ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Diseño e implementación de equipo del AP de Infraestructura STOKES

PROYECTO INTEGRADOR

Previo la obtención del Título de:

Ingeniero en Telemática

Presentado por:

Francisco Antonio Tulcán Velóz

GUAYAQUIL - ECUADOR

Año: 2022

DEDICATORIA

El presente proyecto se lo dedico a todas las personas que aportaron una parte de su tiempo, conocimiento y ayuda.

A mi madre María Veloz y abuela Manuela Baque por ser el sustento y pilar más importante de mi formación académica y profesional, ya que han estado conmigo en los buenos y malos momentos, gracias por sus enseñanzas y la manera que me enseñaron a hacer frente a los obstáculos en mi vida.

A la familia Zambrano Molina que en momentos complicados en mi formación académica siempre me ayudaron a que siga adelante brindándome su apoyo y acogiendome como uno más de su familia.

A la Sra. Beatriz de Posada que es una vieja amiga que apareció en un momento critico en mi familia y su ayuda fue un gran empujón para seguir adelante en mi formación académica.

Francisco Tulcán Veloz

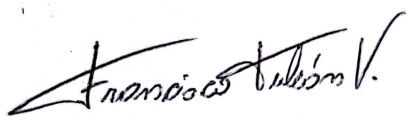
AGRADECIMIENTOS

Mi más sincero agradecimiento al profesor Ignacio Marín García porque con su guía, conocimiento y consejos se logró la culminación del proyecto. A la institución, ESPOL, por ofrecer la oportunidad de formarme como profesional.

Francisco Tulcán Veloz

DECLARACIÓN EXPRESA

”Los derechos de titularidad y explotación, me corresponde conforme al reglamento de propiedad intelectual de la institución; *Francisco Antonio Tulcán Veloz* y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”



Francisco Antonio
Tulcán Veloz

EVALUADORES

Digitally signed by IGNACIO MARIN GARCIA
Date: 2023.03.17 17:27:04 Z

Ignacio Marín García

PROFESOR DE LA MATERIA

Digitally signed by IGNACIO MARIN GARCIA
Date: 2023.03.17 17:26:44 Z

Ignacio Marín García

PROFESOR TUTOR

RESUMEN

Hoy en día existe un alto nivel de inseguridad en las redes inalámbricas, ya que cuando un dispositivo se conecta a la red y la información que se intercambia en este medio queda expuesta. Esto se debe a que los protocolos de seguridad presentes en la red tienen vulnerabilidades.

El proyecto busca la manera de disminuir el riesgo de la intercepción de datos en la por usuarios maliciosos, ofreciendo un método seguro de intercambio de datos. El sistema propuesto brinda un punto de acceso a la red usando un enlace de corto alcance para el intercambio seguro de datos, utilizando la tecnología VLC y OCC. Gracias a esta tecnología se reduce significativamente el espionaje.

Se implementará un punto de acceso a la red (STOKE AP) y una aplicación que interactúe con el AP (STOKE APP), para validar el ingreso a la red de usuarios registrados en el sistema. El punto de acceso STOKE estará ubicado cerca del ingreso a las instalaciones. Si el usuario es válido, el punto de acceso brinda una clave criptográfica al usuario. Luego cuando el usuario obtenga la clave Wi-Fi cifrada de una luminaria VLC, podrá descifrarla con la clave obtenida mediante el punto de acceso.

Palabras Clave: VLC, OCC, STOKE, protocolos de seguridad, usuarios maliciosos, Intercambio de datos.

ABSTRACT

Today there is a high level of insecurity in wireless networks, since when a device connects to the network and the information exchanged in this medium is exposed.This is because the security protocols present in the network have vulnerabilities.

The project seeks to reduce the risk of data interception by malicious users by providing a secure method of data exchange.The proposed system provides a network access point using a short-range link for secure data exchange using VLC and OCC technology.Thanks to this technology, espionage is significantly reduced.

A network access point (STOKE AP) and an application that interacts with the AP (STOKE APP) will be implemented to validate the network access of users registered in the system.The STOKE access point will be located near the entrance to the facility. If the user is valid, the access point provides a cryptographic key to the user.Then when the user obtains the encrypted Wi-Fi key from a VLC luminaire, he can decrypt it with the key obtained through the access point.

keywords: VLC, OCC, STOKE, security protocols, malicious users, data exchange.

ÍNDICE GENERAL

ABREVIATURAS

OCC	Comunicación de Camara Óptica (del Ingles Optical Camera Communication)
Camcom	Comunicación por Camara (del Ingles Camera Communication)
VLC	Comunicación con Luz Visible (del Ingles Visible Light Communication)
Wi-Fi	Fidelidad Inalámbrica (del Ingles Wireless Fidelity)
LED	Diodo Emisor de Luz (del Ingles Light emitting diode)
QR	Respuesta Rápida (del Ingles Quick Response)
AES	Estándar de Cifrado Avanzado (del Ingles Advanced Encryption Standard)
RSA	Rivest, Shamir y Adleman
WPA2	Acceso Inalámbrico Protegido (del Ingles Wireless Protected Access)
STOKES	Transmisión de Corto Alcance para Sistemas de Intercambio de Claves Ópticas (del Ingles Short-Range Transmission for Optical Key Exchange Systems)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

Las redes inalámbricas son el medio más utilizado para el intercambio de información, porque la ausencia de cables permite libertad de movimiento de los dispositivos tecnológicos en cierta área. Estas redes utilizan ondas de radio para interconectar dispositivos y la información viaja a través de este medio. Todos los aparatos electrónicos que estén conectados a la red inalámbrica estarán protegidos debido a sus protocolos de seguridad. Estos protocolos brindan acceso seguro a la red y protegen la información transmitida. Por ejemplo, WPA2 es uno de los protocolos de seguridad más comunes de las redes inalámbricas WI-FI, debido a que ofrece un gran nivel de confianza en asegurar la contraseña. Pero investigaciones [1] han demostrado las vulnerabilidades que tiene el protocolo y sus implementaciones, lo que causa que existan brechas de seguridad y la información quede expuesta.

El intercambio de información se usa en diferentes ámbitos y para diferentes aplicaciones, por ejemplo, el intercambio de credenciales para acceder a un sitio Web o un sistema de autenticación. Este flujo de datos debe ser seguro, porque de lo contrario usuarios maliciosos podrían interceptar la información y usarla a su beneficio. Por lo tanto, nace la necesidad de buscar una manera de aumentar la seguridad del intercambio de datos. Este proyecto se centro en el desarrollo de un sistema y aplicación móvil que permita intercambiar datos cifrados entre sí de manera segura, para el ingreso seguro a un enlace inalámbrico (Wi-Fi en este caso). Se utiliza como medio de intercambio la tecnología de enlace Visible Light Communication (VLC) de corto alcance y un canal Camera Communication (Camcom) [2]. Al usar estas tecnologías dificulta a los usuarios maliciosos interceptar el intercambio de información.

1.1 Definición de la problemática

En la actualidad las redes inalámbricas son uno de los medios más usados para transferencia de datos, pese a que no sea la más segura, ya que sus protocolos de seguridad con el paso del tiempo se vuelven menos seguros. Esto da como consecuencia que atacantes puedan acceder a la información. Por ello, es de suma importancia añadir una capa de seguridad extra, para así disminuir los riesgos del ingreso de cualquier usuario malicioso a la red.

Las redes de área local inalámbricas (Wi-Fi) son un claro ejemplo, debido a que en estas redes es donde el sistema de intercambio de claves ha sido explotado[3]. Por lo tanto, unos de los puntos importantes a tomar en cuenta para desarrollar entornos robustos es el intercambio seguro de datos.

El proyecto busca la manera de disminuir el riesgo de la intercepción de claves por usuarios maliciosos, ofreciendo un método seguro de intercambio de claves. El sistema propuesto brinda un enlace de corto alcance para el intercambio seguro de datos utilizando las tecnologias VLC y OCC. Gracias a esta tecnología se reduce significativamente el espionaje.

1.2 Justificación del proyecto

Las claves de las redes Wi-fi necesitan estar seguras el máximo de tiempo posible, debido a que numerosos dispositivos se interconectan a través de ella y los datos importantes de los usuarios viajan por medio de esta. Las claves al estar expuestas se convierten en objetivo de ataques informáticos. Por lo tanto, es de suma importancia tener una transmisión segura para la protección de claves. Para lograr una transmisión segura se deben utilizar varias técnicas.

Una de las técnicas a utilizar es la tecnología VLC porque ayuda a que la información solo este disponible en un área establecida, evitando así la fuga de datos. La transmisión

de datos se da al encendido y apagado de un LED a partir de modulaciones con una frecuencia tal que no cause molestias en la vista del usuario [4].

Los smartphones hoy en día la mayoría de estos tienen flash LED y cámaras integradas. Gracias a esto logran convertirse en transceptores VLC de manera funcional, sin necesidad de hardware adicional [5]. Por lo cual otra técnica es el uso de la tecnología OCC, ya que se convierte en la manera más viable para el intercambio de información.

1.3 Objetivos

Objetivo general

Diseñar e implementar un dispositivo (punto de acceso) y aplicación móvil (cliente/usuario) que permita el intercambio seguro de claves criptográficas mediante un enlace VLC-OCC de corto alcance para el acceso a una red WI-FI.

Objetivos especificos

- Desarrollar un dispositivo que mediante la utilización de un microcontrolador tipo Raspberry Pi, una pantalla LED y una cámara se realizará la recepción y emisión de claves criptográficas a través de un canal OCC.
- Desarrollar e implementar una aplicación móvil que se comunicara con el dispositivo anteriormente mencionado a través de un canal OCC utilizando la cámara del dispositivo móvil como receptor, y la pantalla del dispositivo móvil como emisor.
- Desarrollar e implementar una aplicación móvil capaz de recibir claves criptográficas de WI-FI, las cuales estarán cifradas mediante la clave obtenida por la aplicación anteriormente mencionada, a través de un canal OCC usando como receptor la cámara del dispositivo móvil.

1.4 Escenario

El sistema propuesto estará fuera de un área cerrada, como laboratorios, oficinas, restaurantes, etc. El cual será usado para poder realizar un intercambio de claves con un dispositivo móvil (el dispositivo móvil deberá tener la aplicación a desarrollar) y así autorizarse para acceder a la red inalámbrica del establecimiento. Este intercambio asegurará que no existan escuchas de la clave y así asegurarse que usuarios maliciosos ingresen a la red. Cabe recalcar que el usuario debe estar registrado en la base de datos del local antes de realizar el intercambio de claves. si el usuario no está registrado, no podrá realizar el intercambio de claves y no accederá a la red Wi-Fi.

1.5 Marco teórico

En esta sección se detallarán los conceptos que serán utilizados en el siguiente proyecto a desarrollar. Para lo cual se menciona el proceso de encriptación y los algoritmos de cifrado. Además, se describe el proceso de codificación de información a través de códigos QR y por ultimo se menciona la tecnología de comunicación.

Cifrado

Cifrado es el proceso de codificar información con el fin de que solo pueda leerlos alguien que tenga las herramientas necesarias para regresarlos a su forma original. Este mecanismo se usa normalmente para proteger datos que están almacenados en sistemas informáticos, también para proteger datos que son transmitidos a través de las redes [6]. Existen diferentes tipos de cifrados, en este proyecto se usaron cifrado simétrico y asimétrico usando el algoritmo AES y RSA respectivamente. El algoritmo AES es un cifrado de bloque simétrico con el que se puede cifrar y descifrar información. También es capaz de utilizar claves criptográficas que permiten cifrar y descifrar bloques de 128 bits [7]. RSA es un algoritmo criptográfico para un cifrado de tipo asimétrico. Se usa un par de claves que están matemáticamente vinculados y así ser capaz de cifrar y descifrar información [8].

Códigos QR

Los códigos QR son un método de almacenar datos en una matriz de puntos, estos pueden se representados en imágenes impresas en hojas o presentadas por pantalla de algún dispositivo. Estos códigos pueden ser decodificados por cualquier dispositivo con la capacidad de captar imágenes y que tenga el software adecuado [9].

Comunicación con luz visible (VLC)

La comunicación con luz visible es el método por el cual se transmite información usando luz visible. La transferencia de datos ocurre de manera que para la visión de una persona se vuelve imperceptible. El ancho de banda de este sistema formado por luminaras dependerá de la distancia del emisor. Con esta tecnología se evita problemas de interferencias y de velocidad de trasferencia. Además, se convierte en una alternativa cuando se tienen problemas en el medio de transmisión, por ejemplo, en las redes inalámbricas [4]. Existe una tecnología que es similar a VLC, su nombre es Li-Fi. Según [10] las diferencias que tiene con el sistema utilizado es que la comunicación es multiusuario, bidireccional y de alta velocidad.

Comunicación de cámara óptica (OCC)

La comunicación de cámara óptica trabaja en las bandas de los canales VLC, presentando mas ventajas en las características del receptor. OCC se presenta como una nueva tecnología que es asequible e incluye entre sus ventajas el uso de cámaras integradas en los dispositivos inteligentes que actúan como los receptores OCC [11].

1.6 Estado del arte

En [12] se estudia los requerimientos de seguridad que debe tener una comunicación D2D. también proponen un sistema de autentificación llamado SeKeQ (intercambio seguro de claves con código QR). Este sistema verifica la identidad del usuario mediante una comparación automática de claves y proporciona una clave compartida usando el acuerdo Diffie-Hellman con hash SHA-256.

Por otro lado, en [13] muestran que el protocolo MCEPAK (protocolo de intercambio de clave autenticado por contraseña basado en una curva elíptica para redes inteligentes) es vulnerable a los ataques de diccionario. Además, proponen un protocolo de intercambio de claves basado en mapas caóticos con el fin de aumentar la seguridad de las redes inteligentes. Al final demuestran que el protocolo propuesto es más seguro y eficiente que el protocolo MCEPAK mediante un análisis formal.

En [14] utilizan un método de transmisión usando las tecnologías VLC Y OCC, para la distribución y recepción segura de claves respectivamente. Gracias a que las claves se transmiten mediante el parpadeo de la luz LED a una frecuencia especifica, complica su detección al ojo humano. También mencionan la eficacia y viabilidad de utilizar un método de comunicación óptica inalámbrica básica para la transmisión de claves.

Adicionalmente en [15] de manera similar utilizan vlc como método de transmisión de texto y para la recepción de este hacen uso de un sensor de luz. El proceso de modulación empleando ook y la demodulación de esta señal es manejada por una raspberry pi. Esta transmisión por diferentes factores solo se puede efectuar cuando el emisor y receptor se encuentran a una distancia de 10 cm.

Por último, en [16] utiliza un sistema de comunicación de cámara óptica que usa como transmisor una fibra óptica acoplada a un diodo laser y como receptor una cámara con obturador rodante. Para la obtención de datos proponen una red neuronal basada en filas de pixeles por bit. Gracias a este método compensa el bit error rate anterior a la corrección de errores en la recepción a una velocidad de datos de 3300 bit/s a una distancia de transmisión de 35 cm.

La presente propuesta a diferencia de los trabajos anteriores es la utilización de un sistema que usa la comunicación de luz visible de corto alcance para el intercambio seguro de claves criptográficas. Con este sistema evitamos las filtraciones de luz, debido a que el intercambio se realiza en una infraestructura cerrada y así evitar datos erróneos. También se evita la fuga de información por la razón ya mencionada. Gracias a esto el intercambio de claves es bastante seguro en la siguiente propuesta.

CAPÍTULO 2

2. METODOLOGIA

El objetivo de este capítulo es detallar paso a paso como se ejecutará el proyecto. La metodología en cascada [17] fue escogida debido a su desarrollo de manera secuencial por etapas. En la Figura 2.1 se detallan las etapas a seguir: Análisis, Diseño, Implementación, Verificación y Mantenimiento. Gracias al desarrollo de cada etapa se logra evitar el mayor número de inconvenientes en la implementación del proyecto.

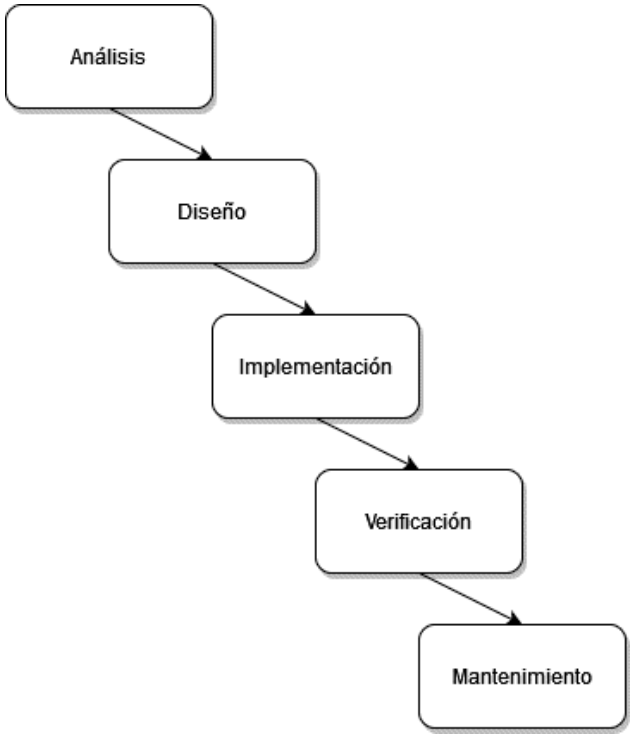


Figura 2.1: **Diagrama de la metodología en cascada**

2.1 ANÁLISIS

En la primera etapa de la metodología se realiza un análisis general de todo el sistema en el cual se trabajará. En la Figura 2.2 se muestra el diagrama esquemático de los elementos del sistema.

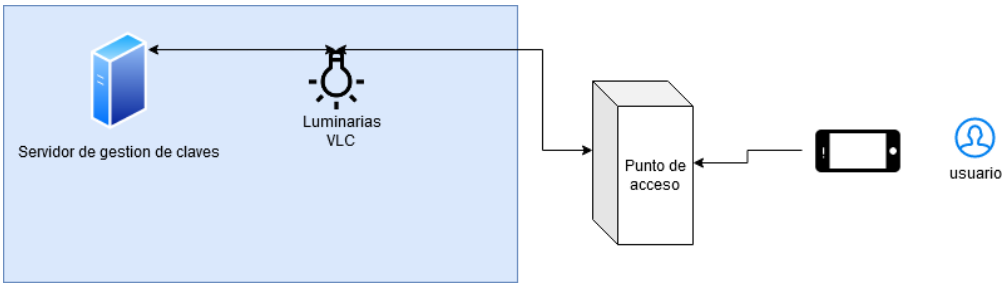


Figura 2.2: **Diagrama Esquemático del Escenario**

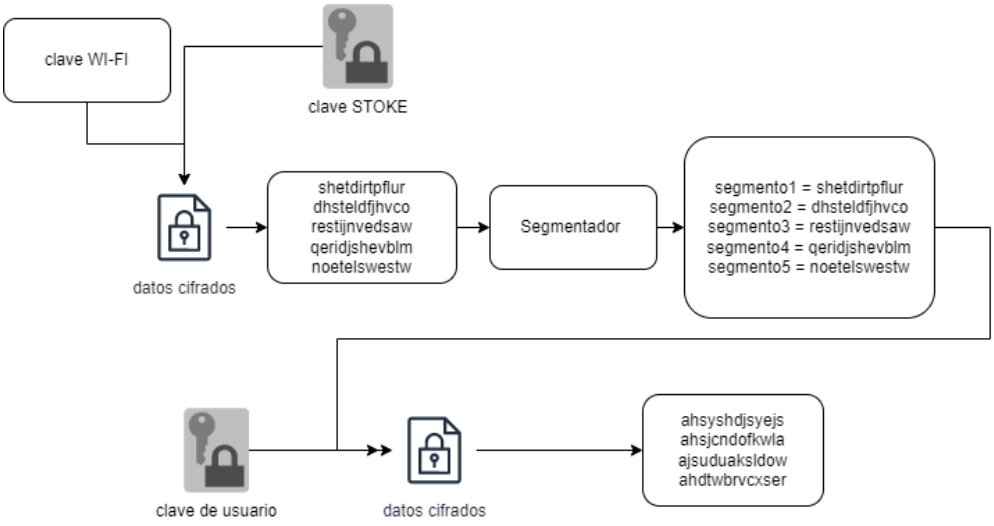


Figura 2.3: **Proceso por el que pasa la contraseña Wi-Fi**

Como se puede observar en la Figura 2.2, el usuario interactúa con el punto de acceso STOKES mediante su dispositivo móvil con el cual se intercambiará información. La información que brinda el usuario al dispositivo punto de acceso son, un usuario y contraseña. El dispositivo validara si el usuario se encuentra registrado en el sistema. Si el usuario es válido, el servidor gestor de claves enviará una clave criptográfica Stokes (esta clave se utiliza para un cifrado simétrico y el algoritmo usado es AES) al dispositivo punto de acceso y mediante el punto de acceso el usuario también recibirá la clave Stoke. Esta clave cifrara la contraseña Wi-Fi, también el usuario al ser valido enviara la

clave criptográfica publica del usuario (el par de claves del usuario es utilizado para un cifrado asimétrico, usando el algoritmo RSA) al punto de acceso. El dispositivo al obtener la clave del usuario procederá a cifrar la contraseña Wi-Fi cifrada y enviarla al usuario para que este con su clave privada pueda descifrar parte del mensaje. En la Figura 2.3 se observa el proceso por el cual pasa la contraseña Wi-Fi hasta enviarlo al usuario.

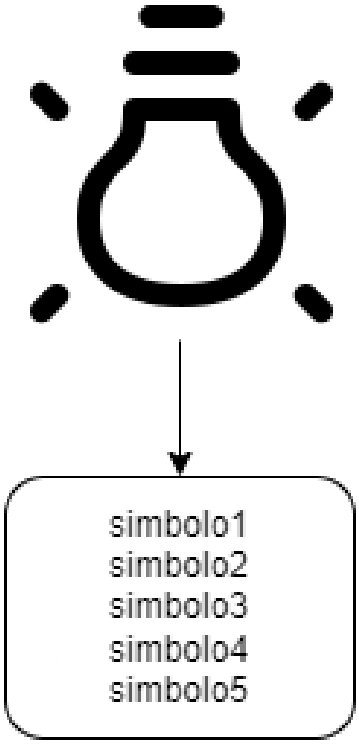


Figura 2.4: **Luminaria VLC**

El usuario a pesar de tener la clave STOKE con la cual esta cifrada la contraseña Wi-Fi todavía no puede obtener la contraseña. Esto se debe los datos cifrados están divididos en 5 símbolos como se observa en la Figura 2.4, además están desordenados. Por lo tanto, para poder obtener la contraseña antes se debe obtener los símbolos en orden. Los símbolos ordenados se los obtiene mediante una luminaria VLC. Así finalmente se obtiene el texto cifrado y se logra descifrar con la clave STOKE obtenida del punto de acceso, para luego obtener la contraseña Wi-Fi.

Luego del análisis se proponen las herramientas necesarias para el desarrollo del dispositivo punto de acceso y la aplicación móvil. Por lo cual, es necesario anunciar el papel que realizan los componentes dentro de la infraestructura. Estos elementos se dividieron en dos partes, hardware y software.

HARDWARE

El dispositivo consiste en una estación base o punto de acceso en donde se intercambian claves criptográficas a través de un enlace VLC-OCC de corto alcance. Este dispositivo integra un microcontrolador que está conectado a una cámara y una pantalla led para realizar el intercambio.

El microcontrolador es de tipo Raspberry pi la versión 4B en específico. Este instrumento fue elegido debido a su tamaño y capacidad de procesamiento. Es el centro de operaciones del proyecto donde se ejecutarán todas las funciones del punto de acceso.

El enlace OCC utiliza una cámara de marca Raspberry Pi para asegurar la compatibilidad con el microcontrolador para no tener problemas de dependencias. Mediante programación este elemento receptara claves ocultas en códigos QR emitidas desde el dispositivo móvil del usuario.

Para el enlace VLC se emplea una pantalla LED de 3,5” conectada a la Raspberry PI. Esta utiliza SPI (Serial Peripheral Interface) para la transferencia de información, la cual es compatible con el microcontrolador y facilita la transmisión de claves hacia el cliente.

SOFTWARE

El software principal es el sistema operativo que usa el microcontrolador llamado Raspbian-Strech OS [18]. Se selecciono esta versión debido a que es compatible con muchas dependencias que serán utilizadas. En este software se programaron todas las funciones principales del sistema punto de acceso

Python es el lenguaje de programación empleado en el sistema. Con el cual se desarrolla los diferentes módulos para el funcionamiento del dispositivo. Las principales librerías para utilizar son Cryptography, QRcode y OpenCV.

La librería Cryptography [19] ayuda a cifrar y descifrar los datos intercambiados entre el punto de acceso y el dispositivo móvil. Esta librería también genera las claves criptográficas públicas y privadas que se usan para cifrar y descifrar datos.

Las librerías QRcode [20] y OpenCV [21] son utilizadas para la generación y decodificación de códigos QR. La utilización de esta codificación es con el fin de ocultar las claves o información intercambiada entre el sistema y el usuario.

la aplicación móvil es desarrollada en Android Studio, el cual es el entorno desarrollo integrado oficial para el desarrollo de aplicaciones para Android. El lenguaje utilizado es Java, el cual es nativo de Android. Las librerías principales usadas en la aplicación son Zxing, Security, Chaquo, mobileffmpeg y camera2.

La librería Zxing [22] ayuda a generar los códigos QR enviados hacia el punto de acceso. Así mismo ayuda a decodificar los códigos enviados desde el punto de acceso usando la cámara frontal del móvil. Con la librería Security se utiliza para poder descifrar y cifrar la información que es receptada y emitida. Además, esta librería genera un par de claves criptográficas con las cuales se cifrarán y descifrarán los datos. El algoritmo de cifrado asimétrico que utiliza es RSA.

Para la etapa de decodificación de mensajes a través de luz visible se trabaja con la

librería Camera2 [23], la cual es la que se utiliza para utilizar la cámara del dispositivo, además de configurar los parámetros de esta. Estos parámetros son la sensibilidad a la luz de un sensor de imagen (ISO) y la duración de la exposición de cada píxel a la luz. Estos dos tienen valores altos para que en la cámara se aprecie las franjas brillantes y oscuras.

Mobileffmpeg [24] es una librería que ayuda a extraer los frames por segundo de un video grabado por la cámara del dispositivo móvil y a la vez las transforma en imágenes. Y por último la librería Chaquo[25] nos permite utilizar un script hecho en Python para extraer la información de cada imagen.

2.2 DISEÑO

Esta etapa se enfoca en los diagramas del sistema para que el lector tenga noción de cómo se integra el hardware del dispositivo. Esta sección se divide en tres secciones, en la primera se muestra el esquemático del dispositivo de punto acceso, en la segunda se observa el diagrama de la aplicación móvil y, por último, se muestra un diagrama esquemático donde se encuentra el punto de acceso y el cliente como conjunto.

Esquemático del punto de acceso

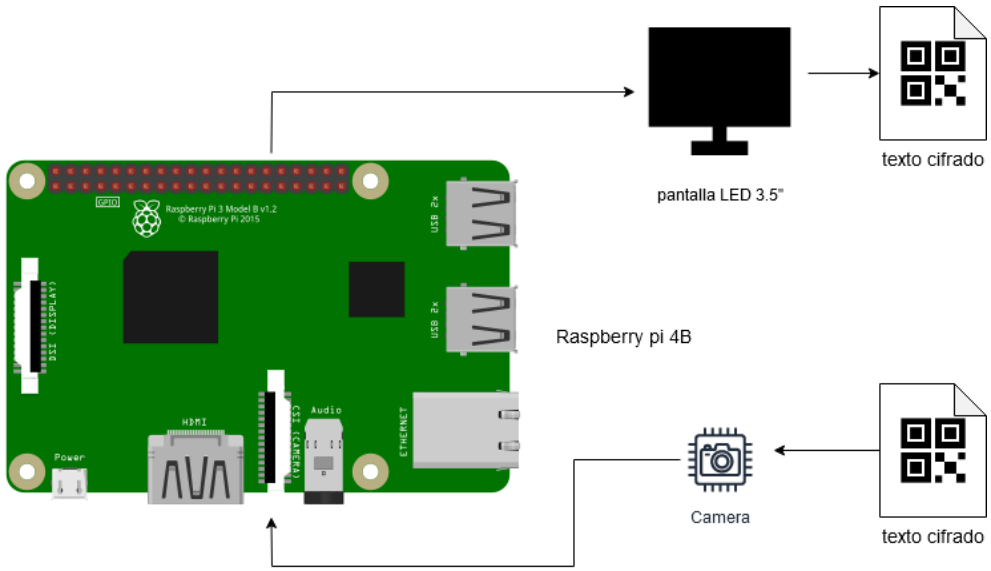


Figura 2.5: **Diagrama Esquemático Punto de Acceso**

En la Figura 2.5 se muestra el diagrama esquemático del punto de acceso el cual está conformado por un microcontrolador de tipo Raspberry, una pantalla LED de 3.5” y una cámara. Estos dos últimos elementos mencionados anteriormente son los que proporcionarán la función de transmitir y receptar los datos ocultos en códigos QR de manera secuencial.

Diagrama de la aplicación móvil

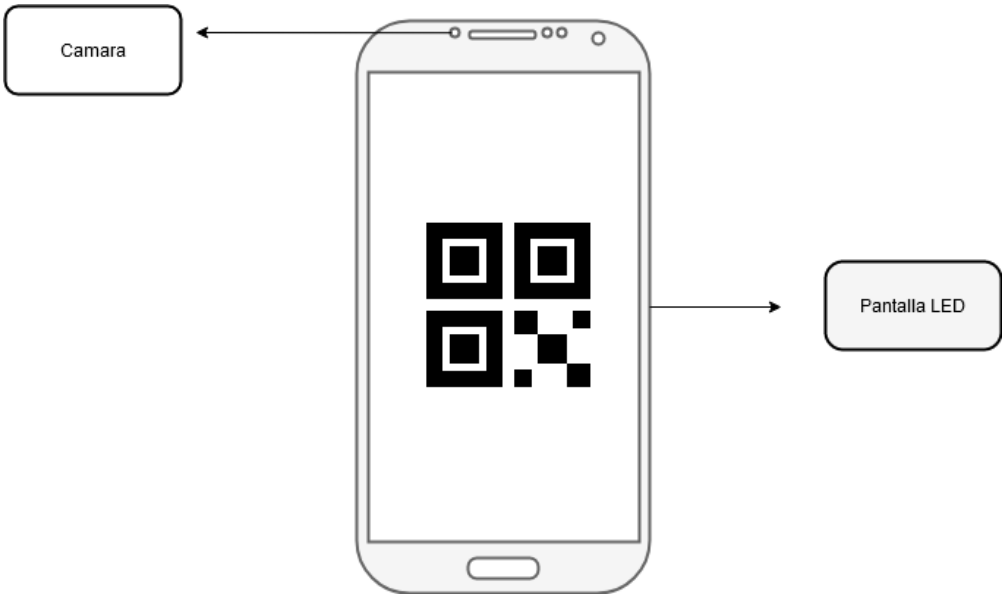


Figura 2.6: **Diagrama aplicación móvil**

En esta sección se observa la Figura 2.6 la cual es la aplicación móvil que se encarga de intercambiar información con el punto de acceso. Esta aplicación utiliza la pantalla como emisor de información y la cámara frontal para receptar la información enviada del punto de acceso. Además, por medio de la cámara trasera se recepta información mediante un enlace VLC-OCC enviada por una luminaria VLC.

Finalmente, como se muestra en la Figura 2.7 será el sistema completo. El dispositivo móvil del usuario con la aplicación abierta deberá ser ingresado dentro del punto de acceso hasta presionar un botón en el interior, también el smartphone estará encajado con la pantalla y cámara del dispositivo. Esto para que se realice el respectivo intercambio y validación de los datos. Este intercambio realizado es seguro debido al uso de la tecnología de comunicación de corto alcance VLC-OCC, además que la información importante está cifrada con las claves indicadas en la sección de análisis.

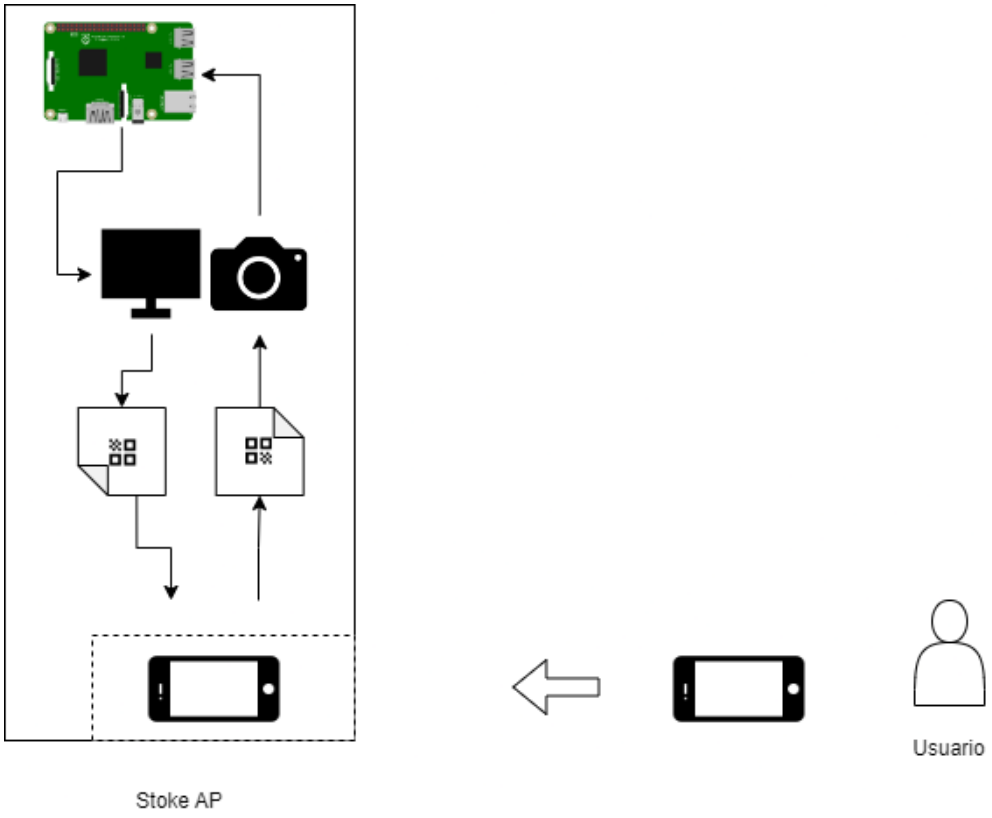


Figura 2.7: **Diagrama Esquemático del sistema**

2.3 Implementación

La parte interna del punto de acceso se aprecia en la figura tal donde se puede observar los componentes que la constituyen. El sistema esta formado por el microcontrolador el cual ya tiene instalado el sistema operativo y su configuración correspondiente. También se observa las conexiones que tiene con la pantalla LED y la cámara. En el microcontrolador se tiene la programación que se usa para el intercambio de información con el dispositivo móvil.

Figura 2.8: **Circuito del punto de acceso implementado vista lateral**

En la segunda etapa se enfocó en la programación que esta en el hardware del dispositivo y así lograr el intercambio de información con el dispositivo móvil. Gracias a esto se puede comprobar el funcionamiento del sistema. Las funciones son realizadas son en Python para el caso del punto de acceso.

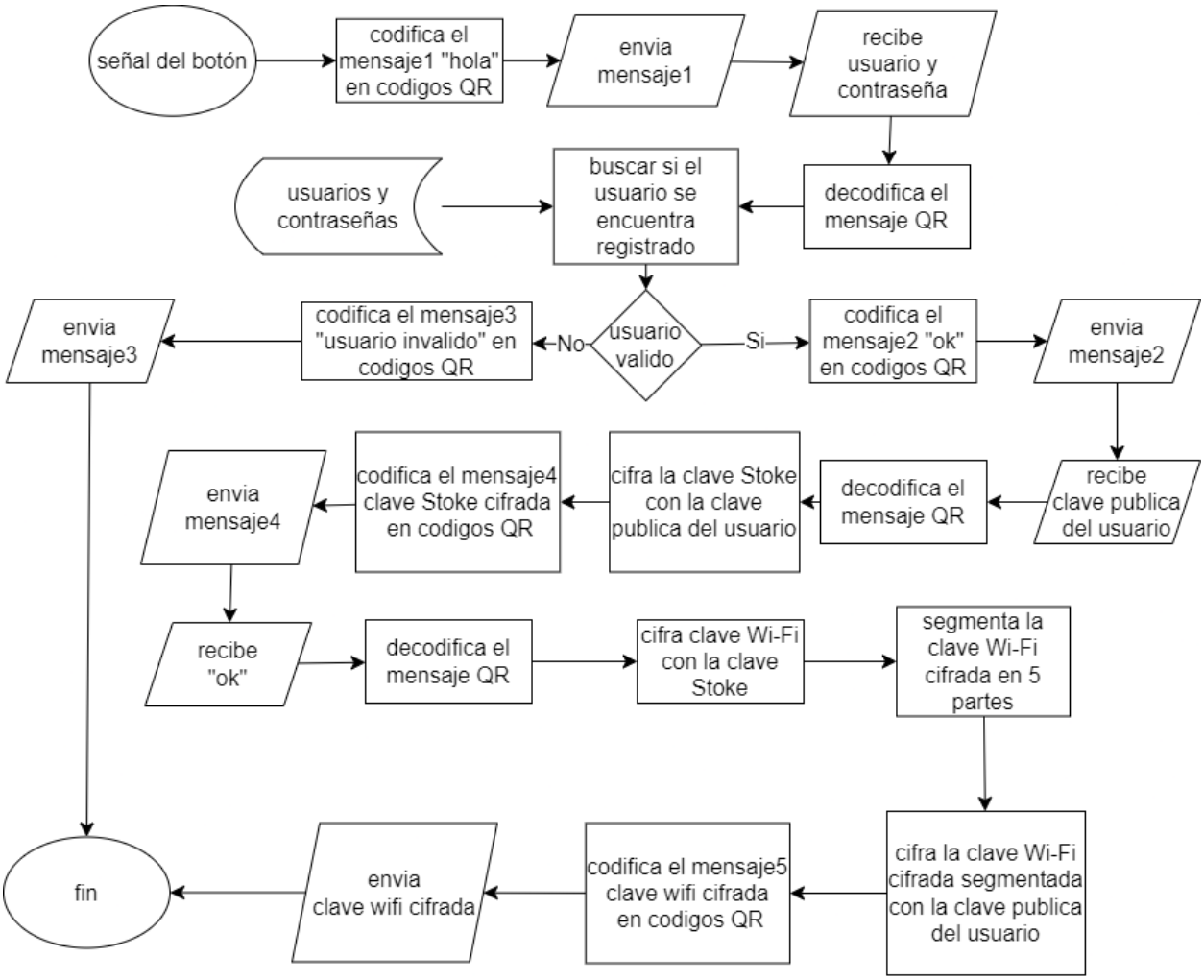


Figura 2.9: **Diagrama de flujo del punto de acceso**

En la Figura 2.9 se observa el diagrama de flujo del punto de acceso, este script permite realizar el intercambio de información y la validación del usuario. Todo inicia al presionar el botón dentro del punto de acceso, el microcontrolador al recibir esta señal empieza a transmitir el mensaje de inicio “hola”. Luego el dispositivo espera recibir un usuario y contraseña por parte del smartphone del usuario. Al recibir el usuario y contraseña, este se valida si se encuentra registrado en el sistema. Si el usuario es válido la script continua, pero si el usuario es invalido el punto de acceso envía un mensaje “usuario invalido” al smartphone y se detiene el script. Al ser el usuario valido el punto de acceso envía un “ok” al dispositivo móvil. El dispositivo responde al punto de acceso con su clave publica y este le envía la clave STOKE cifrada con la clave que envió el usuario. Ahora el cliente envía un “ok” y el punto de acceso al recibir el mensaje, este envía la contraseña Wi-Fi cifrada con la clave STOKE y nuevamente cifrada con la clave publica del usuario. Antes de enviar esta clave el mensaje es segmentado en cinco partes para luego ser enviado. Al enviar finalmente la contraseña Wi-Fi cifrada se termina el proceso.

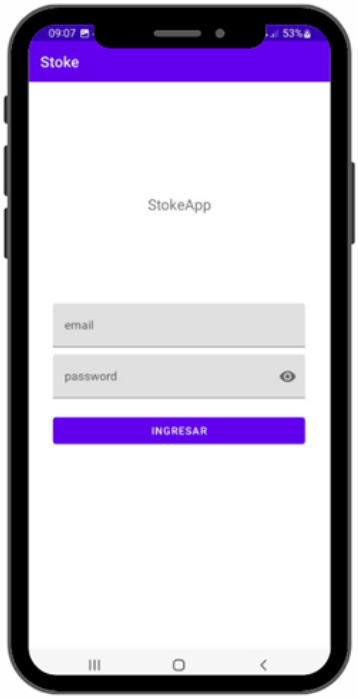


Figura 2.10: **Pantalla de inicio de sesión**

La aplicación móvil comienza con un inicio de sesión para luego poder enviarlo hacia el punto de acceso. La aplicación funciona offline.

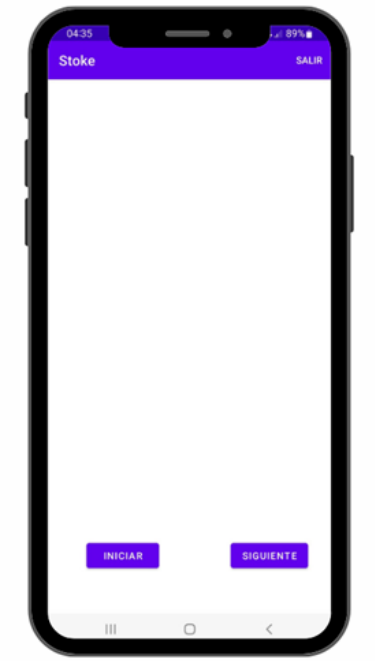


Figura 2.11: **Pantalla para el inicio de intercambio de datos**

En la Figura 2.11 se observa la pantalla luego de que el usuario haya iniciado sesión, aquí es donde se iniciara el intercambio de información con el punto de acceso. Este proceso se dará inicio al seleccionar el botón iniciar. Los códigos QR se mostrarán en la parte superior de la aplicación esto se apreciará de mejor manera en el capítulo de resultados.

Figura 2.12: **Pantalla para el inicio de obtención de datos de la luminaria**

Por último, en esta escena se observa la ultima parte de la aplicación, la cual se observa al seleccionar la opción siguiente que se observa en la Figura 2.12. Aquí es donde se recibe la señal VLC a través la cámara del dispositivo móvil. Aquí se decodifica la señal recibida para poder descifrar el mensaje final y obtener la contraseña Wi-Fi.

2.4 Verificación

Se realizaron pruebas generales del sistema para comprobar que cada componente funciona correctamente. También sirvió para verificar si el código se ejecuta de forma correcta y que el intercambio de información sea exitoso.

Se verificó el funcionamiento del sistema en el entorno donde estará instalado con el fin de evitar algún problema con el hardware completamente operativo en un futuro. El lugar de implementación que se eligió fue el de un laboratorio para realizar las pruebas. Se realizaron pruebas en conjunto el punto de acceso y la aplicación móvil. Se realizo esta prueba para verificar si se cumple el intercambio de información. La luz del laboratorio no impidió el intercambio de datos y se realizó sin problemas.

Se comprobó si la información se podía filtrar. Gracias a que el dispositivo móvil se ingresa dentro del punto de acceso se evita la filtración de información. También se verifico el comportamiento del dispositivo punto de acceso al enviarle datos correctos y erróneos, el comportamiento del punto de acceso y la aplicación móvil fue el esperado. Por ultimo se verifico si cada vez que se encendía el dispositivo se ejecutaba el script.

2.5 Operación y mantenimiento

Finalmente, se revisa que el dispositivo cuando este operable funcione sin ningún inconveniente, es decir que el intercambio de información entre el usuario y el punto de acceso se cumpla. Se realizó la revisión de las librerías para así en un futuro evitar problemas de funcionamiento. El mantenimiento se debe realizar cada 6 meses para la verificación de componentes y código fuente porque las librerías pueden sufrir actualizaciones. Estas actualizaciones pueden ocasionar que se deba cambiar las versiones de los componentes (cámara y pantalla LED). También con las actualizaciones se puede tener mejoras del dispositivo.

CAPÍTULO 3

3. Resultados y análisis de costos

En este capitulo se muestra las pruebas realizadas al dispositivo cuando ya está finalmente implementado, observando que el funcionamiento sea el correcto. Primero se planteo un escenario donde el usuario ingresado sea valido o se encuentre registrado en el sistema. Para realizar esta prueba se utilizó un dispositivo móvil SAMSUNG GALAXY A52.

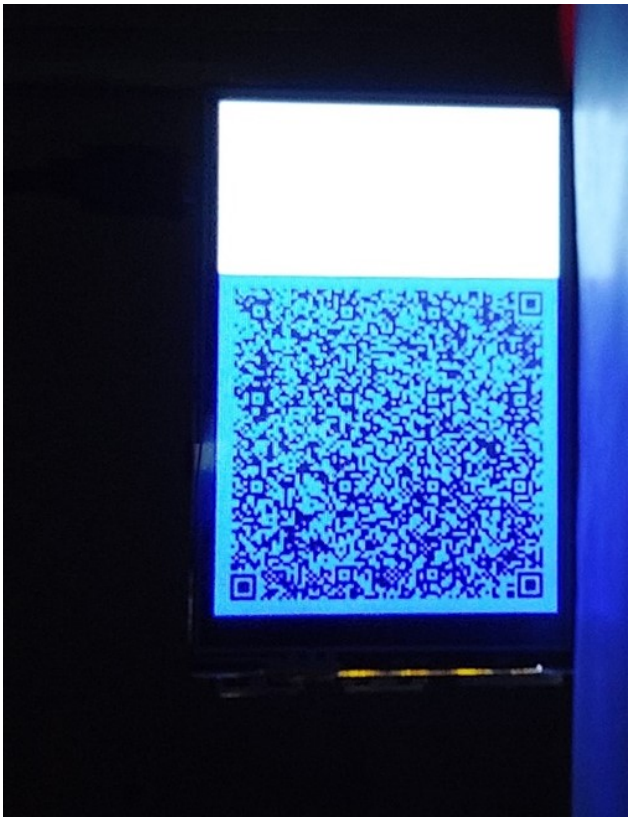


Figura 3.1: **Vista desde el interior del punto de acceso a la pantalla**

Una vez ya comenzó el intercambio de información, se puede observar como en la Figura 3.1 el dispositivo móvil está recibiendo datos desde la pantalla LED del punto de acceso. El fondo se aprecia oscuro porque la cámara frontal del smartphone tiene un

autoenfoque predeterminado y solo enfoca la pantalla por el brillo que tiene. También se usa un fondo escuro en la imagen del código QR porque en este componente no se puede controlar el brillo y este no permitía distinguir la imagen. Además, al no recibir la imagen correctamente se generaban datos erróneos, entonces como alternativa se usa un fondo de color oscuro (azul oscuro en este caso) para evitar esos errores.

Figura 3.2: **Vista desde el interior del punto de acceso a la pantalla del dispositivo móvil**

En la siguiente Figura 3.2 se observa la pantalla del dispositivo móvil enfocada desde la cámara del punto de acceso. Así se muestra la obtención de datos, aquí el punto de acceso al recibir la información la procederá a validar. En este caso se valida el usuario y contraseña. Para este caso no es necesario que la imagen del código QR tenga un fondo oscuro como en el punto de acceso, esto ocurre porque el brillo de la pantalla del smartphone es manipulable.

Figura 3.3: **Mensaje aprobado**

```
>>> %Run main.py

  ok
  recibido: ftulcan-1234
  ok
  clave enviada
```

Figura 3.4: **Mensaje aprobado desde el punto de acceso**

Si el usuario es valido se completa el proceso y en la pantalla del dispositivo móvil se muestra un mensaje de aprobado como se observa en la Figura 3.3. Al completarse el proceso el smartphone obtiene todos los datos necesarios para descifrar la contraseña Wi-Fi que se obtendrá posteriormente. En la siguiente Figura 3.4 también se muestra un mensaje cuando se cumple el proceso en el punto de acceso.

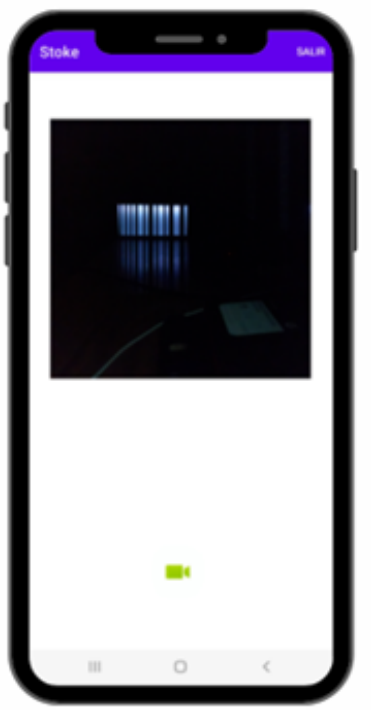


Figura 3.5: **Previsualización de la tercera pantalla**

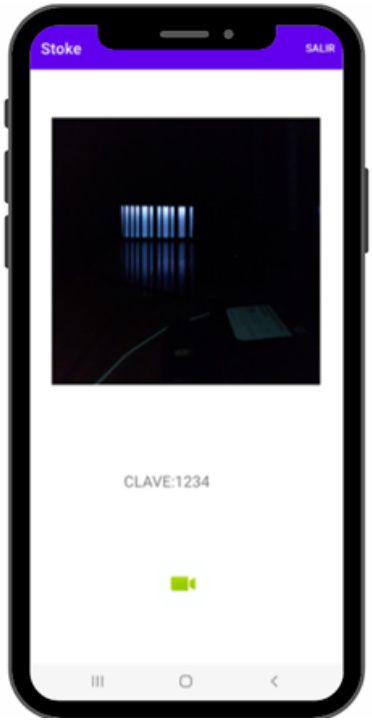


Figura 3.6: **Obtencion de datos desde la luminaria VLC**

En la Figura 3.5 se observa cuando la cámara del dispositivo móvil enfoca la luminaria VLC, se la diferencia de una luminaria común, ya que se aprecia las franjas brillantes y oscuras. En Figura 3.6 se muestra el resultado final de la obtención de clave luego de haber presionado el botón y decodificado la información recibida de la luminaria LED.

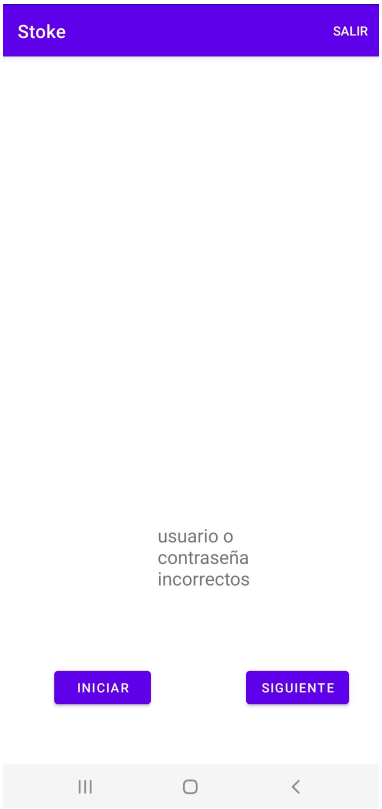


Figura 3.7: **Mensaje en la aplicación móvil usuario no registrado**

```
>>> %Run main.py

  ok
  recibido: mveloz-1234
  invalido
  clave no enviada
```

Figura 3.8: **Mensaje en el punto de acceso usuario no registrado**

Ahora se presenta un escenario donde el usuario no esta registrado en el sistema. En Figura 3.7 se presenta el mensaje que se obtiene en la aplicación móvil al recibir un mensaje de error por parte del punto de acceso. En este caso el smartphone no tiene ningún dato para continuar con la obtención de la contraseña Wi-Fi. El punto de acceso también muestra un mensaje de error o que no se encuentra registrado como se observa en la Figura 3.8.

Si no se obtiene información debido a que el usuario no esta registrado tampoco se podrá obtener información de la luminaria VLC. Además, si se intenta decodificar los datos que envía la luminaria VLC la aplicación muestra un mensaje de vacío como se observa en la Figura 3.9.

Figura 3.9: **Mensaje de la aplicación móvil mostrado al intentar decodificar los datos emitidos de la luminaria**

Ahora se realiza un numero de pruebas para comprobar cual es la probabilidad de acierto cada vez que un usuario quiere entrar a la red. Para obtener los resultados requeridos se divide en dos etapas el ingreso a la red. Primero es la validación de usuario y Segundo la obtención de datos mediante la luminaria VLC.

Tabla 3.1: **Tabla de resultados de la primera etapa**

# de etapa	# de pruebas	# de aciertos	# de errores	Probabilidad de acierto
etapa 1 (valores validos)	20	17	3	85%
etapa 1 (valores erroneos)	20	0	20	0%

Para la primera etapa se realizaron 20 pruebas en el ingreso de usuarios válidos y se obtuvo una probabilidad de acierto de un 85% como se observa en la Tabla 3.1, lo cual es bastante aceptable. Los errores que se obtienen fue porque la cámara del punto de acceso es de baja calidad y debido a esto tomaba datos erróneos a la hora de recibir algún dato.

En la segunda etapa se tomaron datos de las luminarias a diferentes distancias, estas son 50, 100, 150 y 200 centímetros. Las pruebas realizadas también son 20 para cada distancia.

Tabla 3.2: **Tabla de resultados de la segunda etapa**

# de etapa/distancia[cm]	# de pruebas	# de aciertos	# de errores	Probabilidad de acierto
etapa 2 (valores validos)/50cm	20	19	1	95%
etapa 2 (valores validos)/100cm	20	17	3	85%
etapa 2 (valores validos)/150cm	20	4	16	20%
etapa 2 (valores validos)/200cm	20	0	20	0%

En la Tabla 3.2 se muestran los resultados de las pruebas, gracias a estas pruebas se puede observar que a las mejores distancias para receptar datos es de 50 y 100 cm ya que la probabilidad de acierto es de 95 y 85% respectivamente. Como se puede apreciar la lectura de los datos varía de acuerdo con la distancia entre la cámara y la luminaria. Esto se debe a que a mayor distancia hay un mayor ruido que interfiere con los datos transmitidos según [26]

3.1 análisis de costos

En esta sección se detallan el costo de los elementos que conforman el hardware. Se tomaron como referencia los precios del mercado manufacturados por la fábrica.

En la Tabla 3.3 se describe los costos de los materiales que se usaron para el desarrollo del dispositivo. Como se aprecia el valor más alto pertenece a él microcontrolador, aunque el precio puede variar por el modelo y características del dispositivo.

En la siguiente Tabla 3.4 se detalla el costo de implementación del prototipo y la

Tabla 3.3: **Costos de materiales**

Materiales	Precio unitario	Cantidad	Total[US$]
Raspberry pi 4b	$150	1	150
Camara pi 5Mp	$11	1	11
Pantalla LED 3,5”	$24,9	1	24,9
Carcasa	$15	1	15
Piezas de soporte electrónico	20$	1	20
Total			220,9

mano de obra. También se incluyeron los precios por hora de todos los criterios que se encuentren ella. Como referencia del precio por hora de la programación, se toma en cuenta el salario mínimo sectorial de un desarrollador de software, el cual se menciona en el Anexo 1 de estructuras ocupacionales – salarios mínimos sectoriales y tarifas del año 2022 detallado por el ministerio de trabajo [27].

Tabla 3.4: **Costos de mano de obra**

Descripcion	Precio	# de horas	Total[US$]
Diseño del hardware	$2,66	8	21.28
Integración de componentes	$2,69	6	16,14
Programación	$15	92	1380
Total			1417,42

Tabla 3.5: **Costo del prototipo**

Descripcion	precio
Costo de materiales	$150
Costo de mano de obra	$11
Total	$220,9

Ahora se requiere el precio total del prototipo, este se obtiene de la suma del total de costos de materiales y el total de costo de la mano de obra. En la Tabla 3.5 se realiza

esta operación y se obtiene el valor final del prototipo.

Un proceso importante a tomar en cuenta es el análisis de depreciación, que no es otra cosa que un valor activo a través de su vida de servicio [28]. Para obtener el tiempo de vida útil del prototipo se toma de referencia el tiempo vida útil más temprano de un elemento del prototipo [29]. Por lo general, los aparatos de computación se acercan a los 5 años de vida útil.

$$ValorResidual = CostoDelDispositivo * 33\% \tag{3.1}$$

$$Depreciacin = \frac{(CostoDelDispositivo - ValorResidual)}{TiempoDeVida}\% \tag{3.2}$$

Tabla 3.6: **Depreciación del prototipo**

Costo del prototipo	Valor residual	Tiempo de vida	Depreciación
1638,32	540,6456	5	219,53488

Tabla 3.7: **Depreciación acumulada**

AÑO	SLN[$]	DEPRECIACION [$]	DEPRECIACION ACUMULADA
0	1638,32		
1	1418,8	219,5	219,5
2	1199,3	219,5	439,1
3	979,7	219,5	658,6
4	760,2	219,5	878,1
5	540,6	219,5	1097,7

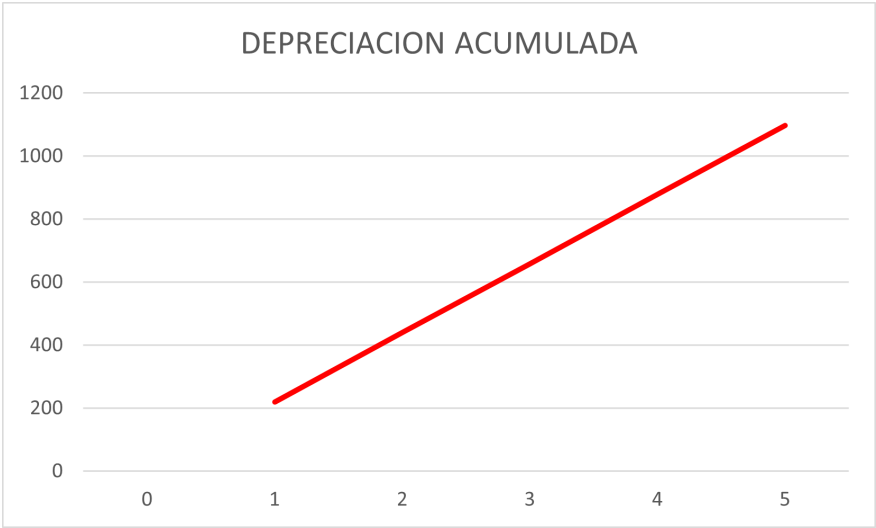


Figura 3.10: **Gráfica de depreciación acumulada**

Una vez realizados los cálculos se determina que la depreciación del prototipo es significativa. El valor residual es el producto entre el valor original y el 33% como se detalla en la ecuación 3.1, el porcentaje propuesto es de cuando un equipo de computación se deprecia cada año [30].

La depreciación fija por cinco años de vida calculada con la ecuación 3.2, este resultado se muestra en la tabla tal. Además, en la gráfica que se muestra en la Figura 3.10 se muestra la depreciación acumulada.

Para determinar el costo de venta al público del prototipo, el precio se obtiene a partir del total del costo de materiales más el coste de mano de obra. Para obtener de vuelta la inversión se escoge un margen de contribucion del 30% y así se obtiene el precio de venta al público [31].

Tabla 3.8: **Precio de valor al público**

Costo del producto	**Margen**	**PVP**
1638,32	30%	2129,816

Para que una empresa externa pueda comerciar el producto se deberá vender a un coste indicada en la Tabla 3.8. Para visualizar el beneficio que se vaya a obtener se muestra en la tabla tal.

Tabla 3.9: **Beneficios de la empresa**

Cantidad	**Costo total**	**Beneficio**
$ 50,00	$ 106.490,80	$ 24.574,80

En la Tabla 3.9 se observa el número de prototipos vendidos, el beneficio de la empresa al vender 50 productos es del 24.574,80$, lo cual ya es mucho más grande que el del precio del prototipo.

CAPÍTULO 4

4. CONCLUSIONES

Gracias a los resultados obtenidos en las pruebas de intercambio de información, se observa un aumento en la seguridad ya que en ningún momento se muestra por parte del cliente o del punto de acceso información que sea útil a terceros. Esto es gracias a que el enlace donde se transmite la información es VLC-OCC, y estos datos son imperceptibles o indescifrables al ojo humano.

Con los resultados mostrados anteriormente se observa que gracias a las tecnologías OCC y VLC en un ambiente cerrado se evitan las filtraciones de información. Además de que se consigue un ahorro de dinero del lado del cliente que no necesita un componente extra para decodificar el mensaje que envía la luminaria. También al dividir la obtención de la contraseña Wi-Fi permite que cualquier usuario que no este registrado no tenga la capacidad de conseguir la clave y así evitar escuchas en la red.

4.1 Recomendaciones

Para futuros trabajos se recomienda que el punto de acceso utilice un sensor y no un botón para iniciar el proceso de intercambio de información. Esta opción también la puede realizar la cámara del dispositivo, pero esta opción implica que la cámara este encendida todo el tiempo. Esto puede causar un recalentamiento en el sistema y un bajo rendimiento. También otra opción es cambiar los indicadores de que el proceso se cumple o no, por una pantalla LED pequeña. Otra recomendación es utilizar para el intercambio de información un LED y una fotorresistencia en el punto de acceso. Esto con el fin de bajar precios en la obtención de componentes y también dificultar más la filtración de datos. Otra posibilidad es aumentar el costo del prototipo para la obtención de pantallas y cámaras más precisas, para el intercambio de datos.

BIBLIOGRAFÍA

[1] M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce reuse in wpa2.,” *Engineering Letters*, pp. 1313–1328, 2017.

[2] S. Yoon, K. Lee, J. Cha, V. Mariappan, K. Young, D. Woo, and J. Kim, “Ieee standard for local and metropolitan area networks—part 15.7: Short-range optical wireless communications,” *IEEE Std*, pp. 1–407, 2019.

[3] D. J. Fehér and B. Sandor, “Effects of the wpa2 krack attack in real environment,” in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, pp. 000239–000242, 2018.

[4] L. E. M. Matheus, A. B. Vieira, L. F. M. Vieira, M. A. M. Vieira, and O. Gnawali, “Visible light communication: Concepts, applications and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3204–3237, 2019.

[5] N. Saha, M. S. Ifthekhar, N. T. Le, and Y. M. Jang, “Survey on optical camera communications: challenges and opportunities,” *Iet Optoelectronics*, vol. 9, no. 5, pp. 172–183, 2015.

[6] I. Strineka-Trbovic, “Internet society,” 2018. `https://www.internetsociety.org/es/issues/encryption/what-is/`, (accessed Dec. 03, 2022).

[7] Q. Li, C. Zhong, K. Zhao, X. Mei, and X. Chu, “Implementation and analysis of aes encryption on gpu,” in *2012 IEEE 14th international conference on high performance computing and communication & 2012 IEEE 9th international conference on embedded software and systems*, pp. 843–848, IEEE, 2012.

[8] E. Milanov, “The rsa algorithm,” *RSA laboratories*, pp. 1–11, 2009.

[9] J. M. Huidobro, “Código qr,” *Bit, dic.-ene*, vol. 172, pp. 47–49, 2009.

[10] K. T. Swami and A. A. Moghe, “A review of lifi technology,” in *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1–5, 2020.

[11] N. T. Le, M. Hossain, and Y. M. Jang, “A survey of design and implementation for optical camera communication,” *Signal Processing: Image Communication*, vol. 53, pp. 95–109, 2017.

[12] Z. Belghazi, N. Benamar, A. Addaim, and C. A. Kerrache, “Secure wifi-direct using key exchange for iot device-to-device communications in a smart environment,” *Future Internet*, vol. 11, no. 12, 2019.

[13] M. Bayat, M. B. Atashgah, and M. R. Aref, “A Secure and Efficient Chaotic Maps Based Authenticated Key-Exchange Protocol for Smart Grid,” *Wireless Personal Communications*, vol. 97, no. 2, pp. 2551–2579, 2017.

[14] M. Domb and G. Leshem, “Secured key distribution by concatenating optical communications and inter-device hand-held video transmission,” *Applied System Innovation*, vol. 3, no. 1, pp. 1–12, 2020.

[15] S. Sandoval-Reyes, “Text and image transmission and reception using light from leds and a light sensor,” in *International Congress of Telematics and Computing*, pp. 98–109, Springer, 2019.

[16] D.-C. Tsai, Y.-H. Chang, C.-W. Chow, Y. Liu, C.-H. Yeh, C.-W. Peng, and L.-S. Hsu, “Optical camera communication (occ) using a laser-diode coupled optical-diffusing fiber (odf) and rolling shutter image sensor,” *Opt. Express*, vol. 30, pp. 16069–16077, May 2022.

[17] C. G. Prieto Álvarez *et al.*, “Adaptación de las metodologías tradicionales cascada y espiral para la inclusión de evaluación inicial de usabilidad en el desarrollo de productos de software en méxico,” *REPOSITORIO NACIONAL CONACYT*, 2015.

[18] W. Harrington, *Learning raspbian*. Packt Publishing Ltd, 2015.

[19] “Cryptography.io,” 2013. `https://cryptography.io`,(accessed Dec. 03, 2022).

[20] “python «qrcode» 7.4.1,” 2017. https://pypi.org/project/qrcode/,(accessed Dec. 08, 2022).

[21] “Open source computer vision 4.7.0,” 2014. https://docs.opencv.org/4.x/d6/d00/tutorial_py_root.html,(accessed Dec. 08, 2022).

[22] “Barcode scanner library for android, based on the zxing decoder,” 2021. https://github.com/journeyapps/zxing-android-embedded,(accessed Dec. 12, 2022).

[23] “Android developer «camera2 overview»,” 2022. https://developer.android.com/training/camera2,(accessed Dec. 12, 2022).

[24] “github «ffmpeg for android, ios and tvos. not maintained anymore. superseded by ffmpegkit»,” 2021. https://github.com/tanersener/mobile-ffmpeg,(accessed Dec. 15, 2022).

[25] “Chaquopy python sdk for android,” 2019. https://chaquo.com/chaquopy/doc/13.0/python.html,(accessed Dec. 15, 2022).

[26] R. E. NETSIANDA, K. Ouahada, and R. Ndjiongue, “A comparative study of different modulations for visible light communications,” *University of Johannesburg Institutional Repository*, 2017.

[27] M. del trabajo, “Estructuras ocupacionales – sueldos y salarios mÍnimos sectoriales y tarifas salarios mÍnimos sectoriales 2022,” p. 951–952, 2022.

[28] I. T. Segarra, E. F. V. Núñez, and D. F. M. Pérez, “Análisis comparativo de depreciación de activos fijos con fines tributarios aplicados a la industria,” *Dominio de las Ciencias*, vol. 8, no. 1, pp. 530–543, 2022.

[29] I. M. R. Mart, B. Leland, “Economica, and m. interamericana, “ingeniería económica tema 4.1. modelos de depreciación,” p. 1–9.

[30] T. Interno, “Reglamento para la aplicación de la ley de régimen tributario interno,” *Gastos no deducibles, Art*, vol. 10, 2015.

[31] “El margen de contribución,” 2019. https://www.ionos.es/startupguide/gestion/margen-de-contribucion/,(accessed Jan. 5, 2023).

APÉNDICES

Apéndice A

MANUAL DE INSTALACIÓN

Punto de acceso y aplicación móvil

2022

Francisco Tulcán Veloz

Requerimientos del sistema

Para la instalación se debe tener en consideración unos requerimientos mínimos de hardware y software.

Requerimientos minimos de Hardware

Raspberry Pi 3 model B

- Procesador: Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- Video: HDMI
- RAM: 1 GB LPDDR2 SDRAM
- Conexiones inalámbricas: Bluetooth 4.2 BLE, Wi-Fi Dual Band b/g/n/ac
- Alimentación 5V / 2,5 A

3.5inch RPi Display

- 320×480 resolución
- Compatible con Raspberry Pi A, B, A+, B+, 2B, 3B, 3B+,4B
- Controladores proporcionados (funciona directamente con su propio Raspbian/Ubuntu)

Raspberry Pi Camera Module 2

- Interfaces de bus admitidas: CSI-2
- Máxima frecuencia de imagen captura: 30fps
- Dimensiones: 23.86 x 25 x 9mm

LEDs

- Colores: Blanco, Verde y Rojo.
- Tamaño: 5mm

Boton

Requerimientos de software

- Sistema operativo base: Raspbian buster (con version de kernel menor a 4.19)

Instalación de hardware

El sistema este compuesto por una Raspberry Pi, una cámara y una pantalla LED como se muestra en la Figura 1.

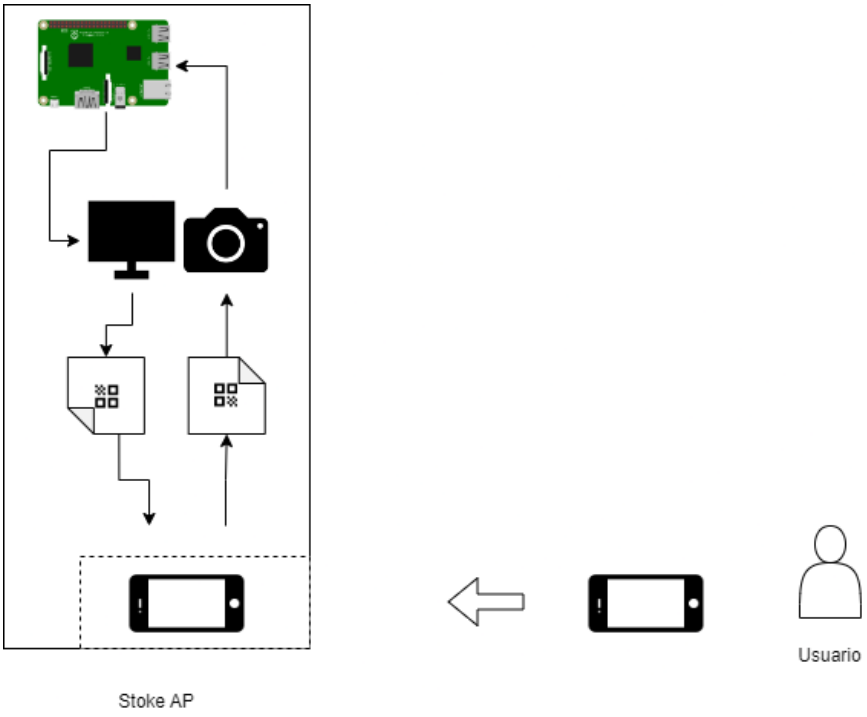


Figura 1: Vista general del sistema

La manera de conectar la cámara al microcontrolador es mediante la ranura CSI (camera serial interface: bus de serie para cámara) y para la pantalla se deben usar una serie de pines para su correcta función.

Cada pin debe estar conectado correctamente para su correcto funcionamiento la enumeración de los pines es de acuerdo con la Figura 2.

- +5v: pin2
- 0v GND: pin14
- DC: pin18
- RST: pin22
- 3.3V(TP_CS): pin26

- SCK: pin23
- MOSI: 19

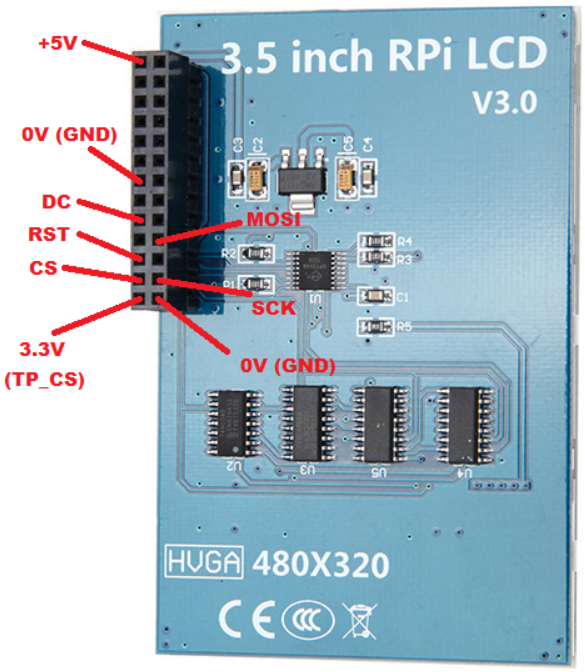


Figura 2: Puertos de la pantalla

Los LEDs son indicadores del proceso del intercambio de datos. Estos LEDs estarán situados como se aprecia en la Figura 3, el LED blanco este encendido durante el intercambio, el LED verde solo se enciende si el usuario ingresado es valido y el LED rojo solo se enciende si el usuario ingresado es invalido. Los Leds estarán conectados a los pines 7, 11 y 13 adicionalmente estos tres se conectarán a cualquier pin Ground. Finalmente se tiene el botón con el cual se iniciara el proceso de intercambio de datos y estará situado dentro del dispositivo como se aprecia en la parte baja de la Figura 4. El pin relacionado con el botón el cual recibirá la señal es el 14.

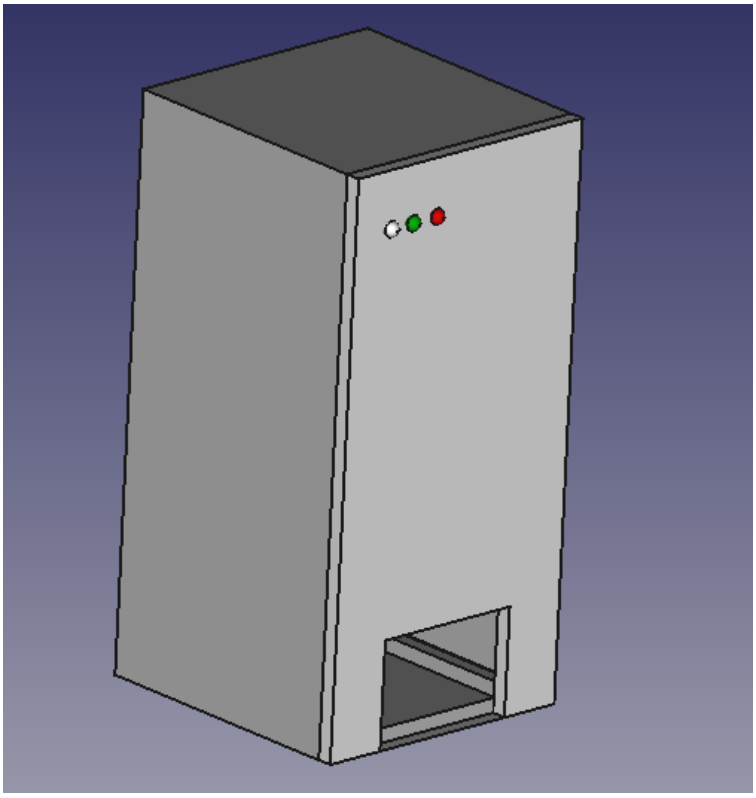


Figura 3: Punto de acceso STOKE

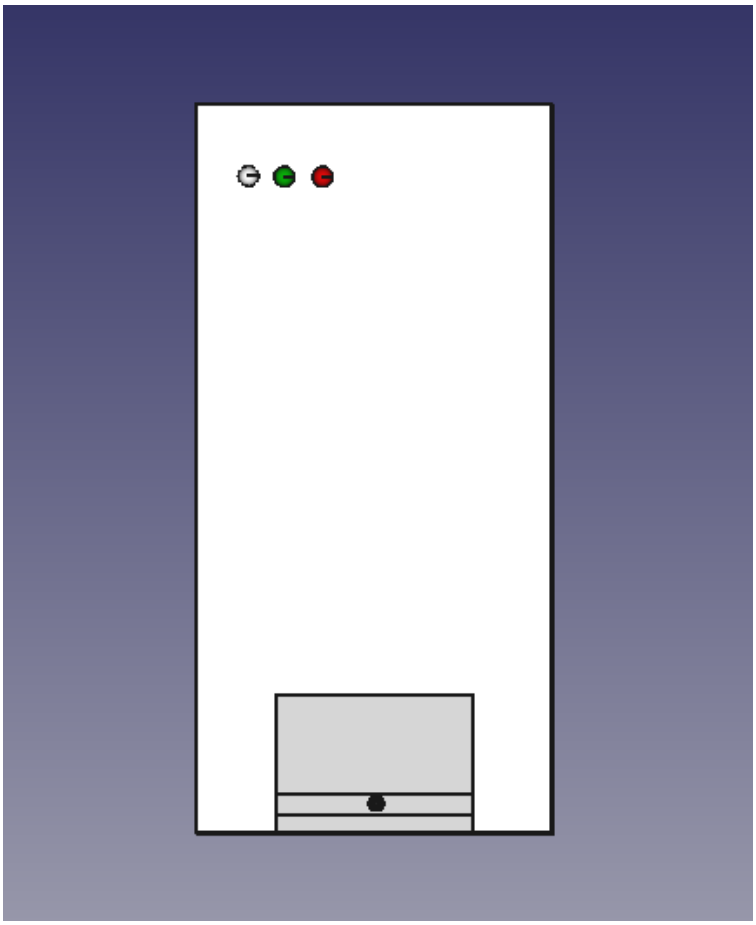


Figura 4: Punto de acceso STOKE - vista frontal

Instalación de software

El prototipo tiene un script en lenguaje Python y archivos con extensión .txt, en los archivos se almacenaran las claves recibidas y las claves que se envían, además de los usuarios validos o registrados.

El microcontrolador debe tener instalado el sistema operativo Rasbian OS versión búster y con un kernel menor o igual a 4.19. Esto se debe a que con un kernel mayor existe una incompatibilidad con la pantalla LED utilizada. Al instalar el sistema operativo se debe fijar el kernel antes de actualizar el sistema. Los siguientes comandos nos sirve para fijar el kernel:

- sudo apt-mark hold libraspberrypi-bin libraspberrypi-dev libraspberrypi-doc libraspberrypi0
- sudo apt-mark hold raspberrypi-bootloader raspberrypi-kernel raspberrypi-kernel-headers

Ya una vez fijado el kernel se procede a actualizar el sistema con los siguientes comandos:

- sudo apt-get update
- sudo apt-get upgrade

Una vez actualizado el sistema se instala las librerías necesarias para el funcionamiento del dispositivo, estas son qrcode, PIL, Python_ILI9486, Adafruit_GPIO, Adafruit_GPIO.SPI, time, OpenCV, numpy, pyzbar, sys, base64, wheel, cryptography y RPi.GPIO. Algunas de estas librerías están instaladas por defecto. Para instalar las librerías o actualizarlas a su versión más recientes se ejecutan los siguientes comandos:

- pip3 install qrcode
- pip3 install Pillow
- pip3 install wheel

- pip3 install adafruit-gpio
- pip3 install pillow
- pip3 install numpy
- pip3 install rpi.gpio
- pip3 install pyzbar
- pip3 install opencv-contrib-python
- pip3 install cryptography

Por último se debe realizar un paso extra y es descargar la librería de forma manual, es decir dirigirte a este enlace `https://github.com/ustropo/Python_ILI9486` y descargar el archivo .zip para luego extraerlo en una carpeta.
Ahora se abre la terminal y si dirige a la ubicación donde se haya extraído el archivo .zip y se ejecuta el siguiente comando:

- sudo python setup.py install

ya se tiene todo lo necesario para poder ejecutar el script main.py, ahora por último se configura el microcontrolador para ejecutar el script durante el arranque del sistema.

Apéndice B

MANUAL DE USO

Punto de acceso y aplicación móvil

2022

Francisco Tulcán Veloz

Inicio de sesión en la aplicación móvil

Cuando se abre la aplicación móvil se presenta la siguiente pantalla de inicio de sesión como se observa en la Figura 1, aquí se debe escribir el usuario y contraseña registrado en el sistema.

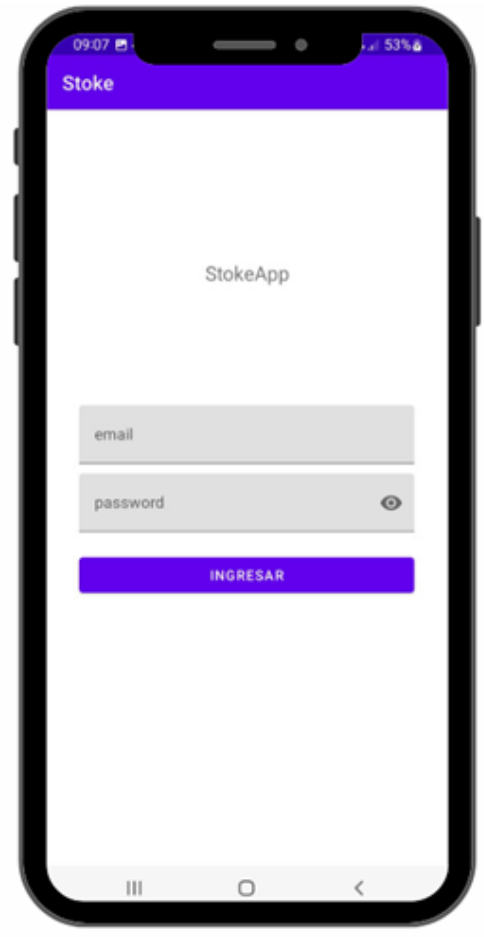


Figura 1: Pantalla de inicio de sesión

La aplicación funciona offline y se debe ser cuidadoso al ingresar los datos para no tener problemas de validación en el punto de acceso. Luego de iniciar sesión se presenta la siguiente pantalla la cual se aprecia en la Figura 2, aquí ya se puede iniciar el proceso de intercambio de datos. Primero se debe ingresar el dispositivo móvil dentro del punto de acceso sin presionar ningún botón. Ahora se debe presionar primeramente el botón iniciar de la aplicación móvil y luego presionar el botón del punto de acceso con el dispositivo móvil para así iniciar el proceso de intercambio de datos. Mientras dure el proceso de intercambio un LED indicador de color blanco estará encendido durante el intercambio.

Si el usuario es válido se iluminará el LED indicador de color verde y se continuara con el proceso, pero si el usuario es invalido se iluminará el LED indicador de color rojo y se terminara el proceso de intercambio.

Figura 2: Pantalla de inicio de intercambio de datos

En el caso de que el usuario sea invalido en la aplicación móvil se presentara un mensaje de error como se observa en la siguiente Figura 3.

Si en el caso de que se ingrese un usuario valido se puede pasar al siguiente paso. El siguiente paso es recibir una trama de símbolos mediante la cámara. Para iniciar el tercer paso se debe presionar el botón siguiente de la aplicación móvil y se presentara la siguiente Figura 4.

Figura 3: Pantalla si el usuario es invalido

Para recibir la trama se debe presionar el botón con una imagen de cámara de video como se aprecia en la figura. La trama que se recibe es enviada por medio de una luminaria VLC. La distancia máxima entre el dispositivo móvil y la luminaria es de 1m, si la distancia es mayor a esta no se recibe correctamente la trama.

Cuando se inicia el proceso de recibir la trama se puede llegar a presenciar un pequeño retraso debido a el alto procesamiento de imágenes. Luego de ese pequeño retraso si todo salió bien se presenta la clave wifi, tal y como se aprecia en la Figura 5.

Figura 4: Pantalla para recibir clave Wi-Fi

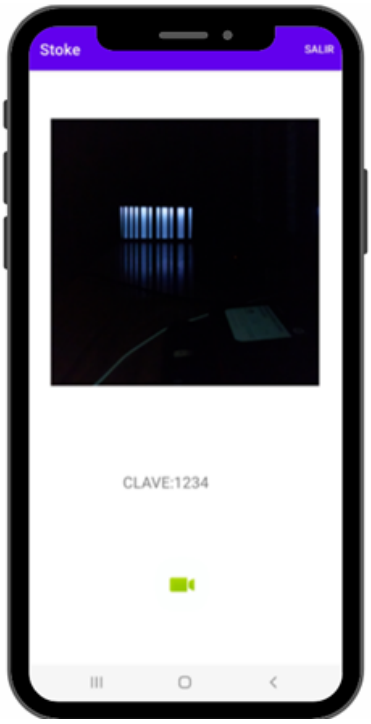


Figura 5: Pantalla al recibir clave Wi-Fi