Diseño de un Sistema de Control de Acceso Seguro Utilizando Autenticación Biométrica y Criptografía

Sebastián García Angarita, Camilo José Rueda Tello y Andrés Fernando Jerez Medina

Trabajo de grado para optar al título de
Ingeniero Electrónico

Director
Jaime Guillermo Barrero Pérez
Mag. en Potencia Eléctrica

Universidad Industrial de Santander
Facultad de Ingenierías Fisicomecánicas
Escuela de Ingeniería
Eléctrica, Electrónica y de Telecomunicaciones
Bucaramanga
2024

Dedicatoria

Yo, **Sebastián García Angarita**, dedico este proyecto a mi madre, **Yenny Patricia Angarita Barajas**, por su inmenso amor y apoyo incondicional que me han acompañado a lo largo de mi vida. Por ser una persona admirable, llena de valores y siempre comprometida con el trabajo y la familia, que me motiva a entregar lo mejor de mí y a mejorar constantemente. A mi abuela, **Maria Elisa Barajas Rojas**, por su amor y crianza durante mi niñez. Por su compañía en las madrugadas de estudio y por cada desayuno que nunca me faltó. A ambas, por mantenerme siempre en sus oraciones y por todos los sacrificios que han hecho para ayudarme a salir adelante. Agradezco a mis dos hermanos, **Maria Fernanda García Angarita** y **Camilo Andres Mantilla Angarita**, por ser siempre una compañía y un apoyo. Finalmente, a mis amigos en la carrera, por convertirse en una segunda familia. Su apoyo académico, económico y sentimental han sido fundamental en este camino. Los mejores momentos los comparto con ustedes. A todos ustedes, dedico este logro, fruto de su amor y apoyo. ¡Gracias!

Yo, **Camilo José Rueda Tello**, dedico la conclusión de este proyecto a las dos pesonas más importantes que me han acompañado a lo largo de esta carrera: mis padres Julia Lucía Tello Esparza y Remberto Pérez Urrea, quienes siempre me han brindado su apoyo, ánimo y buenos consejos cuando más lo necesito. Muchas gracias por enseñarme a sobrellevar los obstáculos que se me han atravesado y a confiar en mí mismo. A los señores Ramiro Cote e Isabela Vargas, quienes me han brindado su techo y su comida en mi estancia como foráneo en Bucaramanga. Muchas gracias por su calidad al hospedarme en su hogar.

Yo **Andrés Fernando Jerez Medina**, agradezco primeramente a la persona que más amo en mi vida, mi madre **Carmenza Medina Anaya**. Gracias por ese apoyo tan incondicional en todo este camino, por cada almuerzo que con mucho amor me envió durante estos 5 años, por todo el esfuerzo que hizo por verme salir adelante, es la principal artifice de que nunca me rindiera, de que siempre tuviera en mente hacerla sentir orgullosa y salir adelante en la vida. A mi nona y segunda madre **Carmen Rosa Anaya Rivera**, que siempre estuvo muy pendiente de mi y me tuvo en todas sus oraciones, nunca olvidaré todos los sacrificios que hicieron por mí y eso me impulsa cada día más. A ustedes dos, con quienes estaré eternamente agradecido, ¡hoy les puedo decir que lo logré!.

Agradecimientos

A nuestro director de trabajo de grado Jaime Guillermo Barrero Pérez por la orientación, sugerencias y correcciones que nos ha brindado para realizar un buen proyecto de grado.

A la Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones, a todos aquellos docentes de quienes tuvimos la oportunidad de aprender en el aula de clase y crecer profesionalmente. A los compañeros con quienes triunfamos y también fallamos, con quienes aprendimos a lo largo del proceso la importancia de la amistad y a defender la universidad pública.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Alimentación del sistema: suministro de energía eléctrica o fuente de potencia que proporciona la electricidad necesaria para el funcionamiento de un sistema.

Algoritmo criptográfico conjunto de instrucciones y operaciones matemáticas diseñadas para cifrar y descifrar datos, garantizando la seguridad y privacidad de la información transmitida o almacenada.

API una interfaz de programación de aplicaciones (API), es un conjunto de reglas definidas que permiten que diferentes aplicaciones se comuniquen entre sí. Actúa como una capa intermedia que procesa las transferencias de datos entre sistemas, permitiendo a las empresas abrir sus datos y funcionalidades de aplicaciones a desarrolladores externos, socios comerciales y departamentos internos dentro de sus empresas.

Biometría uso de características físicas, químicas o de comportamiento para establecer la identidad de un individuo.

Ciberataque intento malicioso de dañar, robar, manipular o acceder de manera no autorizada a sistemas informáticos, redes, datos o dispositivos electrónicos utilizando métodos y tecnologías cibernéticas.

Criptografía proceso de codificación y decodificación de datos mediante el cifrado para proteger su confidencialidad e integridad.

ESP32-CAM módulo basado en el microcontrolador ESP32 que integra capacidades de cámara permitiendo la captura y transmisión de imágenes y vídeo en proyectos de IoT, lo que lo convierte en una solución versátil para aplicaciones de seguridad y monitorización.

I2C “Inter-Integrated Circuit” o “circuito inter-integrado”. Protocolo de comunicación serial utilizado para permitir la transferencia de datos entre componentes electrónicos en un sistema, como microcontroladores, sensores y dispositivos periféricos.

Interfaz de usuario la capa visible de un sistema, aplicación o dispositivo que permite la interacción entre el usuario y la tecnología mediante elementos gráficos, botones y controles que facilitan la comunicación y el uso intuitivo de la plataforma.

IoT “Internet of Things” o ”Internet de las cosas”. interconexión de dispositivos y objetos físicos a través de una red, permitiéndoles recopilar y compartir datos y realizar acciones controladas por software.

PCB "Printed Circuit Board" o "Placa de Circuito Impreso". placa impresa que conecta componentes electrónicos en un sistema.

PIN de acceso secuencia alfanumérica que un usuario puede ingresar en un sistema de seguridad o autenticación para verificar su identidad y obtener acceso a una aplicación, dispositivo o área restringida.

Protocolo de comunicación conjunto de normas que permite a los dispositivos intercambiar datos de manera estructurada.

UART "Universal Asynchronous Receiver Transmitter" o "Transmisor Receptor Asíncrono Universal." protocolo de comunicación serial utilizado para permitir la transferencia de datos de forma bidireccional entre dispositivos electrónicos.

VSC "Visual Studio Code". editor de código abierto desarrollado por Microsoft que proporciona una plataforma versátil y altamente personalizable para editar y depurar código.

Resumen

Título: Diseño de un Sistema de Control de Acceso Seguro utilizando Autenticación Biométrica y Criptografía [1]

Autores: Sebastián García Angarita, Camilo José Rueda Tello, Andrés Fernando Jerez Medina[2]

Palabras Clave: control de acceso, autenticación biométrica, criptografía, comunicación encriptada, autenticación de usuario, diseño de sistema, seguridad residencial.

Descripción: El presente trabajo de investigación presenta el diseño y desarrollo de un sistema de control de acceso seguro utilizando autenticación biométrica y criptografía, con el objetivo de fortalecer la seguridad en el acceso a residencias. El sistema se basa en el reconocimiento de huellas dactilares como método de autenticación, aprovechando la unicidad y dificultad de falsificación de las huellas. Además, se implementaron algoritmos y protocolos criptográficos para garantizar una comunicación segura y privada entre los dispositivos. El sistema permite tres formas de acceso: reconocimiento de huella dactilar, PIN y acceso manual desde el interior apoyado por una cámara. Se abordaron restricciones como presupuesto, tiempo de autenticación y dimensiones del sistema, con el objetivo de ofrecer una solución de bajo costo, rápida y fácil de integrar. Se espera que este proyecto contribuya a mitigar los riesgos asociados a la vulnerabilidad de los sistemas de control de acceso, brindando mayor seguridad, privacidad y confianza a los residentes.

[1]Trabajo de grado

[2]Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Jaime Guillermo Barrero Pérez, M.Sc en Potencia Eléctrica

Abstract

Title: Design of a Secure Access Control System using Biometric Authentication and Cryptography. [3]

Authors: Sebastián García Angarita, Camilo José Rueda Tello, Andrés Fernando Jerez Medina[4]

Keywords: access control, biometric authentication, cryptography, encrypted communication, user authentication, system design, residence security.

Description: This research work presents the design and development of a secure access control system using biometric authentication and cryptography, intending to strengthen the security of access to residences. The system is based on fingerprint recognition as an authentication method, taking advantage of the uniqueness and difficulty of falsification of fingerprints. Additionally, cryptographic algorithms and protocols were implemented to ensure secure and private communication between devices. The system allows three means of access: fingerprint recognition, PIN, and manual access from the inside supported by a camera. Constraints such as budget, authentication time, and system dimensions were addressed, with the aim of offering a low-cost, fast, and easy-to-integrate solution. It is expected that this project contributes to mitigating the risks associated with the vulnerability of access control systems, providing greater security, privacy, and confidence to residents.

[3]Bachelor Thesis

[4]Faculty of Engineering Physicomechanics. School of Electrical, Electronic and Telecommunications Engineering. Advisor: Jaime Guillermo Barrero Pérez, M.Sc in Power Electronics.

Introducción

El mecanismo de acceso a las residencias es fundamental para proteger a los moradores y sus pertenencias. Tradicionalmente, se ha realizado a través de cerraduras que es un método práctico pero que presenta diversos inconvenientes y vulnerabilidades, tales como olvidar las llaves, perderlas o, peor aún, ser víctimas de un robo, lo que implica quedar por fuera de casa e incurrir en gastos adicionales para reparar o reemplazar las cerraduras. Otros sistemas similares permiten el ingreso por medio de un mando, como en el caso de la apertura de garajes; sin embargo, si no se implementan de forma adecuada, son muy vulnerables y permiten la apertura a cualquier persona que pueda simular los datos enviados por el mando Veritasium, 2018. Este problema incluso es presente en algunos modelos de carros que son vulnerables a estos ataques y permiten la apertura o manipulación de todo su sistema Mould, 2020. La problemática global en los sistemas de control de acceso radica en su fragilidad y vulnerabilidades de seguridad y privacidad, lo que expone las residencias a accesos no autorizados, robos, violaciones a la propiedad privada y la seguridad y privacidad de los residentes. Esta problemática se debe a diversas causas, incluyendo la debilidad de los métodos de autenticación tradicionales, la incapacidad de verificar de forma confiable la identidad de los residentes, el incorrecto diseño de los sistemas y la disponibilidad de tecnologías de ataque a bajo costo que incrementa aún más el riesgo de intrusiones. En respuesta a estos factores, este proyecto se enfoca en una solución específica: el uso del reconocimiento de huellas dactilares como método de autenticación y el uso de criptografía para asegurar una comunicación segura y privada del sistema.

La biometría se fundamenta en el uso de características físicas, químicas o de comportamiento para establecer la identidad de un individuo. Su relevancia radica en su efectividad para lograr una identificación precisa y confiable, en comparación con los métodos tradicionales, que se apoyan en el uso de llaves, tarjetas y contraseñas que pueden ser robadas, extraviadas, compartidas u olvidadas con facilidad; dichos métodos suponen una debilidad en términos de confiabilidad y seguridad en cualquier sistema Jain et al., 2008. Por otro lado, la criptografía es la ciencia de mantener en secreto los secretos. Funciona transformando un mensaje a través de una serie de operaciones utilizando una clave de encriptación, generando un resultado completamente diferente e incomprensible. En este sentido, la criptografía se utiliza principalmente para mantener la privacidad y seguridad de la información, asegurando que solo aquellos que posean la clave de desencriptación puedan acceder a ella. Además, permite verificar la autenticidad del mensaje y de su remitente, ya que solo quien conoce la clave de encriptación puede cifrar un mensaje de manera exitosa Delfs and Knebl, 2015.

En respuesta a estas flaquezas, el presente proyecto propone una solución que aprovecha las ventajas de la tecnología biométrica, como la unicidad de las huellas dactilares y la dificultad de falsificación. Además, el uso de protocolos criptográficos garantiza una comunicación segura y brinda protección frente a ataques no deseados. Al implementar este sistema, se espera minimizar las vulnerabilidades asociadas a la seguridad de un sistema de control de acceso. Con esta propuesta, se busca brindar una capa adicional de seguridad que dificulte el acceso no autorizado y ofrezca tranquilidad y confianza a los residentes.

1 Objetivos

1.1 Objetivo General

Diseñar un sistema de control de acceso seguro basado en reconocimiento de huellas dactilares y criptografía, con el fin de mejorar la seguridad y garantizar el acceso únicamente a las personas autorizadas en una residencia

1.2 Objetivos Específicos

- Establecer una comunicación inalámbrica segura y confiable entre los microcontroladores ESP32, asegurando la encriptación de los datos transmitidos y la implementación de un método de autenticación para prevenir ataques de repetición.

- Realizar el diseño de los subsistemas e interconexión de los mismos para trabajar en conjunto y el diseño de la PCB, optimizando el espacio y la duración de una batería de respaldo en aras de asegurar un funcionamiento continuo en caso de fallas en el suministro de energía.

- Incorporar la funcionalidad de múltiples formas de autenticación para el acceso con el fin de brindar una mayor flexibilidad. Esto se logrará mediante el reconocimiento de huella dactilar, el ingreso de un PIN a través de un teclado numérico y la inclusión de una cámara, que permitirá al residente autorizar el acceso de forma manual desde el interior.

- Diseñar una carcasa funcional y estéticamente atractiva para el sistema de control de acceso seguro, utilizando técnicas de modelado 3D y considerando los requisitos de protección de los componentes electrónicos y la facilidad de instalación en la residencia.

- Integrar y probar el sistema completo de control de acceso seguro, evaluando su funcionalidad y rendimiento mediante pruebas exhaustivas y verificando que cumpla con los requerimientos establecidos en términos de comunicación encriptada y gestión de accesos.

2 Marco teórico

2.1 Sistemas de control de acceso

Los sistemas de control de acceso comprenden un conjunto de métodos y componentes destinados a salvaguardar activos de información Solomon and Chapple, 2005. Además, se definen como el proceso mediante el cual se gestiona cada solicitud de acceso a recursos y datos mantenidos por un sistema, determinando si la misma debe ser autorizada o denegada. Esta definición se extiende igualmente a bienes y propiedades físicas, como el control de acceso a una instalación física.

2.2 Criptografía

La criptografía se refiere al conjunto de técnicas y prácticas destinadas a asegurar la comunicación y almacenamiento de información de manera segura, garantizando la confidencialidad, integridad y autenticidad de los datos. El objetivo principal es salvaguardar la información sensible frente a posibles amenazas, contribuyendo así a la creación de soluciones robustas y seguras en el ámbito de la tecnología de la información.

Supongamos que un remitente, designado como el *remitente*, desea enviar un mensaje, representado como m, de forma privada a un destinatario llamado el *destinatario*. Si este intercambio de información se lleva a cabo a través de un canal no seguro, existe el riesgo de que un intruso, referido como el *intruso*, intercepte el mensaje. En tal situación, el intruso no solo podría acceder a esta información sensible, sino también manipularla, generando un mensaje ilegítimo que el destinatario podría recibir.

La tarea fundamental y clásica de la criptografía es proporcionar confidencialidad a través de métodos de cifrado. El mensaje que se va a transmitir, ya sea texto, datos numéricos, un programa ejecutable o cualquier otro tipo de información, se denomina *texto plano*. El *remitente* cifra el texto plano m y obtiene así el texto cifrado c, el cual se transmite al *destinatario*. Para descifrar, se necesita de una clave secreta, con la cual un *intruso*, aún si intercepta el mensaje, no será capaz de descifrarlo. Cada método de cifrado proporciona un algoritmo de cifrado y un algoritmo de descifrado. En los esquemas de cifrado clásicos, ambos algoritmos dependen de la misma clave secreta, que se usa tanto para el cifrado como para el descifrado. Delfs and Knebl, 2015

2.3 AES-128

El algoritmo de encriptación AES-128, o Advanced Encryption Standard con clave de 128 bits, es una técnica altamente segura y eficiente para proteger la confidencialidad de los datos. Funciona dividiendo los datos en bloques de 128 bits y aplicándoles una

serie de operaciones matemáticas que los transforman en un texto indescifrable. La clave de cifrado, también de 128 bits, es esencial para este proceso, ya que determina cómo se realizan estas transformaciones. El algoritmo AES128 se basa en una red de sustitución-permutación (SPN) que consta de 10 rondas. En cada ronda, se realizan las siguientes operaciones:

- **División y expansión:** La clave maestra se divide en subclaves, cada una de las cuales se utiliza en una ronda específica del algoritmo para generar una "clave de ronda" que se utiliza en las operaciones.
- **Sustitución de bytes:** Cada byte del bloque de datos se reemplaza por otro byte de acuerdo con una tabla de sustitución fija.
- **Mezcla de columnas:** Los bytes de cada columna del bloque de datos se mezclan entre sí de forma no lineal.
- **Adición de la clave de ronda:** Se realiza una operación XOR entre el bloque de datos y la clave de ronda correspondiente. Su et al., 2019

Incluso con el cifrado más básico, AES-128, se estima que sería prácticamente imposible descifrarlo mediante un ataque de fuerza bruta en mil millones de millones de años. Además, al ser un algoritmo gratuito, resulta rentable y económico. Su facilidad de implementación y flexibilidad lo convierten en una solución adaptable a diversas plataformas. Por último, su rapidez en comparación con otros métodos de cifrado lo hace ideal para aplicaciones donde la velocidad es crucial.

2.3.1 Modo de operación CBC (Cipher Block Chaining)

La implementación de AES-128 en este proyecto se llevó a cabo en el modo CBC (Cipher Block Chaining), que es una de las modalidades de operación del algoritmo. En este modo, cada bloque de texto cifrado se mezcla con el bloque de texto plano anterior antes de ser cifrado. Esta técnica tiene varias ventajas significativas, entre las que se incluyen:

- **Mayor seguridad:** El modo CBC ayuda a prevenir ataques criptográficos conocidos como ataques de texto plano seleccionado y ataques de texto cifrado seleccionado, lo que aumenta la seguridad de los datos.
- **Protección contra la repetición de patrones:** Al mezclar cada bloque de texto cifrado con el bloque anterior, se evita la repetición de patrones en el texto cifrado, lo que dificulta el análisis por parte de un atacante.

- **Capacidad para cifrar datos de longitud variable:** El modo CBC permite cifrar datos de longitud variable de manera eficiente, lo que lo hace adecuado para aplicaciones donde la longitud de los datos puede variar.

Lo anterior se consigue siguiendo una serie de pasos específicos, a continuación se detalla el funcionamiento del AES-128 en modo CBC:

1. Se genera un vector de inicialización aleatorio de 128 bits, que se utiliza como primer bloque en la cadena de bloques.

2. Cada bloque de datos de 128 bits se encripta utilizando la clave de cifrado y el bloque anterior de la cadena. El resultado del cifrado se agrega a la cadena de bloques. Este proceso se repite hasta que se hayan cifrado todos los datos.

3. El receptor utiliza la clave de descifrado y el vector de inicialización para descifrar los datos. El vector se utiliza para obtener el primer bloque de la cadena, y luego se utiliza la clave de descifrado para obtener el siguiente bloque. Este proceso se repite hasta que se hayan descifrado todos los bloques. Dworkin, 2010

2.4 Biometría

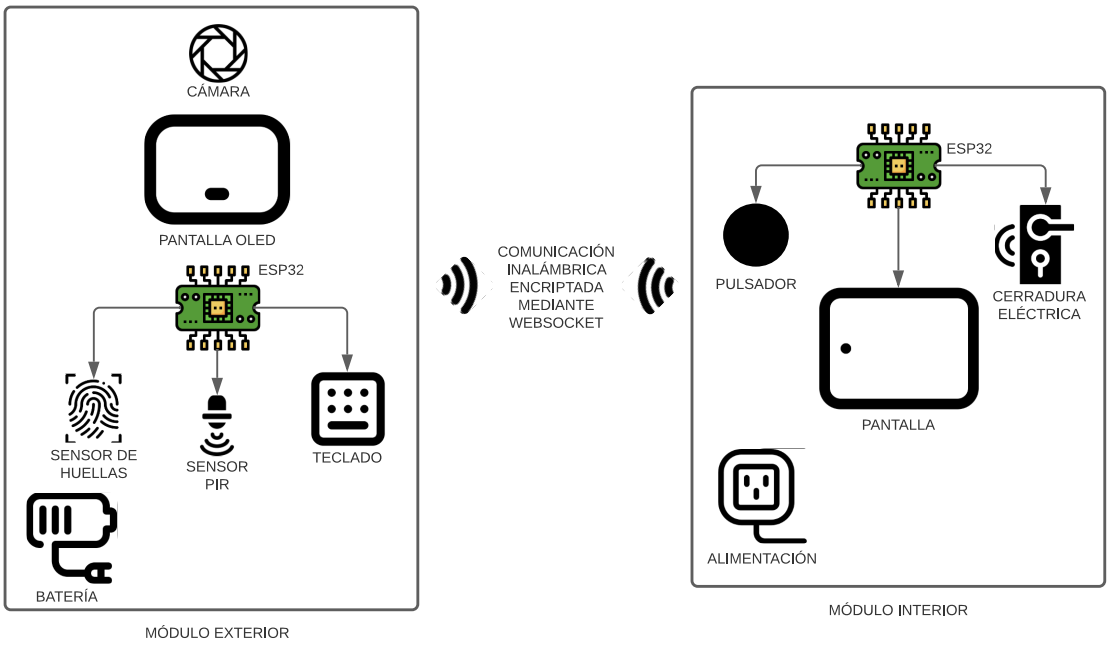
Se entiende por biometría a la ciencia que consiste en establecer la identidad de un individuo en base a sus atributos físicos, químicos o comportamientos únicos. Su relevancia radica en la creciente necesidad de implementar sistemas de gestión de identidad en una escala masiva para diversas aplicaciones cotidianas. Ejemplos frecuentes de esto incluyen compartir recursos en línea, acceder a instalaciones de alta seguridad, llevar a cabo transacciones a distancia o comprar boletos de avión de forma virtual. La biometría proporciona una solución efectiva y confiable para garantizar la identidad de los individuos en estas situaciones Jain et al., 2005

3 Descripción del sistema

3.1 Arquitectura general planteada

La arquitectura del sistema se compone de dos componentes principales: el módulo exterior y el módulo interior, los cuales trabajan en conjunto para facilitar el acceso al usuario. La denominación de estos módulos refleja su ubicación. El módulo exterior se sitúa fuera de la residencia, donde el usuario se autentica, mientras que el módulo interior está instalado dentro de la residencia y se encarga de activar la cerradura. La arquitectura del sistema se muestra más a detalle en la Figura 1

Figura 1: *Arquitectura general del sistema*



- **Módulo exterior**

  El módulo exterior, representado en la Figura 1 (izquierda), es el componente principal del sistema de control de acceso. Se encarga de la interfaz de usuario, autenticación, transmisión de vídeo y autorización de acceso. Este módulo integra una ESP32-CAM que se conecta con el sensor de huellas y el teclado numérico para la autenticación del usuario, así como con un sensor PIR y una pantalla OLED para mejorar la experiencia del usuario. Además, al operar fuera de la residencia, se alimenta con una batería.

- **Módulo interior**

El módulo interior, representado en la Figura 1 (derecha), es el encargado del accionamiento de la cerradura y recepción de vídeo. Este módulo integra una ESP32 junto con una pantalla para la visualización de vídeo. Adicionalmente tiene un pulsador para autorizar el acceso de forma manual desde el interior.

3.2 Lógica del módulo exterior

El módulo exterior, de forma paralela, inicia la conexión al módulo interior mediante una red Wi-Fi a través del protocolo Websocket, ambos instanciados en el módulo interior. Luego, la interfaz de usuario comienza de manera inmediata, ofreciendo al usuario la posibilidad de autenticarse mediante un PIN o con su huella dactilar. Si se realiza una autenticación correcta, se envía una señal de acceso de manera encriptada al módulo interior, lo que permite el accionamiento de la cerradura. Si, por el contrario, el usuario ingresa una credencial incorrecta (una huella que no está registrada o un PIN errado), se le denegará el acceso y tendrá un intento menos para acceder. Si el usuario que intenta acceder acaba con todos los intentos, entonces tendrá que esperar 30 segundos para volver a intentar. Esto se realiza con el fin de prevenir ataques de fuerza bruta para adivinar el PIN.

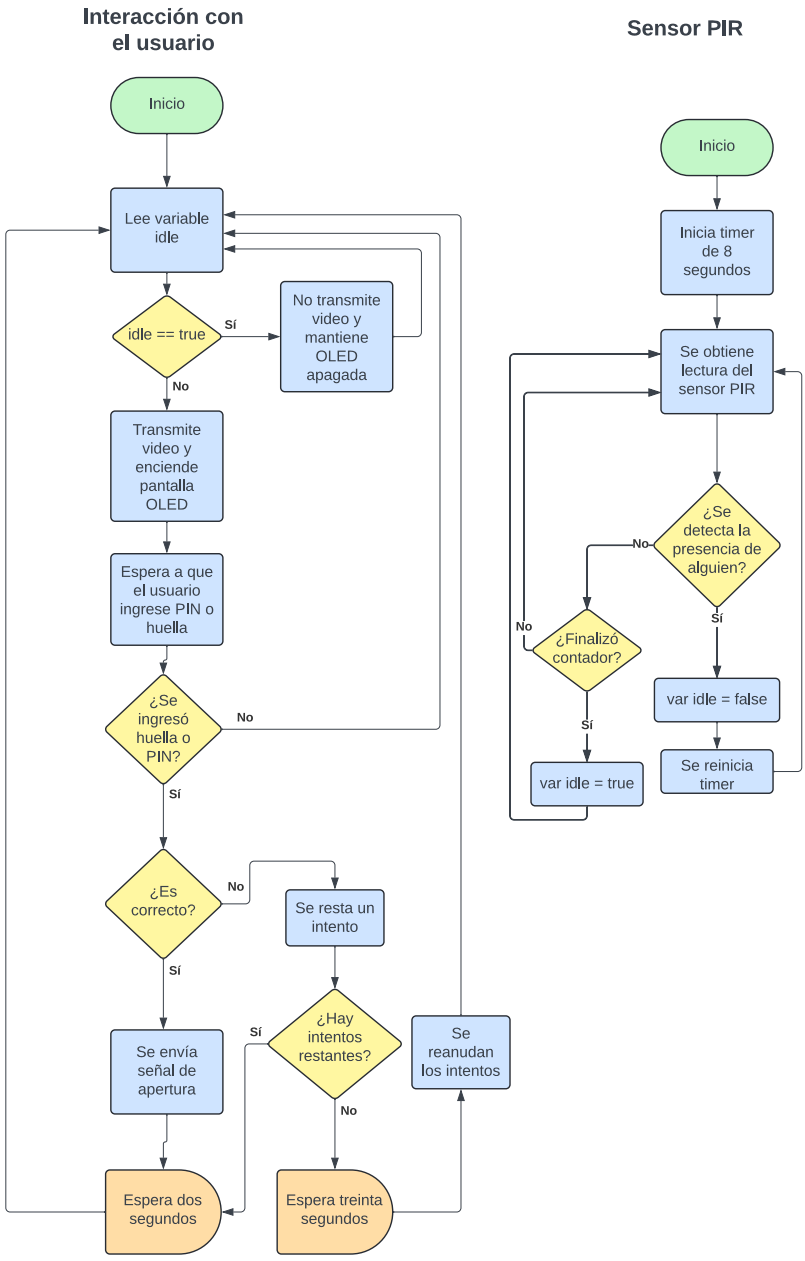
Si el sensor PIR no detecta nada durante más de 8 segundos, el módulo exterior detiene la transmisión de vídeo y apaga la pantalla oled. Esta lógica se puede detallar en el diagrama de flujo de la Figura 2.

La implementación de la lógica del módulo exterior se puede detallar en los códigos al repositorio en Github:
Interacción con el usuario: https://github.com/Sebastian-GA/SICABS/blob/main/src/sicabs_outdoor/Tasks/userInteraction/userInteraction.cpp
Transmisión de video: https://github.com/Sebastian-GA/SICABS/blob/main/src/sicabs_outdoor/Tasks/videoTransmission/videoTransmission.cpp
Sensor PIR: https://github.com/Sebastian-GA/SICABS/blob/main/src/sicabs_outdoor/Tasks/PIRSensorSleepControl/PIRSensorSleepControl.cpp

3.3 Lógica del módulo interior

Tan pronto el módulo interior es encendido, inicia una red Wi-Fi y espera a la conexión con el módulo exterior a través del protocolo Websocket. Una vez el módulo exterior se ha conectado se comienzan a proyectar las imágenes que el módulo exterior le envía. También, por este medio se pueden recibir los mensajes de apertura. Tan pronto el módulo

Figura 2: *Lógica módulo exterior*

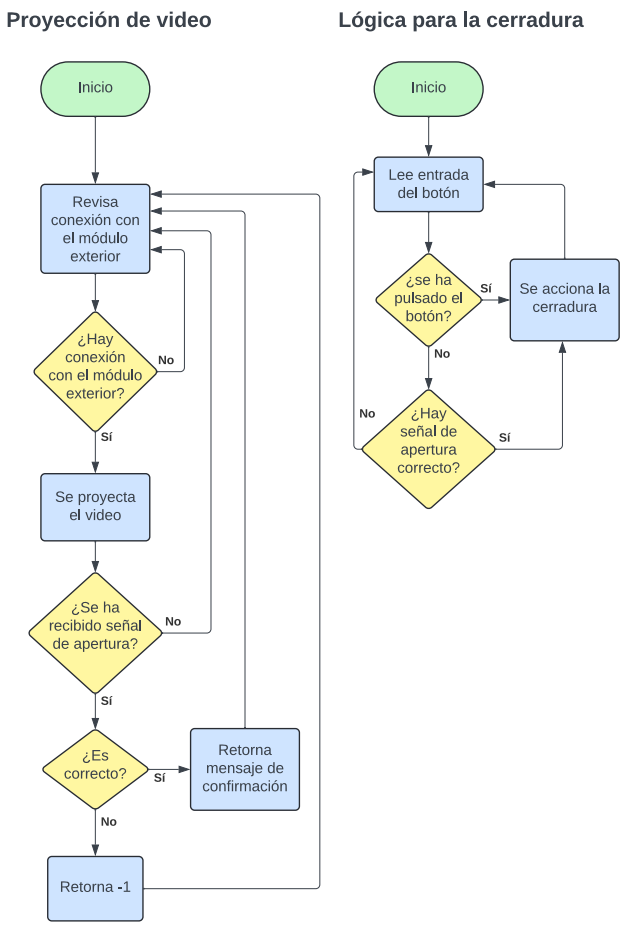


interior recibe un mensaje de apertura, éste va a mandar un mensaje de confirmación en caso de que el mensaje de apertura sea el correcto. Esta lógica se encuentra detallada en el diagrama de flujo de la Figura 3 (izquierda)

Por otro lado, la cerradura del módulo interior va a ser accionada ya sea porque se ha presionado un pulsador en el medio interior o porque se ha mandado un mensaje de apertura correcto (véase la Figura 3 a la derecha)

La implementación de la lógica del módulo interior se puede detallar en los códigos al repositorio en Github:
Proyección de video: https://github.com/Sebastian-GA/SICABS/blob/main/src/sicabs_indoor/Tasks/videoReception/videoReception.cpp
Accionamiento de la cerradura: https://github.com/Sebastian-GA/SICABS/blob/main/src/sicabs_indoor/Tasks/lockControl/lockControl.cpp

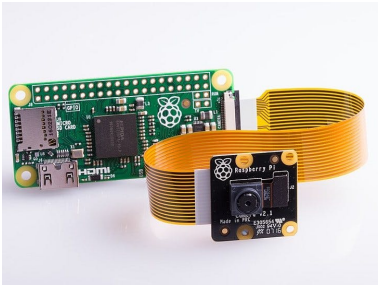
Figura 3: *Lógica módulo interior*



3.4 Dispositivos seleccionados y sus posibles alternativas

1. **Unidad de procesamiento** La selección del dispositivo para la captura de vídeo y de procesamiento se sustentó en diversos factores, abarcando consideraciones económicas, técnicas y energéticas. Se evaluaron principalmente dos opciones: la Raspberry Pi Zero W, equipada con un módulo de cámara, y la ESP32-CAM, ambas ampliamente accesibles en línea. En el cuadro comparativo de la Tabla 1, se presenta una detallada comparación entre ambas alternativas.

Figura 4: *Unidades de procesamiento preseleccionadas*



(a) Raspberry Pi Zero W

(b) ESP32-CAM

Tabla 1: *Tabla comparativa - Unidades de procesamiento preseleccionadas*

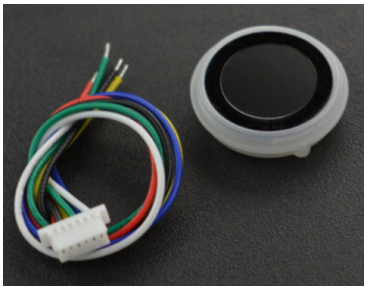
Característica	**Raspberry Pi Zero W**	**ESP32-CAM**
Tipo de dispositivo	Computadora monoplaca	Microcontrolador
Procesador	Arm11 (Arm v6) BCM2835	XtensaLX6
Número de nucleos	1	2
Tecnología	32-bit	32-bit
Frecuencia	1 GHz	240 MHz
Memoria RAM	512 MB	512 MB
GPIO pins	26	10
Cámara	Módulo externo	Incorporada
Wi-Fi	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11b/g/n/e/i
Bluetooth	Bt 4.1, BLE	Bt 4.2, BLE
Sistema Operativo	Raspbian / Linux	FreeRTOS
Consumo de Energía	∼1.15 W	∼0.9 W
Dimensiones	65 mm x 30 mm	27 mm x 40 mm
Precio	$ 130.000 COP	$ 40.000 COP

Entre las dos opciones consideradas, se seleccionó la **ESP32-CAM** por varias razones. En primer lugar, su procesador potente y su arquitectura de doble núcleo con sistema operativo FreeRTOS permiten ejecutar tareas en paralelo, característica usada para la transmisión de vídeo (véase el siguiente enlace en donde se muestra la creación de estas tareas: https://github.com/Sebastian-GA/SICABS/blob/main/

src/sicabs_outdoor/main.cpp). Además, al tratarse de un microcontrolador y no de un ordenador, ofrece una solución menos compleja en comparación con la Raspberry Pi Zero W. En segundo lugar, su cámara integrada y su menor tamaño proporcionan un diseño compacto y eliminan la necesidad de módulos externos. Por último, su bajo consumo energético y su precio son aspectos clave que satisfacen los requisitos del proyecto.

2. **Sensor de huellas** Para el sensor de huellas se evaluaron las siguientes alternativas: SFM-V1.7 y el AS608.

Figura 5: *Sensores de huellas preseleccionados*



(a) SFM-V1.7

(b) AS608

Tabla 2: *Tabla comparativa - Sensores preseleccionados*

Característica	**SFM-V1.7**	**AS608**
Tipo de sensor	Capacitivo	Óptico
Voltaje de Alimentación	3.3 V	3.6 a 6.0 V
Corriente de Funcionamiento	60mA max	120mA max
Interfaz	UART	UART TTL
Capacidad de Almacenamiento	80 huellas	162 huellas
Dimensiones	∅ 21mm x 6mm	48 x 23.5 x 20mm
Tiempo de Adquisición	300 - 400ms	< 1 s
Precio	$50.000 COP	$70.000 COP

Entre los sensores se seleccionó el sensor de huellas SFM-V1.7 por su apariencia y tamaño reducido que permiten diseñar un sistema más compacto. Adicionalmente, es una opción más económica y de menor consumo lo que lo convierte en la mejor alternativa para satisfacer las restricciones del proyecto.

3. **Pantalla** Para la visualización del vídeo transmitido desde el módulo exterior, se evaluaron alternativas preseleccionadas con el objetivo de determinar la pantalla más adecuada. Entre estas opciones se encuentran las pantallas capacitivas Sunton ESP32-S3 y la Nextion NX8048P070-011C.

Figura 6: *Pantallas preseleccionadas*

(a) Sunton ESP32-S3

(b) Nextion NX8048P070-011C

Tabla 3: *Tabla comparativa - Pantallas preseleccionadas*

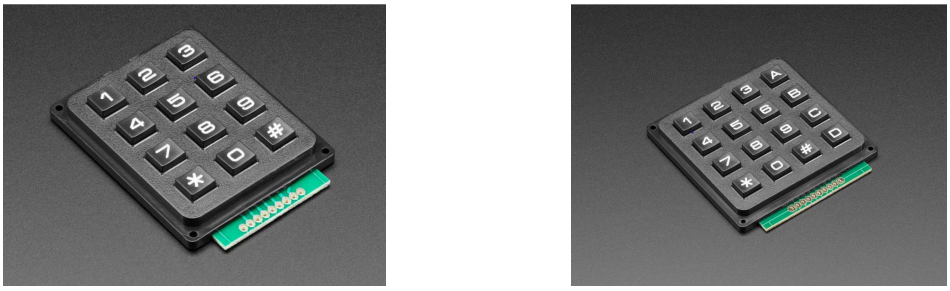
Característica	**Sunton ESP32-S3**	**Nextion NX8048P070-011C**
Tamaño	7.0”	7.0”
Resolución	800*480	800*480
Panel	Capacitivo (CTP)	Capacitivo (CTP)
Área de pantalla efectiva	153.84x85.63[mm]	154.08×85.92[mm]
Voltaje de operación	5V	5V
Consumo	500 mA	430 mA
Flash	16 MB	128 MB
Precio	$150.000 COP	$400.000 COP

La evaluación de las alternativas preseleccionadas para la visualización del video desde el módulo exterior condujo a la elección de la pantalla Sunton ESP32-S3. Esta decisión se basa en que, en términos generales, esta pantalla cumple adecuadamente con los requisitos del proyecto. Además, la considerable diferencia de precios entre la Sunton ESP32-S3 y la Nextion NX8048P070-011C hace que la primera sea una opción más conveniente para este proyecto de bajo costo, sin comprometer la funcionalidad y calidad visual necesarias.

4. **Teclado numérico** Se consideraron dos opciones viables de teclados numéricos para que los usuarios ingresen su PIN: uno con disposición 4x3 y otro con disposición 4x4.

   Dado que la relevancia del acceso mediante PIN no es crucial para el proyecto, se optó por la opción más simple y económica, representada por el teclado de 4x3. Además, la elección de un teclado más compacto implica una ocupación menor de espacio en la carcasa, contribuyendo así a alcanzar el objetivo de diseñar un

Figura 7: *Teclados preseleccionados*



(a) Teclado 4x3 (b) Teclado 4x4

dispositivo con dimensiones reducidas.

Además, debido a la limitada cantidad de pines disponibles en la ESP32-CAM, se optó por utilizar un módulo expansor de pines. Específicamente, se empleó el módulo PCF8574, comúnmente utilizado para convertir una pantalla LCD serial a I2C. De esta manera, se pueden utilizar solo dos pines para controlar el teclado, los cuales también pueden ser empleados para conectar otros periféricos I2C, como una pequeña pantalla OLED.

5. **Sensor de presencia** Para la detección de presencia de un usuario, se evaluaron las siguientes opciones para el sensor de movimiento: el SR602 (ver Figura 8a) y el SR501 (ver Figura 8b).

Figura 8: *Sensores de presencia preseleccionados*

(a) Sensor SR602 (b) Sensor SR501

En este contexto, ambas alternativas satisfacen eficazmente los requisitos fundamentales para el funcionamiento del sistema. No obstante, se seleccionó el sensor SR602 por varias razones clave: Su diseño más compacto en comparación con el SR501 lo hace ideal para aplicaciones con limitaciones de espacio. Además, el SR602 exhibe un consumo de energía inferior, haciéndolo especialmente idóneo para aplicaciones que requieren eficiencia energética y costos reducidos. Finalmente, su precio más

bajo en comparación con el SR501 lo posiciona como una opción más asequible para llevar a cabo este proyecto.

3.5 Protocolo de comunicación

Se evaluaron tres alternativas principales para la comunicación entre los microcontroladores: ESP-NOW, UDP y TCP.

ESP-NOW es un protocolo de comunicación desarrollado por Espressif, el mismo fabricante de los microcontroladores ESP32. Destaca por su simplicidad, bajo consumo y diseño para aplicaciones IoT. Además, es seguro, dado que utiliza el protocolo CCMP para encriptar la comunicación con dos llaves (PMK y LMK) de 128 bits "ESP-NOW - ESP32 - ESP-IDF Programming Guide latest documentation", 2024. Sin embargo, ESP-NOW limita el tamaño máximo de datos a 250 bytes por paquete, dificultando la transmisión de vídeo al requerir la división de las imágenes en múltiples paquetes, afectando la velocidad y complejidad del proceso.

Por esta razón, se optó por establecer la comunicación a través de Wi-Fi, red generada por la ESP32. Para la transmisión de vídeo, se consideraron los protocolos UDP y TCP. UDP es un protocolo más veloz, ofreciendo una mayor fluidez de vídeo, aunque no asegura la recepción de paquetes, lo que resultó en cortes o glitches en el vídeo. Por otro lado, TCP garantiza la recepción de los paquetes, aunque es ligeramente más lento, sin embargo, se seleccionó esta opción por ofrecer una mejor estabilidad de imagen sacrificando un poco los fotogramas por segundo.

Finalmente, se implementó la comunicación utilizando un servidor Websockets en el módulo interior, que espera constantemente los fotogramas enviados por el módulo exterior. Debido a limitaciones en las librerías disponibles, la comunicación del servidor Websockets opera a través de HTTP en lugar de HTTPS, lo que no garantiza la seguridad de la comunicación. Por esta razón, se agregó una capa de encriptación antes del envío de los datos para garantizar la seguridad del proceso. Además, no habría el inconveniente de utilizar HTTP sin certificado, ya que el protocolo solamente se usará para el intercambio de datos y no para el uso de páginas web.

3.6 Algoritmo de encriptación y código rotativo

Los mensajes de apertura enviados al módulo interior son críticos en la implementación del sistema y requieren una atención especial para garantizar la seguridad. Para lograr esto, se emplea el algoritmo de encriptación AES-128, para asegurar una comunicación segura por HTTP.

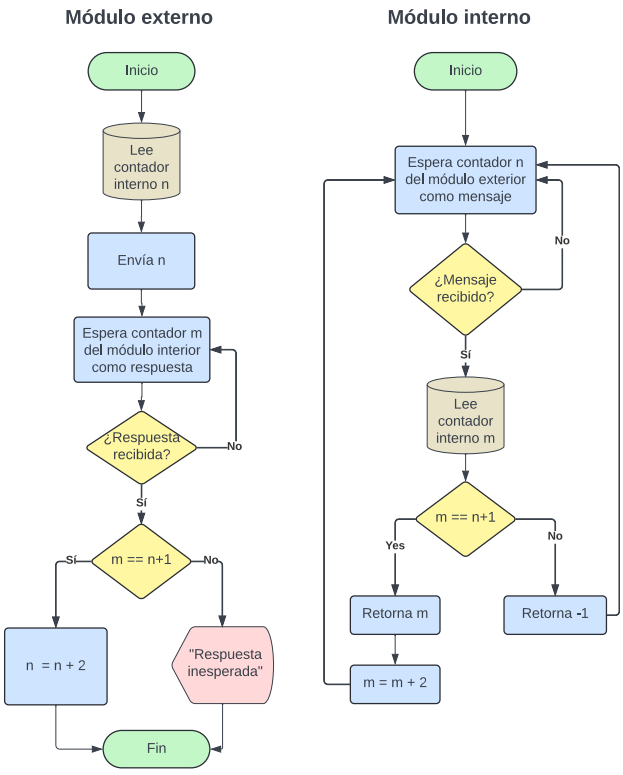
Para asegurar que los mensajes de apertura sean únicos en cada ocasión, se imple-

mentó un sistema de código rotativo. Este sistema genera una clave diferente en cada transmisión, utilizando un contador que se incrementa secuencialmente. Aunque este proceso puede parecer simple, la encriptación convierte estos números secuenciales en mensajes de caracteres aleatorios, evitando la detección de patrones repetitivos.

El funcionamiento del código rotativo es el siguiente: cada módulo almacena en su memoria flash un contador. El módulo interior mantiene su contador igual al del módulo exterior más uno. Cuando se envía un mensaje de apertura, se transmite el valor del contador del módulo exterior. Al recibir este valor, el módulo interior verifica que coincida con su contador actual menos uno. Si la verificación es exitosa, se activa la cerradura y se envía como respuesta el contador interno del módulo interior, que luego se incrementa en dos unidades. Por su parte, el módulo exterior verifica que el valor recibido de vuelta sea igual a su contador interno más uno. Si la verificación es exitosa, el contador interno del módulo exterior también se incrementa en dos unidades. Este doble proceso de verificación asegura la sincronización de los contadores entre los módulos en caso de interrupciones en la comunicación.

Estas medidas de seguridad garantizan un intercambio de mensajes seguro entre los módulos interior y exterior, reduciendo la posibilidad de intrusión debido a patrones repetitivos. La lógica detallada de esta implementación se encuentra representada en los diagramas de flujo de la Figura 9.

Figura 9: *Lógica del código rotativo*



4 Implementación

4.1 Etapa de pruebas

Durante las primeras etapas del proyecto, se llevaron a cabo diversas pruebas para evaluar el funcionamiento de cada periférico. Además, dado debido al limitado número de pines disponibles en la ESP32-CAM, la asignación de cada uno se determinó después de realizar varias pruebas y considerar las funcionalidades de cada pin.

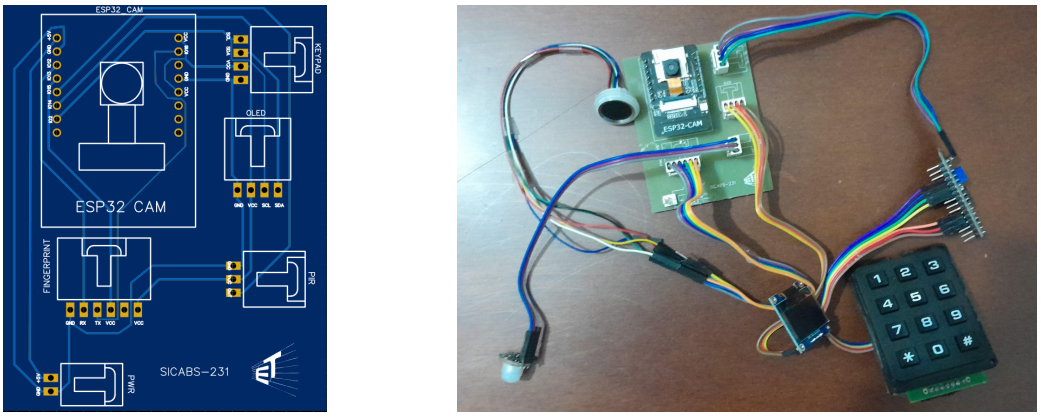
Asimismo, se implementaron los diagramas de flujo previamente explicados sobre la lógica de los módulos. El desarrollo del código se realizó aprovechando las ventajas de FreeRTOS y los dos núcleos de las ESP32. Esto permitió que la interfaz de usuario y el manejo de sensores se llevaran a cabo de manera paralela a la transmisión de vídeo, garantizando así una mayor fluidez en la transmisión.

El código desarrollado y la evolución del proyecto se puede acceder en el repositorio de GitHub del proyecto: https://github.com/Sebastian-GA/SICABS .

4.2 Diseño de PCB y carcasa 3D

El esquema de conexiones del módulo exterior es bastante simple, consistiendo en la interconexión de los distintos periféricos a la ESP32-CAM, tal como se refleja en el Apéndice B. Sin embargo, a pesar de su aparente simplicidad, se presentaron problemas con la estabilidad de las conexiones durante la etapa inicial. No obstante, tras enviar el diseño de la PCB para su fabricación, muchos de estos problemas se resolvieron. Además, esto permitió lograr conexiones más compactas y robustas, mejorando significativamente la fiabilidad del sistema.

Figura 10: *Diseño final de la PCB*



(a) Diseño de la PCB (b) Montaje en la PCB impresa

Además, se diseñaron y mandaron a imprimir carcasas para cada módulo, lo que re-

sultó en un sistema más compacto y estéticamente agradable, proporcionando protección a los circuitos contra elementos externos. El diseño del módulo exterior se hizo respetando la restricción establecida sobre el tamaño máximo. El diseño final del sistema se muestra en la Figura 11.

Figura 11: *Implementación solución propuesta*

(a) Módulo exterior

(b) Módulo interior

4.3 Presupuesto del proyecto

En la Tabla 4 se pueden observar los costos aproximados para el desarrollo del proyecto. Este presupuesto no tiene en cuenta algunas variantes, como la cerradura eléctrica, cuyo costo puede variar significativamente dependiendo del tipo de instalación y de las necesidades específicas. En nuestra implementación, la cerradura fue simulada con un diodo LED para indicar la señal de control cuando esta se desbloquea.

Tabla 4: *Presupuesto general del proyecto*

Descripción	**Cantidad**	**Precio unitario**	**Subtotal**
ESP32-CAM	1	$ 40.000	$ 40.000
Sensor SFM-V1.7	1	$ 50.000	$ 50.000
Pantalla Sunton ESP32-S3	1	$ 150.000	$ 150.000
Teclado numérico	1	$ 8.000	$ 8.000
Módulo adaptador I2C	1	$ 5.000	$ 5.000
Sensor PIR	1	$ 4.000	$ 4.000
Pantalla OLED	1	$ 8.000	$ 8.000
Batería 18650	2	$ 15.000	$ 30.000
Impresión PCB	1	$ 42.000	$ 42.000
Impresión 3D	1	$ 80.000	$ 80.000
Otros	1	$ 50.000	$ 50.000
	Total		$ 467.000

5 Análisis de resultados

Para comprobar el correcto funcionamiento del sistema, primero se realizaron pruebas con la interfaz de usuario, la cual se puede encontrar en el apéndice F.

Luego, se corroboró el funcionamiento del código rotativo capturando imágenes del monitor serial de la ESP32 del módulo interior, como se verá a continuación.

5.1 Encriptación en la memoria interna y autenticación exitosa

En este caso en particular, el contador inicia en 201, y la versión encriptada resalta que el contador no está guardado como un entero, sino como texto plano, que es justamente el que se muestra en la Figura 12.

Figura 12: *Estado inicial del módulo interior*

```
Build:Mar 27 2021
rst:0x1 (POWERON),boot:0x2a (SPI_FAST_FLASH_BOOT)
SPIWP:0xee
mode:DIO, clock div:1
load:0x3fce3808,len:0x44c
load:0x403c9700,len:0xbe4
load:0x403cc700,len:0x2a68
entry 0x403c98d4
[   264][I][esp32-hal-psram.c:96] psramInit(): PSRAM enabled

---SICABS Indoor---

The counter has the value of: 201
And encrypted it looks like: b9UZ0BBvTP8SzUp+0rFvSA==
```

Posteriormente, el módulo interior recibe un mensaje de apertura por parte del módulo exterior, el cual, en este caso, representa el número 200. Como es justamente el número que se espera, entonces el módulo interior manda como respuesta de confirmación el contador interno (Figura 13). Cabe resaltar que el número 201 que se mandó encriptado es totalmente distinto al mismo número encriptado en la memoria interna. Esto garantiza que si un atacante accede a la memoria interna, le sea imposible usar ese mismo mensaje encriptado para obtener acceso.

Figura 13: *Recepción de mensaje de apertura*

```
Mensaje recibido: IR6woN9jY26SPJmlci1GLA==

Es el mensaje de apertura esperado!
Se envió de vuelta el siguiente mensaje: F3r6M02GpzODRP9vItkeAw==
Que equivale al número: 201

Contador interno estaba en: 201
Ahora se ha incrementado a: 203
```

5.2 Autenticación denegada

Si un atacante usara el mismo mensaje de apertura anterior, código de la Figura 13, no le sería posible ingresar, ya que este número representa el 200, y el número que ahora espera el módulo interior es el 202. Esto se puede detallar en la Figura 14

Figura 14: *Autenticación denegada*

```
Mensaje recibido: IR6woN9jY26SPJmlci1GLA==
Mensaje de apertura incorrecto.
```

En cambio, si el usuario ahora ingresa con el siguiente mensaje de apertura correspondiente, se le podrá dar acceso, tal y como se evidencia en la Figura 15

Figura 15: *Recepción de siguiente mensaje de apertura*

```
Mensaje recibido: O5DqeKK7Zg/pyzUXVNtbzw==

Es el mensaje de apertura esperado!
Se envió de vuelta el siguiente mensaje: CLchk/YJk1C1tvYSKCf9oA==
Que equivale al número: 203

Contador interno estaba en: 203
Ahora se ha incrementado a: 205
```

5.3 Reinicio del sistema

En caso de que el sistema se reinicie debido a, por ejemplo, un fallo en la alimentación del sistema, los valores almacenados en los contadores seguirán siendo los mismos, tal y como se evidencia en la Figura 16

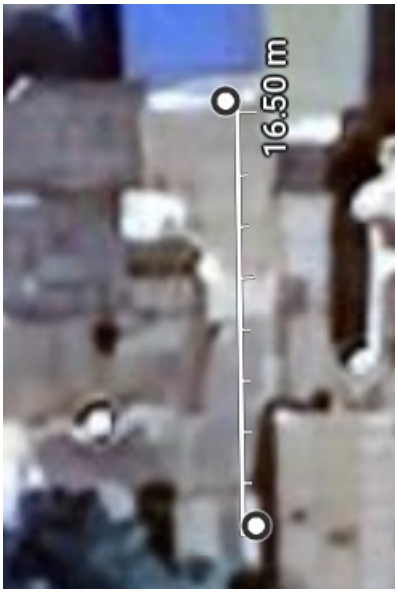
Figura 16: *Reinicio del sistema*

```
ESP-ROM:esp32s3-20210327
Build:Mar 27 2021
rst:0x1 (POWERON),boot:0x2a (SPI_FAST_FLASH_BOOT)
SPIWP:0xee
mode:DIO, clock div:1
load:0x3fce3808,len:0x44c
load:0x403c9700,len:0xbe4
load:0x403cc700,len:0x2a68
entry 0x403c98d4
[   264][I][esp32-hal-psram.c:96] psramInit(): PSRAM enabled

---SICABS Indoor---

The counter has the value of: 205
And encrypted it looks like: 1dGQ83qr99kZKstrKVxDNA==
```

5.4 Máxima distancia de conexión

Para determinar la distancia máxima entre ambos módulos mientras mantienen una conexión, se consideró como referencia la cobertura típica de los productos 11N de TP-Link en el canal de 2.4 GHz, la cual se estima en aproximadamente 20 metros "General questions about Wi-Fi range of TP-Link wireless product — tp-link.com", 2021. Inicialmente se intentó establecer la conexión a esta distancia, pero no se logró. Por lo tanto, se redujo gradualmente la distancia entre los módulos hasta que se establecer la conexión. Finalmente, se logró la conexión a una distancia de 16.5 metros con línea de visión directa. La distancia calculada se puede observar en la Figura 17.

Figura 17: *Distancia máxima de conexión entre los módulos interior y exterior*



5.5 Calidad de imagen

En la Figura 18 se puede evidenciar la calidad de la imagen transmitida hacia el módulo interior, en donde sí es posible distinguir qué persona se encuentra afuera.

Figura 18: *Proyección de video transmitido*

5.6 Consumo por parte del módulo exterior

Las baterías brindan un voltaje de 7.74 [V], tal y como se evidencia en la Figura 19

Figura 19: *Voltaje suministrado al módulo exterior*

Para ese voltaje suministrado, el módulo exterior completo (con transmisión de video y encendiendo el color del sensor de huellas) nos da un consumo de corriente de 150 [mA], tal y como se evidencia en la Figura 20

Figura 20: *Corriente consumida por el módulo exterior*

6 Conclusiones

Al hacer uso del protocolo WebSocket para la transmisión de video, se establece una comunicación sólida entre los módulos del sistema, lo que permite enviar imágenes con una latencia muy baja y con una buena distancia de funcionamiento. Además, con el uso del algoritmo AES-128 la comunicación no solo es rápida, sino también confiable; cada mensaje de apertura es único, lo que lo hace resistente a ataques de repetición. Estos mensaje de apertura están encriptados, lo que los hace ininteligibles para cualquier atacante, impidiendo que reconozcan un patrón. Además, cabe destacar que este sistema permite una comunicación efectiva a larga distancia, alcanzando hasta 16 metros entre los dispositivos.

Se logró el diseño detallado de cada subsistema, consiguiendo cumplir exitosamente con el requerimiento de las dimensiones predefinidas de 160x80 *mm*. Esto utilizando el software de diseño gratuito Onshape, con el que se diseñaron las carcasas específicas para cada módulo, que luego fueron fabricadas mediante impresión 3D con material PLA, garantizando un equilibrio óptimo entre resistencia y peso, y también haciendo el sistema más estético. Posteriormente, se desarrolló una placa de circuito impreso (PCB) compacta, optimizando el espacio mediante terminales de conexión en lugar de soldaduras directas.

Se implementaron múltiples formas de autenticación, incluyendo reconocimiento de huella dactilar, ingreso de PIN mediante teclado numérico y autorización manual a través de un botón ubicado en el módulo interior, proporcionando así una mayor flexibilidad en el acceso.

La integración y prueba exhaustiva del sistema completo de control de acceso seguro fue satisfactoria, confirmando el cumplimiento de los requerimientos establecidos en términos de comunicación encriptada y gestión de accesos. Las pruebas incluyeron diversos escenarios, como reconocimiento de huellas, ingreso de PIN, suspensión automática, apertura manual de la cerradura, verificación del código rotativo y manejo de intentos fallidos de acceso. Estos tests validaron la funcionalidad y el rendimiento del sistema, demostrando su eficacia para garantizar un acceso seguro. La documentación de estas pruebas, respaldada con materiales audiovisuales, se encuentra disponible en el repositorio adjunto para consulta adicional.

7 Recomendaciones

Para garantizar el correcto uso del sistema de control de acceso diseñado y cumplir con los objetivos del proyecto, es fundamental tener en cuenta los siguiente:

- Leer detenidamente el ***Apéndice D. Manual de usuario***, donde se detallan las dos formas de autenticación disponibles y se describen todos los posibles escenarios en el funcionamiento del sistema. Familiarizarse con esta información facilitará el uso adecuado del sistema y la comprensión de su funcionamiento.

- Al emplear el lector de huellas dactilares, asegúrese de colocar el dedo correctamente sobre el sensor y mantenerlo presionado hasta que se complete la lectura. Esto asegurará una lectura precisa y exitosa, disminuyendo los errores en la autenticación.

- Para garantizar un funcionamiento óptimo del sistema, se recomienda instalarlo a una altura que permita un ángulo de visión adecuado para la ESP32-CAM pero que también sea de fácil acceso para colocar la huella y el PIN de acceso. Se recomienda una distancia al suelo de aproximadamente 1.3m. Esto garantizará una buena visibilidad desde el módulo interior y facilitará el proceso de autenticación.

8 Trabajo futuro

Los resultados finales del proyecto son funcionales y cumplen con los objetivos establecidos inicialmente, sin embargo, es importante reconocer que existen oportunidades significativas de mejora en cuanto a seguridad y funcionalidad del sistema.

En primer lugar, sería interesante emplear el sensor PIR para gestionar la activación del modo de reposo en la ESP32-CAM y en la pantalla. De esta manera, mientras el sensor PIR no detecte actividad, el sistema entrará en un estado de bajo consumo de energía, conocido como deep sleep. Cuando el sensor PIR detecte movimiento, activará el sistema. Esto podría no solo optimizar el rendimiento del sistema, sino que también prolongar la duración de la batería de manera significativa.

Aunque la comunicación es segura utilizando el algoritmo AES-128, la librería utilizada para este propósito no aprovecha las capacidades del acelerador de hardware integrado en la ESP32 para realizar operaciones criptográficas. Por lo tanto, al mejorar este aspecto y usar una librería que aproveche esta característica de la ESP32, podríamos obtener mejoras en el rendimiento del sistema y en la velocidad de transmisión.

La implementación del código rotativo garantiza un mensaje de apertura diferente para cada ocasión, lo que evita ataques de repetición. Sin embargo, sería interesante explorar métodos más complejos, como contraseñas de un solo uso (OTP, por sus siglas en inglés), que varíen cada ciertos segundos.

Actualmente, la cámara solo cumple la función de informar a los residentes del interior quién está en la puerta. Sería beneficioso añadir la capacidad de registrar el ingreso de las personas y almacenar esta información en una base de datos para tener un registro del acceso, incluida la hora de ingreso.

Por último, una característica que podría implementarse es mejorar la interfaz de usuario y permitir el registro de nuevos usuarios desde el módulo interior sin necesidad de modificar el código y compilar un nuevo programa.

Referencias Bibliográficas

Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications*. Springer Berlin Heidelberg.

Dworkin, M. (2010, 2010-01-18). Recommendation for block cipher modes of operation: The xts-aes mode for confidentiality on storage devices. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904691

ESP-NOW - ESP32 - ESP-IDF Programming Guide latest documentation [Accessed: 2024-4-8]. (2024).

General questions about Wi-Fi range of TP-Link wireless product — tp-link.com [[Accessed 08-04-2024]]. (2021).

Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2008). *Handbook of biometrics*. Springer US.

Jain, A. K., Ross, A., & Uludag, U. (2005). Biometric template security: Challenges and solutions. *2005 13th European signal processing conference*, 1–4.

Mould, S. (2020, December). I hacked into my own car.

Solomon, M. G., & Chapple, M. (2005). *Information security illuminated*. Jones; Bartlett.

Su, N., Zhang, Y., & Li, M. (2019). Research on data encryption standard based on aes algorithm in internet of things environment. *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2071–2075. https://doi.org/10.1109/ITNEC.2019.8729488

Veritasium. (2018, September). This toy can open any garage. https://www.youtube.com/watch?v=CNodxp9Jy4A

Apéndices

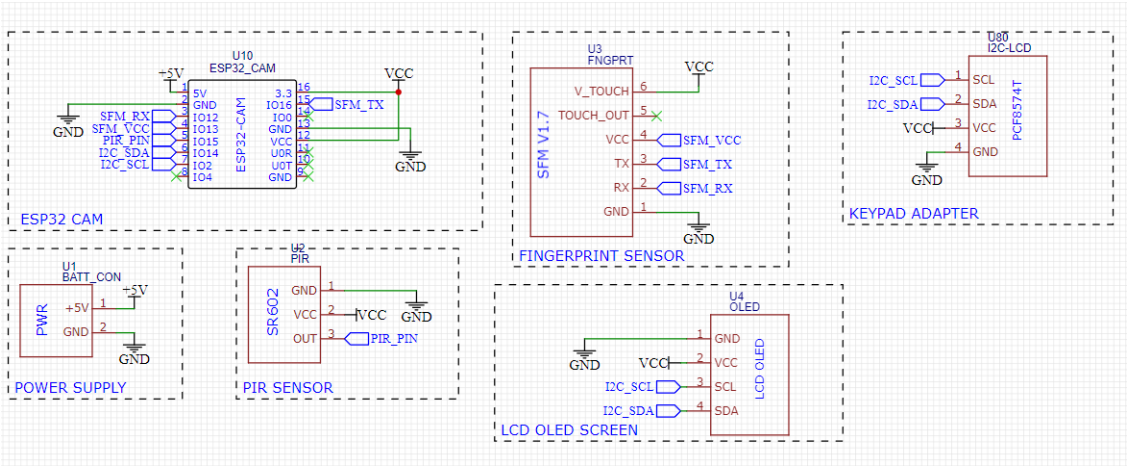
Apéndice A. Repositorio general del proyecto - GitHub

Link: https://github.com/Sebastian-GA/SICABS

Apéndice B. Diseño de la PCB

La creación de la Placa de Circuito Impreso (PCB) se basó en las interconexiones delineadas en el esquemático que se aprecia en detalle en la Figura 21.

Figura 21: *Placa del circuito impreso - Esquemático*



Las imágenes del modelo 2D y 3D de la PCB, al igual que su impresión y su correspondiente archivo Gerber, se encuentran en el siguiente link al repositorio: https://github.com/Sebastian-GA/SICABS/tree/main/hardware/pcb/sicabs_outdoor

Apéndice C. Diseño de las carcasas

Para el diseño de los modelos 3D de las carcasas del sistema, se empleó el software *Onshape*. En los siguientes links al repositorio se tienen tanto imágenes como PDF y archivos STL de las carcasas.

Módulo exterior: https://github.com/Sebastian-GA/SICABS/tree/main/hardware/3d/sicabs_outdoor

Módulo interior: https://github.com/Sebastian-GA/SICABS/tree/main/hardware/3d/sicabs_indoor

Apéndice D. Manual de usuario

En el siguiente link se tiene una descripción detallada del funcionamiento del sistema con posibles escenarios: https://github.com/Sebastian-GA/SICABS/blob/main/docs/README.md

Apéndice E. Página web del trabajo de investigación

Link: https://sites.google.com/e3t.uis.edu.co/SICABS-231

Apéndice F. Enlace al vídeo demostrativo del sistema

Link: https://www.youtube.com/watch?v=bxLjJRd5Bi4

Apéndice G. Librerías auxiliares

- **Sensor de huellas:** https://github.com/Matrixchung/SFM-V1.7
- **Teclado numérico:** https://github.com/joeyoung/arduino_keypads/tree/master/Keypad_I2C
- **Sensor PIR (implementación propia):** https://github.com/Sebastian-GA/SICABS/blob/ab6960c51c8ef7a7a24b0c6fd47bdd0b704af879/src/sicabs_outdoor/Tasks/PIRSensorSleepCo
PIRSensorSleepControl.cpp
- **Pantalla OLED:**
  - https://github.com/adafruit/Adafruit-GFX-Library
  - https://github.com/adafruit/Adafruit_SSD1306
- **Cámara:** https://github.com/espressif/esp32-camera/blob/master/driver/include/esp_camera.h
- **Wi-Fi:** https://github.com/arduino-libraries/WiFi
- **Websockets:** https://github.com/gilmaimon/ArduinoWebsockets
- **Renderizado de imágenes JPG:** https://github.com/Bodmer/TJpg_Decoder

Apéndice H. Hojas de datos

Link: https://github.com/Sebastian-GA/SICABS/tree/main/datasheets