con total fiabilidad.
- **Consumo de energía.** Los dispositivos deben ser capaces de comunicarse con un menor uso de la batería porque estos dispositivos se despliegan lejos y necesitan funcionar con baterías.
- **Interoperabilidad.** Este requiere que los dispositivos se comuniquen entre sí. A nivel de usuario, el usuario puede tener múltiples dispositivos que funcionen en múltiples plataformas. El usuario no querrá quedarse con un solo dispositivo. En cambio, un usuario puede querer diversidad en caso de elegir un dispositivo.

2.2. Seguridad

Durante las primeras décadas de su existencia, las redes informáticas eran utilizadas principalmente por los investigadores universitarios para enviar correos electrónicos y por los empleados de las empresas para compartir impresoras. En estas condiciones, la seguridad no recibía mucha atención. Pero ahora, cuando millones de ciudadanos de a pie utilizan las redes para realizar operaciones bancarias, comprar y presentar sus declaraciones de impuestos, y se han encontrado puntos débiles tras puntos débiles, la seguridad de las redes se ha convertido en un problema de proporciones masivas.

La seguridad, trata de asegurar que los entrometidos no puedan leer, o peor aún, modificar secretamente los mensajes destinados a otros destinatarios. Se trata de que las personas intenten acceder a servicios remotos para los que

no están autorizadas. La seguridad también se ocupa de los problemas de los mensajes legítimos que son capturados y reproducidos, y de las personas que más tarde intentan negar haber enviado ciertos mensajes. La mayoría de los problemas de seguridad son causados intencionadamente por personas malintencionadas que intentan obtener algún beneficio, llamar la atención o perjudicar a alguien.

[15]

2.2.1. Características de seguridad en el IoT

Este trabajo al estar relacionado con el IoT nos centramos en analizar la seguridad relacionada con este. Podemos analizar distintos aspectos de la seguridad, como puede ser en la transmisión de datos, hardware, software, pero todos estos puntos tienen una serie de puntos en común:

- **Confidencialidad.** La confidencialidad puede garantizar que los datos sólo estén disponibles para los usuarios autorizados durante todo el proceso, y que no puedan ser escuchados o interferidos por usuarios no autorizados. En IoT, la confidencialidad es un principio de seguridad importante, ya que un gran número de dispositivos de medición (RFID, sensores, etc.) pueden integrarse en IoT. Por lo tanto, es fundamental garantizar que los datos recogidos por un dispositivo de medición no revelen información segura a sus dispositivos vecinos. Para lograr una gran confidencialidad, deben mejorarse las técnicas, incluyendo mecanismos seguros de gestión de claves.
- **Integridad.** La integridad puede garantizar que los datos no puedan ser manipulados por interferencias intencionadas o no intencionadas durante la entrega de datos en las redes de comunicación, proporcionando en última instancia los datos precisos para los usuarios autorizados. La integridad es importante para IoT, porque si las aplicaciones de IoT reciben datos falsificados o manipulados, se puede estimar un estado de funcionamiento erróneo y se pueden realizar comandos de retroalimentación equivocados, lo que podría interrumpir aún más el funcionamiento de las aplicaciones de IoT. Para lograr una integridad aceptable, deben desarrollarse y aplicarse mecanismos de integridad de datos seguros mejorados y aplicarlos.
- **Disponibilidad.** La disponibilidad puede garantizar que los datos y los dispositivos estén disponibles para los usuarios y servicios autorizados siempre que se soliciten los datos y los dispositivos. En IoT, los servicios suelen solicitarse en tiempo real, y los servicios no pueden programarse y prestarse si los datos solicitados no pueden entregarse a tiempo. Por lo tanto, la disponibilidad es también un importante principio de seguridad. Una de las amenazas más graves para la disponibilidad es el ataque de denegación de servicio (DoS), y las técnicas mejoradas, protocolos de enrutamiento seguros y eficientes, para garantizar la disponibilidad en el IoT. [10]

2.2.2. Aspectos legales y éticos

La seguridad es un requisito importante en el diseño y desarrollo para un proyecto, por ello hay que considerar los aspectos normativos, en especial relacionados con la privacidad, ya que es esencial en el desarrollo de sistemas TIC's.

Se va a destacar la **Agencia Española de Protección de Datos**, que en 2014 realizaron el primer dictamen relacionado con el IoT.

En el **Dictamen 8/2014** del Grupo de Trabajo del Artículo 29, ahora Comité Europeo de Protección de Datos, se define IoT como aquella infraestructura en la que múltiples sensores incorporados a dispositivos comunes y cotidianos registran, someten a tratamiento, almacenan y transfieren datos e interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red. En muchos casos, dichos objetos están asociados a identificadores únicos y tratan datos personales.

El Grupo de trabajo del artículo 29 decidió emitir este Dictamen por considerar que el IoT plantea diversos retos importantes relativos a la intimidad y la protección de los datos, algunos nuevos, otros más tradicionales, pero amplificados por el aumento exponencial del tratamiento de datos que conlleva la evolución de este fenómeno. La importancia de la aplicación del marco jurídico de protección de los datos de la UE y las correspondientes recomendaciones que se presentan más abajo se deben contemplar a la luz de estos retos. [16]

Uno de los puntos que se puede destacar es que para que los usuarios del Internet de las Cosas puedan permanecer siempre en control de sus datos deben saber claramente cómo y para qué se van a utilizar los mismos. Deben dar su consentimiento expreso tras recibir la información de forma clara y transparente.

Relativo al proyecto, hay que tener en cuenta secciones como la de **Creadores de aplicaciones** que dice lo siguiente [17]:

- *“Se deben elaborar avisos o advertencias para recordar frecuentemente a los usuarios que los sensores están recogiendo datos. Si el creador de la aplicación no tiene acceso directo al dispositivo, la aplicación debe enviar periódicamente al usuario una notificación para recordarle que sigue registrando datos. ”*
- *“Las aplicaciones deben facilitar el ejercicio del derecho del interesado al acceso, la modificación y la eliminación de la información personal recogida por los dispositivos de IO. ”*
- *“Los creadores de aplicaciones deben proporcionar herramientas para que los interesados exporten tanto los datos primarios como los agregados en*

un formato normalizado y fácil de utilizar. “

- *“Los creadores deben prestar una atención especial a los tipos de datos que se someten a tratamiento y a la posibilidad de deducir de ellos datos personales sensibles. “*
- *“Los creadores de aplicaciones deben aplicar el principio de minimización de datos. Cuando los fines se puedan alcanzar mediante datos agregados, los creadores no deberán acceder a los datos primarios. De manera más general, los creadores deben seguir un enfoque de intimidad desde el diseño y reducir la cantidad de datos recogidos al mínimo necesario para la prestación del servicio. “*

Como conclusión de este dictamen obtenemos que, los tratamientos basados en IoT precisan de modelos que incorporen los requisitos normativos, estándares y mecanismos de certificación para garantizar un nivel de protección de derechos y libertades de las personas. Pudiendo ser utilizados por las personas sin amplios conocimientos con la confianza de que no se vulnerará su privacidad. [16]

I | Propuesta

CAPÍTULO 3

Planificación

3.1. Planificación a priori

Se trata de planificar como se espera desarrollar el proyecto en el tiempo, para ello se va a hacer uso de un diagrama de Gantt donde se va a proporcionar una vista general de las tareas programadas, estas tareas tendrán que completarse en unas fechas estipuladas.

3.1.1. Diagrama de Gantt

Un diagrama de Gantt es una herramienta útil para planificar proyectos. Proporciona una vista general de las tareas programadas, indicando el periodo de tiempo que tienen para completarse.

El diagrama se mostrará:

- Fecha de inicio y finalización del proyecto.
- Las tareas del proyecto.
- Fecha de programada de cada tarea, tanto la de inicio como la de final.
- Como se superponen las tareas y si hay relación entre ellas.

Con esta planificación se conseguirá una mayor claridad en las tareas a realizar y una mejor gestión del tiempo.

3.1.2. Etapas de desarrollo

- **1ª etapa:** Revisar frameworks para IoT.

- 2ª etapa: Desarrollar aplicación para IoT.
- 3ª etapa: Explotación de una vulnerabilidad.
- 4ª etapa: Documentación.

3.1.3. Temporización

De los 3 meses y medios a que se van a dedicar al proyecto, en todos ellos se va a desarrollar las etapas indicadas anteriormente. Se muestra la fecha de inicio y de fin de cada etapa.

Etapas del desarrollo	Fecha de comienzo	Fecha de finalización
Documentación del proyecto	9 de Marzo	23 de Junio
Revisar frameworks IoT	21 de Marzo	6 de Abril
Desarrollar aplicación para IoT	7 de Abril	12 de Mayo
Explotar vulnerabilidad	13 de Mayo	22 de Junio

Tabla 3.1: Organización temporal del proyecto.

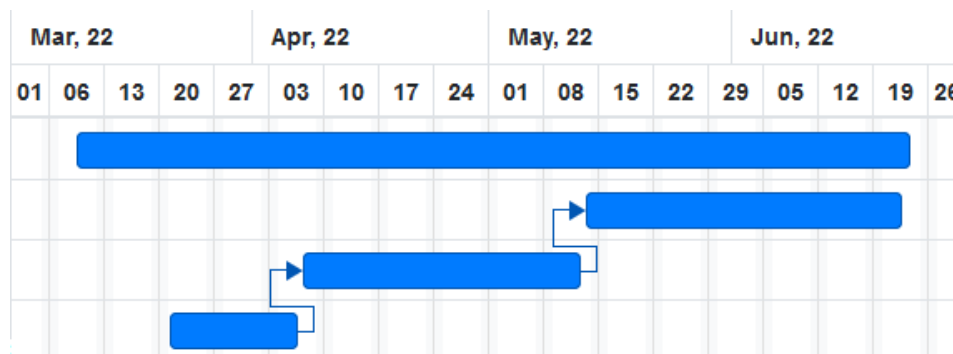


Figura 3.1: Diagrama de Gantt. Gráfico.

Este gráfico corresponde con la duración de cada etapa, comenzando con la documentación. También se indica que hay etapas que para que estas se puedan empezar a desarrollar necesitan que la anterior este terminada, es el caso de la etapa de *Desarrollo de la aplicación* y de *Explotación de una vulnerabilidad*.

3.1.4. Seguimiento del desarrollo

Con el fin de facilitar la visualización del progreso del proyecto se usan distintas herramientas.

3.1.4.1. Trello

Permite gestionar proyectos de forma sencilla y muy visual. Por cada proyecto se crea un tablero donde podemos crear listas y cada lista almacenará *tarjetas* donde se describirá una tarea u objetivo a cumplir. En nuestro caso el tablero se divide en 7 listas:

- **Dudas**, se dejan ancladas preguntas a los tutores.
- **Objetivos**, para recordar los objetivos que se tienen que completar para el proyecto.
- **Pendientes**, tareas que se tienen que realizar pero no se están desarrollando.
- **En proceso**, tareas que se están trabajando.
- **Pendientes de revisión**, tareas finalizadas que requieren de revisión por parte de los tutores.
- **Terminadas**, tareas que han sido aceptadas en la revisión.
- **Hitos**, se agrupan tareas que forman parte de una misma etapa.

3.1.4.2. Github

Se ha creado un repositorio ¹ donde se van añadiendo *issues* por cada tarea que se tenga que realizar. Esta tarea es la misma que nos encontramos en el tablero de Trello, por tanto, cuando se crea una nueva tarea en Trello, creamos un nuevo issue con el mismo nombre y descripción para seguir un progreso coherente.

También se crean *Milestones* que se corresponde con el nombre y descripción de la lista de *Hitos* del tablero de Trello.

Cada vez que terminemos de trabajar en un *Milestone* se creará un *Pull Request* para que los tutores puedan revisar los cambios del proyecto y aceptarlos o rechazarlos. Cada acción que se realice tanto en Trello como en Github se verá reflejado en ambos, de esta manera conseguimos un desarrollo del proyecto realista de principio a final.

3.1.4.3. Clockify

Esta herramienta nos permite seguir el tiempo que estamos trabajando. Cada vez que nos pongamos a trabajar, iniciaremos el contador y nombraremos a ese contador con el nombre de la tarea que estemos realizando en ese momento.

¹Enlace al repositorio: <https://github.com/LuisArostegui/TFG>

3.2. Planificación a posteriori

CAPÍTULO 4

Presupuesto

CAPÍTULO 5

Análisis del problema

Siguiendo los objetivos del proyecto 1.3 se va a analizar los diferentes frameworks que existen para desarrollar una aplicación para posteriormente analizar posibles explotaciones de seguridad.

Como hemos visto en 2.1, normalmente, cuando se generan grandes datos y se transmiten a través de varios dispositivos, tiene que haber un punto específico en el que se recoja y combine todo. Este punto específico es muy esencial en una red, ya que combina todos los datos, lo que permite comprender los datos que se generan. Sin embargo, la transmisión y generación de datos sin problemas no se produce sin más. Más bien, suele ser posible gracias a un framework del Internet de las Cosas.

Un framework para IoT puede describirse como un ecosistema, compuesto por varios dispositivos conectados que se comunican entre sí, a través de Internet. Estos dispositivos conectados suelen funcionar para transferir y detectar datos a través de Internet, y requieren muy poca intervención humana. El framework de IoT es lo que hace posible que los dispositivos conectados tengan una comunicación fluida a través de Internet. Es un elemento tecnológico muy importante en el mundo moderno, que encuentra aplicación en casi todos los sectores. Por ejemplo, una de las principales aplicaciones del IoT es el diseño de casas inteligentes. [18]

Es decir, un framework para IoT recoge todos principales elementos que componen el mundo del Internet de las Cosas para desarrollar una aplicación, estos elementos los podemos ver en la siguiente imagen 5.1.

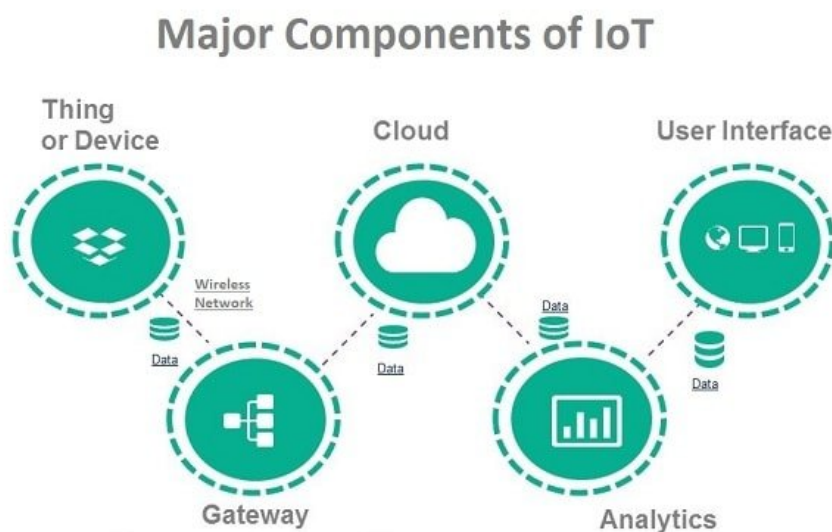


Figura 5.1: Elementos principales de un framework en IoT. [3]

Cuando se esta desarrollando una aplicación, el concepto de “framework” se puede relacionar con otros conceptos como el de “middleware” y “plataforma”. El concepto de “plataforma” hace referencia al lugar donde se permite desplegar y ejecutar la aplicación. Por otro lado el middleware, tiene que ver con la prestación de los servicios. Y por último, el framework se centra más en el diseño del software. Por esto, pese a que en este proyecto se va a trabajar con un framework, hay que tener en cuenta otros conceptos que rodean al desarrollo de una aplicación. [19]

5.1. Middleware

Generalmente, un middleware abstrae las complejidades del sistema o del hardware, permitiendo al desarrollador de la aplicación centrar todo su esfuerzo en la tarea a resolver, sin la distracción de preocupaciones a nivel del sistema o del hardware. Dichas complejidades pueden estar relacionadas con problemas de comunicación o de computación más generales. Un middleware proporciona una capa de software entre las aplicaciones, el sistema operativo y las capas de comunicación de la red, que facilita y coordina que facilita y coordina algún aspecto del procesamiento cooperativo. Desde el punto de vista perspectiva informática, un middleware proporciona una capa entre el software de aplicación y el software de sistema.

En el IoT, es probable que haya una considerable heterogeneidad tanto en las tecnologías de comunicación en uso, como en las tecnologías a nivel de sistema,

y un middleware debe soportar ambas perspectivas según sea necesario.

Basándonos en las características descritas anteriormente 2.1 de la infraestructura del IoT y de las aplicaciones que dependen de ella, se establecen un conjunto de requisitos para que un middleware soporte el IoT. A continuación, estos requisitos se agrupan en dos conjuntos: los servicios que debe proporcionar dicho middleware y la arquitectura del sistema [20]- [21].

5.1.1. Requisitos del servicio de middleware

Los requisitos de los servicios de middleware para el IoT pueden clasificarse en funcionales y no funcionales. Los requisitos funcionales recogen los servicios o funciones, como por ejemplo abstracciones y gestión de recursos un middleware, y los requisitos no funcionales, por ejemplo fiabilidad, seguridad y disponibilidad, captan el soporte de la calidad de servicio o del rendimiento.

En los requisitos funcionales nos encontramos:

- **Descubrimiento de recursos.** Ya que la infraestructura y el entorno del IoT son dinámicos, las suposiciones relacionadas con el conocimiento global y determinista de la disponibilidad de estos recursos es inviable. Pasa lo mismo con la intervención humana, es inviable que este descubra recursos. Por tanto, es importante destacar que el descubrimiento de recursos este automatizado. Cuando no hay infraestructura, el propio dispositivo debe de anunciar su presencia y los recursos que ofrece.
- **Gestión de recursos.** Se espera una QoS (Quality of Service) aceptable para todas las aplicaciones, y en un entorno en el que los recursos que influyen en la QoS son limitados, como el IoT, es importante que las aplicaciones cuenten con un servicio que gestione esos recursos.
- **Gestión de datos.** Los datos son fundamentales en las aplicaciones de IoT. En el IoT, los datos se refieren principalmente a los datos detectados o a cualquier información de infraestructura de red de interés para las aplicaciones.
- **Gestión de eventos.** En las aplicaciones de IoT se genera potencialmente un número masivo de eventos, que deberían gestionarse como parte integral de un middleware de IoT.
- **Gestión del código.** El despliegue de código en un entorno de IoT es un reto, y debe ser soportado directamente por el middleware. En particular, se necesitan servicios de asignación y de código.

En los requisitos no funcionales nos encontramos:

- **Escalabilidad.** Un middleware de IoT debe ser escalable para adaptarse al crecimiento de la red y las aplicaciones/servicios de IoT.

- **Actuación en tiempo real.** Un middleware debe proporcionar servicios en tiempo real cuando la corrección de una operación que soporta depende no sólo de su corrección lógica sino también del tiempo en que se realiza.
- **Fiabilidad.** Un middleware debe permanecer operativo durante la duración de una misión, incluso en presencia de fallos.
- **Disponibilidad.** Un middleware que soporte las aplicaciones de un IoT, especialmente las de misión crítica, debe estar disponible en todo momento.
- **Seguridad y privacidad.** La seguridad es fundamental para el funcionamiento de IoT. En el middleware de IoT, la seguridad debe tenerse en cuenta en todos los bloques funcionales y no funcionales, incluyendo la aplicación a nivel de usuario.
- **Facilidad de despliegue.** Hay que evitar los procedimientos complicados de instalación y configuración.
- **Popularidad.** Un middleware de IoT, como cualquier otra solución de software, debe recibir un apoyo y una ampliación continua.

5.1.2. Requisitos de arquitectura en el middleware

En esta sección se muestran los requisitos para las abstracciones de programación y otros aspectos relacionados con la implementación.

- **Abstracción de la programación.** Para el desarrollador de aplicaciones o servicios, las interfaces de programación de alto nivel deben aislar el desarrollo de las aplicaciones o los servicios de las operaciones proporcionadas por las infraestructuras subyacentes y heterogéneas del IoT.
- **Interoperabilidad.** Un middleware debe funcionar con dispositivos, tecnologías y aplicaciones heterogéneas, sin esfuerzo adicional por parte del desarrollador de aplicaciones o servicios.
- **Basado en el servicio.** Una arquitectura de middleware debe estar basada en servicios para ofrecer una gran flexibilidad cuando sea necesario añadir funciones nuevas y avanzadas al middleware de un IoT.
- **Adaptable.** Un middleware debe ser adaptativo para poder evolucionar y adaptarse a los cambios de su entorno.
- **Consciente del contexto.** El conocimiento del contexto es un requisito clave en la construcción de sistemas adaptativos y también en el establecimiento de valor de los datos recogidos.

- **Autónomo.** Los dispositivos, tecnologías y aplicaciones son participantes activos en los procesos del IoT y deben estar habilitados para interactuar y comunicarse entre sí sin la intervención humana.
- **Distribuido.** Las aplicaciones de un sistema IoT a gran escala de un sistema IoT intercambian información y colaboran entre sí.

5.2. Frameworks IoT

Una vez hemos visto requisitos que necesitamos en nuestro middleware, se van a comentar una serie de requisitos que buscamos en nuestro framework IoT. [6]- [22]- [19]

5.2.1. Requisitos para seleccionar un framework IoT

Algunos requisitos principales en los que nos tenemos que fijar a la hora de seleccionar un entorno de desarrollo son:

- **Seguridad y privacidad.** El framework debe de proporcionar seguridad en la capa de transporte para conexiones seguras (encriptación SSL) y no comprometer en el entorno de trabajo. Con esto, conseguimos privacidad, autenticación e integridad en los datos.
- **Dificultad de uso.** Seleccionar un framework que sea sencillo de usar para desarrolladores. Esto incluye el lenguaje de programación que se use para hacer la aplicación.
- **Código abierto.** Se trata de evitar aquellos framework en los que hay que pagar por su uso o que den un periodo de prueba gratuito. Las plataformas de código abierto permiten que las plataformas sean gestionadas por el desarrollador según sus necesidades.
- **Soporte.** Se busca un framework que sea popular y tenga un equipo y comunidad activa, que continuamente este aportando nuevas características al proyecto.

También existen otras características en las que nos podemos fijar que pueden resultar útiles dependiendo del tipo de aplicación que queremos desarrollar:

- **Tipo de soporte de protocolo de comunicación.** Los dispositivos IoT soportan múltiples protocolos de comunicación. Algunos son ligeros y otros son seguros. El protocolo a elegir depende de los requisitos de la aplicación IoT. CoAP es similar a HTTP pero es ligero, por lo que es más adecuado para aplicaciones móviles. MQTT también es ligero y soporta el concepto de broker, por lo que es bueno para aplicaciones de ancho de banda limitado. CoAP es bueno para la multidifusión y la difusión.

- **Disponibilidad.** La disponibilidad y la estabilidad son parámetros importantes para los requisitos del IoT. Por ejemplo, una aplicación enfocada a la salud requiere que los datos médicos del paciente para ser monitorizados continuamente.
- **Tecnologías de almacenamiento utilizadas.** Diferentes tecnologías de almacenamiento y procesamiento sobre la nube soportan diferentes tipos de análisis. Según los requisitos de procesamiento de datos, se puede seleccionar una nube con diferentes tecnologías de almacenamiento.
- **Tipo de análisis soportado.** Las aplicaciones de IoT suelen requerir datos en tiempo real o datos históricos para el desarrollo de la aplicación. La elección de la tecnología adecuada para aplicar la analítica al tipo de datos generados por el dispositivo en la aplicación es otro factor importante.

5.2.2. Varios framework IoT

5.2.2.1. KAA IoT

Es totalmente gratis, tiene capacidad para gestionar millones de sensores, recoger y analizar datos en tiempo real y visualizarlos, gestionar y conectar productos inteligentes con ayuda de nube. Permite la gestión de los datos de los objetos conectados y la infraestructura de back-end que proporciona los componentes del SDK del servidor y del endpoint. KAA proporciona la funcionalidad de back-end necesaria para operar una solución IoT. Proporciona flexibilidad a los usuarios para implementar sus propias políticas de seguridad.

Kaa proporciona un gateway que aporta la posibilidad de conectar diferentes redes entre si. Los protocolos de comunicación que usa para comunicarse con los dispositivos son MQTT y COAP. Para especificar un dispositivo se hace en JSON, donde cada dispositivo es un objeto. Kaa permite el análisis de datos y para ello usa tecnologías como NoSQL, Cassandra, Hadoop y MongoDB. Kaa soporta lenguajes de programación como Java, C, C++. [23]

5.2.2.2. ThingSpeak

Es un framework que se caracteriza por sus visualizaciones y predicciones utilizando MATLAB. Soporta datos con formato JSON y XML. Es de código abierto. Soporta múltiples dispositivos y permite utilizar protocolos como MQTT o Rest API para la comunicación entre dispositivos. Proporciona seguridad en la capa de transporta con encriptación en las comunicaciones. [24]

5.2.2.3. Macchina.io

Este framework se divide en dos productos, el primero es el **Edge** que permite que las aplicaciones se ejecuten en dispositivos basados en Linux utilizando

C++ y Javascript. Y el segundo producto es el **Remote** que permite gestionar la infraestructura mediante paneles web y aplicaciones móviles. Una de las tecnologías que utiliza es SQLite e incluye soporte para protocolos de comunicación como MQTT, SOAP, HTTP. [25]

5.2.2.4. Altair (Carriots)

Altair, anteriormente "Carriots", es una plataforma diseñada para proyectos IoT. Permite integrar los dispositivos de IoT a una aplicación externa que requiera de los datos mientras ellos se encargan del almacenamiento y la comunicación. Soporta XML, JSON y API Rest. No es gratis, tiene un plan de suscripción. Permite escribir aplicaciones en Java. Para la comunicación entre dispositivos usa MQTT, no posee encriptación en la comunicación pero sí posee un mecanismo de autenticación y autorización. Para el almacenamiento usa NoSQL. [26]

5.2.2.5. Zetta

Es una plataforma de código abierto construida sobre Node.js para crear servidores del Internet de las Cosas que se ejecutan a través de ordenadores geodistribuidos y la nube. Zetta combina las API de REST, los WebSockets y la programación reactiva, lo que resulta perfecto para ensamblar muchos dispositivos en aplicaciones de uso intensivo de datos en tiempo real. Zetta tiene la capacidad de convertir cualquier dispositivo en una API. Al comunicarse con microcontroladores como Arduino y Spark Core, Zetta puede proporcionar a cada dispositivo una API REST tanto localmente como en la nube. Zetta es "developer friendly" lo que significa que es sencillo desarrollar usando esta plataforma. Entre las tecnologías que usa esta API Rest y JSON. [27]

5.2.2.6. Temboo

Es un framework que entra dentro de la categoría de plataformas que son "developer friendly", es decir, para conectar dispositivos y hacer tareas simples se hace de manera rápida y sin complicaciones en el código. Soporta datos en Excel, CSV, XML y JSON. Soporta lenguajes de programación como C, Java, Python y Javascript. No es gratuito, requiere de un plan de suscripción para empezar a utilizarlo. Tiene soporte con múltiples dispositivos, entre ellos Arduino y a destacar Samsung Artik. Los protocolos que soporta son HTTP, MQTT, CoAP. Y tiene soporte de tecnologías como Microsoft Power BI y Google BigQuery. [28]

5.2.2.7. Particle

Particle es una plataforma de IoT escalable, fiable y segura. Una característica clave es la capacidad de ejecutar código de cableado de Arduino y Raspberry Pi haciendo más fácil conectar componentes electrónicos a la nube. Los primeros 100 dispositivos que se conecten son gratuitos. En cuanto a la seguridad, es uno

de los frameworks con más características relacionadas con esta, posee encriptación en las comunicaciones, autenticación, autorización y posibilidad de auditoría de seguridad, todo esto bajo el protocolo HTTP. Soporta datos en formato CSV y se puede desarrollar código Javascript y en particle js, una librería ligera de Javascript.

5.2.2.8. Soluciones comerciales

Hay otras soluciones comerciales donde nos encontramos plataformas como AWS IoT, Microsoft Azure IoT Hub, IBM Watson IoT, Google IoT y Oracle IoT. Todas estas alternativas son bastante similares a todas las comentadas hasta el momento, se diferencian entre si por ciertas características como el soporte en lenguajes de programación, donde aparecen lenguajes que no vemos en otras plataformas como son Ruby, .NET, Go, php. En la siguiente tabla se muestran características de estas plataformas :

Framework IoT	Soporte de datos	Soporte de lenguajes de programación	Protocolos	Seguridad
AWS IoT	JSON	Java, C, NodeJS, Javascript, Python, iOS, Android	HTTP, MQTT, Websockets	Encriptación, autenticación, autorización, auditoría
Microsoft Azure IoT	JSON	.NET, UWP, Java, C, NodeJS, Ruby, Android, iOS	HTTP, AMQP	Encriptación, autenticación, autorización, políticas definidas por usuario
IBM Watson IoT	JSON, CSV	C#, C, Python, Java, NodeJS	MQTT	Autenticación, Autorización
Oracle IoT	JSON, CSV	Java, Javascript, Android, C, iOS	REST API	Autenticación, Autorización
Google IoT	JSON	Go, Java, .NET, Node.js, php, Python, Ruby	MQTT, HTTP	Autenticación

Tabla 5.1: Características de soluciones comerciales para framework IoT. [6]

5.3. Elección del framework

Como framework para desarrollar la aplicación se ha optado por trabajar con **Kaa IoT**. La motivación de su uso viene de cumplir todos los requisitos establecidos en la sección 5.2.1.

- **Seguridad y privacidad.** Kaa IoT proporciona autenticación del cliente

con certificado SSL/TLS, por tanto, todas sus comunicaciones van a estar cifradas. Aparte, para el proyecto puede resultar útil posible implementación de nuestras propias políticas de seguridad.

- **Dificultad de uso.** No llega a ser un framework “developer friendly”, pero en la documentación del framework [23] hay varios tutoriales como para desarrollar sin mucha dificultad una aplicación, explicando en cada apartado las palabras clave o conceptos que se necesitan para entender todo lo que se está haciendo en la construcción de la aplicación. Aquellos frameworks “developer friendly”, por el hecho de ser plataformas donde ofrecen ayudar por desarrollar y desplegar la aplicación requieren de una suscripción para hacer uso de estas.
- **Código abierto.** Es un framework gratuito, evitamos todos los frameworks que requieren de un plan de suscripción.
- **Soporte.** Es de los frameworks más conocidos. Y tienen una comunidad activa, esto se puede observar en su repositorio de github ¹, que cada poco tiempo van añadiendo nuevas características y documentación al proyecto.

Otra elección interesante podría haber sido **macchina.io** no cumple con el requisito de dificultad de uso. En comparación con **Kaa IoT**, **macchina.io** no dispone de tanta documentación como el framework seleccionado.

5.4. Explotación de vulnerabilidad

Para empezar, ya que vamos a trabajar con MQTT vamos a analizar este protocolo de comunicación para posteriormente atacarlo para así explotar una vulnerabilidad de nuestra aplicación. Una vez visto como funciona MQTT, veremos las etapas de un ataque y las herramientas que necesitamos en cada una de las etapas.

5.4.1. MQTT en profundidad

Ya se habló de este protocolo en 2.1.2.2. Cada protocolo IoT requiere diferentes vectores de ataque. MQTT no es, por defecto, seguro, y muchos despliegues de MQTT parecen haberse saltado la letra pequeña cuando se trata de usar MQTT de forma segura. Así que vamos a explotarlo.

La definición oficial de MQTT viene de **mqtt.org** [29]:

“MQTT son las siglas de MQ Telemetry Transport. Se trata de un protocolo de publicación/suscripción, extremadamente sencillo y ligero, diseñado para dispositivos limitados y redes de bajo ancho de banda, alta latencia o poco fiables.

¹Enlace a repositorio de Kaa IoT: <https://github.com/kaaproject/kaa>

Los principios de diseño consisten en minimizar el ancho de banda de la red y los requisitos de recursos de los dispositivos, al tiempo que se intenta garantizar la fiabilidad y cierto grado de seguridad en la entrega. Estos principios también hacen que el protocolo sea ideal para el emergente mundo de los dispositivos conectados "máquina a máquina"(M2M) o "Internet de las cosas", y para aplicaciones móviles en las que el ancho de banda y la energía de la batería son muy importantes. "

MQTT es un protocolo de publicación/suscripción que permite la comunicación de uno a muchos a través de un broker MQTT. Poder comunicarse con todos los dispositivos conectados al broker facilita los ataques activos a gran escala. Un atacante que sea capaz de espiar y saber qué tipo de mensajes se están enviando a través del broker puede utilizar posteriormente esta información para atacar simultáneamente a todos los dispositivos conectados a él.

Tiene una característica llamada suscripción con comodines, y muchos usuarios de MQTT pasan por alto las implicaciones de esto en la seguridad. Un despliegue por defecto de MQTT sin autorización permite a cualquier cliente conectado suscribirse a todos los mensajes, y un atacante puede utilizar esta información para conocer y registrar todos los mensajes intercambiados en una solución IoT. Por esto, es bastante factible realizar un ataque de escalado de privilegios. [30]

5.4.2. Características de MQTT

- Patrón de publicación y suscripción.
- Formatos de paquetes simples: cargas útiles binarias.
- Version actual: 3.1.1 (Dec/2015).
- El protocolo se ejecuta a través de TCP.
- Puerto por defecto: 1883/TCP (no encriptado).

El modelo de **publicación/suscripción** se compone de:

- **Editor**, publica un mensaje en uno (o varios) temas del broker.
- **Broker**, dirige todos los mensajes de los editores a los suscriptores.
- **Tema**, consta de uno o varios niveles separados por una barra diagonal (por ejemplo, /smartshouse/livingroom/temperature).

5.4.3. Seguridad en MQTT

La nota oficial de MQTT acerca de la seguridad de este (mqtt.org) [29]:

“Puedes pasar un nombre de usuario y una contraseña con un paquete MQTT en la V3.1 del protocolo. La encriptación a través de la red puede ser manejada con SSL, independientemente del protocolo MQTT en sí mismo (vale la pena señalar que SSL no es el más ligero de los protocolos, y añade una sobrecarga de red significativa). Se puede añadir seguridad adicional mediante una aplicación que cifre los datos que envía y recibe, pero esto no es algo integrado en el protocolo, con el fin de mantenerlo simple y ligero.”

Aquí tenemos dos puntos a considerar:

1. La autenticación es totalmente opcional
2. Si se realiza la autenticación, el cifrado no se utiliza por defecto (las credenciales se envían en texto claro). Los ataques MITM aún pueden ser ejecutados para robar contraseñas.

5.4.4. Fases de un ataque

Para poder contrarrestar un ataque debemos conocer las fases de este, por esto vamos a hacer un **test de intrusión** o **Pentest**. Esto es una prueba de seguridad ofensiva que simula un ataque real en un entorno controlado. El objetivo principal de este tipo de pruebas es identificar las posibles brechas en la seguridad de un sistema de manera que, al simular el comportamiento de los atacantes reales, podamos descubrir vulnerabilidades y agujeros de seguridad que necesiten ser corregidos para que no sean explotados por parte de atacantes reales. [31]

Las fases y tecnologías dentro de cada fase que nos encontramos son:

1. **Reconocimiento**, se recolecta información del sistema de forma activa o pasiva. En este caso se van a usar herramientas como nmap o netstat para recopilar información de dominios, IPs, puertos y servicios.

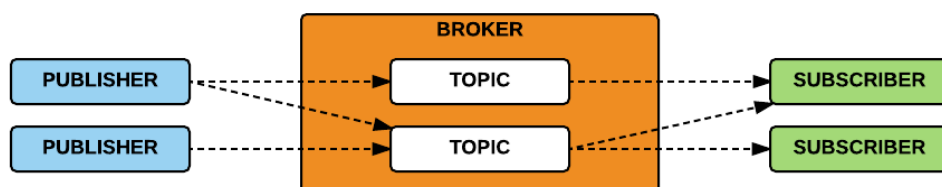


Figura 5.2: Modelo publicación/suscripción [4]

2. **Análisis de vulnerabilidades**, aquí se analizará la información recopilada de la fase de reconocimiento. Se puede investigar por internet posibles vulnerabilidad, por ello se puede mencionar a **CVE**², para conocer posibles vulnerabilidad.
3. **Explotación**, en esta fase se realizan las acciones necesarias para poder comprometer al sistema, los usuarios o la información que se maneja. Para este proyecto se usará **Metasploit**, es una herramienta que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración.

²<https://cve.report/vendor/mqtt>

CAPÍTULO 6

Diseño

Se van a mostrar las tecnologías usadas en el proyecto, así como las decisiones tomadas a la hora del desarrollo del software. En este proyecto, tenemos por un lado nuestra aplicación, la cual va a recoger todos los datos y por otro lado tenemos un dispositivo, que este es una Raspberry PI [32], prestada por mis tutores de proyecto. Para hacer la conexión entre aplicación y dispositivo se necesita hacer uso de un protocolo de mensajería, en este caso se opta por el uso de MQTT.

También se va a mostrar como se va a proceder para la explotación de la vulnerabilidad y cuestiones a tener en cuenta.

6.1. Tecnologías usadas en la creación de la aplicación

6.1.1. Lenguaje de programación

Se ha optado por usar Python, fue creado a principios de los años 90 por Guido van Rossum en el Stichting Mathematisch Centrum en los Países Bajos como sucesor de un lenguaje llamado ABC. Guido sigue siendo el principal autor de Python, aunque incluye muchas contribuciones de otras personas.

En mayo de 2000, Guido y el equipo de desarrollo del núcleo de Python se trasladaron a BeOpen.com para formar el equipo BeOpen PythonLabs. En octubre del mismo año, el equipo de PythonLabs se trasladó a Digital Creations. En 2001, se formó la Python Software Foundation, una organización sin ánimo de lucro creada específicamente para poseer la propiedad intelectual relacionada con Python. [33]

Python es un lenguaje de alto nivel de programación interpretado cuya filosofía hace hincapié en la legibilidad de su código, se utiliza para desarrollar aplicaciones de todo tipo. Se trata de un lenguaje de programación multiparadigma, ya que soporta parcialmente la orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, dinámico y multiplataforma. [34]

Para este proyecto es una buena opción ya que gracias a paquetes como **paho-mqtt**, que proporciona una clase cliente que permite a las aplicaciones conectarse a un broker MQTT para publicar mensajes, y para suscribirse a temas y recibir mensajes publicados, podemos hacer conexiones a mqtt de una manera muy sencilla. [35]

6.1.2. Pycharm

PyCharm es un entorno de desarrollo integrado utilizado en programación informática, concretamente para el lenguaje de programación Python. Está desarrollado por la empresa checa JetBrains. Proporciona análisis de código, un depurador gráfico, un probador de unidades integrado, integración con sistemas de control de versiones (VCS), y soporta el desarrollo web con Django, así como la ciencia de datos con Anaconda.

PyCharm es multiplataforma, con versiones para Windows, macOS y Linux. La Community Edition (edición comunitaria) se publica bajo la Licencia apache, y también hay una Professional Edition (edición profesional) con características adicionales publicada bajo una licencia propietaria financiada por suscripción y también una versión educativa, que gracias a la universidad de Granada podemos hacer uso de esta licencia. [36]

6.1.3. Diagrama de clases

Para hacer la comunicación entre el dispositivo y la aplicación se propone el siguiente diagrama de clases que describe la estructura del sistema.

La clase *MetadataClient* 6.1 establece una primera conexión con la aplicación, recoge los datos a nivel hardware de la Raspberry y los envía para actualizar la información en la aplicación.

La segunda clase *KaaClient*, hace una conexión con la cual enviamos datos de telemetría, en concreto, obtenemos cada cierto tiempo la temperatura de la CPU de la Raspberry y se envía esta y el momento de tiempo en el que se produce el envío. También incluye funciones para gestionar el encendido y apagado de un led conectado a la Raspberry.

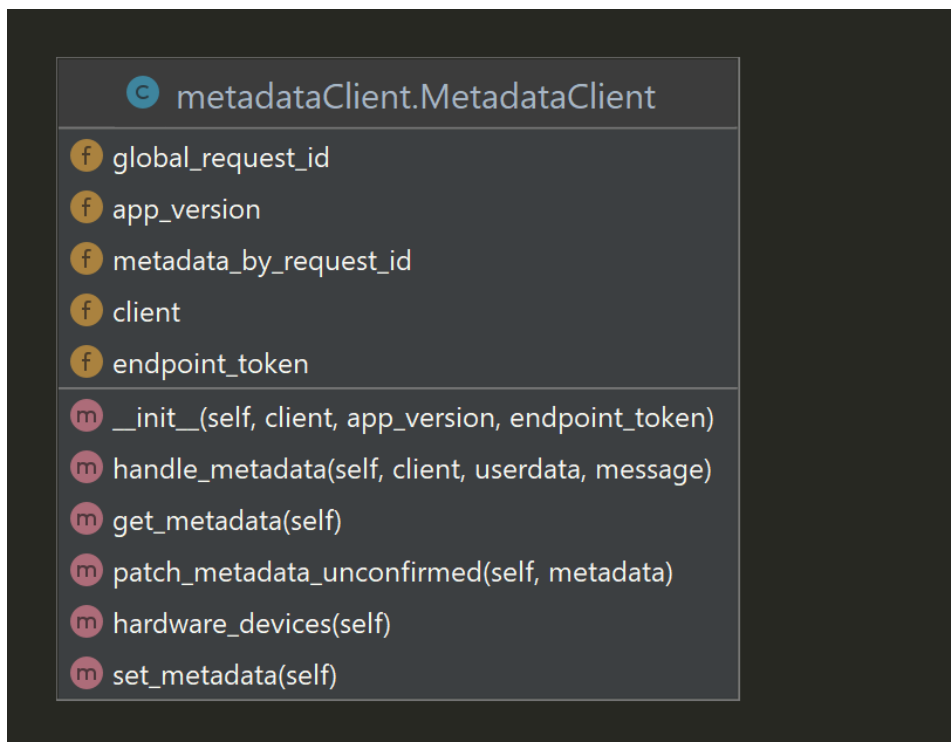


Figura 6.1: Clase de envío de metadatos del dispositivo

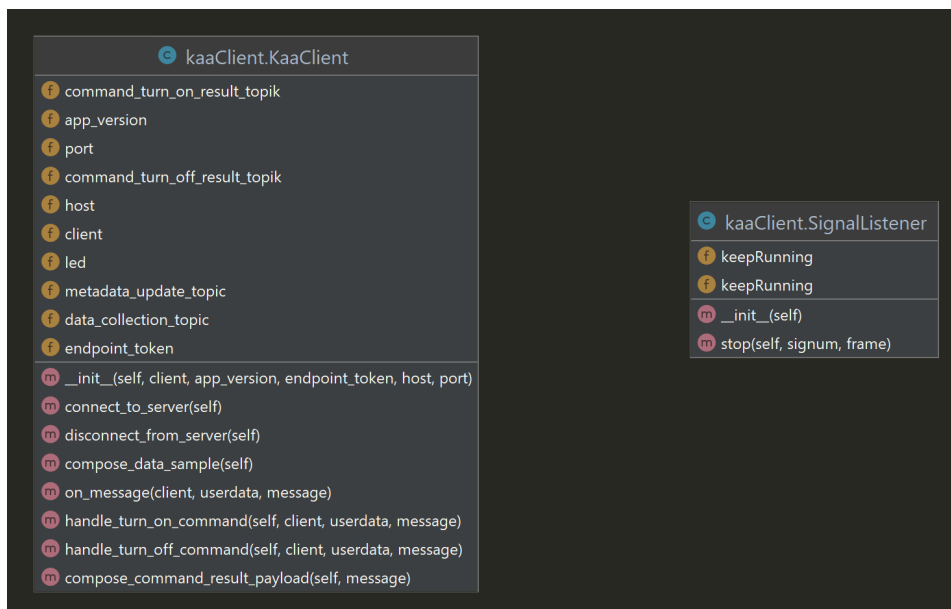


Figura 6.2: Clase de envío de datos de telemetría y ejecución de comandos

El led estará conectado a la Raspberry como se muestra en la figura 6.3.

Por último, la clase **SignalListener** que se usa para poder parar la ejecución de la comunicación desde una E/S.

6.1.4. Bibliotecas usadas

6.1.4.1. subprocess

Para obtener los dispositivos conectados a la Raspberry se usa **subprocess**. El módulo de subprocesos permite generar nuevos procesos, conectarse a sus tuberías de entrada/salida/error y obtener sus códigos de retorno. [37]

6.1.4.2. GPIO Zero

Una sencilla interfaz para dispositivos GPIO con Raspberry Pi, desarrollada y mantenida por Ben Nuttall y Dave Jones. Se usa para obtener la temperatura de la CPU y para encender/apagar el led de la Raspberry. [38]

6.1.4.3. decouple

Decouple ayuda a organizar la configuración para que puedas cambiar los parámetros sin tener que volver a desplegar la aplicación. En un fichero .env se almacena los datos sensibles para no mostrarlos al público y se cargan una vez antes de iniciar la comunicación. [39]

6.1.4.4. paho mqtt

Como se ha mencionado ya, sirve para establecer la conexión mqtt. [35]

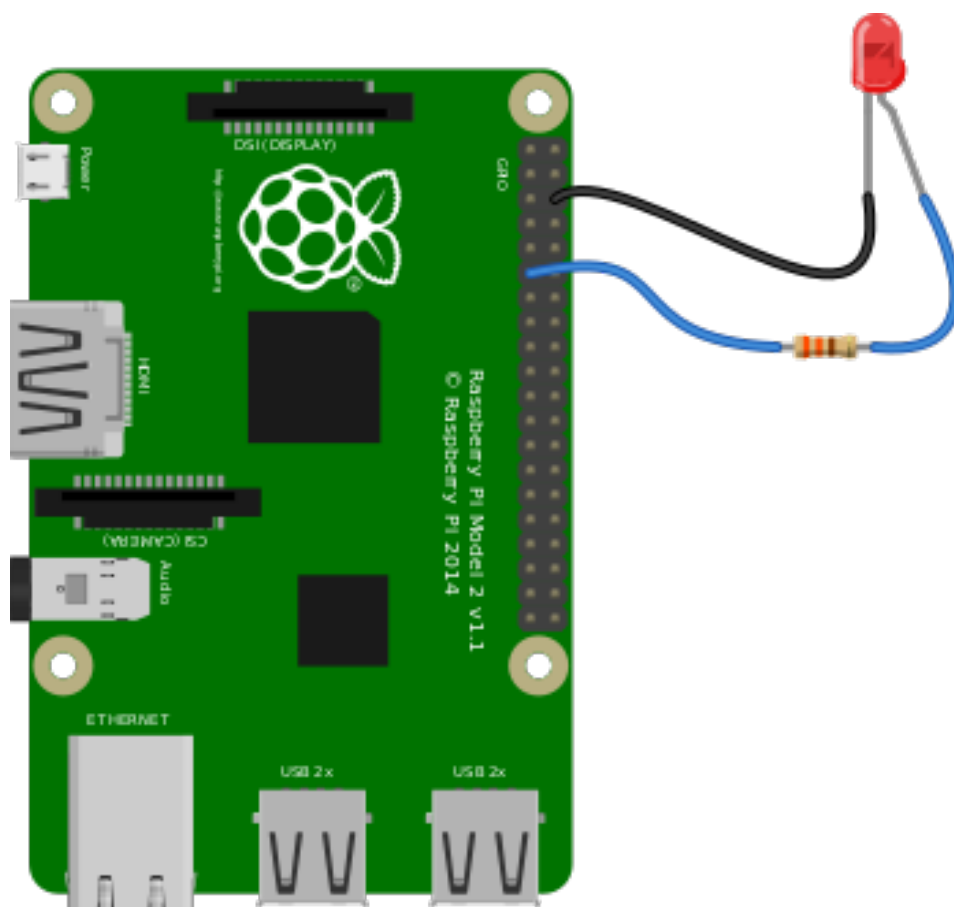


Figura 6.3: Conexion del led con Raspberry [5]

CAPÍTULO 7

Implementación

La implementación de la aplicación se realiza con **Kaa IoT** tal y como se analizó anteriormente 5.3. Para empezar a usar el framework, hay que registrarse en sistema. Una vez registrados tendremos acceso a nuestro *dashboard* ¹. En este capítulo se trata de mostrar una guía con la que se consiga conectar un dispositivo, recoger y enviar datos desde/hacia el dispositivo y mostrar las opciones que nos ofrece Kaa IoT como framework IoT. Para empezar, vamos a conectar nuestro primer dispositivo.

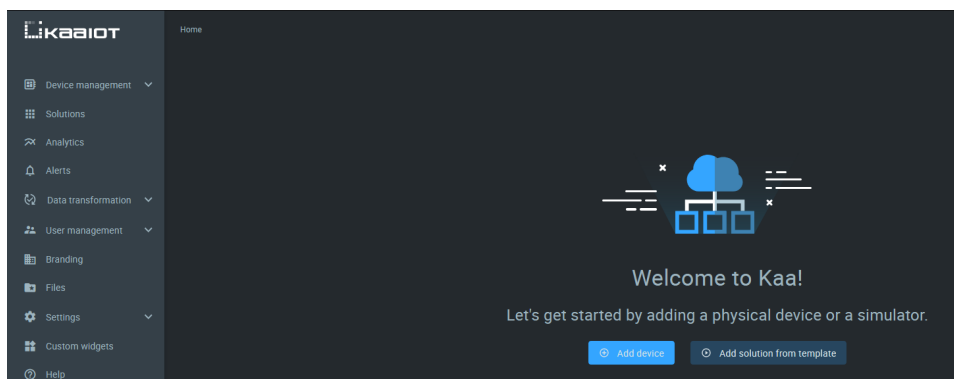


Figura 7.1: Dashboard Kaa IoT.

¹Hace referencia al cuadro de mandos al que tenemos acceso para interactuar con nuestro dispositivo y todas las posibles configuraciones

7.1. Conectar dispositivo

En este apartado se trata de explicar el proceso de conexión de un dispositivo con nuestra aplicación, desde crear un endpoint hasta ver la información del dispositivo en nuestra interfaz de usuario. Esto engloba varios términos y conceptos que se van a definir a continuación. [40]

7.1.1. Términos y conceptos

7.1.1.1. Endpoints

Los endpoints representan “el elemento de las cosas” del IoT. Un endpoint es cualquier dispositivo terminal que se quiera gestionar, en nuestro caso desde Kaa IoT. Un endpoint puede ser un dispositivo físico o una emulación de software del mismo. Todos los datos que llegan a la aplicación están asociados a endpoints. [41]

Para ser precisos, un endpoint puede ser una unidad menor que un dispositivo, lo que significa que un dispositivo físico puede incluir múltiples endpoints. Por ejemplo, quieres gestionar un termostato, para que el aire acondicionado se encienda y apague automáticamente a cierta temperatura.

Se puede gestionar el termostato de una de las siguientes maneras:

- Toda la unidad del termostato actúa como un endpoint único que intercambia datos con el servidor.
- Los componentes del termostato, como los sensores de temperatura y humedad, interruptor de encendido/apagado, actúan como endpoints individuales.

7.1.1.2. ID de Endpoint

El ID de endpoints se utiliza para identificar de forma única un endpoint dentro de una instancia. Un ID de endpoints suele ser un UUID generado automáticamente por el framework en el momento de crear un nuevo endpoint. No obstante, también se permiten los ID de endpoints definidos por el usuario. El ID de los endpoints no puede modificarse una vez creado.

Todos los datos de los endpoints, como los atributos de los metadatos, los puntos de datos de series temporales recopilados, los comandos, etc., están asociados a un ID de endpoint específico. Siempre que recupere o gestione datos relacionados con endpoints en Kaa, principalmente a través de la API REST, se verá los ID de endpoints.

7.1.1.3. Token del Endpoint

Los tokens de endpoints se utilizan para la identificación de endpoints cuando se intercambian datos relacionados con los endpoints, utilizando los protocolos compatibles basados en MQTT y HTTP. Los tokens de endpoint son únicos dentro de una aplicación IoT y se asignan exactamente a un endpoint.

Cuando llega un mensaje de un cliente, el token del endpoint se resuelve en el correspondiente ID del endpoint. Un ejemplo sobre el protocolo MQTT, el token del endpoint va dentro de la llamada MQTT, por ejemplo:

```
1 kp1/<APPLICATION_VERSION>/epmx/<ENDPOINT_TOKEN>/get
```

Normalmente, los tokens son cadenas generadas automáticamente por el framework, pero también se puede crear un token como el usuario quiera, por ejemplo, por el número de serie del dispositivo, dirección MAC, etc.

7.1.1.4. Metadatos del endpoint

Los metadatos de los endpoints son un conjunto de atributos clave-valor asociados a un endpoint. Se representan en el framework como un documento JSON de formato arbitrario.

Los metadatos de endpoints suelen incluir alguna información relacionada con los endpoints, como la ubicación, la descripción, el número de serie, la versión de hardware, etc. Los metadatos se almacenan en el servicio de registro de endpoints y pueden leerse o actualizarse de dos maneras:

- A través de la capa de comunicación.
- A través de la API REST.

También se pueden gestionar los metadatos mediante la interfaz de usuario del framework.

7.1.1.5. Aplicaciones y versiones

Las aplicaciones en Kaa IoT sirven como contenedores para endpoints de diferentes tipos. Se puede tener una aplicación que contenga todos los endpoints que representan a un determinado dispositivo, y una aplicación para otro dispositivo, independiente de la otra aplicación. Las aplicaciones IoT también albergan toda la configuración del sistema necesaria para que el framework conozca las capacidades de sus dispositivos conectados y cómo trabajar con ellos.

Puede pasar que ya hemos configurado nuestro dispositivo, pero queremos implementar una nueva característica. Al implementarla se actualiza el firmware del dispositivo y se empieza a desplegar pero, ¿cómo diferenciamos entre los dispositivos que ya tienen el nuevo firmware y las que no? Aquí aparecen las versiones de una aplicación.

Cada aplicación puede tener varias versiones al mismo tiempo. Cada versión representa un conjunto de capacidades soportadas por los endpoints. En cualquier momento, cada endpoint está asociado a una versión de su aplicación. El conocimiento de la versión actual de la aplicación de un endpoint ayuda al framework a entender qué funcionalidad soporta el endpoint, cómo se formatean los datos, etc. Se puede utilizar las versiones para hacer evolucionar los dispositivos añadiendo o retirando funcionalidades mientras mantiene sus versiones antiguas en funcionamiento. Para diferenciar llamadas entre versiones se puede indicar como hemos visto en 7.1.1.3.

7.1.2. Pasos a seguir

7.1.2.1. Crear una aplicación y una versión

Como hemos visto en 7.1.1, para registrar un endpoint en nuestro framework necesitamos una aplicación y una versión de esta. Esto podemos gestionarlo desde la interfaz de usuario, concretamente en la sección “Applications”, una vez en la sección usaremos el botón de “Add application”. Introduciremos el nombre de la aplicación (campo obligatorio) y tendremos la posibilidad de introducir una descripción. En nuestro caso la aplicación se llamará “TFG-DASIoT”.

Hay que tener en cuenta que tanto las aplicaciones como las versiones tienen:

- Nombres autoasignados e inmutables que suelen ser como **7bfdd6b9-ff44-4098-a4dc-58c0f3c9f693-v1**. Se utilizarán para las llamadas a la API, la integración con el cliente, etc.
- Nombres de visualización arbitrarios que se pueden cambiar en cualquier momento. Estos nombres se utilizan en la interfaz de usuario de la plataforma para una mejor experiencia de usuario. Por ejemplo, en nuestro caso el nombre de la aplicación y la descripción que hayamos puesto.



Figura 7.2: Nombre y descripción de la aplicación

En la imagen también se puede observar como hay un identificador justo debajo del nombre que le hemos asignado a la aplicación, esto es para referenciar de manera univoca a esta. Y ahora que tenemos la aplicación, creamos una versión de esta.

La primera versión que hemos creado se llama “test”. Y en la información de la aplicación podemos ver los servicios que tenemos activos.

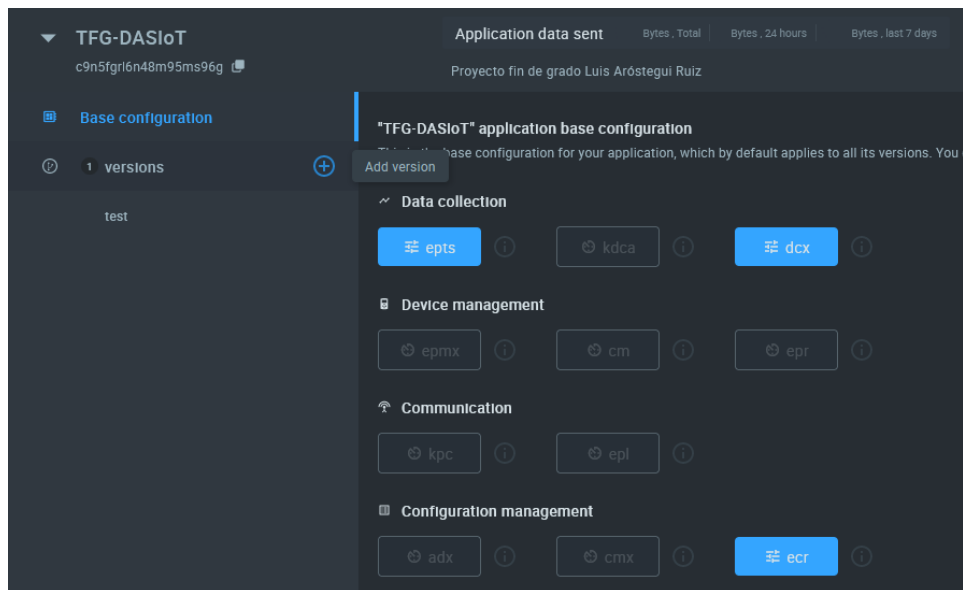


Figura 7.3: Versiones de la aplicación

- **Data collection.** *epts*, se refiere al servicio de series temporales de endpoints. Recibe muestras de datos de endpoints y los transforma en series temporales. *dcx*, es un servicio de recogida de datos, permite a los endpoints enviar muestras de datos de telemetría a la aplicación.
- **Configuration management.** *ecr*, configuración del repositorio del endpoint, almacena los datos de configuración de los endpoints y proporciona una API REST para la gestión.

7.1.2.2. Crear un endpoint

En la sección de “Devices” de nuestro dashboard, podremos añadir un nuevo dispositivo. Aquí indicaremos, la aplicación a la que va a estar asociada el dispositivo, un nombre para nuestro endpoint y opcionalmente podremos añadir metadatos.

En nuestro caso, para referirnos al endpoint lo hacemos mediante el *token endpoint* 7.1.1.3, que como vemos en 7.4, se llama token1. Esto lo usaremos en nuestra llamada mqtt para hacer referencia a este dispositivo.

Para ver todos los datos del dispositivo se nos muestra como vemos en 7.5. Donde podemos ver la aplicación a la que esta asociada, la fecha de creación y de su última actualización.

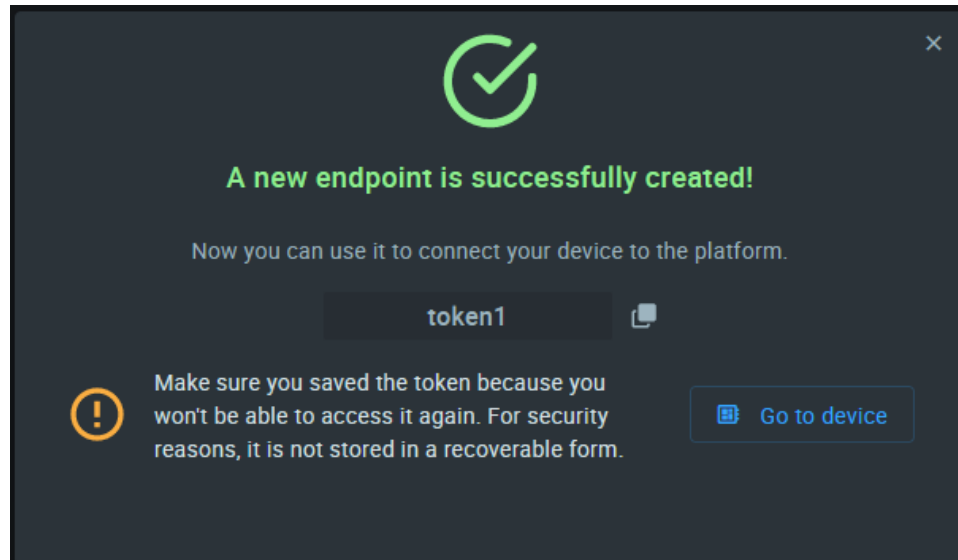


Figura 7.4: Endpoint creado

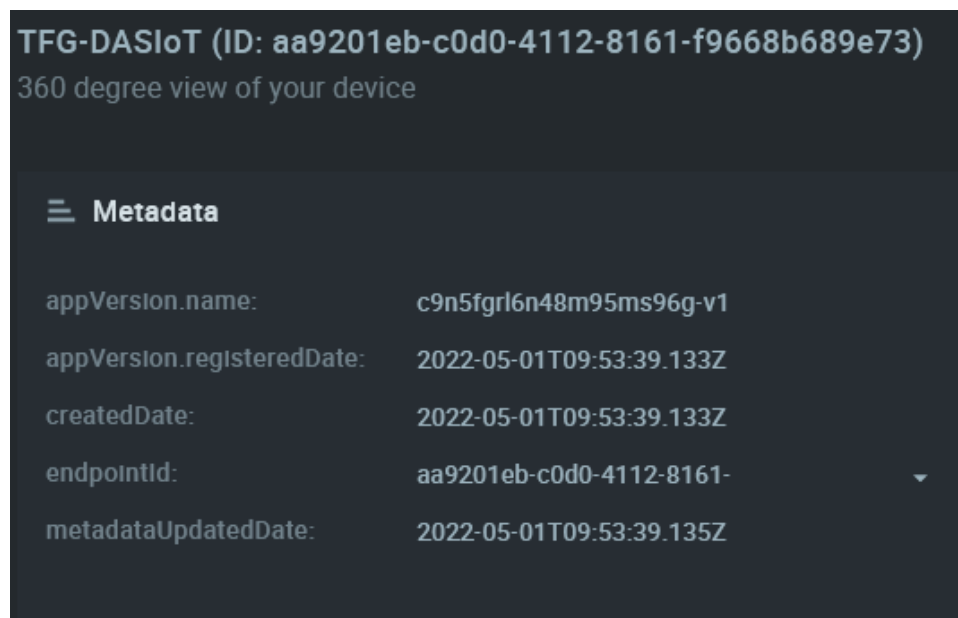


Figura 7.5: Datos del dispositivo creado

7.2. Recogida de datos de un dispositivo

En esta sección se trata de seguir completando nuestra aplicación, para ello vamos a ver como recoger datos de un dispositivo, visualizar estos datos y como transformarlos para darles un uso productivo. Antes de empezar con la implementación se definen, como anteriormente, términos y conceptos claves relacionados con el framework para entender el desarrollo. [42]

7.2.1. Términos y conceptos

7.2.1.1. Muestra de datos

Una muestra de datos hay que pensar en ella como un bloque de datos en formato **JSON**, este será enviado por un cliente a la aplicación. Un dispositivo recogerá datos del entorno para el que se haya configurado, estos datos los formateará y los enviará al framework en formato JSON para que sean tratados. Por ejemplo, si tenemos un dispositivo destinado a medir el tiempo meteorológico podremos obtener datos como los siguientes:

```
1 {  
2   "temperature": 25,  
3   "humidity": 46,  
4   "pressure": 800  
5 }
```

7.2.1.2. Series temporales

Las series temporales son una secuencia de puntos de datos con nombre. Cada punto de datos contiene una marca de tiempo y uno o más valores con nombre. Un conjunto de nombres de valores y sus tipos (numérico, string, booleano) define una serie temporal.

Es posible definir diferentes series temporales para varias cosas. Por ejemplo, una serie temporal puede tener sólo un valor numérico o por otro lado, otra serie temporal puede tener varios valores numéricos.

Se puede configurar la aplicación para que transforme las muestras de datos recibidas del endpoint en series temporales para mostrarlas en gráficos, indicadores, mapas, etc. El microservicio responsable de extraer los puntos de datos de las muestras de datos, almacenarlos y recuperarlos, es el servicio Endpoint Time Series (EPTS).

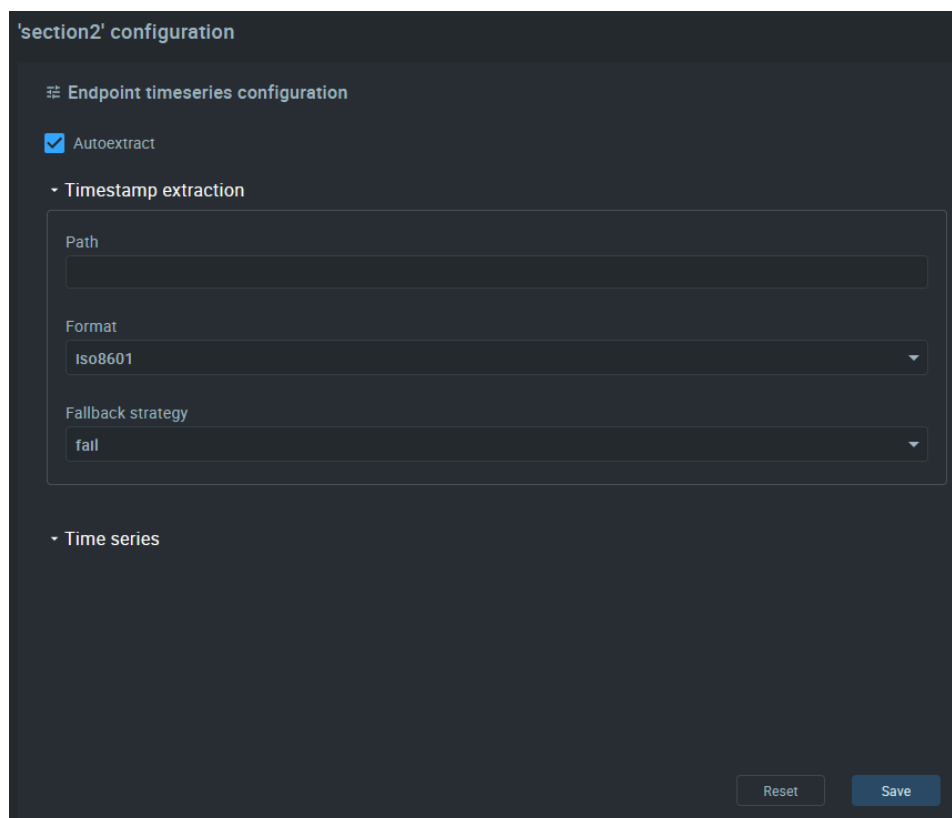
Además, el EPTS tiene una función de auto-extracción que almacena cada campo numérico de muestra de datos de nivel superior en una serie temporal separada. Todas las series temporales auto-extraídas tienen un nombre que sigue el patrón auto <nombre del campo>y un valor numérico con el valor del nombre.

Así, si un endpoint envía datos con una muestra con dos campos y la función de auto-extracción está activada, el EPTS crea dos series temporales.

7.2.2. Pasos a seguir

7.2.2.1. Activar la autoextracción de series temporales

Vamos a usar la opción de auto-extracción del EPTS. Para activarla tenemos que ir a la sección de “Gestión de dispositivos” -> “Aplicaciones” -> “EPTS” (en nuestra aplicación) -> Activar la casilla de **Auto extracción**.



The image shows a configuration interface for 'section2'. The main section is 'Endpoint timeseries configuration'. It includes a checkbox for 'Autoextract' which is checked. Below this is a section for 'Timestamp extraction' containing three fields: 'Path' (empty), 'Format' (set to 'iso8601'), and 'Fallback strategy' (set to 'fail'). There is also a 'Time series' section which is currently empty. At the bottom right, there are 'Reset' and 'Save' buttons.

Figura 7.6: Habilitar opción de auto extracción de datos

En nuestro caso hemos creado una versión nueva de nuestra aplicación llamada “section2” para probar esta nueva característica de nuestra aplicación.

Con esta función activada, se crearán automáticamente series temporales para cada campo numérico que se encuentre en la raíz de las muestras de datos que el endpoint envíe. A continuación, podremos ver estas series temporales en

la interfaz de usuario del framework, sin necesidad de realizar ninguna configuración adicional.

Ahora en la vista de nuestro dispositivo, concretamente en la sección de “telemetría del dispositivo”, podremos analizar los datos que recoge nuestro dispositivo.

7.3. Envío de comandos al dispositivo

En esta sección se trata de ejecutar comandos en nuestro dispositivo.

7.3.1. Términos y conceptos

7.3.1.1. Comando

Un comando es un mensaje de corta duración enviado a un endpoint. Con los comandos se pueden encender y apagar las luces o solicitar un informe inmediato del estado de un endpoint.

Cualquier comando puede estar en estado pendiente o ejecutado. El estado pendiente significa que el comando ha sido invocado pero aún no se conoce el resultado de su ejecución. El estado ejecutado se asigna al comando que ha obtenido una respuesta del endpoint, lo que significa que un endpoint recibió el comando, lo ejecutó y envió el resultado de la ejecución a la aplicación.

7.3.1.2. Tipo de comando

Representa el comando que se desea ejecutar en un endpoint, por ejemplo, reiniciar o encender la luz. Un endpoint puede manejar tantos tipos de comandos como se definan en su firmware.

7.3.2. Pasos a seguir

7.3.2.1. Invocar un comando

7.3.2.1.1. Ejecución con HTTP

Cuando se invoca un comando en un dispositivo que se conecta a la aplicación a través de un protocolo **síncrono**, por ejemplo, HTTP, no hay manera de que la plataforma envíe dicho comando al dispositivo. En su lugar, el framework persiste el comando y espera hasta que el dispositivo lo solicite para su ejecución. Esto significa que para los dispositivos con protocolos **síncronos** es nuestra responsabilidad sondear periódicamente la aplicación para nuevos comandos.

Para invocar un comando en la sección de “Dispositivos” hay un cuadro llamado *Ejecución de comandos*. Aquí indicamos el nombre del tipo de comando y una retención máxima. La retención máxima para la entrega define el tiempo en el que el comando está disponible para su ejecución. Una vez rellenado estos campos podemos clicar en “run”. Con esto hemos conseguido que si durante la próxima hora se llama a este comando, se ejecutará en el dispositivo.

7.3.2.1.2. Ejecución con MQTT

Con este protocolo el proceso se simplifica. Simplemente tenemos que dejar ejecutando el siguiente código y desde nuestro framework indicamos el tipo de comando y acción sobre el dispositivo.

7.4. Explotación de vulnerabilidad

Una vez terminada nuestra aplicación vamos a empezar a explotar MQTT teniendo en cuenta el análisis realizado en 5.4. Vamos a proceder siguiendo las fases de un ataque.

7.4.1. Reconocimiento

Como todo pentest de IoT comienza con el paso de reconocimiento, empezaremos por escanear la red. Para ello vamos usar **nmap**. Vamos a iniciar nuestra aplicación para empezar a transmitir datos desde el dispositivo hasta el framework y en ese momento empezaremos a escanear la red.

La orden para usar nmap:

```
1 sudo nmap -sS -sV -v -p 1883,8883 -oA mqtt-scan <ip>
```

Con esta orden se escanearán en la ip indicada los puertos indicados (1883,8883) y se nos indicará si están abiertos o cerrados.

7.4.2. Análisis de vulnerabilidades

En este caso al ver ambos puertos abiertos, sobre todo nos vamos a centrar en el puerto 1883 ya que este puerto carece de encriptación. Por tanto, vamos a explotar ese puerto mediante un ataque de fuerza bruta para conseguir acceso a la aplicación y poder enviar datos.

7.4.3. Explotación de una vulnerabilidad

Para explotar MQTT vamos a hacer uso de **Metasploit** ².

Se va a hacer uso del paquete **MQTT Authentication Scanner** [43]. En concreto, se va a usar el módulo **auxiliary/scanner/mqtt/connect**. Este módulo intenta autenticarse en MQTT.

Para hacer uso de la herramienta vamos a usar las siguientes órdenes:

- Uso del paquete. **use auxiliary/scanner/mqtt/connect**
- Insertar Hosts y puertos a explotar. **use RHOST** y **use RPORT**
- Insertar ruta a ficheros que contienen usuario y contraseñas típicos. **set PASS_FILE <path>** y **set USER_FILE <path>**
- Ejecutar la explotación e intento de inicio de sesión. **exploit**.

El resultado que obtenemos que se ha podido iniciar sesión sin autenticación. Esto se puede solucionar de varias maneras con nuestro framework. En concreto, podemos crear un usuario con su correspondiente contraseña.

Se creará un usuario con un identificador. Una vez creado en nuestra aplicación hacemos uso de **paho-mqtt** para indicar que cuando se inicie la conexión se va a requerir de unas credenciales. Se indicará de la siguiente manera:

```
1 client.username_pw_set("user1@ceb70d5b-8945-4991-bbaf-2022  
f54fc057", "1234")
```

En el capítulo 8 se analizará la seguridad de la creación de un usuario, ya que este se sigue haciendo sobre el puerto 1883. Se usará **tcpdump** en el momento de inicio de la conexión y se analizarán los paquetes.

La orden a ejecutar es:

```
1 sudo tcpdump port 1883 -w <nombre_fichero>.pcap
```

Se usará wireshark para mostrar el tráfico.

²Para su instalación se ha seguido la siguiente guía: <https://www.stiw.org/msf-pi.html>

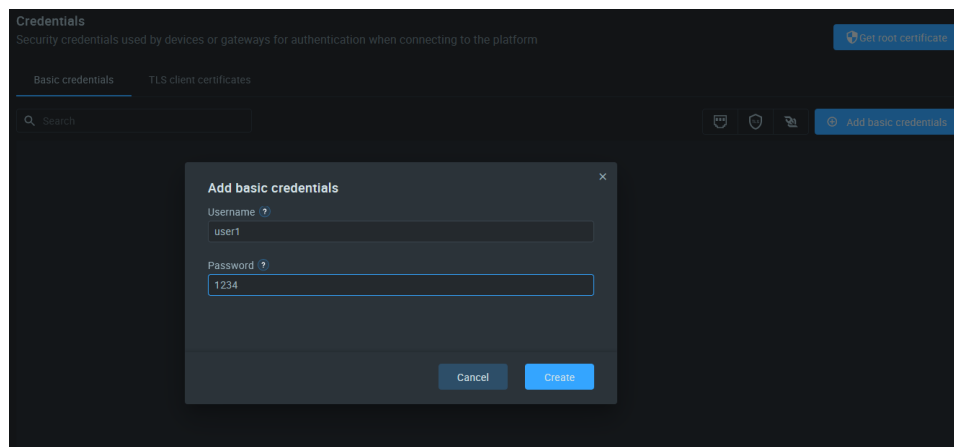


Figura 7.7: Crear usuario para iniciar conexión

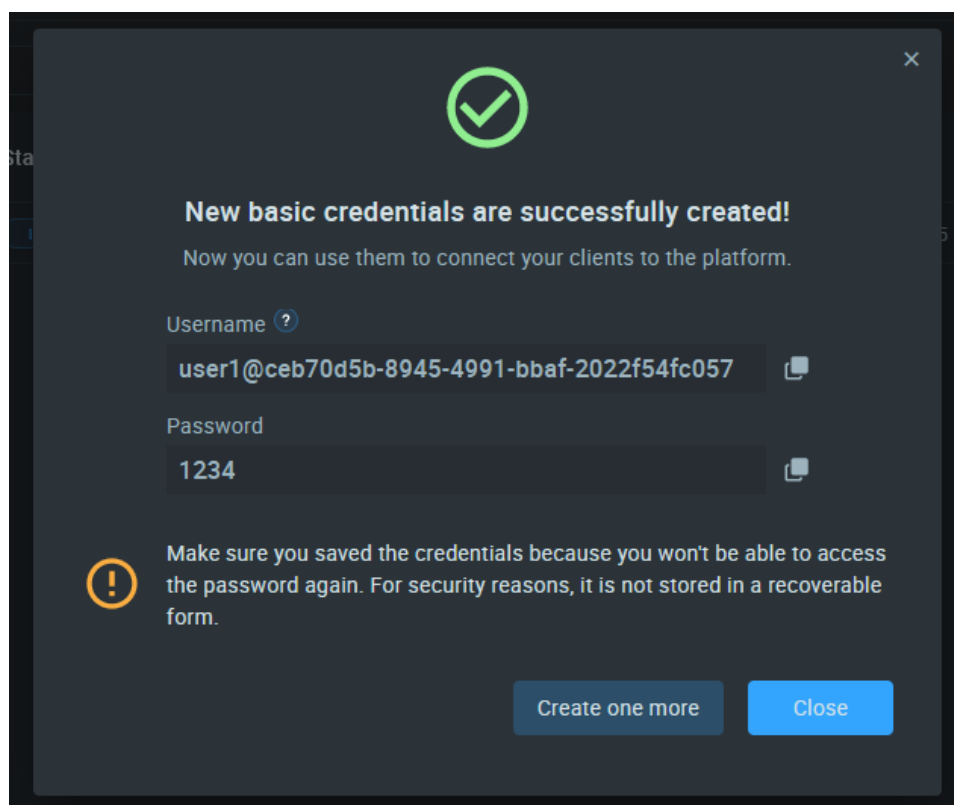


Figura 7.8: Identificador para el nuevo usuario

CAPÍTULO 8

Pruebas

Para realizar las pruebas, he tenido la oportunidad de usar una Raspberry PI [32]. De esta manera he podido hacer uso de las funcionalidades de este dispositivo para mostrar de una manera más realista el potencial de la aplicación y también de explotar una vulnerabilidad.

8.1. Conectar un cliente

Tal y como vimos en 7.1, una vez ya hemos creado nuestro primer endpoint, podemos conectar un cliente y obtener y enviar algunos metadatos. Como se analizó 5.3, Kaa IoT es un framework que soporta varios protocolos donde nos encontramos con HTTP y MQTT 2.1.2.2.

Para hacer uso de los protocolos y completar la integración del cliente necesitaremos el nombre de la versión y el token del endpoint. En esta sección se va a mostrar como hacer uso de ambos protocolos, concretamente de las órdenes para poder ejecutar la conexión con nuestro dispositivo, en la sección de *Pruebas 8* se mostrarán los datos que obtenemos tras su ejecución.

8.1.1. Conexión mediante HTTP

Para obtener todos los atributos de los metadatos con **HTTP** vamos a hacer uso de **cURL** ¹ para enviar una solicitud de actualización de datos del dispositivo.

¹Es un proyecto de software consistente en una biblioteca y un intérprete de comandos orientado a la transferencia de archivos. Soporta los protocolos FTP, FTPS, HTTP, HTTPS, TFTP, SCP, SFTP, Telnet, DICT, FILE y LDAP, entre otros.

```

1 curl - -location - -request POST 'https://connect.cloud.kaaiot.
    com:443/kp1/
2 <app-version-name>/epmx/<endpoint-token>/update/keys' \
3 - -data-raw '{
4     "model": "Raspberry PI",
5     "mac": "00-14-22-01-23-45"
6 }',

```

Ejecutando esta instrucción añadiremos nuevos metadatos a nuestro dispositivo, concretamente la dirección física y el modelo de este.

8.1.2. Conexión mediante MQTT

Para hacer la conexión mediante MQTT se ha optado por la opción de usar Python en su versión 3.10, obtenemos un código como el siguiente.

```

1 import itertools
2 import json
3 import queue
4 import sys
5 from subprocess import Popen, PIPE
6
7
8 class MetadataClient:
9
10     def __init__(self, client, app_version, endpoint_token):
11         self.client = client
12         self.app_version = app_version
13         self.endpoint_token = endpoint_token
14         self.metadata_by_request_id = {}
15         self.global_request_id = itertools.count()
16         get_metadata_subscribe_topic = f'kp1/{self.app_version}
17         /epmx/{self.endpoint_token}/get/#'
18         self.client.message_callback_add(
19             get_metadata_subscribe_topic, self.handle_metadata)
20
21     def handle_metadata(self, client, userdata, message):
22         request_id = int(message.topic.split('/')[2])
23         if message.topic.split('/')[1] == 'status' and
24         request_id in self.metadata_by_request_id:
25             print(f'<--- Received metadata response on topic {
26             message.topic}')
27             metadata_queue = self.metadata_by_request_id[
28             request_id]
29             metadata_queue.put_nowait(message.payload)
30         else:
31             print(
32                 f'<--- Received bad metadata response on topic
33                 {message.topic}:\n{str(message.payload.decode("utf-8"))}')
34
35     def get_metadata(self):
36         request_id = next(self.global_request_id)
37         get_metadata_publish_topic = f'kp1/{self.app_version}/
38         epmx/{self.endpoint_token}/get/{request_id}'

```

```

32
33     metadata_queue = queue.Queue()
34     self.metadata_by_request_id[request_id] =
metadata_queue
35
36     print(f'--> Requesting metadata by topic {
get_metadata_publish_topic}')
37     self.client.publish(topic=get_metadata_publish_topic,
payload=json.dumps({}))
38     try:
39         metadata = metadata_queue.get(True, 5)
40         del self.metadata_by_request_id[request_id]
41         return str(metadata.decode("utf-8"))
42     except queue.Empty:
43         print('Timed out waiting for metadata response from
server')
44         sys.exit()
45
46     def patch_metadata_unconfirmed(self, metadata):
47         partial_metadata_update_publish_topic = f'kp1/{self.
app_version}/epmx/{self.endpoint_token}/update/keys'
48
49         print(f'--> Reporting metadata on topic {
partial_metadata_update_publish_topic}\nwith payload {
metadata}')
50         self.client.publish(topic=
partial_metadata_update_publish_topic, payload=metadata)
51
52     def hardware_devices(self):
53         return Popen(['lsusb'], stdout=PIPE, encoding='utf-8').
communicate()[0]
54
55     def set_metadata(self):
56         metadata_to_report = json.dumps(
57             {"model": "Raspberry PI",
58              "mac": "b8-27-eb-f8-00-af",
59              "devices": self.hardware_devices()
60             }
61         )
62         return metadata_to_report

```

La ejecución de este código produce un efecto similar que el visto con HTTP. En este caso se ha creado una clase *MetadataClient*, su objetivo es el de actualizar los metadatos del dispositivo en nuestra aplicación. Cada vez que se establece la conexión se analiza los dispositivos conectados a la Raspberry y se envían a la aplicación (como ejecutar en la terminal de linux, `lsusb`).

8.2. Recogida de datos y ejecución de comandos de un dispositivo

8.2.1. Envío de datos mediante MQTT

Al igual que en la sección 8.1.2 tenemos un código para hacer el envío de datos y la ejecución de comandos, para ello definimos dos endpoints, uno para encender un led y el otro para apagar un led.

El código es el siguiente:

```

1 import json
2 import signal
3 import time
4
5 from gpiozero import LED, CPUTemperature
6
7
8 def temp_data():
9     cpu = CPUTemperature()
10    return cpu.temperature
11
12
13 class KaaClient:
14
15     def __init__(self, client, app_version, endpoint_token,
16                 host, port):
17         self.client = client
18         self.app_version = app_version
19         self.endpoint_token = endpoint_token
20         self.host = host
21         self.port = port
22         self.metadata_update_topic = f'kp1/{self.app_version}/
23         epmx/{self.endpoint_token}/update/keys'
24         self.data_collection_topic = f'kp1/{self.app_version}/
25         dcx/{self.endpoint_token}/json'
26
27         self.led = LED(17)
28
29         command_turn_on_topic = f'kp1/{self.app_version}/cex/{
30         self.endpoint_token}/command/turnon/status'
31         self.client.message_callback_add(command_turn_on_topic,
32         self.handle_turn_on_command)
33         self.command_turn_on_result_topik = f'kp1/{self.
34         app_version}/cex/{self.endpoint_token}/result/turnon'
35
36         command_turn_off_topic = f'kp1/{self.app_version}/cex/{
37         self.endpoint_token}/command/turnoff/status'
38         self.client.message_callback_add(command_turn_off_topic
39         , self.handle_turn_off_command)
40         self.command_turn_off_result_topik = f'kp1/{self.
41         app_version}/cex/{self.endpoint_token}/result/turnoff'

```

```

33
34     def connect_to_server(self):
35         print(
36             f'Connecting to Kaa server at {self.host}:{self.
port} using application version {self.app_version}'
37             f' and endpoint token {self.endpoint_token}')
38         self.client.connect(self.host, self.port, 60)
39         print('Successfully connected')
40
41     def disconnect_from_server(self):
42         print(f'Disconnecting from Kaa server at {self.host}:{
self.port}...')
43         self.client.loop_stop()
44         self.client.disconnect()
45         print('Successfully disconnected')
46
47     def compose_data_sample(self):
48         return json.dumps([
49             {
50                 "timestamp": int(round(time.time() * 1000)),
51                 "temperature": int(temp_data())
52             }
53         ])
54
55     def on_message(client, userdata, message):
56         print(f'<-- Received message on topic "{message.topic
}":\n{str(message.payload.decode("utf-8"))}')
57
58     def handle_turn_on_command(self, client, userdata, message)
:
59         print(f'<--- Received "turn on" command on topic {
message.topic} \nTurning on...')
60         self.led.on()
61         command_result = self.compose_command_result_payload(
message)
62         print(f'command result {command_result}')
63         client.publish(topic=self.command_turn_on_result_topik,
payload=command_result)
64         # With below approach we don't receive the command
confirmation on the server side.
65         # self.client.disconnect()
66         # time.sleep(5) # Simulate the reboot
67         # self.connect_to_server()
68
69     def handle_turn_off_command(self, client, userdata, message
):
70         print(f'<--- Received "turn on" command on topic {
message.topic} \nTurning off...')
71         self.led.off()
72         command_result = self.compose_command_result_payload(
message)
73         print(f'command result {command_result}')
74         client.publish(topic=self.command_turn_on_result_topik,
payload=command_result)

```

```

75
76     def compose_command_result_payload(self, message):
77         command_payload = json.loads(str(message.payload.decode(
78             "utf-8")))
79         print(f'command payload: {command_payload}')
80         command_result_list = []
81         for command in command_payload:
82             commandResult = {"id": command['id'], "statusCode":
200, "reasonPhrase": "OK", "payload": "Success"}
83             command_result_list.append(commandResult)
84         return json.dumps(
85             command_result_list
86         )
87
88 class Signallistener:
89     keepRunning = True
90
91     def __init__(self):
92         signal.signal(signal.SIGINT, self.stop)
93         signal.signal(signal.SIGTERM, self.stop)
94
95     def stop(self, signum, frame):
96         print('Shutting down...')
97         self.keepRunning = False

```

Con este código se entra en un bucle donde se van haciendo llamadas al dispositivo y recogiendo información. La información que nos llega viene en formato JSON. Se usa la librería *gpiozero* para encender/apagar el led y obtener la temperatura de la CPU.

También se ha creado un fichero para cargar la configuración necesaria (endpoint ID, host, puerto) y ejecutar el programa.

```

1
2 import random
3 import string
4 import time
5
6 from metadataClient import MetadataClient
7 from kaaClient import KaaClient
8 from kaaClient import Signallistener
9
10 import paho.mqtt.client as mqtt
11 from decouple import config
12
13 KPC_HOST = config('KPC_HOST', cast=str)
14 KPC_PORT = config('KPC_PORT', cast=int)
15
16 APPLICATION_VERSION = config('APPLICATION_VERSION', cast=str)
17 ENDPOINT_TOKEN = config('ENDPOINT_TOKEN', cast=str)
18
19

```



```

20 def main():
21     # Iniciar la conexión con el servidor
22     print(
23         f'Connecting to Kaa server at {KPC_HOST}:{KPC_PORT}
24         using application version {APPLICATION_VERSION}'
25         f' and endpoint token {ENDPOINT_TOKEN}')
26
27     client_id = ''.join(random.choice(string.ascii_uppercase +
28     string.digits) for _ in range(6))
29     client = mqtt.Client(client_id=client_id)
30     client.connect(KPC_HOST, KPC_PORT, 60)
31     client.loop_start()
32
33     metadata_client = MetadataClient(client,
34     APPLICATION_VERSION, ENDPOINT_TOKEN)
35
36     # Obtener los atributos de los metadatos del endpoint
37     actual
38     retrieved_metadata = metadata_client.get_metadata()
39     print(f'Retrieved metadata from server: {retrieved_metadata
40     }')
41
42     # Actualizar parcialmente los metadatos del endpoint
43     metadata_to_report = metadata_client.set_metadata()
44     metadata_client.patch_metadata_unconfirmed(
45     metadata_to_report)
46
47     time.sleep(5)
48     client.disconnect()
49
50     # Initiate server connection
51     client = mqtt.Client(client_id=''.join(random.choice(string
52     .ascii_uppercase + string.digits) for _ in range(6)))
53
54     data_collection_client = KaaClient(client,
55     APPLICATION_VERSION, ENDPOINT_TOKEN, KPC_HOST, KPC_PORT)
56     data_collection_client.connect_to_server()
57
58     client.on_message = data_collection_client.on_message
59
60     # Start the loop
61     client.loop_start()
62
63     # Send data samples in loop
64     listener = SignalListener()
65     while listener.keepRunning:
66
67         payload = data_collection_client.compose_data_sample()
68
69         result = data_collection_client.client.publish(topic=
70         data_collection_client.data_collection_topic,
71         payload=
72         payload)
73         if result.rc != 0:

```

```
64         print('Server connection lost, attempting to
           reconnect')
65         data_collection_client.connect_to_server()
66     else:
67         print(f'--> Sent message on topic "{
           data_collection_client.data_collection_topic}":\n{payload}'
           )
68
69         time.sleep(3)
70
71         data_collection_client.disconnect_from_server()
72
73
74 if __name__ == '__main__':
75     main()
```

Se usa *decouple* para evitar mostrar los datos de configuración de la aplicación, usando un fichero *.env*.

Se muestra a continuación pruebas de la ejecución del código.

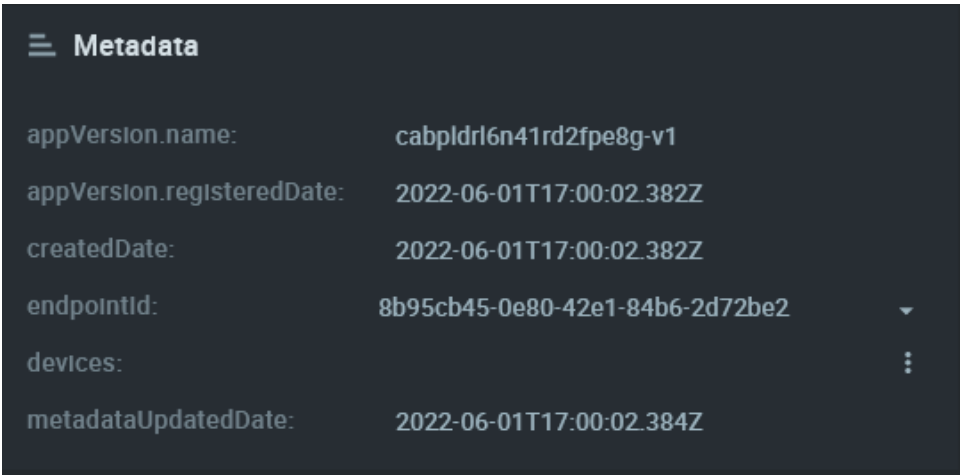


Figura 8.1: Metadatos una vez creada nuestra aplicación

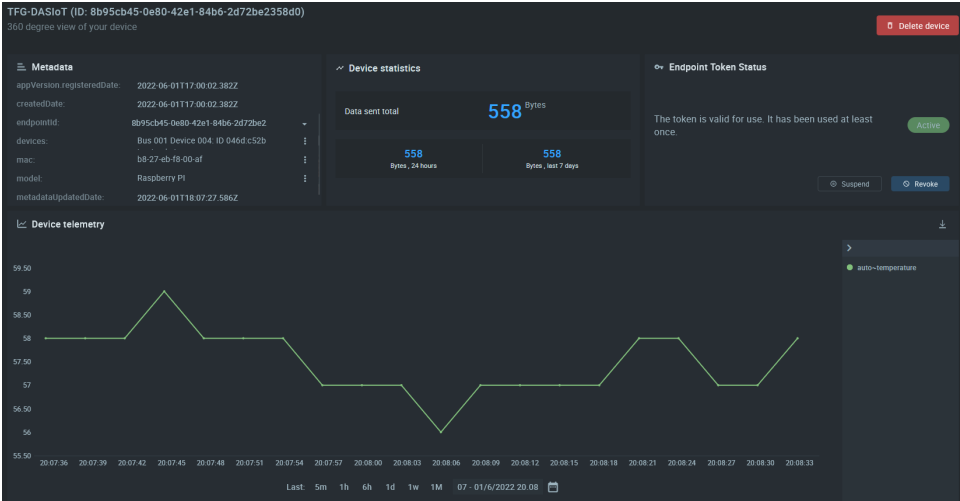


Figura 8.2: Metadatos actualizados y telemetría de la temperatura de la CPU

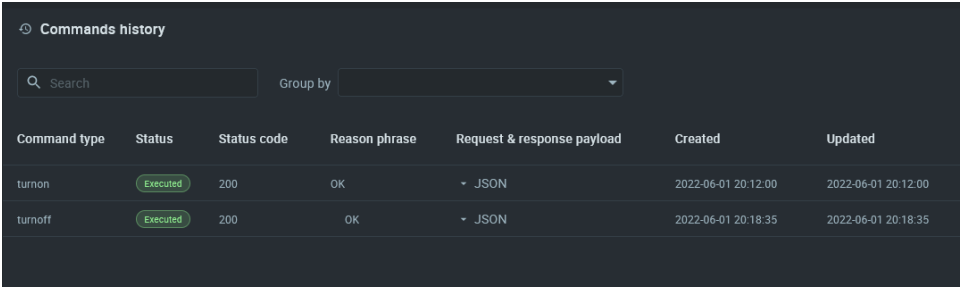


Figura 8.3: Encendido y apagado del led

>_ **Command execution**

Command type* ?

turnon

Command body in JSON*

```
{"led": "turning on led"}
```

Execution type ?

☒ Asynchronous ☐ Synchronous

Waiting timeout ?

5 seconds

Maximum command retention for delivery

1 minutes

Run

Figura 8.4: Petición de encendido del led

```

--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107512178, "temperature": 58}]
<-- Received "turn on" command on topic kpl/cabpldr16n41rd2fpe8g-v1/cex/token1/command/turnoff/status
Turning off...
command payload: [{"id": 771092615, "payload": {"led": "turning off led"}}]
command result [{"id": 771092615, "statusCode": 200, "reasonPhrase": "OK", "payload": "Success"}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107515201, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107510244, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107521263, "temperature": 59}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107524282, "temperature": 58}]

```

Figura 8.5: Inicio de conexión y envío de datos a la aplicación

```

--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107115565, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107118584, "temperature": 57}]
<-- Received "turn on" command on topic kpl/cabpldr16n41rd2fpe8g-v1/cex/token1/command/turnon/status
Turning on...
command payload: [{"id": 1357491370, "payload": {"led": "turning on led"}}]
command result [{"id": 1357491370, "statusCode": 200, "reasonPhrase": "OK", "payload": "Success"}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107121605, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107124624, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654107127644, "temperature": 57}]

```

Figura 8.6: Encendiendo el led

```

luisarostegui@raspberrypi: ~/TFG/dasiot
File Edit Tabs Help
luisarostegui@raspberrypi:~/TFG/dasiot $ python dasiot.py
Connecting to Kaa server at mqtt.cloud.kaaaiot.com:1883 using application version cabpldr16n41rd2fpe8g-v1 and endpoint token token1
--> Requesting metadata by topic kpl/cabpldr16n41rd2fpe8g-v1/epmx/token1/get/0
<-- Received metadata response on topic kpl/cabpldr16n41rd2fpe8g-v1/epmx/token1/get/0/status
Retrieved metadata from server: {"devices": ""}
--> Reporting metadata on topic kpl/cabpldr16n41rd2fpe8g-v1/epmx/token1/update/keys
with payload {"model": "Raspberry Pi", "mac": "b8-27-eb-f8-00-af", "devices": "Bus 001 Device 004: ID 046d:c52b Logitech, Inc."}
Connecting to Kaa server at mqtt.cloud.kaaaiot.com:1883 using application version cabpldr16n41rd2fpe8g-v1 and endpoint token token1
Successfully connected
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106852779, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106855811, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106858830, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106861849, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106864868, "temperature": 59}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106867887, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106870906, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106873925, "temperature": 58}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106876944, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106879964, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106882983, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106886002, "temperature": 56}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106889021, "temperature": 57}]
--> Sent message on topic "kpl/cabpldr16n41rd2fpe8g-v1/dcx/token1/json":
[{"timestamp": 1654106892041, "temperature": 57}]

```

Figura 8.7: Apagando el led

8.3. Escanear red

Se muestra el escaneo de la red con **nmap**. 8.8

8.4. Explotación de una vulnerabilidad

Se muestra el uso de Metasploit para iniciar sesión en la aplicación y poder enviar datos a la aplicación. 8.9 - 8.10

Para analizar la seguridad de crear un usuario para iniciar la conexión entre dispositivo y aplicación se ha escaneado el tráfico en el momento del inicio de sesión.

Si observamos los datos enviados al estar en el puerto 1883, todos los datos se envían sin encriptación y por tanto podemos leer las credenciales para el inicio de sesión. 8.11

```

luisarostegui@raspberrypi:~/TFG/dasiot $ sudo nmap -sS -sV -v -p 1883,8883 -oA mqttt-scan 54.194.250.238
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-20 19:18 CEST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 19:18
Scanning 54.194.250.238 [4 ports]
Completed Ping Scan at 19:18, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:18
Completed Parallel DNS resolution of 1 host. at 19:18, 0.10s elapsed
Initiating SYN Stealth Scan at 19:18
Scanning ec2-54-194-250-238.eu-west-1.compute.amazonaws.com (54.194.250.238) [2 ports]
Discovered open port 1883/tcp on 54.194.250.238
Discovered open port 8883/tcp on 54.194.250.238
Completed SYN Stealth Scan at 19:18, 0.09s elapsed (2 total ports)
Initiating Service scan at 19:18
Scanning 2 services on ec2-54-194-250-238.eu-west-1.compute.amazonaws.com (54.194.250.238)
Completed Service scan at 19:18, 12.48s elapsed (2 services on 1 host)
NSE: Script scanning 54.194.250.238.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.48s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.01s elapsed
Nmap scan report for ec2-54-194-250-238.eu-west-1.compute.amazonaws.com (54.194.250.238)
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
1883/tcp  open  mqtt
8883/tcp  open  ssl/mqtt

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (128B)
luisarostegui@raspberrypi:~/TFG/dasiot $

```

Figura 8.8: Escaneo de red con nmap

```

msf6 auxiliary(scanner/mqtt/connect) > set PASS_FILE /home/luisarostegui/TFG/metasploit-data/passwords.txt
PASS_FILE => /home/luisarostegui/TFG/metasploit-data/passwords.txt
msf6 auxiliary(scanner/mqtt/connect) > set USER_FILE /home/luisarostegui/TFG/metasploit-data/users.txt
USER_FILE => /home/luisarostegui/TFG/metasploit-data/users.txt
msf6 auxiliary(scanner/mqtt/connect) >

```

Figura 8.9: Insertar PASS_FILE y USER_FILE

```

msf6 auxiliary(scanner/mqtt/connect) > set RHOST 52.49.159.114
RHOST => 52.49.159.114
msf6 auxiliary(scanner/mqtt/connect) > set RPORT 1883
RPORT => 1883
msf6 auxiliary(scanner/mqtt/connect) > exploit

[*] 52.49.159.114:1883 - 52.49.159.114:1883 - Testing without credentials
[*] 52.49.159.114:1883 - Does not require authentication
[*] 52.49.159.114:1883 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mqtt/connect) >

```

Figura 8.10: Insertar host y puerto para ejecución. Resultado de la explotación

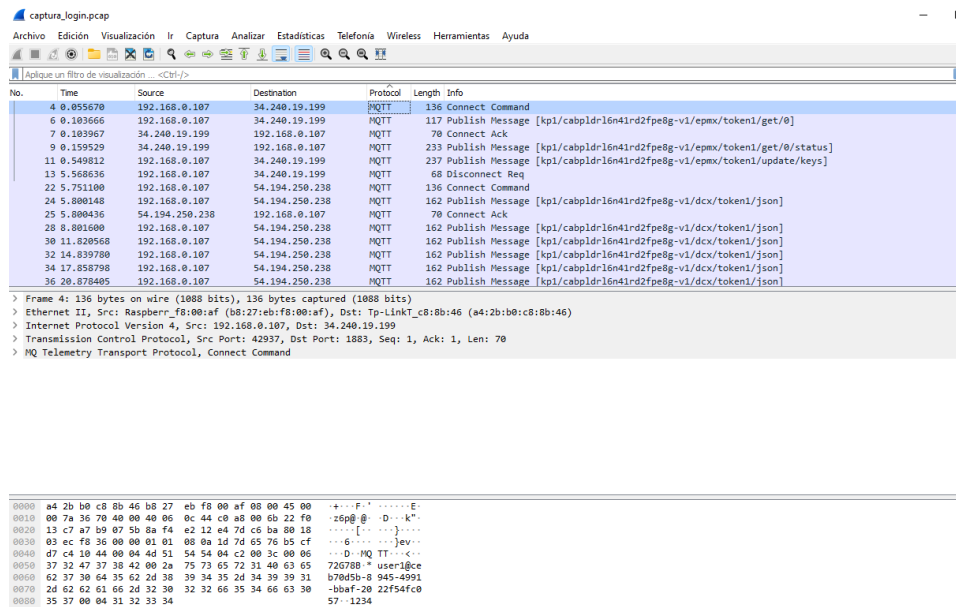


Figura 8.11: Captura de tráfico con tcpdump. Inicio de sesión

CAPÍTULO 9

Conclusiones y trabajos futuros

Bibliografía

- [1] labplus. https://mpython.readthedocs.io/en/master/_images/three-layer-iot-architecture.png, consultado el 11 de Abril de 2022.
- [2] Haider Al-Shammari. <https://www.researchgate.net/publication/338166577/figure/fig1/as:840165425676289@1577322455370/soa-based-architecture-for-iot-middleware-1.jpg>, consultado el 11 de Abril de 2022.
- [3] RF Page. <https://www.rfpage.com/what-are-the-major-components-of-internet-of-things/>, consultado el 15 de Abril de 2022.
- [4] Victor Pasknel. <https://morphuslabs.com/hacking-the-iot-with-mqtt-8edaf0d07b9b>, consultado el 19 de Junio de 2022.
- [5] Ben Nuttall Revision. <https://gpiozero.readthedocs.io/en/stable/recipes.html>, consultado el 1 de Junio de 2022.
- [6] Preeti Agarwal and Mansaf Alam. Investigating iot middleware platforms for smart application development. In *Smart Cities—Opportunities and Challenges*, pages 231–244. Springer, 2020.
- [7] D. Serpanos and M. Wolf. *Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies*. Springer International Publishing, 2018.
- [8] P. Lea. *IoT and Edge Computing for Architects: Implementing Edge and IoT Systems from Sensors to Clouds with Communication Systems, Analytics, and Security, 2nd Edition*. Expert insight. Packt Publishing, 2020.
- [9] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry. *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Fundamentals. Pearson Education, 2017.

- [10] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, 4(5):1125–1142, 2017.
- [11] Wan Haslina Hassan et al. Current research on internet of things (iot) security: A survey. *Computer networks*, 148:283–294, 2019.
- [12] Sajjad Hussain Shah and Ilyas Yaqoob. A survey: Internet of things (iot) technologies, applications and challenges. In *2016 IEEE Smart Energy Grid Engineering (SEGE)*, pages 381–385, 2016.
- [13] BK Tripathy and J. Anuradha. *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions*. CRC Press, 2017.
- [14] Farhana Javed, Muhamamd Khalil Afzal, Muhammad Sharif, and Byung-Seo Kim. Internet of things (iot) operating systems support, networking technologies, applications, and challenges: A comparative review. *IEEE Communications Surveys Tutorials*, 20(3):2062–2100, 2018.
- [15] Andrew S. Tanenbaum and David Wetherall. *Computer networks*, 5th edition. 2011.
- [16] PymeLegal. <https://www.pymelegal.es/noticias/aepd/proteccion-de-datos-y-el-internet-de-las-cosas>, consultado el 11 de Junio de 2022.
- [17] AEPD. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf, consultado el 11 de Junio de 2022.
- [18] IoTDunia. <https://iotdunia.com/what-is-iot-framework-list-top-10-open-source-iot-frameworks/#what-is-iot-framework>, consultado el 15 de Abril de 2022.
- [19] Bhumi Nakhuva and Tushar Champaneria. Study of various internet of things platforms. *International Journal of Computer Science & Engineering Survey*, 6(6):61–74, 2015.
- [20] Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, and Siobhán Clarke. Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, 3(1):70–95, 2016.
- [21] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng. Iot middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal*, 4(1):1–20, 2017.
- [22] Rusu Liviu Dumitru. Iot platforms: Analysis for building projects. *Informatica Economica*, 21(2), 2017.

- [23] KaaloT Technologies. <https://www.kaaiot.com/>, consultado el 17 de Abril de 2022.
- [24] Inc. The MathWorks. <https://thingspeak.com/>, consultado el 17 de Abril de 2022.
- [25] Applied Informatics Software Engineering GmbH. <https://macchina.io/>, consultado el 17 de Abril de 2022.
- [26] Altair Engineering Inc. <https://www.altair.com/smartworks/>, consultado el 17 de Abril de 2022.
- [27] Apigee. <https://www.zettajs.org/>, consultado el 17 de Abril de 2022.
- [28] Inc Temboo. <https://temboo.com/iot>, consultado el 18 de Abril de 2022.
- [29] MQTT.org. <https://mqtt.org/>, consultado el 19 de Junio de 2022.
- [30] OpenSystems Media. <https://embeddedcomputing.com/technology/security/how-to-hack-iot-devices-from-your-couch>, consultado el 19 de Junio de 2022.
- [31] hiberus TECNOLOGÍA. <https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/>, consultado el 19 de Junio de 2022.
- [32] IBEX UK Ltd. <https://raspberrypi-projects.com/pi/pi-hardware/raspberrypi-pcb-versions>, consultado el 1 de Junio de 2022.
- [33] Python Software Foundation. <https://docs.python.org/3/license.html>, consultado el 4 de Junio de 2022.
- [34] Wikipedia. <https://es.wikipedia.org/wiki/python>, consultado el 4 de Junio de 2022.
- [35] Python Software Foundation. <https://pypi.org/project/paho-mqtt/>, consultado el 4 de Junio de 2022.
- [36] Wikipedia. <https://es.wikipedia.org/wiki/pycharm>, consultado el 4 de Junio de 2022.
- [37] Python Software Foundation. <https://docs.python.org/3/library/subprocess.html>, consultado el 4 de Junio de 2022.
- [38] Ben Nuttall. <https://gpiozero.readthedocs.io/en/stable/index.html>, consultado el 4 de Junio de 2022.
- [39] Python Software Foundation. <https://pypi.org/project/python-decouple/>, consultado el 4 de Junio de 2022.

- [40] KaaloT Technologies. <https://docs.kaaiot.io/kaa/docs/current/tutorials/getting-started/connecting-your-first-device/>, consultado el 8 de Mayo de 2022.
- [41] KaaloT Technologies. <https://docs.kaaiot.io/kaa/docs/current/kaa-concepts>, consultado el 1 de Mayo de 2022.
- [42] KaaloT Technologies. <https://docs.kaaiot.io/kaa/docs/current/tutorials/getting-started/collecting-data-from-a-device/>, consultado el 9 de Mayo de 2022.
- [43] InfosecMatter. <https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/mqtt/connect>, consultado el 26 de Junio de 2022.