UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE SEGURIDAD IOT PARA UN SISTEMA DOMÓTICO

ORELLANA MARTINEZ HAYDEE BRIGGITTE
INGENIERA DE SISTEMAS

MACHALA
2020

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE SEGURIDAD IOT PARA UN SISTEMA DOMÓTICO

ORELLANA MARTINEZ HAYDEE BRIGGITTE
INGENIERA DE SISTEMAS

MACHALA
2020

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

ANÁLISIS DE SEGURIDAD IOT PARA UN SISTEMA DOMÓTICO

ORELLANA MARTINEZ HAYDEE BRIGGITTE
INGENIERA DE SISTEMAS

HERNANDEZ ROJAS DIXYS LEONARDO

MACHALA, 22 DE DICIEMBRE DE 2020

MACHALA
2020

tesis bridg

INFORME DE ORIGINALIDAD

3%	3%	1%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	erecursos.uacj.mx Fuente de Internet	<1%
2	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1%
3	www.geoconsult-inc.com Fuente de Internet	<1%
4	enviomedical.com Fuente de Internet	<1%
5	moam.info Fuente de Internet	<1%
6	eresmama.com Fuente de Internet	<1%
7	web.netexplora.com Fuente de Internet	<1%
8	www.revistafuturos.info Fuente de Internet	<1%
9	thepowermba.com Fuente de Internet	<1%

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, ORELLANA MARTINEZ HAYDEE BRIGGITTE, en calidad de autora del siguiente trabajo escrito titulado ANÁLISIS DE SEGURIDAD IOT PARA UN SISTEMA DOMÓTICO, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 22 de diciembre de 2020

Brigitte Orellana M.

ORELLANA MARTINEZ HAYDEE BRIGGITTE
0705314532

DEDICATORIA

El presente trabajo lo dedico principalmente a Dios y a la Virgen María, por ser mi fuente de inspiración para no rendirme y ayudarme a perseverar.

A mis padres, que con su sacrificio y amor fueron capaces de sacarme adelante, enseñándome que todo se alcanza con esfuerzo, que en los momentos difíciles que tenía que pasar, siempre tuvieron una palabra, una sonrisa, una oración para mí.

Dedico también este trabajo a cada una de las personas que confiaron en mí, que siempre estuvieron con un mensaje para incentivarme a ser mejor, a no rendirme y a buscar cumplir lo que me proponga, recordando siempre por qué empecé y que siempre puedo sacar lo mejor de mí en cada momento.

AGRADECIMIENTO

Quiero expresar inicialmente mi agradecimiento a Dios, por sostenerme durante toda mi etapa universitaria, y aún más en esta que es la más importante para lograr alcanzar una de mis metas.

Agradezco a las personas que me permitieron llegar hasta donde estoy ahora, que son mis padres, mi familia, gracias por las enseñanzas impartidas, por siempre estar para mí.

También agradezco a todos los docentes de la Escuela de Informática por sus enseñanzas, por siempre ayudarnos a ser mejores personas y profesionales, de una manera especial a mi tutor el Ing. Dixys Leonardo Hernández Rojas por depositar su confianza en mí para este proyecto, por alentarme a ser mejor profesionalmente y por transmitir sus valiosos conocimientos.

RESUMEN

El hecho de que el internet se encuentre presente en gran parte del mundo, y que su uso sea de gran importancia para los usuarios al facilitar varias actividades que generaban un esfuerzo físico por parte de este, permite que cada día los diversos sectores opten por implementar las nuevas tecnologías, es aquí donde se debe hacer mención al gran conocido Internet de las cosas (IoT) que ofrece mantener conectado por medio de la red cualquier dispositivo cotidiano.

El internet de las cosas hace uso de sensores, microprocesadores, circuitos eléctricos, entre otros, para poder establecer una interacción máquina a máquina (M2M). Esta tecnología busca ampliar el concepto de Internet en el uso de las computadoras y celulares, involucrando así diferentes aparatos electrónicos que sean capaces de contar con el hardware necesario para conectarse a Internet, reconociendo que no todos presentan la infraestructura correcta para ser llamados dispositivos IoT.

La IoT es utilizada en diferentes ámbitos, desde la salud, sector agropecuario, hogares, etc. Es inevitable no considerar que ésta ya forma parte de nuestra vida diaria, por lo que ha sido adoptada por diversos usuarios alrededor del mundo, y una de la más utilizada es la que concierne a la domótica, que ha tenido una acogida muy exitosa.

Sin duda la domótica brinda una facilidad de confort a los usuarios, convirtiendo su casa en una casa inteligente capaz de ser controlada desde un aplicación, y realizando las actividades más sencillas hasta la más compleja, como encender y apagar las luces, interruptores, el control de aparatos electrónicos hasta el control de riego de un jardín, y muchos otros servicios que ofrece esta tecnología, brindando beneficios como el ahorro de energía, tiempo, seguridad, mejorando así el estilo de vida. Una de las cosas importantes que hay que resaltar es que para hacer uso de los dispositivos IoT y la domótica no se necesita ser un experto en el conocimiento tecnológico, porque los beneficios de estos es su facilidad de uso.

La implementación del Internet de las cosas presenta un desafío importante en lo que concierne a seguridad, por lo que debe ser una prioridad fundamental buscar proteger todo tipo de información que pueda estar involucrada en el uso de dispositivos IoT. La mayoría de usuarios que han implementado esta tecnología normalmente desconocen de las vulnerabilidades a las que se encuentran expuestos, omitiendo así que se

convierten en un punto de partida para los ataques cibernéticos gracias a la exposición de sus datos sin darse cuenta.

Como solución a lo planteado se buscó implementar en este proyecto un nivel de seguridad para proteger al usuario de las amenazas al que se encuentra expuesto cada vez que gestiona sus dispositivos inteligentes, convirtiendo así un ambiente IoT libre de riesgos y amenazas. Se debe considerar que entre mayores dispositivos IoT estén conectados, mayor será la vulnerabilidad para el usuario. La solución que se le dio al problema presentado es el control local de dispositivos en los sistemas domóticos Open HAB y Home Assistant, ayudando así a que la información no se encuentre accesible para los atacantes. Para comprobar la metodología utilizada se aplicó también a otros dispositivos IoT y un dispositivo simulado de los distribuidores de Tuya, confirmando así el correcto desarrollo de esta.

Los resultados que se obtuvieron de las pruebas de latencia que se realizaron a los sistemas domóticos y a Smart Life presentó un resultado satisfactorio para Home Assistant porque fue el sistema que logró tener el menor tiempo al ejecutar las instrucciones enviadas para el encendido y apagado del dispositivo.

Palabras claves: Internet de las cosas, sistema domótico, seguridad, internet, Smart Life

ABSTRACT

The fact that the Internet is present in much of the world, and that its use is of great importance to users by facilitating various activities that generated a physical effort by this, allows every day the various sectors choose to implement new technologies, this is where we must mention the great known Internet of things (IoT) that offers to keep connected through the network any daily device.

The Internet of things makes use of sensors, microprocessors, electrical circuits, among others, to be able to establish a machine-to-machine (M2M) interaction. This technology seeks to expand the concept of the Internet in the use of computers and cell phones, thus involving different electronic devices that are capable of having the necessary hardware to connect to the Internet, recognizing that not all have the right infrastructure to be called IoT devices.

The IoT is used in different areas, from health, agricultural sector, homes, etc. It is inevitable not to consider that this is already part of our daily life, so it has been adopted by several users around the world, and one of the most used is the one concerning home automation, which has been very successful.

Without a doubt, home automation offers a comfort facility to users, turning their home into an intelligent house capable of being controlled from one application, and performing the simplest activities to the most complex, such as turning on and off lights, switches, the control of electronic devices to the control of irrigation of a garden, and many other services offered by this technology, providing benefits such as energy saving, time, security, thus improving the lifestyle. One of the important things to emphasize is that to make use of IoT devices and home automation you do not need to be an expert in technological knowledge because the benefit of these is its ease of use.

The implementation of the Internet of things presents a major challenge in terms of security, so it should be a top priority to seek to protect all types of information that may be involved in the use of IoT devices. Most users who have implemented this technology are usually unaware of the vulnerabilities they are exposed to, thus missing out on a starting point for cyber attacks by unwittingly exposing their data.

As a solution to the above, we sought to implement in this project a level of security to protect users from the threats they are exposed to every time they manage their intelligent devices, thus making an IoT environment free of risks and threats. It should be noted that the more IoT devices are connected, the greater the vulnerability for the

user. The solution to this problem is local control of devices in Open HAB and Home Assistant home automation systems, helping to keep information inaccessible to attackers. To test the methodology used, it was also applied to other IoT devices and a simulated device of the Tuya distributors, confirming the correct development of this one.

The results obtained from the latency tests carried out on the home automation systems and Smart Life presented a satisfactory result for Home Assistant because it was the system that managed to have the least amount of time to execute the instructions sent for turning the device on and off.

Keywords: Internet of things, home automation system, security, internet, Smart Life

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

INTRODUCCIÓN

Uno de los temas que más impacto ha creado dentro de la sociedad en los últimos años, es el Internet de las Cosas conocido también por sus siglas IoT, que permite a los usuarios controlar desde una aplicación todo tipo de dispositivo conectado a Internet que hacen uso de protocolos IoT para su comunicación, es aquí donde entramos al concepto de domótica que busca automatizar una vivienda, facilitando la gestión del usuario con sus dispositivos, y presentando varios beneficios como el ahorro de energía.

La calidad y comodidad que puede presentar el implementar un sistema domótico en una vivienda puede sonar muy interesante, pero lo que muchos usuarios no consideran es que también presenta riesgos, que su seguridad no está totalmente cuidada, porque al involucrarse con dispositivos IoT estos obtienen información del usuario para poder conectarse, dando una apertura al ataque de las vulnerabilidades expuestas en la red.

El presente trabajo de titulación describe el análisis de seguridad IoT para un sistema domótico, donde se inició integrando a la aplicación Smart Life un dispositivo IoT, luego se capturó con Wireshark y PCAP Remote el tráfico que existía cuando se enviaba una instrucción al dispositivo con el propósito de conocer su nivel de seguridad y la información que se puede obtener de este. Con el análisis respectivo y con los datos importantes obtenidos se integró el dispositivo a los sistemas domóticos Home Assistant y Open HAB, luego se implementó un nivel de seguridad haciendo uso de la herramienta Node Red, dónde se creó un flujo basado en el protocolo de comunicación MQTT y el uso del nodo tuya local que permite que los dispositivos IoT de los distribuidores Tuya logren funcionar localmente sin depender de la cloud, lo que evita la exposición de la información y que se convierta en un punto de partida para los ataques cibernéticos.

Este informe presenta la siguiente estructura:

El **Capítulo 1** describe las necesidades de realizar este proyecto y los requerimientos que se presentan para su aplicación.

El **Capítulo 2** describe el desarrollo del proyecto, donde se detalla el prototipo utilizado para aplicar el nivel de seguridad IoT, la fundamentación teórica en la cual se basó para encontrar una solución, el objetivo y ejecución del proyecto.

El **Capítulo 3** presenta un plan de evaluación, los resultados obtenidos con su respectivo análisis, además las conclusiones y recomendaciones.

1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1 ÁMBITO DE APLICACIÓN: DESCRIPCIÓN DEL CONTEXTO Y HECHOS DE INTERÉS.

El Internet de las cosas ha generado mucha expectativa por la gran acogida que ha tenido por parte de los usuarios, es por eso que cada vez que se presenta una nueva innovación se espera siempre que rompa todo tipo de barreras y sea abierta para futuras aplicaciones, lo que conlleva a un aporte en gran escala para el avance de un país.

Al mencionar el internet de las cosas no nos debemos de olvidar de una de las grandes aplicaciones que ya forma parte de la vida del ser humano como es la domótica, que aunque muchos piensan que está enfocada a personas con alto conocimiento en tecnología, vale la pena descartar esa idea ya que la domótica se encuentra al alcance de todos.

Existen varias aplicaciones domóticas que se encuentran disponibles para diferentes sistemas operativos lo que brinda al usuario la comodidad de ajustarse a lo que tiene, así mismo existen una variedad de dispositivos IoT presentados en el mercado, desarrollados por diferentes empresas, donde muchas de estas cuentan incluso con su propia aplicación para gestionar sus dispositivos.

Uno de los aspectos más importantes que implica utilizar la domótica y sus componentes es el tema de seguridad, como avanza la tecnología así también avanzan los ataques en la red, por lo que los dispositivos IoT se han vuelto un punto importante en los hackers que buscan obtener la mayor información del usuario que se encuentre expuesta en la red.

El propósito de esta propuesta tecnológica es analizar la seguridad IoT de un sistema domótico para luego implementar un nivel de seguridad en los sistemas domóticos Open HAB y Home Assistant mediante la realización de un flujo desarrollado en la herramienta Node Red, lo que brindará un funcionamiento local para los dispositivos IoT del desarrollador Tuya, permitiendo que la información del usuario se encuentre protegida y libre de los posibles ataques.

1.2 ESTABLECIMIENTO DE REQUERIMIENTOS

El Internet de las cosas (IoT) permite que los diferentes dispositivos puedan interactuar entre sí para compartir información, ejecutar alguna orden enviada por el usuario, etc. Este aspecto llama la atención de cualquier persona además que una de las principales características que brinda la IoT es la comodidad, y tan solo pensar en esta seguramente no se dudaría en implementarla, razón por la que cada vez más se está incorporando el uso de esta tecnología que lleva consigo a una de sus aplicaciones como es la domótica.

Al mencionar que los dispositivos se comunican entre ellos y que para esto necesitan de internet ya debemos hacernos una idea de que la información que estos se envían estará expuesta indudablemente en la red, por lo que será una vulnerabilidad presente cada vez que se utilice estos dispositivos, característica que no todos los usuarios conocen ni la tienen presente al involucrarse con la IoT.

La variedad de sistemas domóticos está al alcance de los usuarios de acuerdo a la interfaz más amigable, seguridad, facilidad de uso, cada aspecto depende de lo cada usuario busque, pero todos los sistemas tienen una misma finalidad que es facilitar el control de los dispositivos, ofreciendo automatizaciones de escenarios y otras características.

Este proyecto está orientado a brindar una mejora en lo que concierne a seguridad en el uso de los sistemas domóticos, lo que ayudará al usuario a gestionar los dispositivos Tuya de forma local evitando que la información quede expuesta y sea de fácil acceso para el atacante. Para la implementación del nivel de seguridad se realizará un flujo en Node Red basado en el protocolo de comunicación MQTT, donde uno de los principales componentes que se utilizará será el nodo tuya local, cada flujo será implementado en los sistemas domóticos Open HAB y Home Assistant.

1.3 JUSTIFICACIÓN DEL REQUERIMIENTO A SATISFACER

La seguridad IoT es uno de los temas que más relevancia debería tener en las investigaciones diarias, por lo que el avance del Internet de las cosas ha sido arrollador y muy innovador que puede presentarse como algo realmente interesante y que lo es, pero que al mencionar Internet debemos también mencionar los ataques cibernéticos que existen, porque no se puede omitir la realidad.

El robo de información en la red se ha vuelto muy común por parte de las personas que lo practican donde buscan aprovecharse de las vulnerabilidades que tienen los usuarios al desconocer de este tema y querer involucrarse en el mundo IoT sin tener conocimiento más allá de lo que puede presentar este nuevo desafío.

La contribución que brinda este proyecto es el desarrollo de nuevas metodologías basadas en seguridad IoT donde se busque implementar niveles de seguridad eficientes permitiendo que el usuario cada vez que utilice un sistema domótico o un dispositivo IoT esté libre de amenazas y vulnerabilidades, donde los desarrolladores de estas tecnologías además de brindar un confort también brinden lo más importante, la seguridad.

El funcionamiento local de dispositivos es una de las medidas más acertadas porque además de brindar seguridad al no exponer la información del usuario y del dispositivo, brinda una mejora en lo que concierne a los tiempos en que se gestionan los dispositivos, porque al ser de manera local es más rápida la ejecución de la instrucción que le envíe el usuario por medio de la aplicación que utilice, ya sea esta desde una computadora o celular.

2. CAPÍTULO II. DESARROLLO DEL PROYECTO

2.1 DEFINICIÓN DEL PROTOTIPO TECNOLÓGICO

La arquitectura que se puede visualizar en la Imagen 1, es la solución propuesta como un nivel de seguridad la cual se basa en el protocolo MQTT que permitirá el control local de los dispositivos Tuya en los sistemas domóticos de Open HAB y Home Assistant.

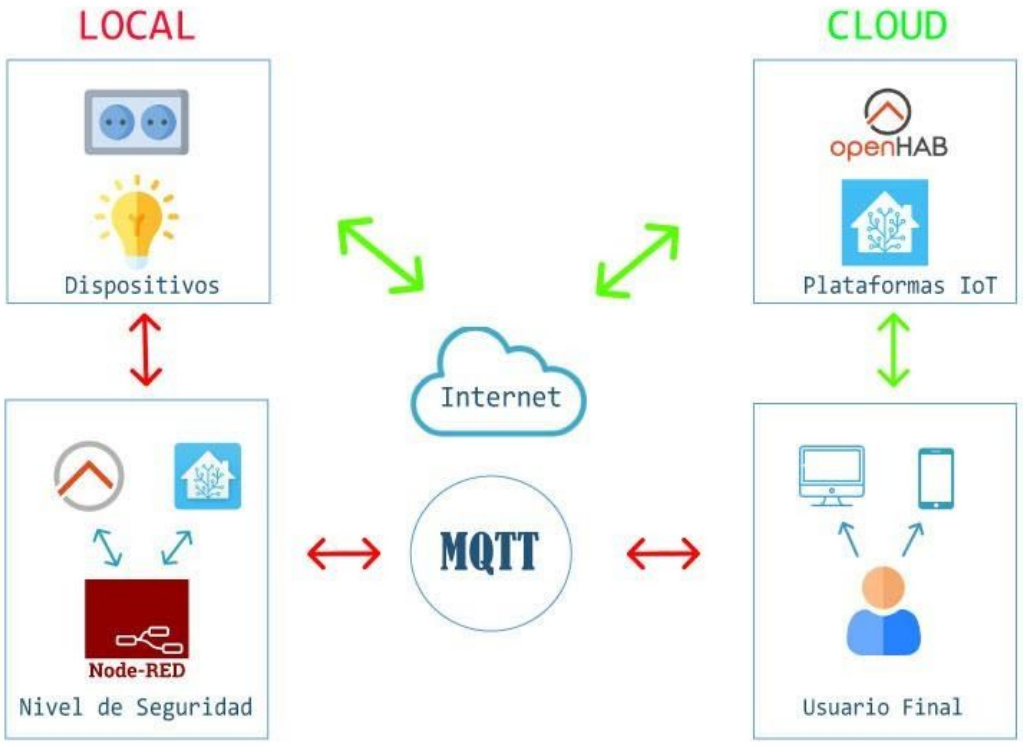

Imagen 1: Arquitectura del proyecto

Fuente: Elaboración propia

Se encuentran dos tipos de niveles de funcionamiento, el local y el de la cloud:

- El funcionamiento local tendrá la implementación de un flujo creado en Node Red que se basará en MQTT y que será complemento para los sistemas domóticos Home Assistant y Open HAB que permitirán gestionar los dispositivos desde su aplicación en la computadora o en el celular.
- El funcionamiento de los dispositivos haciendo uso de la cloud, es el que básicamente presenta cada sistema domótico cada vez que se realiza una integración, pero que para comparaciones de los diferentes funcionamientos se consideró esta integración.

2.2 FUNDAMENTACIÓN TEÓRICA DEL PROTOTIPO

2.2.1 INTERNET DE LAS COSAS

La evolución de la tecnología en los últimos años ha permitido al ser humano involucrarse mucho más con esta, siendo de alguna forma novedosa y presentando una gran acogida con las diversas innovaciones que expone, una de las grandes tendencias es el Internet de las cosas, que su concepto hace referencia a la conexión que existe entre dispositivos inteligentes conectados a la red y sistemas capaces de gestionarlos a través de un protocolo de comunicación, permitiendo comunicarse entre ellos en tiempo real de forma local o en la cloud, facilitando así la interacción que existe entre usuario y dispositivo, hasta al punto de no necesitar del propio usuario físicamente para realizar una tarea, sino que puede ser capaz de ejecutar una tarea programada desde el sistema inteligente [1] [2] [3].

Para que exista una comunicación donde los dispositivos sean capaces de transmitir información se necesita que estos tengan una dirección IP y esto sucede gracias al uso de diversas tecnologías aplicadas hoy en día por el Internet de las cosas [4] [5].

Con todo lo que presenta el Internet de las cosas, ofreciendo mejorar nuestra calidad de vida y trabajo, este ha sido introducido en diversos sectores como la agricultura, medicina, hogar, etc. Su aplicación en el mundo ha crecido de gran manera que podemos encontrarla desde un simple enchufe hasta una aplicación capaz de detectar el cáncer, permitiendo así un sin número de estudios que se realizan todos los días gracias a las innovaciones de la IoT [6] [7] [8].

2.2.1.1 DISPOSITIVOS IOT

Cualquier dispositivo que sea capaz de conectarse a la red y lograr ser gestionado desde un sistema, puede ser considerado un dispositivo inteligente o también conocido como dispositivo IoT, que van desde un simple interruptor hasta un auto manejado sin conductor, son varios tipos de dispositivos que existen hoy en día, donde varían mucho en su precio, calidad y gusto del usuario, como se puede observar en la Imagen 2, 3 y 4 de los dispositivos utilizados para este proyecto. La forma de controlar estos dispositivos es lo que resulta una de las principales características que más llaman la atención, porque no requiere de un gran esfuerzo por parte del usuario para poder utilizarlos [9] [10].

El uso de dispositivos IoT también presenta un gran desafío en el tema de seguridad, lo que no todo es felicidad en el uso de esta tecnología, porque al involucrarse la privacidad del usuario hace que se vean expuestos todo tipo de datos que abren una

puerta inmensa al ataque cibernético, provocando todo tipo de riego y amenazas para la persona que adquiere estos productos sin darse cuenta a lo que estos conllevan, estos ataques han ido creciendo a lo largo de los años, es por eso que varias empresas se han dedicado a buscar soluciones implementando varios tipos de protección en el uso de los dispositivos IoT presentado un panorama más alentador para los usuarios [11] [12].

Imagen 2: Smart Socket
Fuente: Elaboración propia

Imagen 3: Smart Socket 2
Fuente: Elaboración propia

Imagen 4: Smart Bulb
Fuente: Elaboración propia

2.2.2 DOMÓTICA

Escuchar hablar de domótica hoy en día es tan normal, porque es una de las áreas que más alcance ha tenido en el Internet de las Cosas, llevando así al usuario a involucrarse con esta hasta el punto de convivir con ella desde la comodidad de su hogar, desde una simple aplicación puede controlar todo lo que se encuentra en su vivienda sin necesidad de mayor esfuerzo.

Manipular dispositivos de una forma manual ya sea para su encendido, apagado, regulación, es cosa del pasado, ya que gracias a las tecnologías existentes del Internet de las cosas, permiten que la domótica facilite la vida del usuario, además de

brindarle el confort en su hogar, aporta en el ahorro de energía que es una de las ventajas que más llama la atención del usuario [13] [14].

En la domótica existen algunos protocolos de comunicación como son X-10, ZigBee, Jini, entre otros. Al mencionar el protocolo X-10 se debe recordar que este es uno de los más antiguos utilizados en este ámbito, su comunicación se basa en la red eléctrica sin tener necesidad de añadir más complemento físico del que ya se encuentra en la instalación de la vivienda, lo que facilita al usuario en su ahorro [15]. Los dispositivos que presentan este protocolo son de fácil acceso y no necesitan de conocimientos especiales para controlarlos.

2.2.2.1 PROTOCOLOS DE COMUNICACIÓN

El Internet de las cosas presenta un sin número de dispositivos inteligentes que el usuario puede adquirir para su uso, pero al decir que estos dispositivos se comunican por medio de la red para ser gestionados desde un sistema, sabemos que se necesita de algo que permita su comunicación, es aquí donde aparecen los protocolos de comunicación que han resultado ser una de las elecciones importantes en la fabricación de dispositivos porque será la clave para el proceso de comunicación de información, lo que conlleva a considerar varios aspectos en el momento de su elección, entre esos la seguridad que tendrá el dispositivo con el uso de ese protocolo [16] [17] [18].

Los protocolos de comunicación son muy variados, desde protocolos para la capa de aplicación como MQTT, DNS, HTTP, etc., hasta protocolos para la capa de transporte como son los más conocidos UDP, TCP, etc. Lo que gracias a estos los dispositivos IoT pueden comunicarse y transferirse todo tipo de información.

2.2.2.1.1 PROTOCOLO INTERNET RELAY CHAT (IRC)

Este es un protocolo conocido también por sus siglas IRC, que se basa en la comunicación por medio de texto en tiempo real con los dispositivos, donde utiliza el puerto 6667 o 6668 para su mensajería. Es uno de los protocolos más antiguos pero que se siguen utilizando en la actualidad para la implementación de dispositivos inteligentes, por lo que ha tenido un gran alcance, pero al ser un protocolo sencillo también presenta sus riesgos en la seguridad, ya que tiene puertos abiertos y libres para el acceso de los atacantes cibernéticos [19].

2.2.2.1.2 PROTOCOLO MESSAGE QUEUING TELEMETRY TRANSPORT (MQTT)

El protocolo MQTT es uno de los más utilizados en la comunicación de dispositivos IoT, gracias a algunas ventajas que este presenta, entre las que destacan están el bajo consumo de recursos, la sencillez de su configuración, etc. Se basa en un modelo de publicación y subscripción, orientado a la comunicación máquina a máquina(M2M), los puertos que utiliza son el 8883 y 1883, pero al hacer uso del puerto 8883 presenta una seguridad de TLS [20] [21].

El funcionamiento de este protocolo consiste en la suscripción por medio de un topic que es indispensable para la comunicación que se tendrá con el bróker donde este ayudará en la publicación del mensaje enviado y será recibido por quienes se encuentren suscritos al mismo topic, lo que ofrece este protocolo es una manera fácil de entender la comunicación que existirá al momento de que los dispositivos se empiecen a transferir información [22].

2.2.2.2 PLATAFORMAS DOMÓTICAS

2.2.2.2.1 OPEN HAB

Es un software de código libre que permite la automatización de viviendas mediante el control de dispositivos IoT en su plataforma, presenta varias funciones que el usuario puede considerar para la automatización de acuerdo a su gusto, este software puede ser instalado en Windows, Linux, Raspberry Pi, y otros [23].

Permite la adaptación de dispositivos de diferentes protocolos lo que la lleva hacer una de las más usadas, no presenta una interfaz compleja y su instalación es bastante sencilla, necesita de Java para poder funcionar. En la integración de OpenHAB existe varias interfaces en las que el usuario puede trabajar para el control de dispositivos, entre esas están Basic UI, Paper UI, Classic UI y HAB Panel, cada una de ellas tienen sus características y son escogidas de acuerdo a la facilidad de entendimiento que puede considerar el usuario para la ejecución de su panel de control [24].

2.2.2.2.2 HOME ASSISTANT

Es un sistema domótico de software libre que permite la automatización y control de diferentes escenarios en un hogar, o en algún lugar donde este sea implementado, la facilidad de entendimiento y de uso de este sistema son de las ventajas más consideradas por quienes se deciden por su aplicación, está disponible para diversos sistemas operativos como Windows, Linux, Raspberry Pi, etc [25].

Una de las características que se debe resaltar de este sistema es la interfaz amigable que presenta, fácil de entender y gestionar, además presenta varios paneles y una sección de dashboard donde se puede visualizar todas actividades de sus dispositivos, el usuario tiene la libertad de crear, editar paneles de acuerdo a su gusto, esta plataforma brinda una gran oportunidad para poder automatizar su hogar de una manera sencilla.

2.2.2.2.3 SMART LIFE

Es una aplicación móvil para el control de todo tipo de dispositivo inteligente, es gratuita y se encuentra disponible para las plataformas de iOS y Android. Las funciones que tiene la aplicación van desde cambiar el estado de un dispositivo de apagado a encendido, creación de escenarios para diferentes momentos, automatizaciones de acuerdo al clima, entre otros, lo que busca Smart Life es brindar la oportunidad al usuario de ser protagonista de la gestión de sus dispositivos, la sencillez de la interfaz de la aplicación es la clave para que el usuario logre entender cómo utilizarla sin necesidad de tener un gran conocimiento en aplicaciones [26].

La aplicación fue desarrollada por Tuya y tiene su versión similar a la aplicación Tuya Smart, con la creación de una cuenta e integrar los dispositivos a la app, esta genera un archivo donde contiene los identificadores de cada dispositivo como son su ID y clave, pero esta información cambia cada vez que el usuario busque integrar el dispositivo a una cuenta diferente a la asociada al inicio.

2.2.3 DESARROLLADOR TUYA

Es uno de los desarrolladores más conocidos en los últimos tiempos que abarca el tema tendencia que es el Internet de las cosas, presenta aplicaciones como Tuya Smart, Jinvoo, Smart Life, y varios productos IoT fabricados por ellos, entre los que se destacan se encuentran los Enchufes, focos, interruptores, etc. Cuenta con una plataforma IoT en la nube que permite a los usuarios crear su propio software donde podrán adecuarlo de acuerdo a su preferencia permitiéndoles gestionar sus dispositivos.

2.2.3.1 SMART SOCKET

Los dispositivos IoT más fabricados y utilizados gracias a su facilidad de uso y control son los enchufes inteligentes, una de las ventajas que más llama la atención son las automatizaciones que se les puede dar a estos dispositivos ahorrando así tiempo y energía al usuario, ya que tienen integrado en su circuito estas funciones que desde una aplicación pueden ser gestionadas. Uno de los principales factores es el control de

energía que tiene el usuario en sus manos con el uso de estos dispositivos, al ser capaz de gestionar su encendido, apagado y hasta programar estas tareas en el tiempo que desee que se ejecuten, permite que su vivienda tenga regulada el consumo de electricidad.

Existen varios proveedores de estos enchufes inteligentes, que incluyen diversas características en sus dispositivos, modelos basados en Wifi, Bluetooth, hasta ser capaz de controlar las cargas de energía [27].

2.2.4 SEGURIDAD IOT

La seguridad de esta nueva tecnología se ha visto afectada en diversos aspectos con el uso de una aplicación inteligente, un dispositivo IoT, un sistema domótico, muchas veces sin que el propietario se dé cuenta que sus equipos han sufrido un ataque.

Es un tema que está muy presente en la actualidad, por lo que ya investigaciones muestran cómo los atacantes cibernéticos se aprovechan de las vulnerabilidades que presentan el uso de esta tecnología, tan solo basta que el usuario la tenga implementada en su hogar, para que el atacante inicie su proceso de hackeo, este puede ser mientras el usuario está gestionando el dispositivo, donde el objetivo del atacante será capturar el patrón que está realizando el usuario, otro de los ataques es conocer la comunicación que tienen los dispositivos, que puertos utiliza, cuál es su protocolo de comunicación, todos estos son algunos de muchos de los ataques cibernéticos que están rondando a los usuarios [28] [29].

La gran acogida que ha tenido el avance de la tecnología es de gran importancia, pero lo que no podemos descartar son las vulnerabilidades que están presentes, lo que da apertura a diversos ataques a la privacidad del usuario, la comunicación que utilizan varios dispositivos IoT no es totalmente cifrada, por lo que genera la desconfianza al usuario y su vez la oportunidad del libre acceso para el atacante, reconociendo así que muchos dispositivos son deficientes en seguridad en su software y hardware [30] [31]. Más que comprometer la información del dispositivo, compromete la información del usuario que lo utiliza, porque los atacantes acceden a la red y roban toda la información que ellos necesiten para poder realizar su ataque, es un tema delicado ya que el usuario se está exponiendo a un gran riesgo [32] [33].

Lo que se busca hoy en día es ayudar al usuario a prevenir todos estos tipos de ataques y que sea capaz de elegir lo seguro y no solo lo sencillo, es por eso que frente al estudio de todas las vulnerabilidades que presenta la implementación de esta

tecnología, se propone crear varias soluciones como la autenticación, autorización, etc [34] [35].

2.3 OBJETIVOS DEL PROTOTIPO

2.3.1 OBJETIVO GENERAL

Implementar un nivel de seguridad de protección de datos en los sistemas domóticos Open HAB y Home Assistant, mediante el control local de los dispositivos IoT, para evitar ataques y robos de información de los usuarios.

2.3.2 OBJETIVOS ESPECÍFICOS

- Revisar las fuentes bibliográficas de trabajos relacionados con el tema de investigación.
- Analizar la seguridad IoT de los dispositivos Tuya mediante su control desde la aplicación Smart Life.
- Diseñar un nivel de seguridad para los sistemas domóticos seleccionados.
- Realizar pruebas de latencia a nivel local y en la cloud para encontrar el sistema domótico más rápido en ejecutar las instrucciones.

2.4 DISEÑO DEL PROTOTIPO

El diseño consistió en la creación de un flujo basado en MQTT que permitirá el control de encendido y apagado de los dispositivos desarrollados por Tuya y que será un complemento para los sistemas domóticos Open HAB y Home Assistant que desde su principal interfaz se logrará gestionarlos.

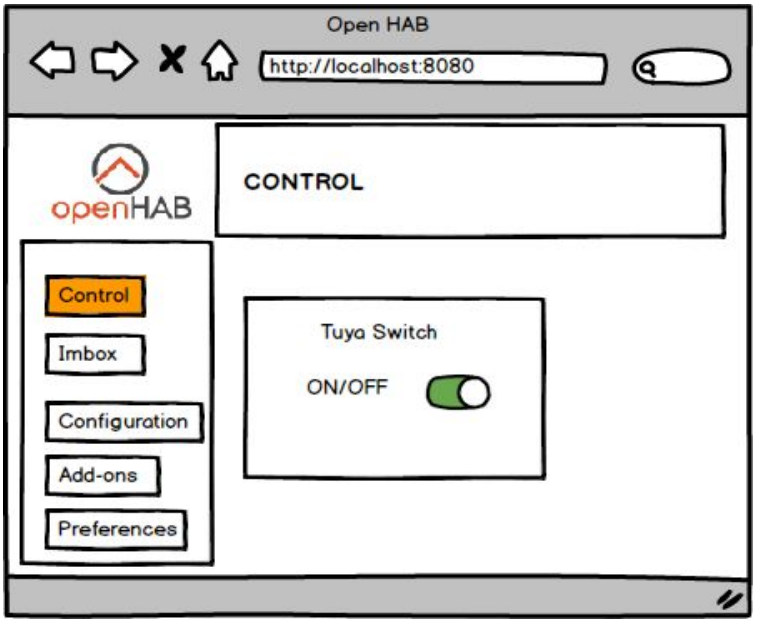

Imagen 5: Prototipo de Interfaz de control de Open HAB
Fuente: Elaboración propia

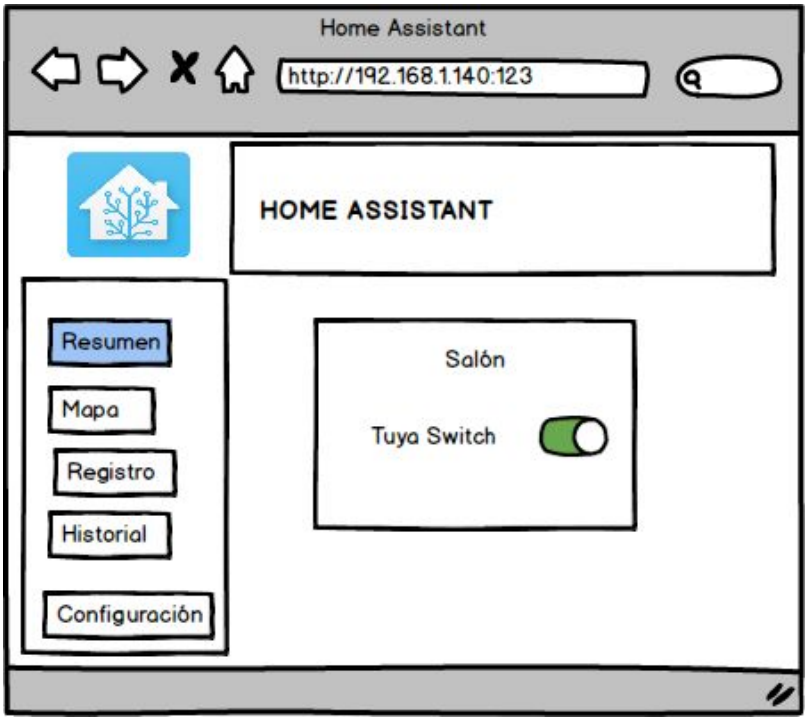

Imagen 6: Prototipo de Interfaz de control de Home Assistant
Fuente: Elaboración propia

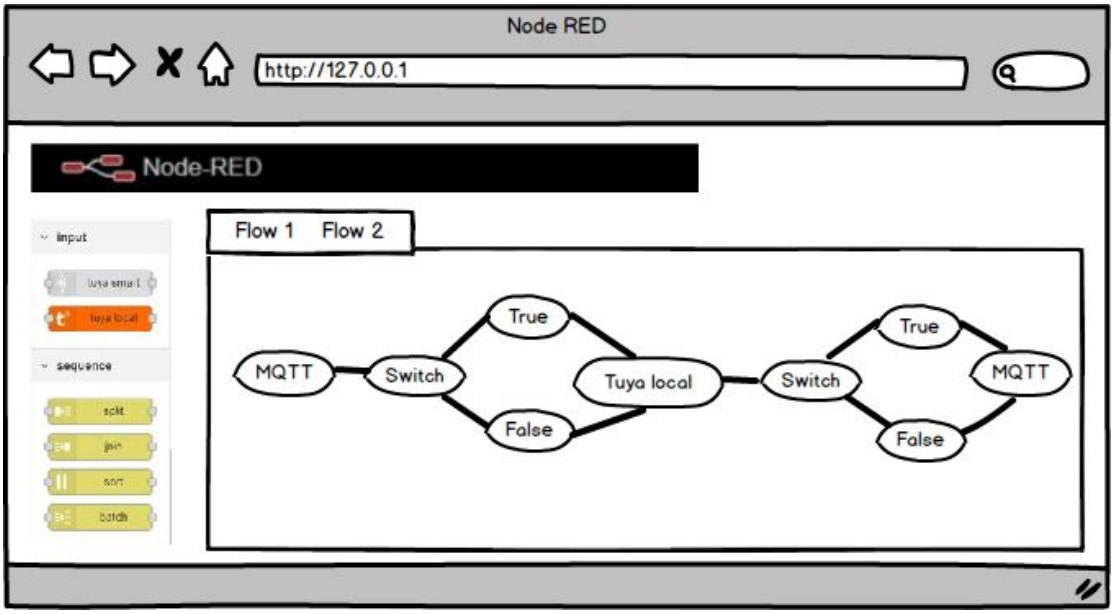

Imagen 7: Prototipo Flujo MQTT para el control local
Fuente: Elaboración propia

2.5 EJECUCIÓN Y/O ENSAMBLAJE DEL PROTOTIPO

2.5.1 ANÁLISIS DE SEGURIDAD

Se realizó el análisis de seguridad a la integración del dispositivo IoT con la aplicación Smart Life, donde se logró descubrir información importante el cual fue clave para implementar el nivel de seguridad para las integraciones con Home Assistant y Open HAB.

2.5.1.1 INTEGRACIÓN CON SMART LIFE

Se descargó la aplicación para gestionar el dispositivo IoT llamada Smart Life versión 3.21.4 desde Google Play Store como se puede ver en la Imagen 8. La interfaz que presenta Smart Life es amigable e intuitiva.

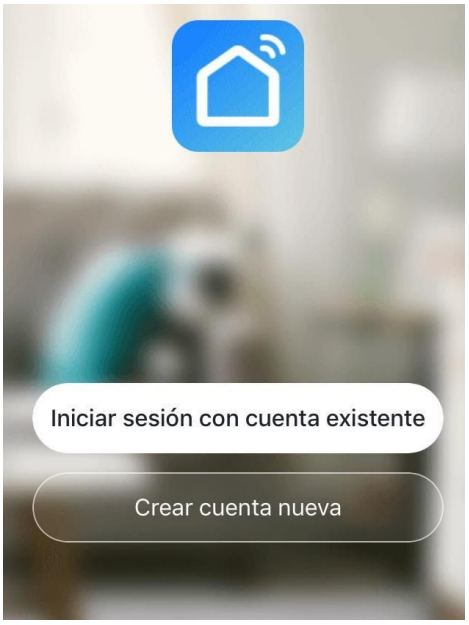

Imagen 8: Aplicación Smart Life
Fuente: Elaboración propia

Se añadió el dispositivo IoT de manera manual mediante Wifi, para esto se escogió entre la lista que presenta Smart Life el tipo de dispositivo que se desea añadir como se muestra en la Imagen 9, en este caso un Enchufe Wifi. Para empezar con el proceso de integración se seleccionó la red Wifi a la que estará asociado el dispositivo, luego se pulsó por 5 segundos el botón de reinicio del enchufe hasta que indicó el parpadeo de la luz led que dio la señal que está listo para registrarse y en la aplicación se logró ver como el proceso de registro avanza automáticamente como se puede observar en la Imagen 10.

Imagen 9: Smart Life
Fuente: Elaboración propia

Imagen 10: Integración con Smart Life
Fuente: Elaboración propia

2.5.1.2 OBTENCIÓN DE LA KEY DEL DISPOSITIVO

2.5.1.2.1 MÉTODO 1: USO DEL EMULADOR BLUESTACK

Para obtener la key del dispositivo IoT se hizo uso del emulador BlueStack rooteado, esto permitió acceder a los archivos root de la aplicación Smart Life donde se encuentra almacenada la key, se buscó el archivo en los documentos root del sistema como se puede visualizar en la Imagen 11, donde se encontró el ID del dispositivo y junto a éste su local key, teniendo ambos datos se logró cumplir el objetivo.

Imagen 11: Obtención de la key del dispositivo
Fuente: Elaboración propia

2.5.1.2.2 MÉTODO 2: TRAMAS DE WIRESHARK

Para la aplicación de este método se tiene que tener instalado Smart Life versión 3.4.1 en el celular, donde se ingresó a la aplicación iniciando sesión con la cuenta creada anteriormente como se muestra en la imagen 12.

Imagen 12: Smart Life versión 3.4.1
Fuente: Elaboración propia

Se hizo uso de la aplicación PCAP Remote que permitió la captura de los paquetes mientras se gestiona el dispositivo en la aplicación Smart Life como se muestra en la Imagen 13, luego se revisó las pruebas capturadas haciendo uso de Wireshark y se analizó la información de las tramas, donde se logró encontrar el ID y local key del dispositivo.

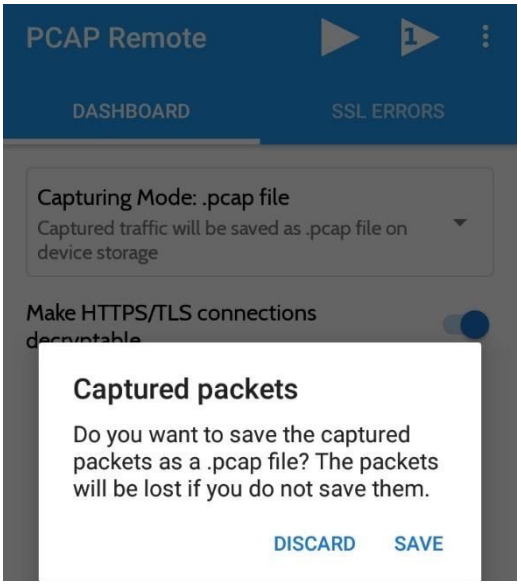

Imagen 13: Captura de paquetes
Fuente: Elaboración propia

2.5.1.2.3 MÉTODO 3: USO DE TUYA-CLI

Para este último método se creó una cuenta de desarrollador en la página oficial de Tuya, donde se creó un nuevo proyecto que permitió obtener dos credenciales de identificación que se las utilizó más adelante, como se muestra en la Imagen 14.

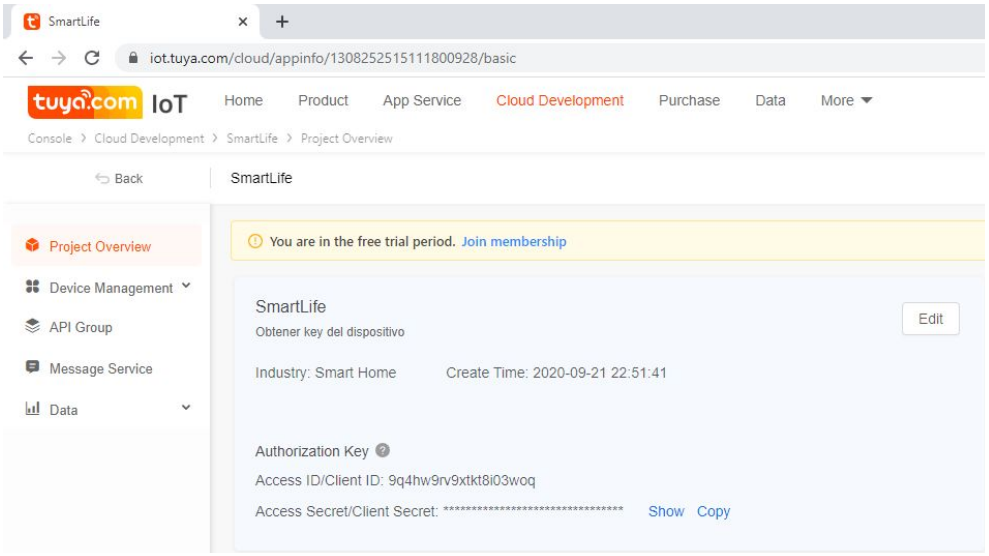

Imagen 14: Tuya desarrollador
Fuente: Elaboración propia

Como se puede ver en la Imagen 15, se ingresó a la pestaña Device Management en la opción Link Device donde se agregó el dispositivo asociado a la aplicación Smart Life, con el código QR que se escaneó desde la aplicación se activó la autorización para permitir que el proyecto creado tenga acceso a la información.

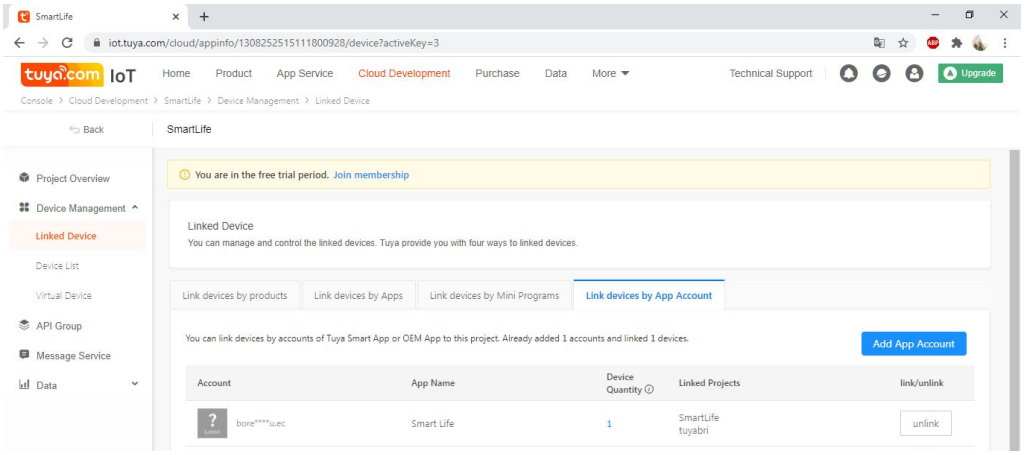

Imagen 15: Integración del dispositivo a Tuya Desarrollador
Fuente: Elaboración propia

Por último, se descargó e instaló el proyecto alojado en Github llamado Tuya-Cli que es el que se utilizó para obtener la información del dispositivo, se ejecutó el proyecto y se escribió las credenciales obtenidas de Tuya desarrollador y el ID del dispositivo

como se muestra en la Imagen 16, luego de ingresar todo correctamente se pudo obtener la información que se necesitaba que era la key del dispositivo.

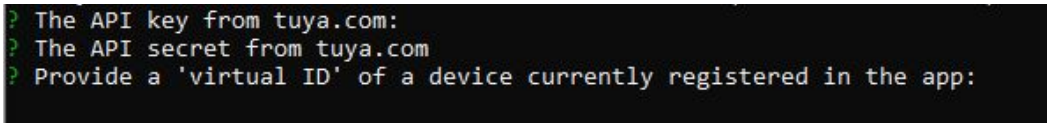

Imagen 16: Tuya Cli
Fuente: Elaboración propia

2.5.2 INTEGRACIONES CON LOS SISTEMAS DOMÓTICOS

2.5.2.1 INTEGRACIÓN CON HOME ASSISTANT

Se instaló Home Assistant Supervisor desde una máquina virtual, para esto se descargó la imagen VDI presente en la página oficial, luego de su ejecución se inició el servidor con el comando **core start** como se puede observar en la Imagen 17.

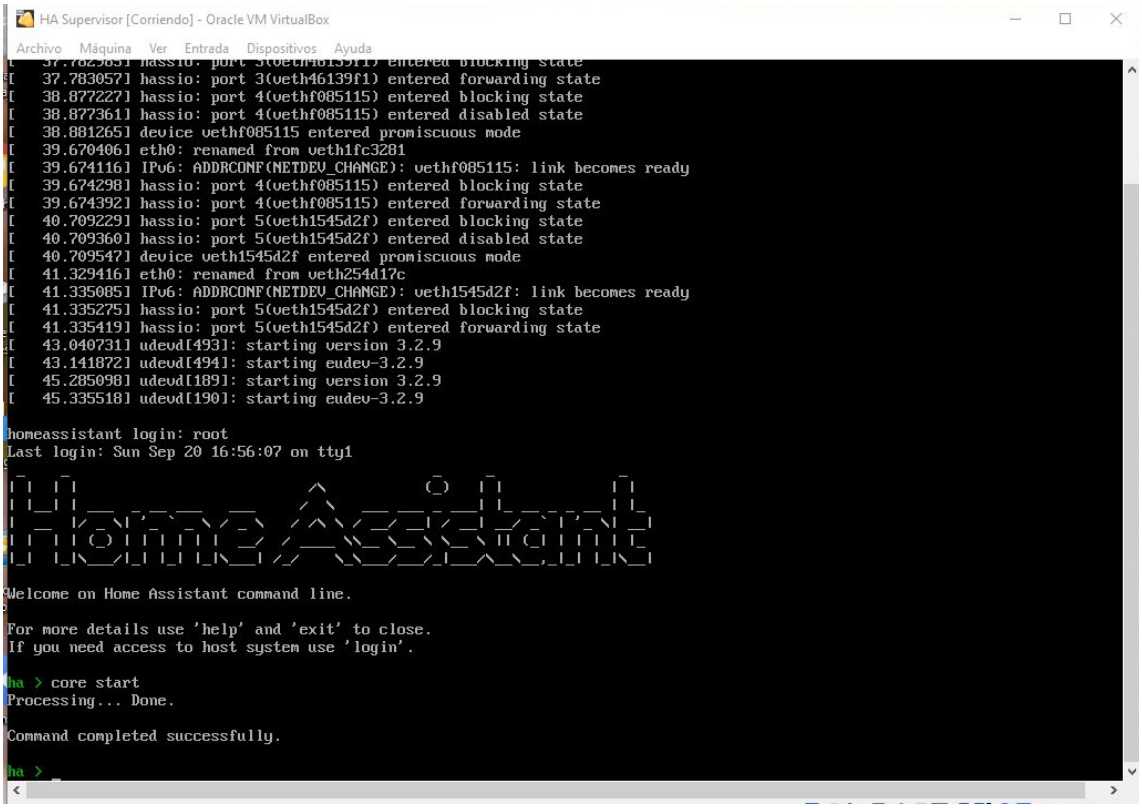

Imagen 17: Home Assistant
Fuente: Elaboración propia

Desde el navegador se accedió a Home Assistant y se creó una cuenta como se muestra en la imagen 18 y se accedió a la página principal como se observa en la imagen 19.

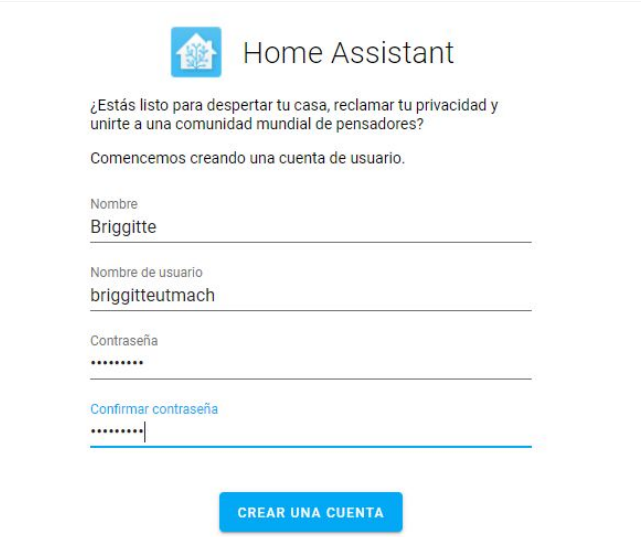

Imagen 18: Creación de Usuario en Home Assistant
Fuente: Elaboración propia

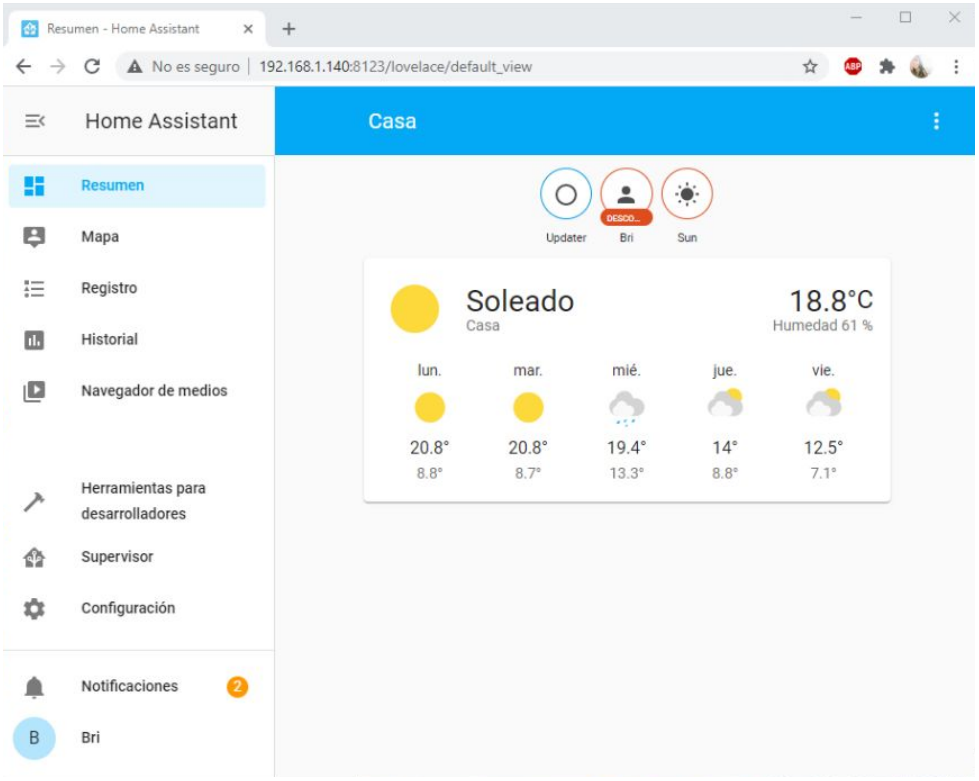

Imagen 19: Página principal de Home Assistant
Fuente: Elaboración propia

Luego, en la opción de configuración se agregó una nueva integración y se buscó la opción como Tuya como se puede observar en la imagen 20.

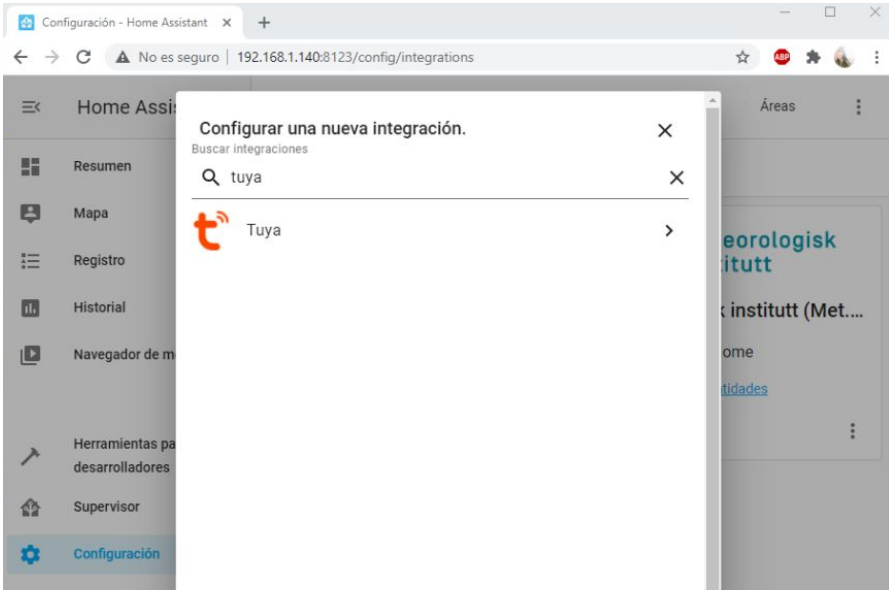

Imagen 20: Integración Tuya
Fuente: Elaboración propia

Se ingresó las credenciales de la cuenta de Smart Life para que Home Assistant tenga acceso a la información.

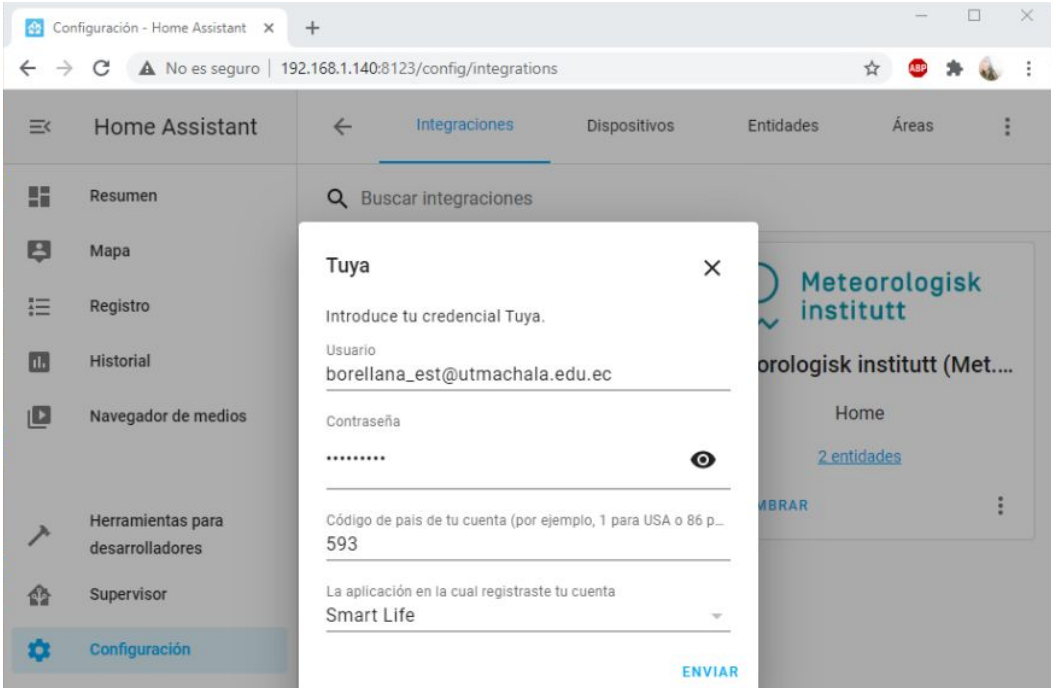

Imagen 21: Ingreso de credenciales
Fuente: Elaboración propia

Se pudo observar que aparece el dispositivo asociado a la cuenta de Smart Life listo para ser gestionado desde el panel de control como se muestra en la Imagen 22.

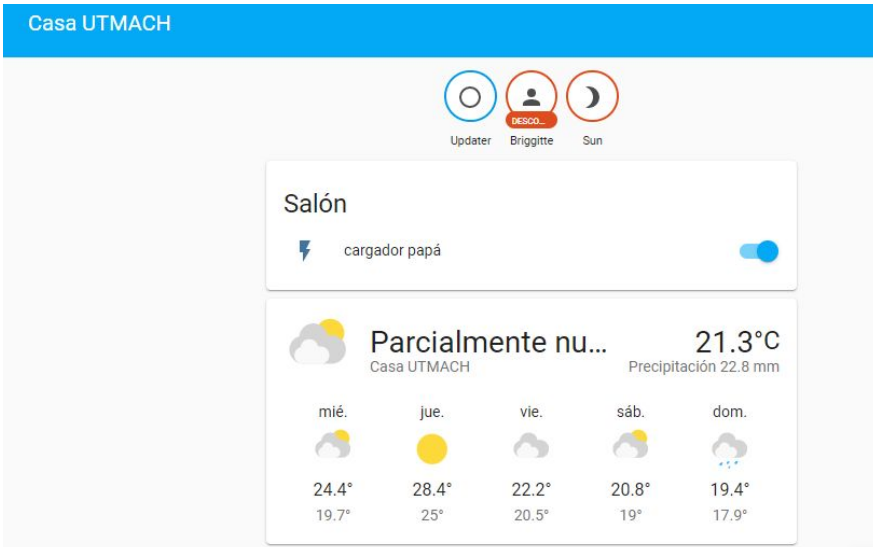

Imagen 22: Dispositivo asociado
Fuente: Elaboración propia

2.5.2.2 INTEGRACIÓN CON OPEN HAB

Para iniciar se debió tener instalado Java, luego se descargó el archivo de instalación versión 2.5.7 desde la página oficial de Open HAB donde se consideró el tipo de sistema operativo como se observa en la imagen 23.

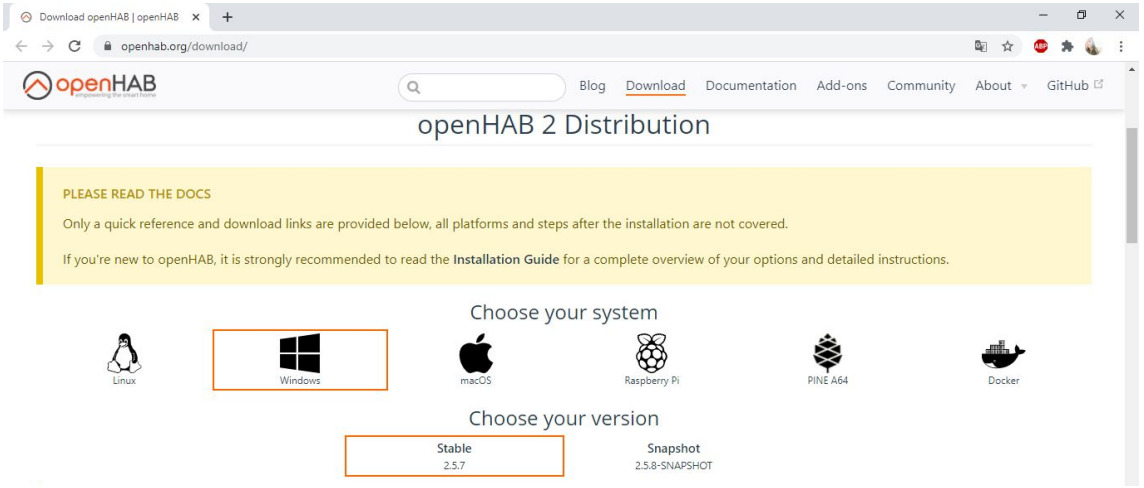

Imagen 23: Descarga de Open HAB
Fuente: Elaboración propia

Se descomprimió el archivo descargado y se inició el servidor de Open HAB ejecutando el archivo start.bat como se muestra en la imagen 24.

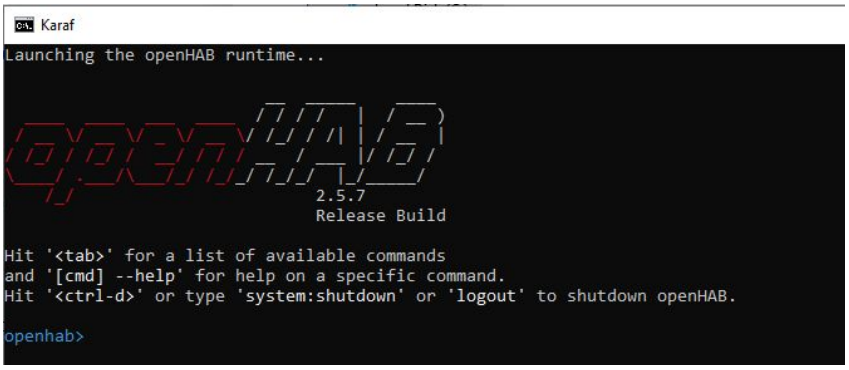

Imagen 24: Inicio del servidor Open HAB
Fuente: Elaboración propia

Se ingresó en el navegador la dirección localhost:8080, luego se escogió el paquete estándar como se puede observar en la imagen 25 y se esperó hasta que se inicialice Open HAB.

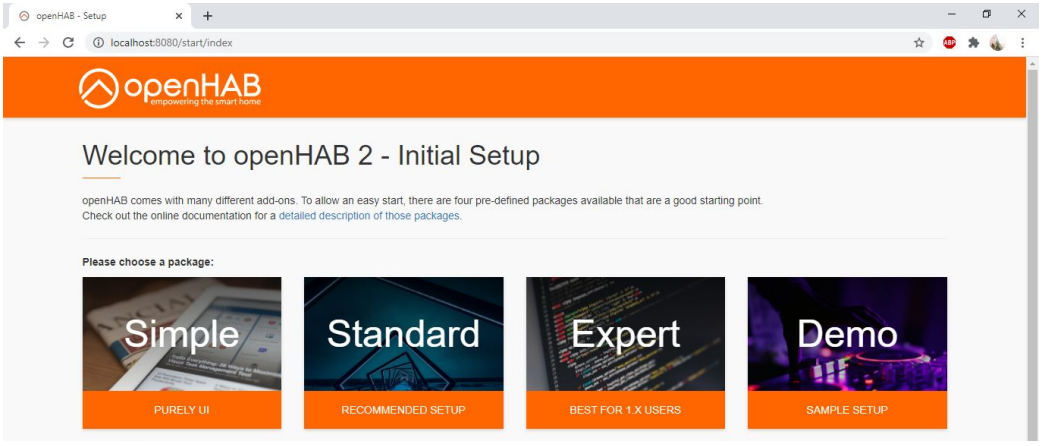

Imagen 25: Configuración de Open HAB
Fuente: Elaboración propia

Se escogió la interfaz en la cual se trabajó como se muestra en la imagen 26, en este caso Paper UI como se muestra en la imagen 27.

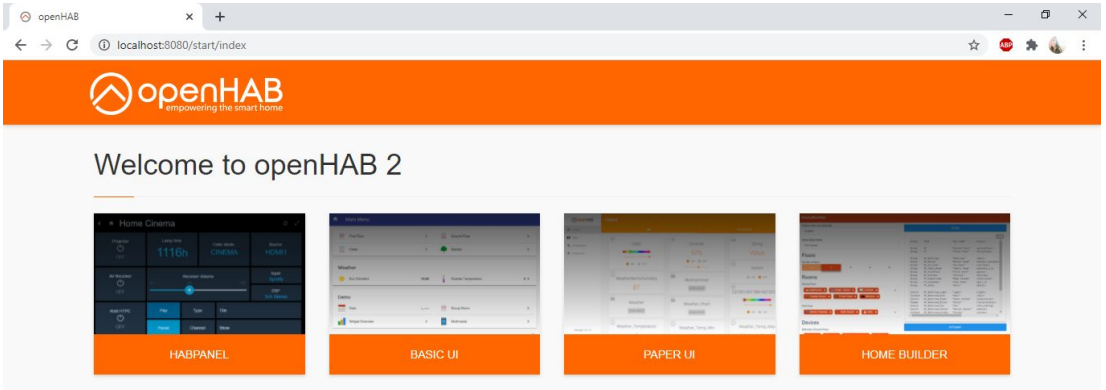

Imagen 26: Elección de interfaz de Open HAB
Fuente: Elaboración propia

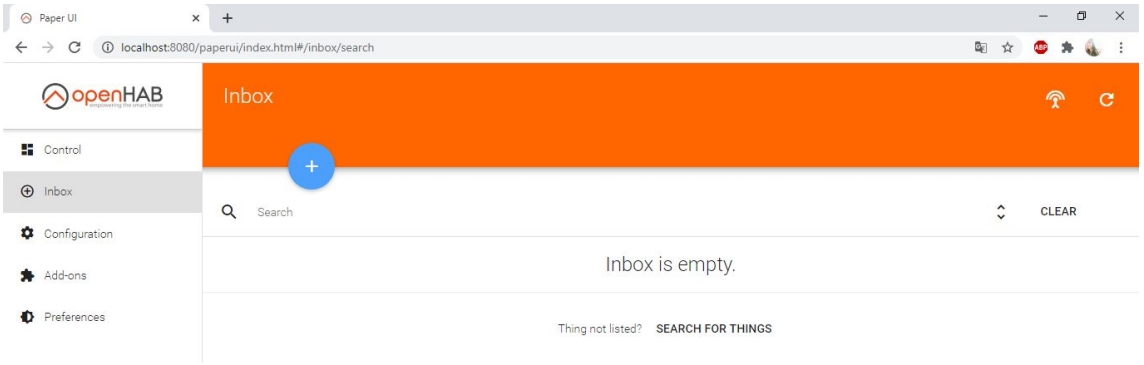

Imagen 27: Interfaz Paper UI
Fuente: Elaboración propia

Luego se descargó el plugin de Tuya que permitió la gestión de dispositivos Tuya desde Open HAB ya que no se encuentra disponible en los complementos por defecto que presenta OH. Como se puede observar en la imagen 28 se ubicó el archivo descargado en la dirección C:/openHAB2/addons y se reinició Open HAB.

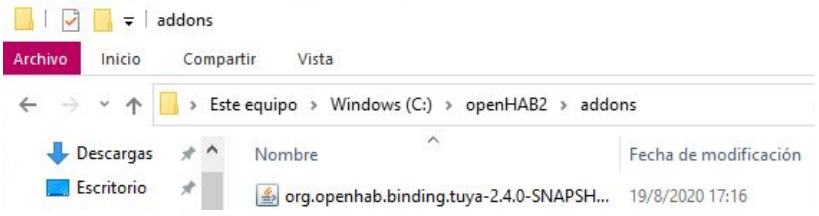

Imagen 28: Plugin Tuya
Fuente: Elaboración propia

Ahora se pudo visualizar que ya se encuentra disponible Tuya Binding y se empezó con la configuración del mismo. Se seleccionó el tipo de dispositivo Tuya que se va a configurar, en este caso un Tuya Smart Power Plug como se muestra en la imagen 29 donde luego se ingresó la información necesaria para su configuración, como son el ID y local key.

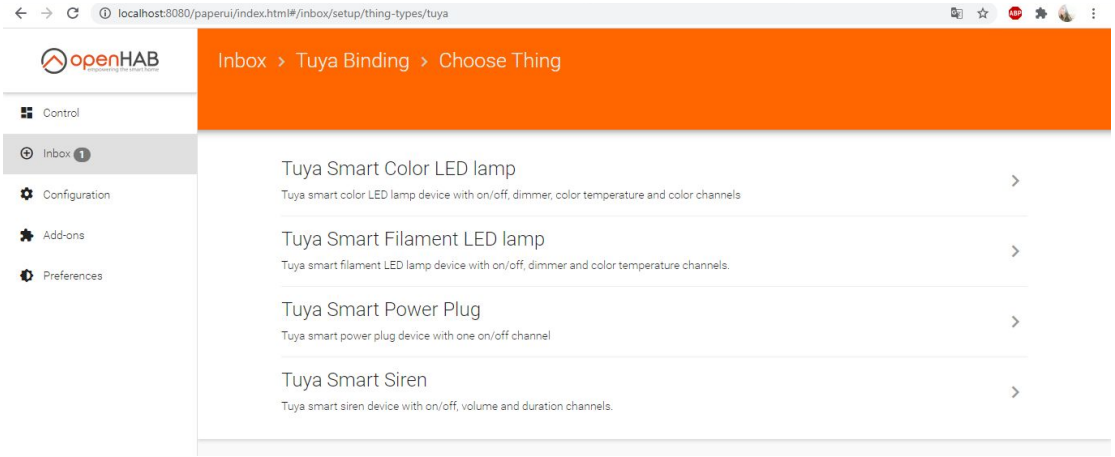

Imagen 29: Tuya Binding
Fuente: Elaboración propia

En la opción Things donde se encuentra la configuración del dispositivo, se creó un ítem tipo Switch para el canal que tiene Tuya Smart Power Plug como se muestra en la imagen 30 para su correcto funcionamiento.

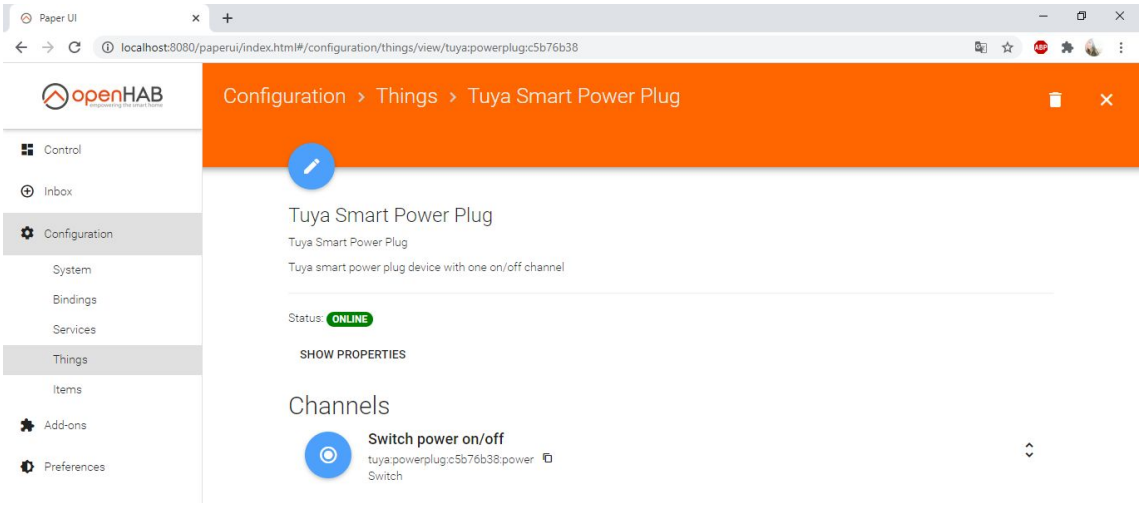

Imagen 30: Configuración Tuya Smart Power Plug
Fuente: Elaboración propia

Como se puede observar en la imagen 31, ya se logró visualizar el dispositivo disponible para ser gestionado desde el panel de control de open HAB.

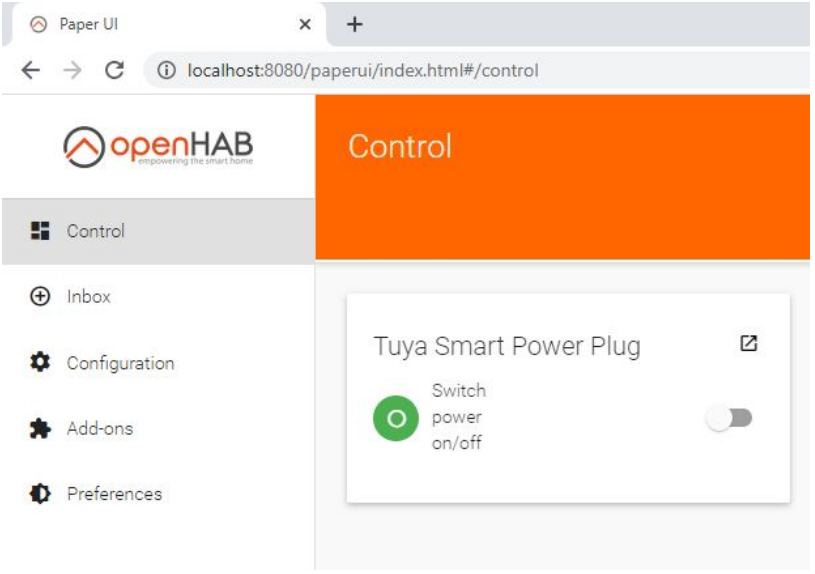

Imagen 31: Panel de control
Fuente: Elaboración propia

2.5.3 IMPLEMENTACIÓN DE NIVEL DE SEGURIDAD

La implementación de seguridad que se agregó a los sistemas domóticos como Home Assistant y Open HAB es la gestión de los dispositivos Tuya de forma local, para esto se hizo uso de Node Red en ambas plataformas, donde se creó un programa basado en el protocolo de comunicación MQTT y se utilizó un nodo Tuya Local.

2.5.3.1 HOME ASSISTANT

Se inició descargando Node Red desde la tienda de Home Assistant y se empezó con su instalación, luego se añadió el nodo de tuya local en la sección nom_packages y finalmente se inició Node-RED donde se verificó el log para ver que el proceso esté correcto, como se muestra en la imagen 32.

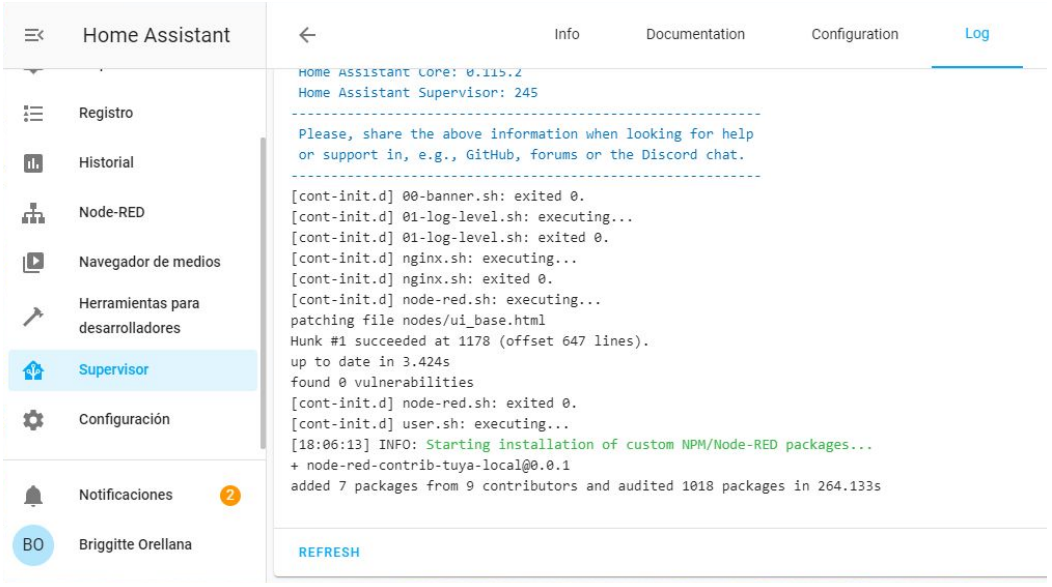

Imagen 32: Ejecución de Node-RED
Fuente: Elaboración propia

Iniciado Node-Red se empezó con la creación del flujo como se muestra en la imagen 33, que permitió la gestión local de los dispositivos Tuya.

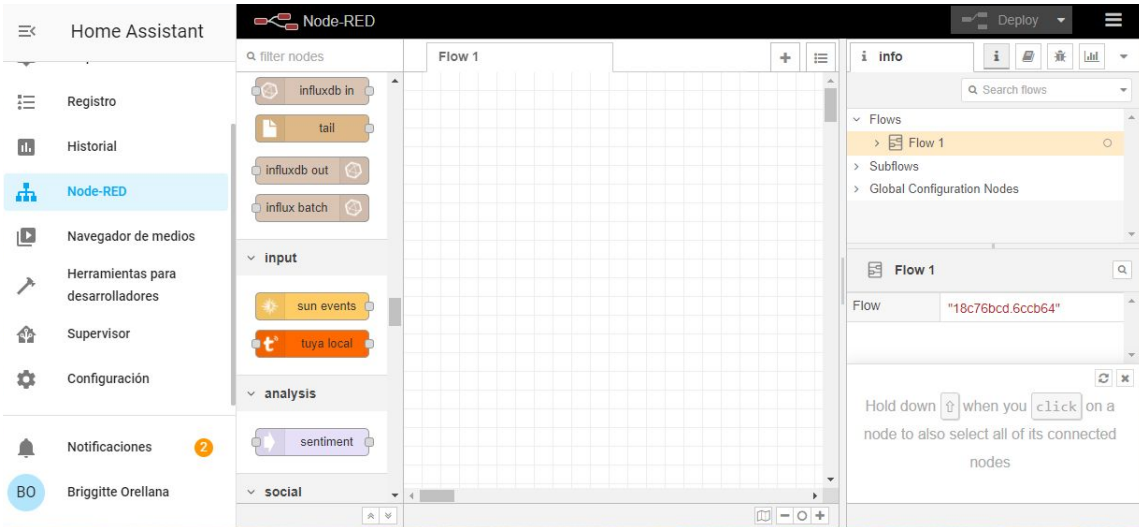

Imagen 33: Creación del flujo local Tuya
Fuente: Elaboración propia

La metodología que se utilizó para mejorar la seguridad es el control local de los dispositivos Tuya, para esto se realizó el flujo que se muestra en la imagen 34, que se basó en la comunicación MQTT para el funcionamiento local desde Home Assistant.

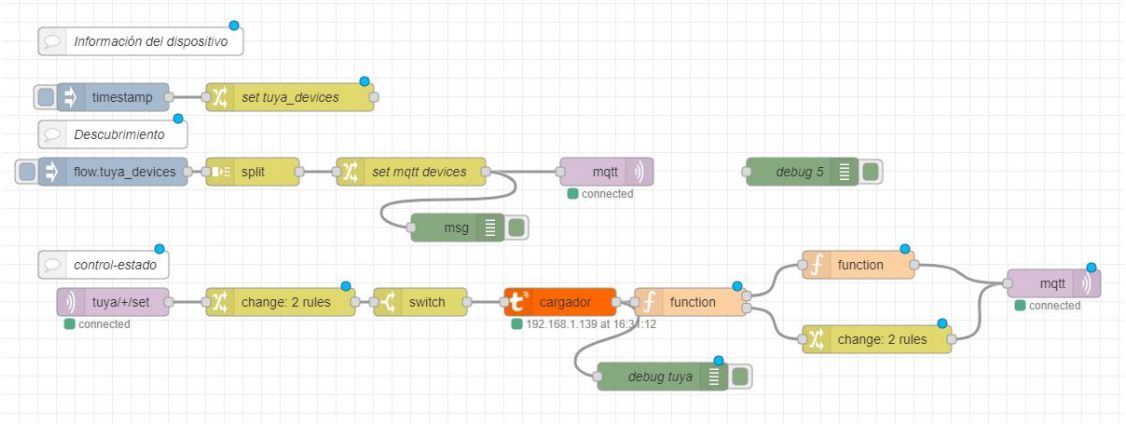

Imagen 34: Flujo local para dispositivos Tuya
Fuente: Elaboración propia

Para confirmar que la metodología utilizada esté correcta, se la aplicó a otros dispositivos tipo switch, un foco y un dispositivo simulado, como se muestra en la imagen 35 y 36. Para obtener el ID y local key de cada dispositivo se utilizó los métodos mencionados anteriormente para obtener esa información, comprobando también que esos métodos son útiles para otros dispositivos.

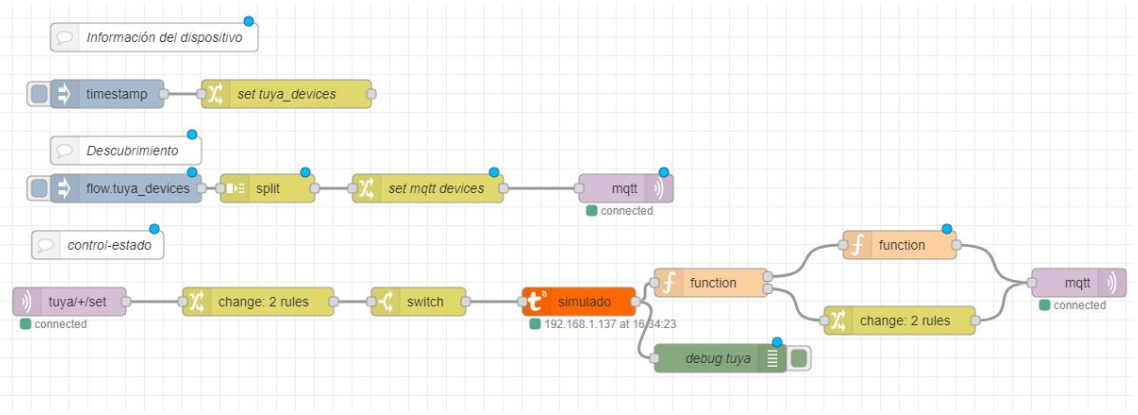

Imagen 35: Flujo de dispositivo Tuya simulado
Fuente: Elaboración propia

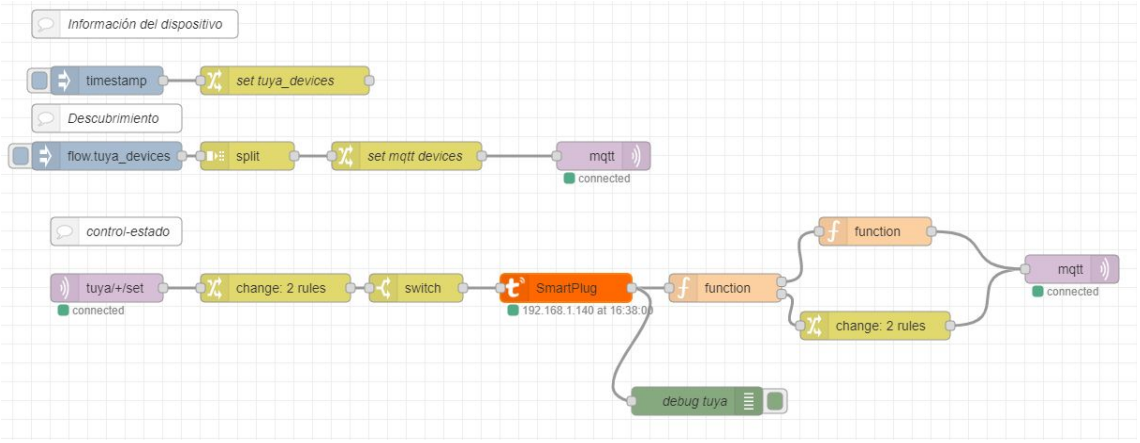

Imagen 36: Flujo del switch Tuya
Fuente: Elaboración propia

2.5.3.2 OPENHAB

Para la implementación de seguridad con Open HAB se descargó e instaló Node Red versión 1.1.3 en Windows, luego se descargó el nodo de tuya local desde el proyecto de github, donde se ubicó el archivo en la dirección de los módulos de node red como se muestra en la imagen 37 y se lo instaló desde esa ubicación.

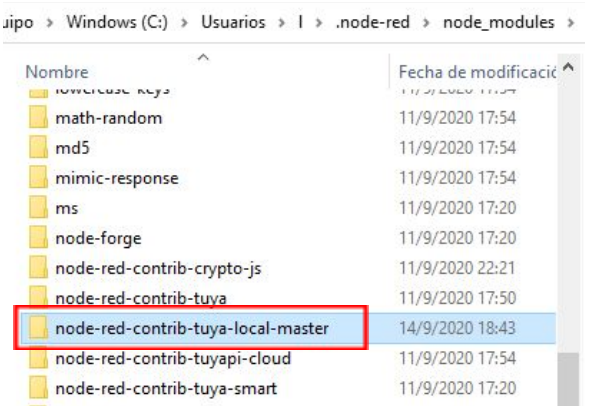

Imagen 37: Instalación de Nodo Tuya Local
Fuente: Elaboración propia

Después se inició Open HAB para configurar el dispositivo con MQTT, en la opción Addons, en la pestaña MISC se instaló MQTT Broker, se lo configuró manualmente con la dirección 127.0.0.1 como se muestra en la imagen 38.

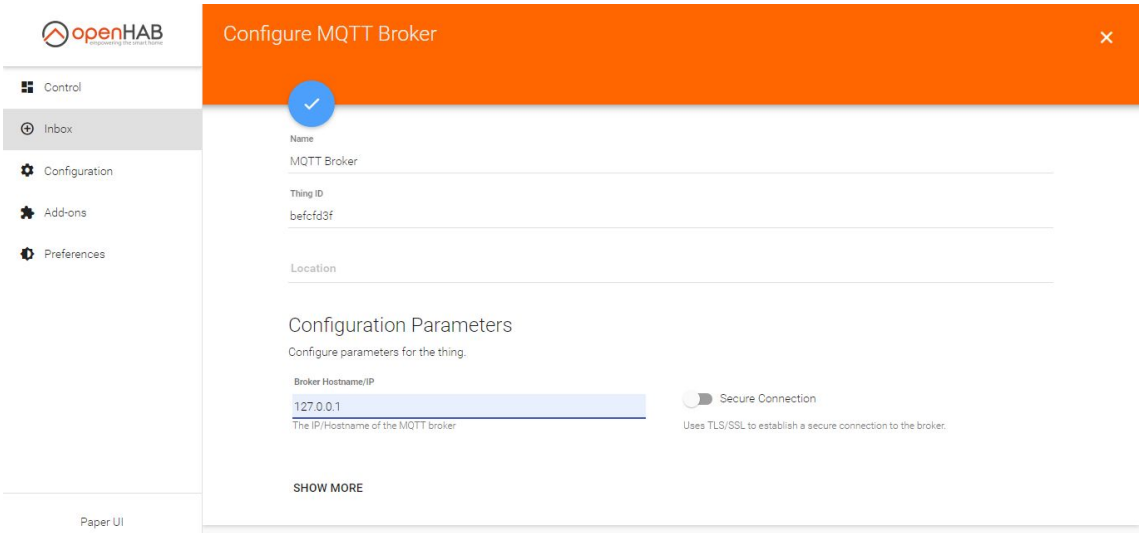

Imagen 38: Configuración MQTT Broker
Fuente: Elaboración propia

Se añadió una cosa genérica donde se utilizó el MQTT Broker como puente para la comunicación y luego se agregó un canal de tipo Switch donde se añadió el topic que tendrá el dispositivo para su estado y envío de comando, en ambos se debe considerar el ID, local key y la ip del dispositivo que se gestionó. Por último, se creó un ítem tipo Switch y con eso se terminó la configuración en Open HAB como se muestra en la imagen 39.

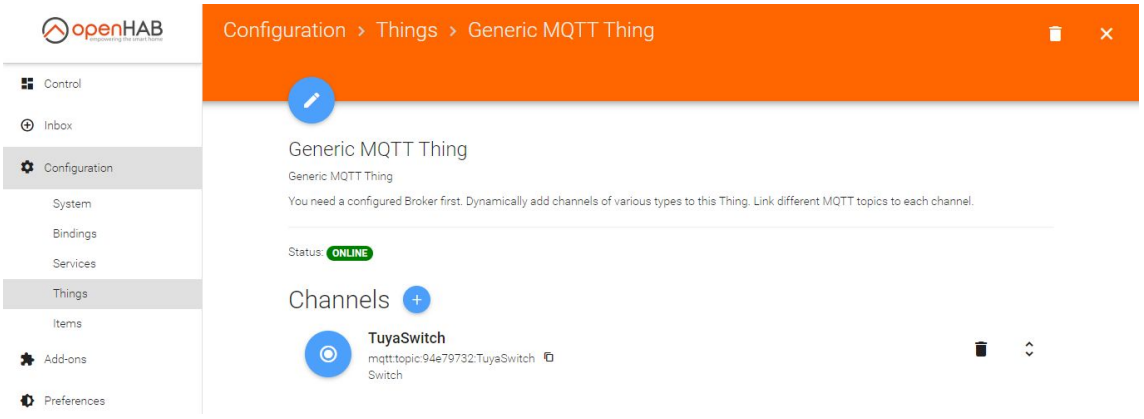

Imagen 39: Configuración del puente MQTT
Fuente: Elaboración propia

La misma metodología que se utilizó en Home Assistant también se la utilizó para Open HAB permitiendo el control local de los dispositivos tipo switch, foco y un simulado, como se muestra en la imagen 40, 42 y 43. Cada flujo que se desarrolló en Node Red tiene la información correspondiente al dispositivo que se configuró para su correcto funcionamiento.

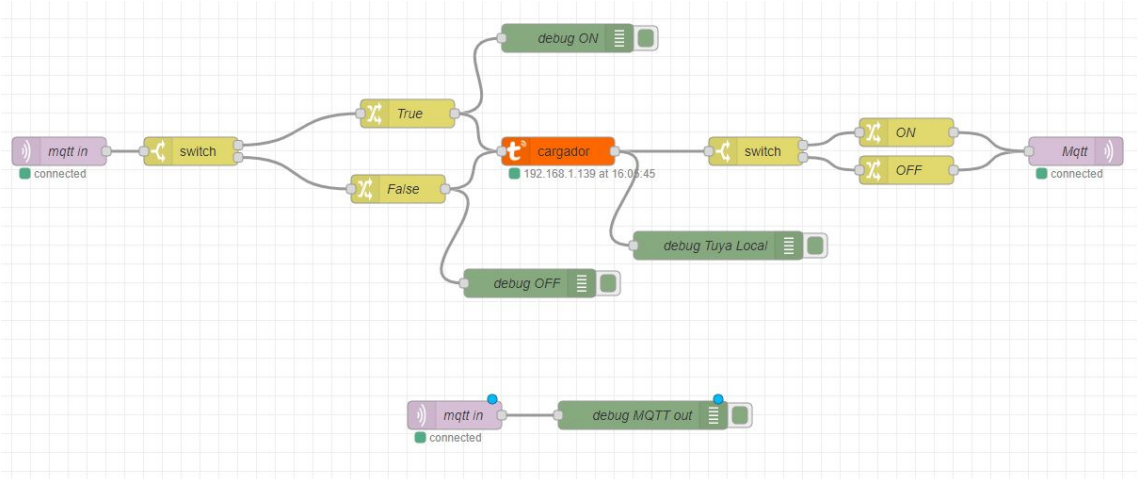

Imagen 40: Flujo local del switch Tuya
Fuente: Elaboración propia

Cada dispositivo genera una información cuando se ejecuta el flujo donde se puede observar la ip, el ID y el estado del dispositivo, así como se muestra en la imagen 41.

Imagen 41: Debug del nodo Tuya local
Fuente: Elaboración propia

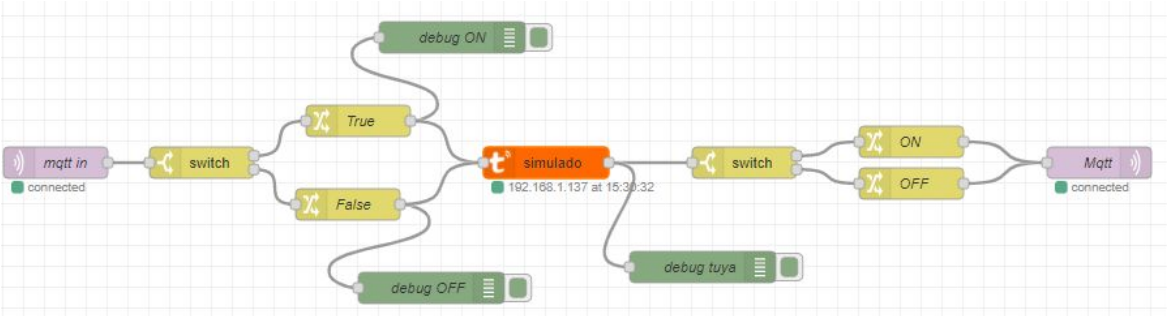

Imagen 42: Flujo del dispositivo Tuya simulado
Fuente: Elaboración propia

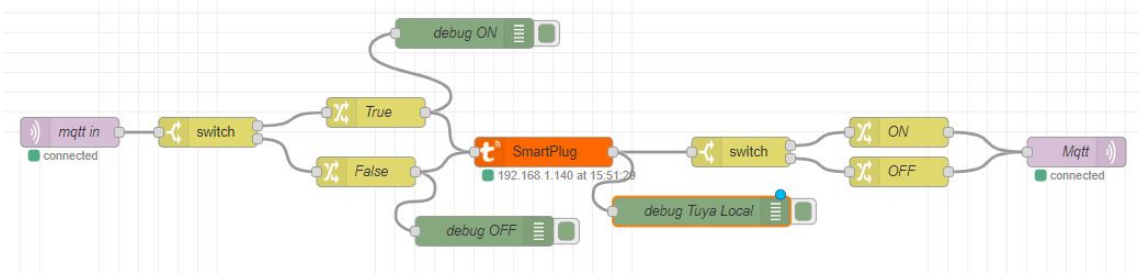

Imagen 43: Flujo del switch 2 Tuya
Fuente: Elaboración propia

3. CAPÍTULO III: EVALUACIÓN DEL PROTOTIPO

3.1 PLAN DE EVALUACIÓN

Para las pruebas del proyecto se consideró las siguientes herramientas:

- Computadora Lenovo
  - Sistema Operativo Windows 10
  - 4 GB de RAM
- Celular Huawei Y6 2018
  - Sistema ATU-LX3 8.0.0.176
  - 2 GB de RAM
- Wireshark versión 3.2.5
- PCAP Remote versión 1.0.0.19

Las pruebas consistieron en el análisis de latencia con respecto al tiempo en milisegundos que tarda en gestionar el dispositivo IoT luego de enviarle un comando de encendido o apagado por medio de los Sistemas domóticos utilizados. Se gestionó un dispositivo físico y un dispositivo simulado de forma local haciendo uso de Home Assistant y Open HAB en la computadora y el celular, además se realizó pruebas en la cloud de los sistemas domóticos mencionados anteriormente y de Smart Life actual y la versión 3.4.1 en el celular, cada una de estas pruebas ayudó para realizar una tabla comparativa que dio un resultado listo para ser analizado.

3.2 RESULTADOS DE EVALUACIÓN

3.2.1 PRUEBAS LOCALES (COMPUTADORA)

Para las pruebas se utilizó dos tipos de dispositivos, uno físico y otro simulado, luego se capturó el tráfico con la herramienta Wireshark mientras se ejecutaba cada instrucción. Los resultados que se obtuvieron en las pruebas locales haciendo uso de los Sistemas domóticos Open HAB y Home Assistant fueron los siguientes:

Tabla 1: Latencias en milisegundos con pruebas locales PC

	Open HAB				Home Assistant			
	SIMULADO		FÍSICO		SIMULADO		FÍSICO	
	ON	OFF	ON	OFF	ON	OFF	ON	OFF
MÍNIMO	47	22	118	123	5	6	71	72
MÁXIMO	1.052	1.001	4.222	42.609	1.462	334	1.475	1.709
PROMEDIO	548	483	681	1.323	53	42	271	288

Fuente: Elaboración propia

3.2.2 PRUEBAS LOCALES (CELULAR)

En estas pruebas también se consideró los dos dispositivos y se hizo uso de la aplicación móvil PCAP Remote para capturar las tramas obtenidas cada vez que se gestiona el dispositivo donde luego se las analizó en Wireshark. Cada prueba se gestionó desde la aplicación móvil de Open HAB y Home Assistant, , lo cual se tuvo los siguientes resultados:

Tabla 2: Latencias en milisegundos con pruebas locales desde el celular

	Open HAB				Home Assistant			
	SIMULADO		FÍSICO		SIMULADO		FÍSICO	
	ON	OFF	ON	OFF	ON	OFF	ON	OFF
MÍNIMO	42	10	86	87	5	6	72	80
MÁXIMO	1.013	1.062	13.375	41.128	903	339	1.964	2.094
PROMEDIO	531	506	417	829	42	34	275	266

Fuente: Elaboración propia

3.2.3 PRUEBAS EN LA CLOUD

Para estas pruebas se consideró el uso de la aplicación Smart Life versión actual y versión 3.4.1, además de los sistemas domóticos de Open HAB y Home Assistant, donde cada trama se capturó con la herramienta PCAP Remote y luego se las analizó con Wireshark para así tener un resultado más consolidado, los tiempos obtenidos fueron los siguientes:

Tabla 3: Latencias en milisegundos con pruebas en la cloud

	Open HAB		Home Assistant		Smart Life		Smart Life vs 3.4.1	
	FÍSICO		FÍSICO		FÍSICO		FÍSICO	
	ON	OFF	ON	OFF	ON	OFF	ON	OFF
MÍNIMO	153	213	102	138	60	31	79	75
MÁXIMO	15.325	35.927	5.739	3.464	12.628	9.120	13.947	7.082
PROMEDIO	4.172	4.277	1.089	1.126	1.868	1.556	1.922	1.487

Fuente: Elaboración propia

3.2.4 ANÁLISIS DE RESULTADOS

Con los tiempos que se obtuvieron con cada una de las pruebas se calculó el mínimo, máximo y promedio de los resultados individuales de 100 comandos ON y 100 comandos OFF que se enviaron al dispositivo IoT desde cada uno de los sistemas domóticos de forma local y en la cloud, la unidad de medida de los valores que se encuentran representados en los gráficos están en milisegundos.

Los resultados que se obtuvieron con respecto a los mínimos como se muestra en la imagen 44, reflejan que Home Assistant al ser controlado de forma local no se tarda tanto en gestionar el dispositivo a diferencia de los otros sistemas, mientras lo que corresponde a gestionar haciendo uso de la Cloud, se puede analizar que desde la aplicación actual de Smart life presenta el menor tiempo, pero algo que se debe tener en cuenta es que Home Assistant está instalado desde una máquina virtual lo que conlleva a que el tiempo aumente cuando se considera la Cloud.

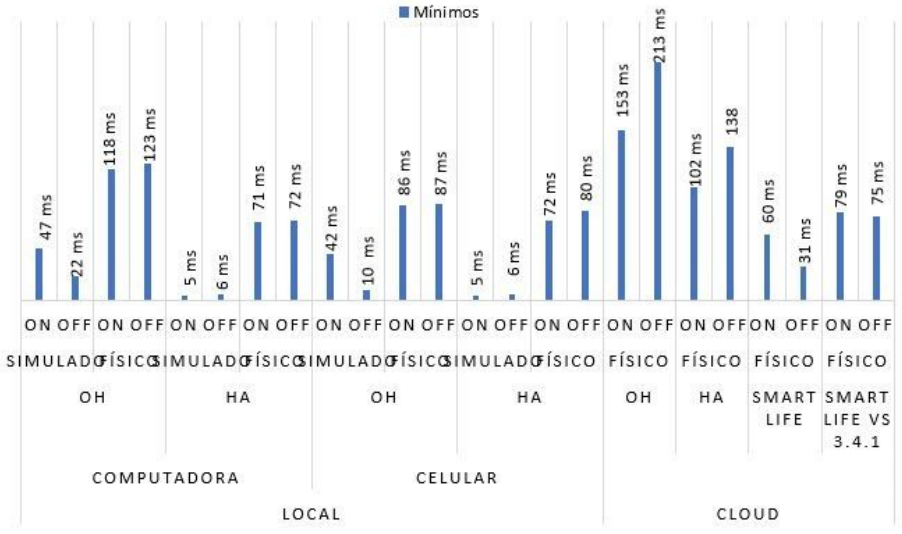

Imagen 44: Análisis de los mínimos en milisegundos
Fuente: Elaboración propia

Los mayores tiempos de los máximos corresponden a Open HAB tanto de forma local como de la cloud, y como se puede visualizar en la imagen 45, los resultados de Home Assistant ocupan el menor tiempo para gestionar los dispositivos.

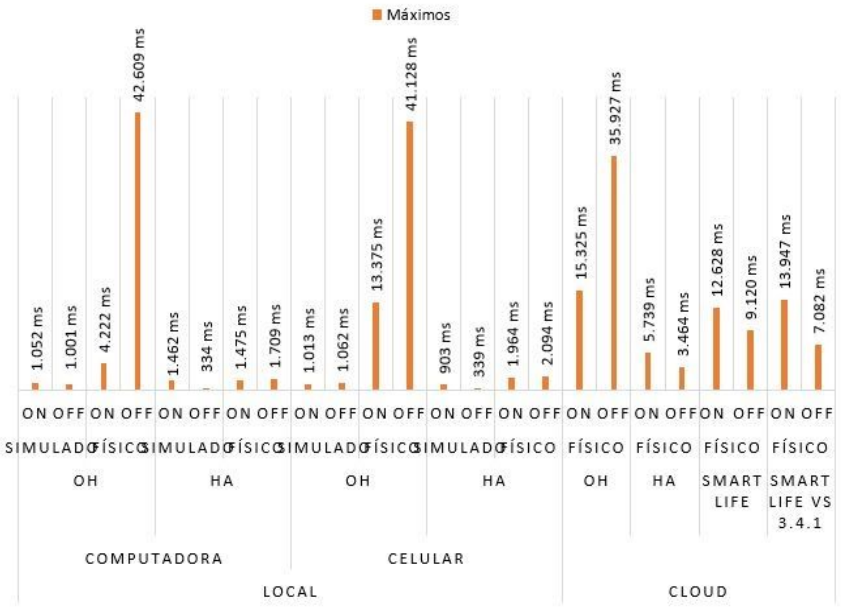

Imagen 45: Análisis de los máximos en milisegundos
Fuente: Elaboración propia

Por último, los promedios permitieron tener una visión resumida como se muestra en la imagen 46, conociendo cual es el mejor sistema domótico a utilizar con respecto al tiempo en que se tardó para gestionar los dispositivos, brindando como resultado que el sistema domótico con mejor tiempo de respuesta para gestionar de forma local o considerando la cloud es Home Assistant, que es el que se mantuvo con los menores tiempos en todas las pruebas realizadas.

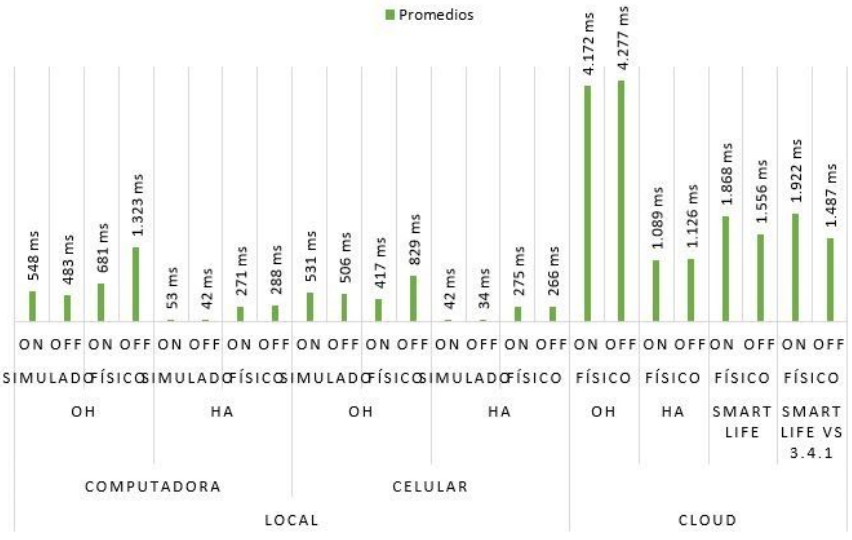

Imagen 46: Análisis de los promedios en milisegundos
Fuente: Elaboración propia

3.3 CONCLUSIONES

- Se logró alcanzar un mejor conocimiento en lo que respecta a seguridad IoT gracias a las investigaciones bibliográficas realizadas.
- Se identificó las vulnerabilidades que se presentan cada vez que se gestiona un dispositivo desde la aplicación Smart Life.
- Se consiguió brindar al usuario un método de seguridad para que su información no quede expuesta cada vez que gestiona sus dispositivos desde los sistemas domóticos Open HAB y Home Assistant, haciendo uso de la herramienta Node Red y el nodo tuya local, permitiendo el control local y seguro de sus dispositivos.
- Se pudo comprobar en las pruebas de latencia que Home Assistant es el sistema domótico más rápido en ejecutar las instrucciones, lo que además de brindar la seguridad de la información por el uso local de este, aporta con el buen tiempo de respuesta.

3.4 RECOMENDACIONES

- Se recomienda que el tema de seguridad sea una de las prioridades de los desarrolladores de dispositivos IoT para brindar un mejor aspecto a los usuarios y confiabilidad en la implementación de esta tecnología, considerando que el hardware debe ser un complemento del software donde ambos presenten una mejora con respecto a seguridad.
- Para trabajos futuros se recomienda que los sistemas domóticos presenten una mejora en su funcionalidad permitiendo el control local de los dispositivos IoT sin depender de la cloud.

BIBLIOGRAFÍA

[1] R. C. Parocha y E. Q. B. Macabebe, «Implementation of Home Automation System Using OpenHAB Framework for Heterogeneous IoT Devices,» *IEEE International Conference on Internet of Things and Intelligence System (IoTaIS),* pp. pp. 67-73, 2019.

[2] G. Reggio, M. Leottaa, M. Cerioli, R. Spalazzese y F. Alkhabbas, «What Are IoT Systems for Real? An Experts' Survey on Software Engineering Aspects,» *Internet of Things,* p. 28, 2020.

[3] J. Novillo-Vicuña, D. Hernández Rojas, B. Mazón Olivo, J. Molina Ríos y O. Cárdenas Villavicencio, «Arduino y el internet de las cosas,» vol. 45, 2018.

[4] U. Singh y M. A. Ansari, «Smart Home Automation System Using Internet of Things,» *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC),* pp. pp. 144-149, 2019.

[5] D. L. Hernández-Rojas, P. Fraga-Lamas, C. J. Escudero y . T. M. Fernández-Caramés, «A Plug-and-Play Human-Centered Virtual TEDS Architecture for the Web of Things,» *Sensors,* vol. 18, nº 7, p. 2052, Junio 2018.

[6] A. M. Campoverde, D. L. Hernández y B. E. Mazón, «Cloud computing con herramientas open-source para Internet de las cosas,» *Maskana,* vol. 6, pp. 173-182, 2015.

[7] B. Mazon-Olivo, D. Hernández-Rojas, J. Maza-Salinas y A. Pan, «Rules engine and complex event processor in the context of internet of things for precision agriculture,» *Computers and Electronics in Agriculture,* vol. 154, pp. 347-360, 2018.

[8] J. Berrú-Ayala, D. Hernandez-Rojas, P. Morocho-Díaz, J. Novillo-Vicuña, B. Mazon-Olivo y A. Pan, «SCADA System Based on IoT for Intelligent Control of Banana Crop Irrigation,» *International Conference on Applied Technologies,* pp. 243-256, 2019.

[9] S. Prange, E. v. Zezschwitz y F. Alt, «Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home,» *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* pp. pp. 154-158, 2019.

[10] U. Matchi Aïvodji, S. Gambs y A. Martin, «IOTFLA : A secured and privacy-preserving smart home architecture implementing federated learning,» *IEEE Security and Privacy Workshops (SPW),* pp. pp. 175-180, 2019.

[11] D. Georgakopoulos, «A Global IoT Device Discovery and Integration Vision,» *IEEE 5th International Conference on Collaboration and Internet Computing (CIC),* pp. pp. 214-221, 2019.

[12] D. K. Sharma, N. Baghel y S. Agarwal, «Multiple Degree Authentication in Sensible Homes basedon IoT Device Vulnerability,» *International Conference on*

Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), pp. pp. 539-543, 2020.

[13] K. Agarwal, A. Agarwal y G. Misra, «Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT,» *Proceedings of the Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* pp. pp. 629-633, 2019.

[14] T. Chaurasia y P. K. Jain, «Enhanced Smart Home Automation System based on Internet of Things,» *Proceedings of the Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* pp. pp. 709-713, 2019.

[15] A. S. Delfino, R. P. Brandão, T. S. Bumpus, M. Z. Fortes, H. O. Henriques y V. H. Ferreira, «Evaluation of the Impact of LED and Compact Fluorescent Lamps on the PLC Transmission with X-10 Technology,» *2019 IEEE Milan PowerTech,* pp. 1-6, 2019.

[16] E. Al-Masri, K. Raj Kalyanam, J. Batts, J. Kim, S. Singh, T. Vo y C. Yan, «Investigating Messaging Protocols for the Internet of Things (IoT),» *IEEE Access,* vol. vol. 8, pp. pp. 94880-94911, 2020.

[17] M. Stusek, K. Zeman, P. Masek, J. Sedova y J. Hosek, «IoT Protocols for Low-power Massive IoT: A Communication Perspective,» *11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),* pp. pp. 1-7, 2019.

[18] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas y C. J. Escudero, «Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications,» *Sensors,* vol. 18, nº 1, p. 57, Diciembre 2018.

[19] X. Jun Li, M. Ma y Y. L. Yen, «Detecting IRC-based Botnets by Network Traffic Analysis Through Machine Learning,» *29th International Telecommunication Networks and Applications Conference (ITNAC),* pp. pp. 1-6, 2019.

[20] O. Sadio, I. Ngom y C. Lishou, «Lightweight Security Scheme for MQTT/MQTT-SN Protocol,» *Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS),* pp. pp. 119-123, 2019.

[21] W. Mazurczyk, A. Velinov, A. Mileva y S. Wendzel, «Covert Channels in the MQTT-Based Internet of Things,» *IEEE Access,* vol. vol. 7, pp. pp. 161899-161915, 2019.

[22] D. Hernandez-Rojas, B. Mazon-Olivo, J. Novillo-Vicuña, C. Escudero-Cascon, A. Pan-Bermudez y G. Belduma-Vacacela, «IoT android gateway for monitoring and control a WSN,» *International Conference on Technology Trends,* pp. 18-32, 2017.

[23] S. Saxena, S. Jain, D. Arora y P. Sharma, «Implications of MQTT Connectivity Protocol for IoT based Device Automation using Home Assistant and OpenHAB,»

6th International Conference on Computing for Sustainable Global Development (INDIACom), pp. pp. 475-480, 2019.

[24] J. W. Li, Y. C. Huang y Y. C. Chang, «Space Borrowing System based on Internet of Things Technology,» *8th International Conference on Innovation, Communication and Engineering (ICICE),* pp. pp. 121-125, 2019.

[25] J. Molnár, T. Lorinc y O. Slavko, «Design and Implementation of an Intelligent Air Quality Sensor,» *IEEE International Conference on Modern Electrical and Energy Systems (MEES),* pp. pp. 74-77, 2019.

[26] Y. Mao, X. Li, Y. Jia, S. Zhao y Y. Zhang, «Security Analysis of Smart Home Based on Life Cycle,» *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI),* pp. pp. 1444-1449, 2019.

[27] R. E. Alden, P. Han y D. M. Ionel, «Smart Plug and Circuit Breaker Technologies for Residential Buildings in the US,» *8th International Conference on Renewable Energy Research and Applications (ICRERA),* pp. 1018-1021, 2019.

[28] R. Xu, Q. Zeng, L. Zhu, H. Chi, X. Du y M. Guizani, «Privacy Leakage in Smart Homes and Its Mitigation: IFTTT as a Case Study,» *IEEE Access,* vol. vol. 7, pp. pp 63457 - 63471, 2019.

[29] C. Ye, P. P. Indra y D. Aspinall, «Retrofitting Security and Privacy Measures to Smart Home Devices,» *Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS),* pp. pp. 283-290, 2019.

[30] H. Liu, T. Spink y P. Patras, «Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem,» *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* pp. pp. 894-899, 2019.

[31] Y. Xiao, Y. Jia, C. Liu, A. Alrawais, M. Rekik y Z. Shan, «HomeShield: A Credential-Less Authentication Framework for Smart Home Systems,» *IEEE Internet of Things Journal,* 2020.

[32] I. Nadir, Z. Ahmad, H. Mahmood, G. Asadullah Shah, F. Shahzad, M. Umair, H. Khan y U. Gulzar, «An Auditing Framework for Vulnerability Analysis of IoT System,» *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* pp. pp. 39-47, 2019.

[33] D. K. Sharma, N. Baghel y S. Agarwal, «Multiple Degree Authentication in Sensible Homes basedon IoT Device Vulnerability,» *International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC),* pp. pp. 539-543, 2020.

[34] S. Arif, M. Arif Khan, S. Ur Rehman, M. Ashad Kabir y M. Imran, «Investigating Smart Home Security: Is Blockchain the Answer?,» *IEEE Access,* vol. vol. 8, pp. pp. 117802-117816, 2020.

[35] R. B. da Silva Andrade y N. S. Rosa, «MidSecThings: Assurance Solution for Security Smart Homes in IoT,» *IEEE 19th International Symposium on High Assurance Systems Engineering (HASE),* pp. pp. 171-178, 2019.