Sistemas inteligentes aplicados a la seguridad de objetos en locales, utilizando tecnologías IoT y biométrica para el monitoreo y la gestión de alarmas

Hernán Darío Montenegro Zambrano

Universidad Mariana

Facultad De Ingeniería

Ingeniería Mecatrónica

San Juan De Pasto

2024

Sistemas inteligentes aplicados a la seguridad de objetos en locales, utilizando tecnologías IoT y biométrica para el monitoreo y la gestión de alarmas

Hernán Darío Montenegro Zambrano
Autor

Jorge Andrés Chamorro Enríquez
Ingeniero Electrónico

Asesor

Universidad Mariana
Facultad De Ingeniería
Ingeniería Mecatrónica
San Juan De Pasto
2024

-

Artículo 71: Los conceptos, afirmaciones y opiniones emitidas en el Trabajo de Grado son responsabilidad única y exclusiva de los educandos. Reglamento de Investigaciones,2007 y Publicaciones Universidad Mariana

Agradecimientos

Quiero expresar mi más sincero agradecimiento al Ingeniero Jorge Chamorro, cuya orientación experta, conocimiento y dedicación fueron fundamentales en el desarrollo de este trabajo. Sus comentarios asertivos y su apoyo constante me guiaron a lo largo de este proceso . También deseo agradecer a la Universidad Mariana, por brindarme la oportunidad de realizar este trabajo de investigación y por su compromiso con la excelencia académica. Agradezco especialmente al programa de ingeniería Mecatrónica, por su constante apoyo y por proporcionar un entorno propicio para el aprendizaje y la investigación. Estoy profundamente agradecido por la educación de calidad que he recibido aquí y por el impacto positivo que ha tenido en mi desarrollo profesional y personal.

Dedicatoria

A Dios, por su guía y fortaleza durante todo el proceso de este proyecto. A mi madre, por su amor incondicional, apoyo inquebrantable y constante inspiración, A Jader Gordillo por su amistad, aliento y compañía en cada paso del camino. Sin su apoyo, este logro no habría sido posible.

Contenido

Índice de tablas

Índice de Figuras

Introducción

En este trabajo se planea corroborar como los sistemas de seguridad con tecnología IoT y la incorporación de sistemas de acceso biométrico logran brindar mayor seguridad, para esto se desarrollarlo un sistema de placas modular con módulos intercambiables que le permitirán actualizar y adaptar el sistema a la necesidad del usuario. Los sistemas biométricos jugaran una parte importante debido a que estos sistemas permiten aumentar la seguridad en la activación y desactivación del sistema, como primera capa de seguridad el sistema cuenta con un control inalámbrico que trabaja mediante dirección MAC mucho más difícil de clonar para no dejar vulnerable el sistema.

cómo se incorpora la tecnología IoT al sistema se requiere de un servidor que en este caso se integrara un servidor web propio, lo que permite que el sistema tenga una comunicación más eficaz y en tiempo real donde el usuario puede estar en interacción con el sistema en cualquier momento, esta interacción y monitoreo se realizara desde el aplicativo en este caso una página web.

1. Resumen del proyecto

El proyecto aborda la investigación en sistemas de seguridad para mitigar la inseguridad en la ciudad de San Juan de Pasto, con un enfoque especial en locales comerciales. Se desarrolla un sistema que utiliza tecnología IoT y permite actualizaciones mediante módulos diversos, como Modulo de multiplexación, Modulo de actuadores, acceso biométrico y control Inalámbrico. EL módulo de multiplexación soporta la conexión de múltiples sensores, incluidos los magnéticos para puertas y ventanas, y sensores de movimiento PIR, con la capacidad de conectar hasta 32 sensores cableados según los requisitos de seguridad específicos.

Para la transmisión de datos a través de Internet, se implementa un servidor propio dedicado al sistema de seguridad. Este enfoque garantiza una comunicación eficiente entre el sistema y el usuario, quien puede monitorear la seguridad desde una página web. El sistema recopila información de los sensores y otros periféricos, como dispositivos de acceso biométrico, y la envía al servidor a través de Internet mediante Wi-Fi o cable UTP. Además, en ausencia de conexión a Internet, el sistema tiene la capacidad de enviar mensajes de texto al usuario para informar sobre eventos importantes, asegurando una notificación inmediata en situaciones críticas.

1.1. Descripción del problema

En San Juan de Pasto, según el Plan Integral de Seguridad y Convivencia Ciudadana, los robos a establecimientos comerciales ocurren principalmente cuando los delincuentes acceden a locales o bodegas estando cerrados al público, generalmente mediante violación o forcejeo de cerraduras. Aunque se observa una disminución en los casos de robo, pasando de 714 casos en 2017 a 504 en 2019 (Rachman, 2020)., la cifra sigue siendo significativa y requiere medidas preventivas.

Los propietarios de pequeños y grandes negocios se ven obligados a proteger sus bienes, optando por tecnologías de seguridad como los sistemas de alarmas. Aunque estos sistemas son funcionales, presentan deficiencias en cuanto al monitoreo en tiempo real. Además, su desventaja económica radica en la posibilidad de que el sistema no cumpla con los requisitos necesarios, lo

que puede requerir su reemplazo completo, generando costos adicionales y pérdidas por la eliminación del sistema anterior.

A pesar de la disponibilidad de sistemas de seguridad económicos en el mercado, muchas personas carecen de la habilidad técnica para instalarlos, lo que las lleva a contratar servicios de empresas especializadas. Esto eleva el costo total del sistema y deja a algunos comerciantes sin recursos para proteger sus locales, dejándolos vulnerables a posibles robos.

1.1. Justificación

para mejorar la seguridad en locales comerciales a través de sistemas de seguridad tecnológicos radica en la necesidad de proporcionar a los usuarios una sensación de protección hacia sus bienes materiales mediante la interacción constante con el sistema. Esto se logra implementando sistemas vanguardistas que utilicen tecnología IoT para monitorear los establecimientos en tiempo real.

Aunque existen varios sistemas de seguridad en el mercado, se busca ofrecer una solución diferenciada en la ciudad de San Juan de Pasto mediante la implementación de una placa de circuitos modular. Esta característica permitirá realizar actualizaciones de hardware según las necesidades del usuario, lo que resultará en ahorros económicos al evitar la sustitución completa de la tarjeta de control al incorporar nuevos periféricos.

El enfoque modular del sistema de seguridad permitirá la conexión de diversos dispositivos, como sensores de huella, cámaras para reconocimiento facial, micrófonos para reconocimiento de voz y controles RF, lo que aumentará la seguridad en la activación y desactivación del sistema.

A pesar de la disponibilidad de sistemas IoT en el mercado, la dependencia de servidores de terceros puede ocasionar retrasos en la comunicación de datos con las aplicaciones móviles, además de vulnerabilidades en caso de falla del servidor. Por ello, se opta por implementar un servidor web en una Raspberry Pi para garantizar una comunicación eficiente entre los dispositivos y aplicativos móviles, así como para asegurar una respuesta rápida ante eventualidades.

Además, se contempla la posibilidad de comunicación alternativa mediante mensajes de texto o llamadas telefónicas en caso de pérdida de conexión a internet, lo que garantiza una notificación inmediata al propietario en situaciones de emergencia.

1.2. Objetivos

1.2.1. Objetivo general

Desarrollar un sistema de seguridad inteligente y modular basado en tecnología IoT con servidor que permita el monitoreo y control mediante un aplicativo móvil para brindar seguridad en locales comerciales.

1.2.2. Objetivos específicos

- Obtener un sistema de hardware modular que integre la conexión de distintas tecnologías como la tecnología IoT, sensores biométricos, y canales que permitan la conexión de sensores. para el monitoreo y control de parámetros de seguridad en locales comerciales. este sistema debe presentar una autonomía no menor a 20 horas respaldado por una UPS para mantener el sistema funcionando en corte de energía eléctrica.

- Integrar un servidor web utilizando principalmente una *Raspberry pi* para la recepción y procesamiento de datos de los sistemas de seguridad con una interface amigable con el usuario.

- integrar el sistema de hardware con el servidor IoT que permita él envió de datos obtenidos de los parámetros de seguridad para el monitoreo y control del sistema de seguridad a través de internet.

1.3. Marco teórico y conceptual

1.3.1. Servidor

Un servidor es aquel que se encarga de recibir y transmitir información por un sistema de redes denominado internet, cuando un usuario ingresas a un servidor este recibir y trasmite información para determinar que mostrarles a los usuarios.

Un servidor está compuesto por hardware y software que trabajan en conjunto, en otras palabras es una computadora que se encarga de recibir y trasmitir datos, pero estos datos deben recibirse y trasmitirse de alguna parte por esta razón todos los dispositivos conectados a internet tiene asignada una dirección IP única e irrepetible, cuando un dispositivo solicita información a un servidor el IP este sería el remitente y el IP del servidor seria el destinatario, el servidor procesa la solicitud y envía la respuesta al solicitante que ahora vendría siendo el destinatario y el servidor el remitente, esto sucede cada vez que se navega en internet aunque a simple vista no se note, cada vez que se busca algo en internet la información que se muestra proviene de algún servidor Gustavo, B., Por, B. V., & Por, D. A. (2018, agosto 31).

Los servidores son necesarios debido a que en ellos se almacena la mayor parte de información de internet si estos no existieran la red global no sería tan grande como se lo conoce hoy en día, pero los servidores no solo cumplen con guardar la información, sino que esto están constantemente recibiendo y respondiendo solicitudes de los usuarios.(*¿Qué Son Los Servidores Web y Por Qué Son Necesarios? - Duplika*, n.d.)

1.3.2. Servidor web

El servidor web es el software que se ejecuta en la máquina, este software se encarga de administrar los recursos de la maquina como es lectura y escritura de la información en las unidades de almacenamiento, además de recibir y responder las solicitudes de los clientes, este proceso influye directamente en el uso de los recursos del hosting, debido a que entre más usuarios realicen solicitudes simultáneamente al servidor este requiere del uso de ms recursos.

estos softwares tienen una estructura de comunicación cliente servidor, la comunicación entre el cliente y el servidor se realiza por medio del protocolo de comunicación HTTP o su variante cifrada HTTPS, cuando el servidor recibe una petición se comienza a ejecutar una serie de pasos. Axarnet. (s. f.). ¿Cómo funciona un servidor web?【Características】. https://axarnet.es/blog/como-funciona-servidor

1.3.3. Tipos de servidor web

cómo se ha mencionado antes servidor web es denominado al software o sistema operativo del servidor físico, por lo que en la actualidad existen una gran variedad con diferentes características solo se mencionara los más destacados.

1.3.3.1. **Apache.** es el software más popular debido a que es gratuito y de código abierto lo que le permite ejecutarse en casi cualquier sistema operativo, se comunica mediante el protocolo HTTP, este servidor web fue lanzado hace aproximadamente 20 años y en la actualidad el 46% de los sitios web utilizan este servidor**.**

1.3.3.2. **Nginx.** es un servidor web que ha ido ganando fama en los últimos años siendo utilizado por el 26% de los servidores web en el mundo, este servidor es de código abierto y gratuito, aunque también cuenta con versión paga de uso comercial, su mayor ventaja es su alto rendimiento y su poco uso de memoria

1.4.3.3. **Microsoft IIS.** Es un servidor web propio de Microsoft que viene específicamente para el sistema operativo de Windows por lo que su mayor ventaja es ser compatible con la mayoría de tecnologías disponibles de Microsoft, pero su mayor desventaja se da en cuanto a compatibilidad con otras tecnologías distintas a las de su fabricante.

1.4.3.4. **Lite speed.** Es un servidor moderno caracterizado por soportar grandes cargas de trabajo y responder con eficacia, una de sus mayores ventajas aparte de ser robusto y eficaz, es su protocolo de comunicación HTTP/3 lo que le garantiza ser un servidor seguro, aunque para hacer uso de este software se debe pagar una licencia.

1.3.4. Tecnología IoT

IoT o internet de las cosas se describe como la red de objetos cotidianos, como electrodomésticos hasta maquinas industriales que tienen la capacidad de conectarse a internet para compartir información del dispositivo por este medio, esto permite que se pueda controlar desde la maquina más sofisticada hasta el dispositivo más sencillo desde cualquier lugar del mundo. Wigmore, I. (2021, abril 7).

1.3.5. Dispositivos IoT

Un dispositivo IoT es aquel dispositivo con acceso a internet, hoy en día es raro no encontrar un dispositivo con conexión a internet, estos dispositivos permiten al usuario gestionar, monitorear y contralar en tiempo real desde una acción básica como prender un bombillo hasta un proceso industrial completo, existen una gran variedad de dispositivos IoT que tienen características dependientes de su uso pero en este ocasión se hablara de los controladores capaces de conectarse a internet, hay un gran variedad con diferentes propiedades, para los controladores que no cuenta con conexión a internet en la actualidad existen módulos que se conectan al controlador por medio de algún protocolo de comunicación como lo es SPI, I2C, RS232 para darle conexión a internet.

Los controladores más conocidos y populares que tienen acceso a internet por medio de WIFI son: ESP32, ESP8266 estos ya vienen con la conexión wifi incorporada, en cuanto a módulos que permiten conexión a internet se tienen: modulo ethernet w5500, enc28j60.

1.3.6. ESP32

Es un microcontrolador que tiene como característica principal su bajo consumo, su alimentación es 3.3 voltios cuenta con conexión bluetooth y Wifi, tiene dos núcleos esta es una virtud que tiene este microcontrolador en comparativa con otros microcontroladores, fue creado y desarrollado por la empresa *Espressif System*, es el sucesor de la ESP8266 estos microcontroladores pueden ser programados en el IDE de Arduino esto quiere decir que son *Open Source*.

1.3.7. ESP8266

Este microcontrolador es el antecesor de la ESP32 es la evolución de los ESP más antiguos y fueron el inicio de los controladores con conexión wifi, esp8266 cuenta con un solo núcleo es su procesador y conexión Wifi y bluetooth, fue creado y desarrollado por la empresa *Espressif System*.

1.3.8. Modulo ethernet w5500

Este módulo de internet cuenta con un puerto RJ45 lo que permite una comunicación a internet por medio cable, cuenta también con una interface TCP/IP lo que le facilita la conexión a internet, sus voltaje de alimentación esta entre 3.3v a 5v este módulo es compatible con controladores que cuenten con comunicación SPI, aunque para algunos controladores como Arduino ya cuenta con librerías que facilitan la programación del mismo, pero en el caso de controladores que no cuentan con una librería se debe realizar una programación más extensa, además de tener un conocimiento amplio acerca del funcionamiento de este módulo.

1.3.9. Enc28j60

El módulo ENC28J60 es un módulo que permite conectar los microcontroladores a la red de internet, este módulo cuenta con un puerto RJ45 para conexión por medio de cable al enrutador, cuenta con hardware específico para el cálculo de las sumas de control, su alimentación esta entre 3.3v a 5v es compatible con controladores que tenga comunicación SPI este módulo a diferencia del w5500 cuenta con librerías para la mayoría de controladores lo que permite que sea más sencilla su utilización con casi cualquier controlador.

1.3.10. Plataformas IoT

Una plataforma IoT es la encargar de gestionar la recolección y la trasmisión de datos a los usuarios, estas plataformas cuentan con interfaces de visualización que le permiten al usuario observas los datos gráficamente, interna mente cuenta con un software que gestiona los dispositivos a los cuales se les enviara información, además de tener un hardware que es capaz de procesar esta información en otras palabras las plataformas IoT trabajan con un servidor web.

1.3.11. Raspberry pi

Raspberry pi es un ordenador de tamaño reducido capaz de interactuar con pantallas como lo son televisores o periféricos como mouse o teclado, este mini ordenador es tan pequeño que alcanza en la palma de la mano, fue diseño para ser un ordenar asequible por los usuarios por lo que se lo consigue por un bajo costo, funciona igual que un ordenador de escritorio, se puede desarrollar proyectos electrónicos ya que cuenta con pines disponibles como un microcontrolador

Como se ha mencionado anteriormente raspberry pi es mini ordenador por lo que cuenta con puertos USB, una entrada para la alimentación de voltaje, salida de audio y video, además de contar con una CPU que varía sus especificaciones dependiendo del modelo, cuenta con memoria RAM y un puerto para memoria SD.

Se sabe que todo computador para funcionar necesita de un sistema operativo que en este caso raspberry pi cuenta con un sistema operativo propio, este sistema se debe grabar en la memoria SD para posteriormente ejecutarlo en la raspberry pi. Solé, R. (2021, julio 18)

1.3.12. Sistemas de seguridad

Un sistema de seguridad es un conjunto de elementos que se entre conecta entre sí, estos pueden ser sensores, actuadores etc. estos elementos interconectados tienen el objetivo de brindar seguridad y protección ante un evento que pueda afectar la integridad de una persona o ya sea un bien material. (2021, junio 14). Verisure.pe.

1.3.13. Tipos de sistemas de seguridad

Existen una gran variedad de sistemas de seguridad desarrollados con distintos propósitos y necesidades, hay sistemas de seguridad enfocados en el área de seguridad de la integridad física de las personas estos sistemas cuentan sensores que pueden medir los signos vitales de las personas y advertir si se encuentra en riesgo la salud y poder dar una solución temprana.

En esta área también se encuentra la parte de protección física en caso de algún accidente, estos sistemas cuentan con sensores que analizan el entorno donde se encuentran ubicadas las personas y determina si pueden estar en peligro y así poder evitar o al menos activar un sistema de protección que garantice la integridad fisca de las personas, un ejemplo claro de esto es el sistema de airbag de los vehículos que cuentan con un sensor de impacto que al activarse infla las bolsas de aire para proteger a las personas en una colisión.

También hay sistemas de seguridad enfocados en proteger los bienes materiales de las personas estos tipos de sistemas son capaces de detectar intrusos en un establecimiento o vehículos, estos sistemas al ser activados por medio de la detención de un intruso pueden alertar al propietario por medio de una sirena, cabe aclarar que también existen sistemas silenciosos que pueden ser activados de forma manual en caso de que la persona se sienta que su seguridad ha sido vulnerada y el sistema se comunica ya sea con la policía o con una persona de confianza que pueda brindar seguridad.

1.3.14. Sensores para sistemas de seguridad

Estos sistemas para poder funcionar necesitan de sensores que recolecten información para que el sistema pueda analizar los datos y dependiendo de esto pueda tomar una decisión.

Hay una gran variedad de sensores que son utilizados en los sistemas de seguridad como lo son los sensores PIR, sensores magnéticos, sensores tipo switch, sensores de impacto etc.

1.3.15. Sensor PIR

Los sensores PIR reaccionan al cambio de energía en un entorno, su principal componente es un sensor piroeléctrico, este sensor fue diseñado para detectar los cambios de radiación infrarroja, esta radiación pasa por un lente Fresnel, este lente se encarga de dividir la zona protegida por sectores, una vez se detecta una cambio de radiación infrarroja se genera una pequeña señal, que es amplificada y procesada por los circuitos internos del sensor para determinar si se ha detectado un cambio de radiación.

Cuando se energiza estos sensores estos empiezan a acostumbrase a sus entorno, como se sabe que este sensor detecta radiación infrarroja y todo objeto que irradie temperatura tiene radiación infrarroja, lo que hace este sensor es detectar por un lapso de tiempo la radiación infrarroja del entorno y cuando no detecta cambios de radiación mantiene su relé de salida desactivado en el caso de ser un sensor normalmente abierto y activado en el caso de ser un sensor normalmente cerrado, como se mencionó anterior mente el lente Fresnel divide por zonas el área protegida esto ayuda a que el lente logre ser más sensible al cambio de radiación infrarroja. (s/f). Netatmo.com.

1.3.16. Sensor magnético mecánico

El sensor magnético mecánico no se basa en el efecto hall sino en algo más simple como lo es un interruptor encapsulado con dos terminales de material ferromagnético esto quiere decir que es conductor y posee propiedades magnéticas, se denomina un sensor mecánico debido a que no necesita de un circuito electrónico para su funcionamiento si no de movimiento mecánico, este movimiento mecánico se produce al acercar un imán al sensor haciendo que los terminales ferromagnéticos hagan contacto entre si permitiendo así el paso de corriente atrás vez de ellos, estos sensores dependiendo de la configuración que tenga pueden ser normalmente abiertos o normalmente cerrado.

Este tipo de control son utilizados en los sistemas de seguridad con el fin de realizar la activación y desactivación del sistema como primera capa de acceso los controles que se utilizan actualmente son los RF a 433mhz los cuales son de un solo canal por lo que requieren de un trasmisor y un receptor.

1.3.17. Sensor de huella dactilar

El sensor de huella digital es capaz de proteger un sistema mediante el análisis de imágenes de huella digital, estos sensores se basan en el procesamiento de imágenes este dispositivo captura imágenes de las huella dactilares y realiza la comparación con la base de datos interna y valida la similitud de con las huellas ya registradas por lo que este sensor es capaz de volver más seguro casi

cualquier sistema, el protocolo de comunicación de esto sensores se realiza mediante comunicación serial lo que hace sea compatible con casi cualquier controlador o tarjeta de desarrollo. (Lector De Huella Digital Arduino : 7 Steps (with Pictures) - Instructables, n.d.)

1.4. Marco de antecedentes

1.4.1. Bases de datos y criterios de búsqueda

Tabla 1

Base de datos y criterios de búsqueda

Criterios de búsqueda	System alarm IOT
Periodo de búsqueda	2016 - 2021
Número de documentos encontrados sin filtros	8
Idioma	Solo artículos en ingles
Filtro por área temática	Computación Ingeniería
Tipo de documentos	Artículos
Número de documentos encontrados sin filtros	12

Nota: Datos corresponde a un ejercicio académico realizado en seminario de investigación para un proyecto de sistemas de seguridad.

1.4.2. Descripción de los estudios

Tabla 2

Citaciones realizadas en el periodo 2003 - 2021

Número	Autores y año	Número de Citaciones	Área temática
1	(Andrés et al., n.d.)	7	Sistema de seguridad para locales comerciales mediante Raspberry Pi, cámara y sensor PIR *
2	(Mélany et al., 2019)		Sistema de alarma doméstica a escala controlado por un aplicativo móvil Scale domestic alarm system controlled by a mobile application
3	(Barillaro et al., n.d.)	4	Diseño de sistema IoT de monitoreo y alarma para personas mayores
4	(Rodríguez et al., n.d.)	2	Técnicas de ML Implementación con Raspberry PI de un Servidor Portátil de Contenido de señales digitales
5	(Augusto & Gil, 2016)	3	Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT
6	(Karina dolores Gaibor carrillo et al., n.d.)	3	Diseñar un sistema de alarma inalámbrico de bajo costo para la protección de viviendas tipo, en sectores de bajo recursos económicos de la ciudad de guayaquil.
7	(Rufino et al., 2020)		Sistema de monitoreo y servidor WEB con Raspberry Pi para el control de un robot neumático
8	(Alexander et al., n.d.)		Sistema de Acceso RFID

Nota: Datos corresponde a un ejercicio académico realizado en seminario de investigación para un proyecto de arritmias.

1.4.3. Análisis de los estudios

González, C. & Salcedo, O. (2017). El acompañamiento educativo como estrategia de cercanía impulsadora del aprendizaje del estudiante. Revista Virtual Universidad Católica del Norte, 51, 175-193. Recuperado de https://acortar.link/bXcdIH Propone un sistema antirrobo controlado por *Raspberry pi 2* modelo B, un sensor PIR y una cámara. la información es comunicada con el propietario por medio de correo electrónico adjuntando la imagen capturada. Aunque el proyecto menciona que se puede comunicar con el propietario por medio de correo electrónico estos sistemas deben evolucionar a una comunicación más efectiva como lo es la recepción y envió de datos por medio de internet a un servidor web que este se encargara de enviar la información a un aplicativo móvil

Alayo, C. M. P., Celis, P. Z. A., & Guzmán, D. A. D. (2019). Sistema de alarma doméstica a escala controlado por un aplicativo móvil. *PUEBLO CONTINENTE*, *30*(1), 93-99. En este proyecto se propone el desarrollo de una alarma doméstica controlada por la tarjeta de desarrollo Wemos D1 mini, que usa la plataforma IoT *Clyn* para la recepción y envió de datos de la alarma al aplicativo móvil. Aunque este proyecto contempla el envío de datos a través de IoT la plataforma usada es un tercero lo cual en caso de haber una falla en el servidor no se le puede dar solución temprana, sino que se dependería de como solucione el fallo el tercero.

Barillaro, S., De Luca, G., Valiente, W., Carnuccio, E., García, G., Volker, M., ... & Pérez, M. (2016, May). Diseño de sistema IoT de monitoreo y alarma para personas mayores. In *XVIII Workshop de Investigadores en Ciencias de la Computación (WICC 2016, Entre Ríos, Argentina)*. En este proyecto se planteó un sistema de alarma con monitoreo IoT enfocado en las personas mayores y sus prioridades medicas por lo que se basa en lecturas de sensores biomédicos y no en sensores antirrobo, aunque la base para el control de sensores es la misma a la planteada.

Rodríguez, R. A., Vera, P. M., Giulianelli, D. A., & Cammarano, P. (2017). Implementación con Raspberry PI de un servidor portátil de contenidos. In *XXIII Congreso Argentino de Ciencias de la Computación (La Plata, 2017).* Se planteo el desarrollo de un servidor web portátil con *raspberry* pi, ya que esta es un una mini computadora de bajo costo este servidor está enfocado para el uso de red local es decir que no necesita necesariamente una conexión a internet y solo los usuarios conectados al mismo router podrán acceder a él. La forma en la que trabaja este servidor con la información que recibe y envía es muy similar a la del servidor web la diferencia está en que el servidor web necesita una infraestructura de red

Estrada Bolívar, L. B. (2021). Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT. Se habla sobre la confiabilidad de los sistemas IoT ya que estos sistemas están conectados a internet hay muchos factores de riesgo que gente inescrupulosa aprovecha para entrar a la red de los usuarios robar información por eso se habla de medidas de seguridad usando firewall, antivirus VPN etc. Estos aspectos son muy importantes a tomar en cuenta ya que se trabajará con dispositivos IoT, y la información que se trasmite de los sistemas de seguridad por medio de internet no pueden ser expuesto a personas mal intencionadas.

Moreira Guzmán, A. R. (2020). *Sistema electrónico de seguridad y monitoreo GPS/GSM para vehículos livianos* (Bachelor's tesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería Electrónica y Comunicaciones). Este proyecto propone el desarrollo de un sistema monitoreado por GPS, GSM que se comunican con el propietario cuando la seguridad de su vehículo es vulnerada, para poder reaccionar rápidamente por medio de circuitos que corten la energía del vehículo. Como en este proyecto también se desarrollará sistemas de seguridad para vehículos automotores se puede basar en las ideas de esta tesis.

Gaibor Carrillo, K. D., & Loor Morán, F. A. (2018). *Diseñar un sistema de alarma inalámbrico de bajo costo para la protección de viviendas tipo, en sectores de bajo recursos económicos de la ciudad de Guayaquil* (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Networking y Telecomunicaciones). Se plantea el desarrollo de un sistema de seguridad con la placa de desarrollo *open source* Arduino para la lectura y sensores PIR, sensores magnéticos y comunicación por medio de GSM con el

módulo Sim800. Este proyecto es similar a la base del proyecto presentado y da una idea de que módulos GSM se puede usar para este proyecto, como la familia de los módulos SIM es muy amplia se debe realizar una comparativa para elegir al módulo más adecuado para este proyecto.

Antonio, C. R. M., Arreguín, J. M. R., Rivas-Araiza, E. A., Hurtado, E. G., & Ortega, J. C. P. (2020). Sistema de monitoreo y servidor WEB con Raspberry Pi para el control de un robot neumático. Se propuso el desarrollo de un servidor web basado en *raspberry* pi para el monitoreo de las señales de un controlador que serán almacenadas en una base de datos para graficarlas en tiempo real o después en cierto tiempo. Aunque este proyecto está enfocado para el monitoreo de un controlador para un robot neumático es el mismo mecanismo de monitoreo que se usara para este proyecto que monitorear las señales de los sensores PIR, sensores magnéticos y otros periféricos.

Alpala colimba, j. A., & moreno cabrera, j. S. (2020). *Implementación de un sistema de seguridad, mediante tecnología de 4 generación industrial* (Doctoral dissertation, AUNAR). Propone el desarrollo de un sistema basado en IoT para evitar el duplicado de las llaves en una clínica odontológica para ello utilizaron tecnología RFID que por medio de una tarjeta RF registrada se puede tener acceso, pero en el caso de no estar registrada este suceso es guardado en una base de datos en este caso la plataforma THINGSPEAK, esto datos serán visibles en un aplicativo móvil.

1.5. Marco metodológico

1.5.1. Tipo de investigación

Este trabajo se basa en un tipo de investigación aplicada, debido a que se centra en los aspectos de implementación de dispositivos físicos y de desarrollo de software, como lo es la infraestructura

del servidor web, el diseño de placas para soportar la tecnología IoT, elección de dispositivos con accesos a internet e incorporación de sensores biométricos.

1.5.2. Línea de investigación

Este trabajo de grado está vinculado a la línea de investigación de diseño y desarrollo mecatrónico del grupo de investigación GRIM , del programa de ingeniería mecatrónica de la Universidad Mariana debido a la naturaleza de esta investigación se enfoca al área de automatización y control dado que se aborda temas como son el monitoreo de dispositivos con tecnologías IoT mismos dispositivos que deben hacer lecturas de sensores de movimiento, sensores magnéticos, y otros periféricos para el control de dispositivos de seguridad.

1.5.3. Hipótesis de investigación

Los sistemas de seguridad con tecnología IoT y la incorporación de sistemas de reconocimiento biométrico logran brindar mayor seguridad

1.5.4. Descripción metodológica

1.5.4.1. Fase 1. En esta fase del proyecto, se realizará un cálculo detallado de voltajes y consumo de corriente para todos los elementos y módulos que se utilizarán. Se iniciará con el análisis y funcionamiento de los sensores empleados en sistemas de seguridad. Este análisis se llevará a cabo con el objetivo de determinar cómo conectar los sensores al controlador, incluyendo la determinación del voltaje de alimentación y el consumo de corriente.

Debido a que el primer objetivo es conectar un máximo de 32 sensores y los controladores o tarjetas de desarrollo disponibles tienen una cantidad limitada de pines, se utilizarán multiplexores. Por lo tanto, se realizará una cuidadosa selección de un multiplexor adecuado para este proyecto. Es crucial que este multiplexor trabaje con el

mismo voltaje que los sensores. En caso contrario, se incorporará una etapa de aislamiento utilizando optoacopladores.

Una vez completado el análisis e investigación de los sensores, se procederá al diseño de la PCB del módulo que permitirá la conexión de los sensores. Durante el diseño de esta PCB, se considerará la corriente que fluirá por cada vía del PCB para evitar el sobrecalentamiento y prevenir daños prematuros en la placa. Si el consumo de corriente es demasiado elevado y supera la capacidad de los reguladores de voltaje previstos, se calculará un circuito que permita el paso de la corriente necesaria y proporcione un voltaje adecuado para cada elemento electrónico de la placa.

Es importante destacar que los controladores que gestionan el módulo no estarán integrados en el módulo de control de sensores, sino que estarán alojados en una PCB independiente. Esta PCB central alojará los controladores y las placas de desarrollo encargadas del control de los distintos módulos.

Tras completar la selección de sensores y diseñar la PCB, se procederá a elegir un módulo de actuadores para el control de la sirena y otros elementos adicionales que satisfagan las necesidades de los clientes. Este módulo debe tener la capacidad de controlar múltiples canales para garantizar la versatilidad en el control de distintos dispositivos.

Se optará por un módulo comercialmente disponible, ya que el control de salidas mediante el uso de relés es una práctica estándar y existen en el mercado módulos que cumplen con estas características. La incorporación de un módulo comercial facilitará y agilizará el proceso, evitando la necesidad de diseñarlo desde cero.

Considerando que los siguiente modulo y la placa central a diseñar requerirán la conexión al servidor para pruebas, es necesario realizar la configuración del servidor en la Raspberry Pi antes de abordar el diseño de estas PCB.

Para ello, se instalarán en el servidor todos los programas necesarios para su funcionamiento, así como las librerías correspondientes de cada uno de los programas compatibles con Raspberry Pi.

Una vez configurado el servidor, se procede al diseño de la placa central seguido por el módulo de biometría. La placa central tendrá diversas funciones cruciales: enviar los estados de la alarma al servidor, emitir órdenes a los controladores de los módulos de sensores y actuadores que estarán integrados en esta placa, así como enviar la orden de inicio de verificación biométrica al módulo de biometría. Además, la placa central debe recibir las respuestas del módulo de biometría tras la verificación biométrica, así como recibir órdenes del control inalámbrico para activar y desactivar el sistema.

Para asegurar la conectividad a Internet a través de un cable UTP como una medida de respaldo, se elegirá un módulo que brinde esta capacidad y se integrará en la placa central. Además, se incluirá un módulo adicional que permita el envío de mensajes de texto a los usuarios mediante una red celular. La comunicación entre esta placa central, el módulo de biometría y el control inalámbrico se llevará a cabo a través del protocolo ESP-NOW, asegurando así una comunicación eficiente y confiable entre los distintos componentes del sistema, ya sabiendo esto se procede al diseño de la PCB de la placa central

Para diseñar el módulo de biometría, que será responsable de la verificación biométrica, se requiere un conjunto de componentes específicos. Este módulo debe ser capaz de reconocer huellas dactilares, voz y rostro. Para lograr esto, necesitamos integrar un sensor de huellas dactilares, un micrófono y una cámara en el diseño. Además, se debe incluir una memoria SD para el almacenamiento de estos datos biométricos.

Para garantizar la conectividad, el módulo de biometría debe contar con una conexión wifi que permita el envío de los archivos que contienen los datos biométricos, como archivos de formato WAV y JPG. Con estos parámetros definidos, procederemos al diseño de la PCB del módulo de biometría.

Para finalizar esta fase, es crucial obtener el consumo de energía de cada módulo y placa para calcular las características de la UPS. La decisión de incorporar una UPS completa dependerá de su costo comercial. Si este resulta ser prohibitivamente alto, se establecerá únicamente la UPS que se debe usar. El cálculo de la UPS se realizará utilizando una suposición extrema del consumo, considerando, por ejemplo, la conexión de los 32 sensores. Este paso es esencial para garantizar la fiabilidad del sistema y su capacidad para mantenerse en funcionamiento incluso durante cortes de energía.

1.5.4.2. Fase 2. En la Fase 2 del proyecto, se centra en el desarrollo de los scripts que se alojarán en el servidor. Estos scripts tienen la función de recibir archivos tanto en formato WAV como JPG, enviados desde el módulo de biometría. Además, deben ser capaces de recibir los estados de alerta de la placa central y almacenarlos en la base de datos MySQL.

Para lograr esto, se desarrollarán los siguientes scripts:

1.5.4.2.1. **Script de Recepción de Archivos:** Este script estará escrito en PHP y será responsable de recibir los archivos enviados desde el módulo de biometría. Utilizando el método POST, el script recibirá tanto archivos de audio en formato WAV como archivos de imagen en formato JPG. Una vez recibidos, los archivos se guardarán en el servidor para su posterior procesamiento.

1.5.4.2.2. **Script de Recepción de Estados de Alerta:** Otro script en PHP será desarrollado para recibir los estados de alerta enviados por la placa central. Estos estados de alerta pueden indicar activaciones, desactivaciones o alarmas disparadas. El script registrará estos estados en la base de datos MySQL para su posterior análisis y visualización.

1.5.4.2.3. **Scripts de Reconocimiento Facial y de Voz en Python:** Se desarrollarán scripts en Python para llevar a cabo el reconocimiento facial y de voz. Estos scripts utilizarán bibliotecas como *OpenCV* para el reconocimiento facial y *SpeechRecognition* para el reconocimiento de voz. El reconocimiento facial permitirá verificar la identidad de las personas capturadas por la cámara del sistema, mientras que el reconocimiento de voz permitirá procesar comandos de voz enviados desde el módulo de biometría.

1.5.4.3. Fase 3. En la Fase 3 del proyecto, se llevará a cabo el montaje físico de las placas en un gabinete para garantizar una disposición ordenada y segura de los componentes del sistema de seguridad. En esta etapa, el objetivo es asegurar que el servidor web, la placa de control y, si es posible, la aplicación móvil, trabajen de manera conjunta para realizar pruebas de funcionamiento efectivas.

Las actividades principales de esta fase incluirán:

1.5.4.3.2. **Montaje en el Gabinete:** Se procederá a instalar físicamente las placas de control, el servidor web y cualquier otro componente relevante dentro del gabinete. Se prestará especial atención a la disposición y fijación de los componentes para garantizar un montaje seguro y ordenado.

1.5.4.3.3. **Conexión de los Componentes:** Se realizarán todas las conexiones necesarias entre las placas de control, el servidor web y otros dispositivos dentro del gabinete. Esto incluirá la conexión de cables de alimentación, cables de red, cables de comunicación y cualquier otro cableado necesario para el funcionamiento del sistema.

1.5.4.3.4. **Pruebas de Funcionamiento Conjunto:** Una vez que todos los componentes estén montados y conectados, se llevarán a cabo pruebas exhaustivas para verificar la interoperabilidad entre el servidor web, la placa de control y otros dispositivos. Se simularán diferentes escenarios de activación, desactivación y detección de intrusos para garantizar que el sistema funcione correctamente en todas las situaciones.

1.5.4.3.5. **Integración con la Página Web:** En caso de que la aplicación móvil no esté disponible, se integrará la visualización de datos y el control del sistema a través de una página web. Se configurará la comunicación entre el servidor web y la página web para permitir el acceso remoto y la interacción con el sistema de seguridad.

En resumen, en esta fase se completará el montaje físico de las placas en el gabinete y se llevarán a cabo pruebas de funcionamiento conjunto para garantizar la efectividad y fiabilidad del sistema de seguridad. Además, se establecerá la integración con una página web para permitir la visualización y control remoto del sistema.

1.6. Validez de los resultados

1.6.1. Validez interna

la validez interna del sistema de seguridad se asegurará mediante una serie de pruebas por etapas que cubrirán diferentes aspectos del funcionamiento del sistema y garantizarán que cumpla con los criterios establecidos:

Prueba de Funcionamiento de Sensores y Periféricos**: Se** realizarán pruebas simulando situaciones donde el sistema debe responder, como la detección de intrusos, activación y desactivación del sistema, y otras condiciones relevantes. Esto permitirá validar el correcto funcionamiento de los sensores y periféricos conectados al sistema.

Validación del Módulo de Biometría: Se verificará que el módulo de biometría pueda enviar los datos al servidor de manera efectiva para su procesamiento. Se espera recibir una respuesta desde el servidor que determine la acción a realizar, como la activación o desactivación del sistema, basada en la información biométrica proporcionada.

Validación del Sistema de UPS: Se estimará el consumo de corriente del sistema en diversas condiciones y situaciones. Esta estimación se utilizará para determinar el tipo de UPS comercial más adecuado para garantizar el suministro de energía en caso de cortes eléctricos u otras eventualidades. Se realizarán pruebas para validar la capacidad y eficacia del UPS seleccionado.

Estas pruebas por etapas garantizarán que el sistema de seguridad funcione de manera confiable y cumpla con los requisitos de seguridad establecidos. Cada fase de validación proporcionará información crucial sobre el rendimiento del sistema y ayudará a identificar posibles áreas de mejora o ajuste

2. Resultados

2.1. Resultados del objetivo 1

2.1.1. Selección de sensores PIR

2.1.1.1. Sensores PIR.

Los sensores PIR (infrarrojos pasivos) y los sensores magnéticos son altamente valorados en los sistemas de seguridad debido a sus características específicas y ventajas.

- **Precisión en la Detección de Movimiento**. Los sensores PIR detectan cambios en la radiación infrarroja emitida por objetos calientes, como los seres humanos. Esto les permite distinguir de manera efectiva entre personas y otros objetos, reduciendo los falsos positivos causados por factores ambientales como el viento o la luz (Swann Security, 2019).
- **Eficiencia Energética**. Operan en modo de espera hasta que detectan movimiento, lo que ahorra energía y prolonga la vida útil del sistema (Swann Security, 2019).
- **Costo Efectivo**. Son económicos debido a su diseño simple y la tecnología pasiva utilizada, lo que los hace accesibles para una amplia gama de aplicaciones de seguridad (HomeProtex, n.d.).
- **Integración Sencilla**. Los sensores PIR pueden integrarse fácilmente con otros sistemas de seguridad, como luces y alarmas, y ofrecen ajustes de sensibilidad y tiempo de retardo para personalizar su funcionamiento (HomeProtex, n.d.).

2.1.2. Sensores Magnéticos.

- **Simplicidad y Confiabilidad**. Los sensores magnéticos, comúnmente usados en puertas y ventanas, son muy confiables para detectar aperturas no autorizadas. Funcionan mediante la interrupción de un circuito magnético, lo que desencadena una alarma cuando se abre la puerta o ventana protegida (Electricity & Magnetism, n.d.).
- **Bajo Mantenimiento**. Estos sensores requieren poco mantenimiento y son menos propensos a fallos mecánicos o eléctricos, lo que los hace duraderos y fiables a largo plazo (Electricity & Magnetism, n.d.).

- **Instalación Versátil**: Pueden instalarse en una variedad de superficies y configuraciones, lo que permite su uso en diferentes tipos de edificios y entornos (Electricity & Magnetism, n.d.).

2.1.2.1. Ventajas Combinadas. La combinación de sensores PIR y magnéticos en un sistema de seguridad permite una protección integral. Mientras que los sensores magnéticos garantizan que las entradas físicas no sean abiertas sin autorización, los sensores PIR monitorizan el movimiento dentro de un área, proporcionando una capa adicional de seguridad que puede activar alarmas o cámaras solo cuando es realmente necesario, minimizando falsos positivos y optimizando la respuesta del sistema de seguridad.

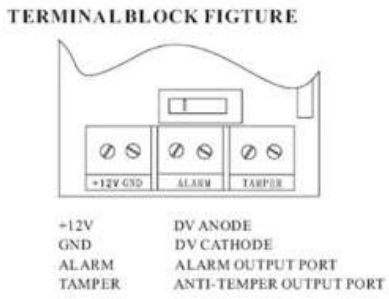
2.1.3. Análisis funcionamiento sensores PIR y magnéticos

2.1.3.1. *Sensor PIR.* Los sensores PIR para su funcionamiento necesitan de una fuente de voltaje de 12 voltios y tienen un consumo de funcionamiento de 20 miliamperios en activación y 10 miliamperios en desactivación, estos sensores al momento de detectar un cambio de radiación en la zona a la cual tienen cubierta activan un relé el cual genera un estado lógico, el cual será un estado alto si el sensor es normalmente abierto y bajo si el sensor es normalmente cerrado.

Adicionalmente los sensores PIR cuentan con una protección llamada TAMPER la cual permite saber si el sensor es manipulado, este pin TAMPER mantiene un estado lógico alto, cuando el sensor se ha manipulado ya sea cortando su cableado o abriendo su carcasa el sensor activa un relé el cual genera un estado lógico bajo haciéndole saber al controlador que el sensor fue manipulado, como se tiene un estado lógico alto constante mientras no se manipule la integridad del sensor para el caso de cortar el cableado esta señal de estado lógico de 12 voltios se perderá por lo que el controlador determinara que el cable ha sido cortado.

Figura 1

Pinout sensor PIR



(Etiampro Pir Sensor With Double Twin Optics User Manual - Manuals+, n.d.)

2.1.3.2. Sensor Magnético. El sensor magnético tiene un funcionamiento simple ya que este internamente cuenta con un interruptor magnético el cual al acercarle un imán se activa y al alejarlo se desactiva, cuando este se activa retorna un voltaje de 12 voltios el cual se lo podría considerar un estado lógico alto, el cual es leído por el controlado.

El sensor magnético se compone de dos partes separadas, una parte que contiene al interruptor magnético y la otra parte que contiene el imán, cuando se instala un sensor magnético en una puerta o una ventana la parte con el cableado del interruptor magnético debe ir instalada en la parte fija y el imán debe ir instalado en la parte móvil de la puerta o ventana.

Cuando la puerta o ventana se encuentran cerradas las partes que componen al sensor se encontraran juntas por lo que el sensor estará enviando en estado lógico alto, que al momento de abrir la puerta o ventana cambiará, el consumo de corriente de este sensor lo definirá la resistencia de acople con el controlador.

Figura 2

Sensor magnético

(*¿Qué Es Un Detector Magnético de Apertura?*, n.d.)

Para comprobar el funcionamiento de los sensores y la alarma, se realizará una simulación con cuatro sensores. Se utilizará un controlador PIC 16F628A para leer los estados lógicos generados por los sensores. Además, se incluirán dos pulsadores para la activación y desactivación de la alarma. Debido a la diferencia de voltaje entre el controlador PIC (5V) y los sensores (12V), se empleará una etapa de aislamiento utilizando optoacopladores de referencia PC817.

2.1.4. Componentes y Funcionamiento del Optoacoplador

El optoacoplador PC817 contiene internamente un diodo LED y un transistor con una base fotosensible. La conexión es la siguiente:

- Entrada (diodo LED): Conectada a la señal lógica de 12V generada por el sensor.
- Salida (transistor): Genera una señal lógica de 5V para el PIC.
- Cuando el sensor genera una señal de 12V, el diodo LED del optoacoplador se ilumina. Esta luz es recibida por el transistor fotosensible, lo que lo satura y permite que la señal lógica de 5V se genere en la salida.

2.1.4.1. Cálculo de las Resistencias de Entrada y Salida del Optoacoplador. Para asegurar que el optoacoplador opere de manera eficiente y evitar sobrecalentamientos, la corriente máxima que circulará tanto por la entrada como por la salida será de 25 mA. A continuación, se detallan los cálculos para determinar las resistencias adecuadas:

Resistencia de Entrada

La resistencia de entrada (R_in) debe limitar la corriente a través del diodo LED del optoacoplador.

- Voltaje de entrada del sensor (V_in): 12V
- Voltaje de caída del LED (V_f): 1.2V (valor típico, revisar el datasheet específico para confirmarlo)
- Corriente deseada (I_in): 25 mA

Utilizamos la ley de Ohm para calcular la resistencia de entrada:

$$\frac{12V - 1.2}{25ma} = 432\Omega$$

Redondeando al valor comercial más cercano, podemos usar una resistencia de 430 Ω o 480 Ω para R_in.

Resistencia de Salida

La resistencia de salida (R_out) debe limitar la corriente a través del transistor del optoacoplador.

- Voltaje de salida del PIC (V_out): 5V
- Corriente deseada (I_out): 25 mA

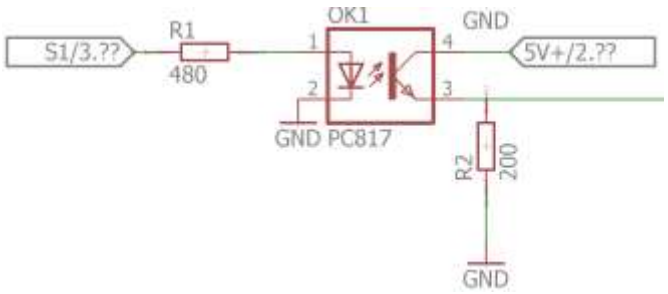
Asumiendo que el transistor tiene una caída de voltaje muy baja cuando está saturado (aproximadamente 0.2V), el cálculo es:

$$\frac{5V - 0.2}{25ma} = 192\Omega$$

Redondeando al valor comercial más cercano, podemos usar una resistencia de 180 Ω o 200 Ω para R_out.

Figura 3

Circuito optoacoplador



Para lograr que el sistema se adapte a las distintas necesidades de los usuarios, se contemplan situaciones como la disposición de sensores que permitan al sistema detectar intrusiones en locales comerciales con diversas dimensiones y distribuciones internas. Los obstáculos en estos locales pueden afectar la lectura adecuada de los sensores PIR (*Passive InfraRed*). Por esta razón, el diseño considera un máximo de 32 sensores y un mínimo de 8 sensores.

2.1.5. Diseño Modular para Flexibilidad

Se diseñaron dos módulos para la conexión de 8 y 16 sensores, respectivamente. Esto permite que el sistema se adapte a los requerimientos de seguridad específicos de cada local. Utilizar un módulo con demasiados sensores en un espacio pequeño no solo desperdicia hardware, sino que también reduce la eficiencia del sistema. Además, soportar más sensores requiere más componentes electrónicos, incrementando los costos de manufactura.

Para locales que requieren hasta 32 sensores, se opta por usar dos módulos de 16 canales en cascada. Para 24 sensores, se usa un módulo de 16 canales y uno de 8 canales en cascada. Este

enfoque modular permite una adaptación precisa y coste-efectiva según las necesidades de cada instalación.

2.1.5.1. Diseño de los Circuitos de Conexión. El sistema debe soportar la conexión de hasta 32 sensores, cada uno generando dos señales. Esto implica la necesidad de 64 pines en un controlador, lo cual excede la cantidad de pines disponibles en los controladores típicos. Para resolver esto, se utilizan multiplexores, que permiten controlar una gran cantidad de pines de entrada y salida con una cantidad mínima de pines del controlador.

2.1.5.2. Selección de Multiplexores. Para conectar de 8 a 32 sensores y evitar el desperdicio de hardware cuando no se utilicen todos los sensores, se utilizarán 4 multiplexores de 8 entradas a 1 salida. Estos multiplexores leerán secuencialmente 8 canales. En el mercado, existen varias referencias de multiplexores de 8 a 1. Se preseleccionaron los modelos 74LS151 y 74HC4051. A continuación, se presenta una comparativa basada en sus hojas de datos:

74LS151:

- Tecnología: TTL (*Transistor-Transistor Logic*)
- Voltaje de Operación: 4.75V a 5.25V
- Corriente de Consumo: Moderada
- Velocidad: Alta
- Compatibilidad: Compatible con sistemas TTL

74HC4051:

- Tecnología: CMOS (*Complementary Metal-Oxide-Semiconductor*)
- Voltaje de Operación: 2V a 6V
- Corriente de Consumo: Baja
- Velocidad: Moderada
- Compatibilidad: Compatible con sistemas CMOS
- Decisión de Implementación

Para la implementación del sistema, se elige el 74HC4051 por su menor consumo de corriente y mayor rango de voltaje, que ofrecen una mayor flexibilidad y eficiencia energética, importantes en un sistema de seguridad con múltiples componentes.

Para satisfacer las necesidades de detección de movimiento y de la señal TAMPER por cada sensor, es esencial leer estas señales simultáneamente. Por ello, se configura un circuito que permite que dos multiplexores trabajen en paralelo. De esta manera, se utilizarán 2 multiplexores por cada ocho sensores, resultando en un total de 8 multiplexores para la conexión de 32 sensores.

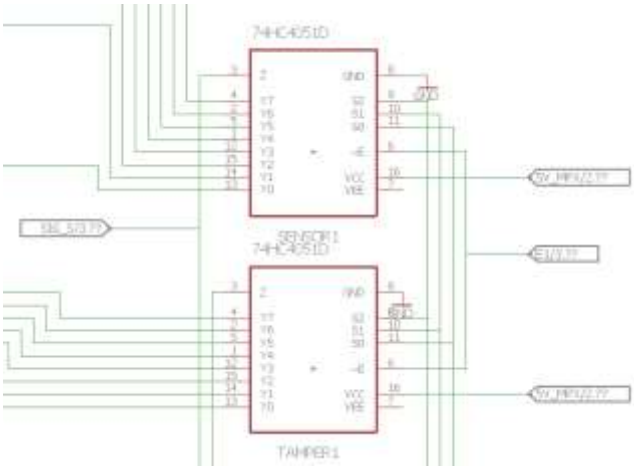
2.1.5.3. Configuración del Sistema. Paralelismo dos multiplexores se configuran en paralelo por cada grupo de ocho sensores.

Multiplexor 1: Lee la señal de detección de movimiento.
Multiplexor 2: Lee la señal TAMPER.

Control de Multiplexores: Los selectores de los multiplexores se controlan simultáneamente para garantizar que ambos multiplexores leen del mismo sensor a la vez.

Figura 4

configuración en paralelo de multiplexores



2.1.5.4. Control de Selectores. Los selectores (S1, S2, S3) de los multiplexores se conectan en paralelo, de manera que ambos multiplexores seleccionan la misma entrada al mismo tiempo.

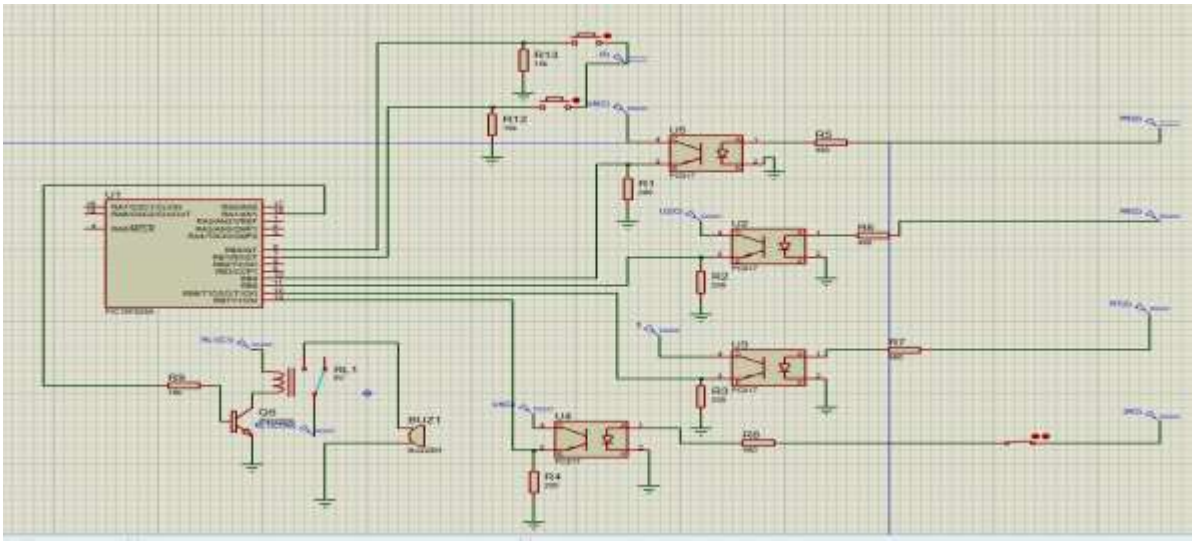
2.1.6. Diseño del Circuito

2.1.6.1.1. **Resistencias y Componentes.** Se usa el cálculo anterior de optoacopladores para aislar las señales de 12v de TAMPER y movimiento y entregar en el multiplexor un voltaje de 5v y un consumo de 50ma entre la entrada y salida

2.1.6.1.2. **Optimización y Pruebas.** Antes de la implementación completa, se realiza una simulación del circuito con 4 sensores para validar el funcionamiento y realizar ajustes necesarios.

Figura 5

Circuito simulación alamar con cuatro sensores



2.1.6.1.3. **Finalización del Diseño.** Una vez validado el diseño con la simulación de 4 sensores, se procede a escalar el diseño para soportar hasta 32 sensores.

Para el control de la selección de canales y la lectura de los sensores, se emplea un microcontrolador PIC16F628A, que debe ejecutar un código de programación para manejar los 8 multiplexores. Dado que cada par de multiplexores trabaja en paralelo, es como si solo se controlaran 4 multiplexores en total. A continuación, se detalla cómo se realiza este control:

2.1.7. figuración y Control de Multiplexores

2.1.7.1. ***Pines de Selección.*** Los multiplexores tienen tres pines de selección: S1, S2 y S3, Estos pines reciben una secuencia binaria generada por el controlador, que en decimal va de 0 a 7 cada número en la secuencia representa un canal seleccionado.

2.1.7.2. ***Pin de Habilitación (Enable).*** Además de los pines de selección, cada multiplexor tiene un pin de habilitación denominado "enable", Este pin debe estar en un estado lógico bajo (0) para habilitar el multiplexor.

Mientras el controlador realiza la lectura de los sensores, enviará un estado lógico bajo al multiplexor que está leyendo y un estado lógico alto (1) a los otros multiplexores para mantenerlos deshabilitados.

2.1.8. Algoritmo de Control

2.1.8.1. **Secuencia de Selección.** El controlador genera una secuencia binaria en los pines S1, S2 y S3 que va de 0 a 7, seleccionando secuencialmente cada canal de los multiplexores.

2.1.8.2. **Habilitación del Multiplexor.** El controlador activa el pin de habilitación del multiplexor correspondiente con un estado lógico bajo, Todos los demás multiplexores reciben un estado lógico alto en su pin de habilitación para mantenerlos deshabilitados.

2.1.8.3. **Lectura de Sensores.** El controlador lee la señal del sensor a través del canal seleccionado del multiplexor habilitado.

Este proceso se repite rápidamente para cada canal y multiplexor, creando la percepción de una lectura simultánea de todos los sensores

.

2.1.9. Simulación y Resultados

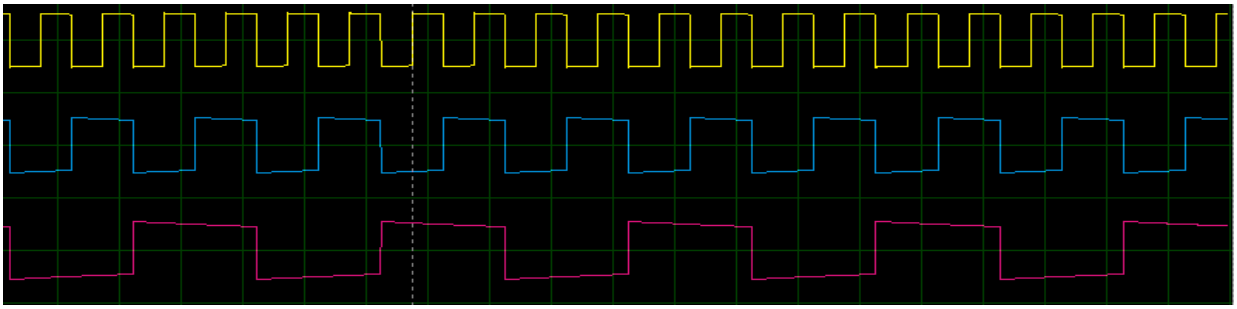
2.1.9.1. **Simulación grafica pines de selección.** Se realiza una simulación del control del multiplexor. Conectando los pines de control al osciloscopio, se obtiene una gráfica que muestra la secuencia de selección de canales. Esta gráfica permite verificar que el controlador selecciona los canales de los multiplexores correctamente, realizando las lecturas de los sensores en la secuencia esperada.

Se realiza una simulación del control del multiplexor. Conectando los pines de control al osciloscopio, se obtiene una gráfica que muestra la secuencia de selección de canales.

- Gráfica Amarilla: Entrada S1 del multiplexor.
- Gráfica Azul: Entrada S2 del multiplexor.
- Gráfica Roja: Entrada S3 del multiplexor.

Figura 6

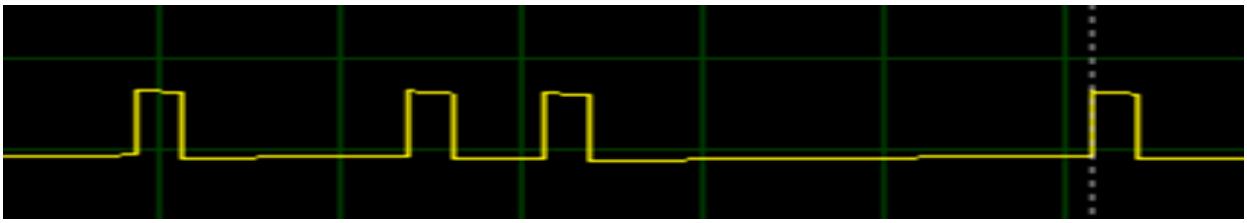
Estados lógicos selección de canal en osciloscopio



2.1.9.2. Simulación lectura de señales con 1 sensor activo por multiplexor. Cada salida de señal de los multiplexores va conectada a un mismo pin de entrada del controlador. Dado que los sensores generan dos señales, se requieren dos pines de entrada en el controlador: uno para la señal de detección y otro para la señal de TAMPER.

Figura 7

Señal obtenida en simulación de la lectura de señales. Con un sensor activo por multiplexor



En la imagen de la simulación, se observa que solo se generan cuatro estados lógicos altos, cada uno correspondiente a un sensor activo. Si se tuvieran más sensores activos, se podrían observar más estados lógicos altos en el osciloscopio, correspondientes a esos sensores adicionales.

Esto se realiza con el fin de comprobar el funcionamiento del código del controlador en este caso se obtiene un resultado éxito ya que se determina que el código del multiplexor funciona.

Nota: Revisar el código de programación del controlador de multiplexación en anexos

2.1.10. Circuitos reguladores de voltaje para el módulo de multiplexación

Para poder lograr un correcto funcionamiento de los componentes electrónicos para evitar caídas de tensión se debe tener en cuenta el consumo y voltaje de cada uno les sensores, multiplexores y optoacopladores, se debe realizar un circuito de reguladores que permitan una salida de voltaje adecuada para cada componente y un paso de corriente suficiente para el funcionamiento de los circuitos.

Cómo se tiene la información que los sensores PIR tienen un consumo de 20 miliamperios y se alimentan a 12v. se hace la suposición que se van a conectar 32 sensores PIR ya que estos tienen un consumo más alto que los sensores magnéticos, esta conjetura se la realiza para poder determinar el caso más extremo en consumo de corriente por parte de los sensores.

Para calcular el consumo de corriente total por parte de los sensores se debe multiplicar el número de sensores por el consumo individual.

$$consumo\ corriente\ total = n\ sensores * I\ individual$$

$$I\ total = 32 * 20ma = 0.64amp$$

Cada sensor genera dos señales, y cada señal tiene un consumo de 50 mA a través de la entrada de los optoacopladores. Esto significa que, por cada sensor, hay un consumo adicional de 50 mA en la etapa de acoplamiento.

$$I\ acoplamiento = 32 * 50ma = 1.6Amp$$

Realizando la suma de las dos corrientes se tiene un total de 3.84 amperios de consumo por parte de los sensores, este cálculo de corrientes será usando tanto como para el diseño de la PCB, como para determinar la capacidad que debe tener la UPS.

Para cumplir con los parámetros de funcionamiento de los sensores, se ha diseñado un circuito en el que se utiliza un regulador de voltaje 7812, el cual proporciona una salida de 12 voltios. Sin embargo, dado que el regulador 7812 está limitado a un paso de corriente de 1 amperio, se ha implementado un transistor TIP42C de tipo PNP para manejar corrientes más altas sin sobrecargar el regulador.

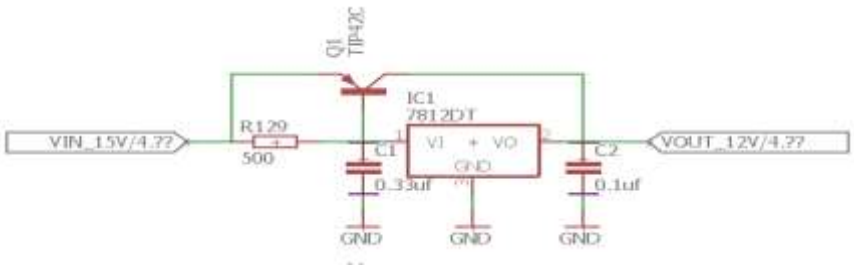
2.1.10.1. Funcionamiento del Circuito

- **Regulador 7812**: Proporciona 12V en la salida.
- **TIP42C**: Este transistor PNP tiene su base conectada a través de una resistencia de 500 ohmios (R129). La saturación de la base permite que el transistor conduzca.
- **Carga del Sensor**: Los sensores PIR, que requieren 12V y tienen un consumo total de 0.64A, se alimentan a través del TIP42C. Este transistor maneja la corriente total requerida por los sensores, mientras que el 7812 asegura un voltaje estable de 12V.

Para evitar caídas de tensión y asegurar el correcto funcionamiento de los sensores PIR, se utiliza un regulador 7812 complementado con un transistor TIP42C. Esta configuración permite manejar corrientes más altas sin sobrecargar el regulador, asegurando un suministro de 12V estable y adecuado para los sensores.

Figura 8

circuito regulador de 12 voltios con etapa de potencia



Para la alimentación de los optoacopladores y de los multiplexores se utiliza el mismo circuito descrito anteriormente, con la modificación de cambiar el regulador por un 7805 para obtener una salida de 5 voltios. Aquí se detallan los cálculos y el diseño del circuito:

2.1.11. Cálculo de Consumo

Multiplexores CD4051:

- Consumo individual: 50 mA.
- Número de multiplexores: 8.
- Consumo total de los multiplexores: 8 * 50 mA = 0.4 A.

Optoacopladores:

- Consumo individual por salida: 25 mA.
- Número de optoacopladores: 64.

$$\boldsymbol{Consumo\ total\ de\ los\ optoacopladores}: 64 * 25\,mA = 1.6\,A.$$

Consumo total:

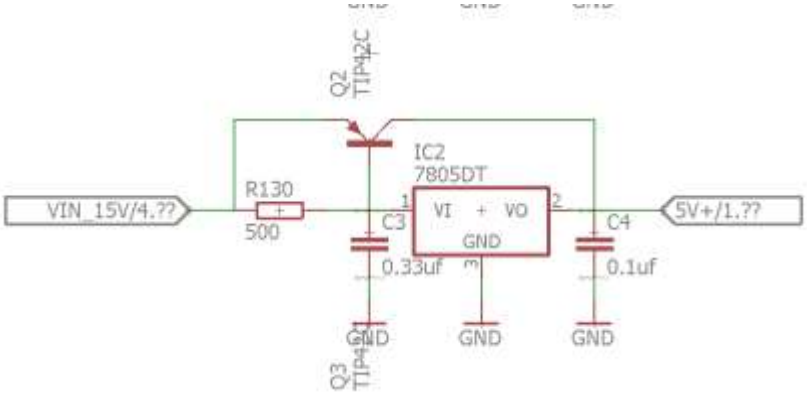
- Multiplexores: 0.4 A.
- Optoacopladores: 1.6 A.

$$\boldsymbol{Consumo\ total}: 0.4\,A + 1.6\,A = 2\,A.$$

Nota: Dado que el regulador 7805 está limitado a 1A, se utiliza un transistor PNP TIP42C para manejar corrientes mayores, como se hizo con el regulador 7812.

Figura 9

circuito regulador de 5 voltios con etapa de potencia



2.1.12. Diseño de Módulo de Multiplexación para Sensores PIR y Magnéticos

2.1.12.1. Descripción General. Se ha diseñado el módulo de multiplexación para conectar sensores PIR y magnéticos. Este módulo tiene la capacidad de conectar hasta 16 sensores, y varios de estos módulos pueden conectarse en cascada para alcanzar hasta 32 sensores. Además, se ha diseñado un módulo más pequeño de 8 canales para aplicaciones donde se necesite conectar un número menor de sensores. Este enfoque modular permite adaptarse a diferentes necesidades y tamaños de instalaciones.

Figura 10

PCB modulo multiplexación 16 sensores

,

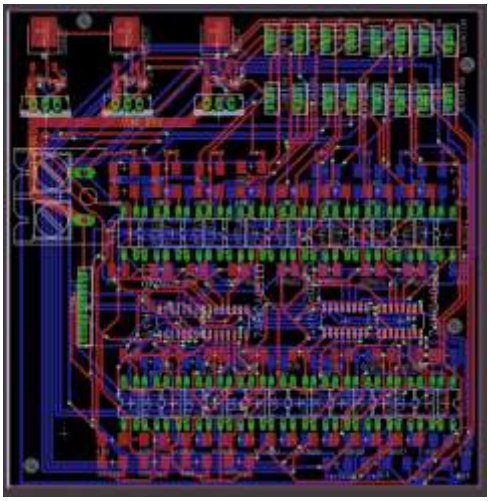
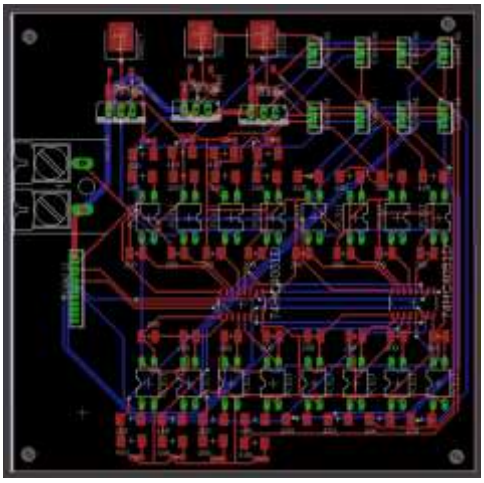


Figura 11

PCB modulo multiplexación 8 sensores

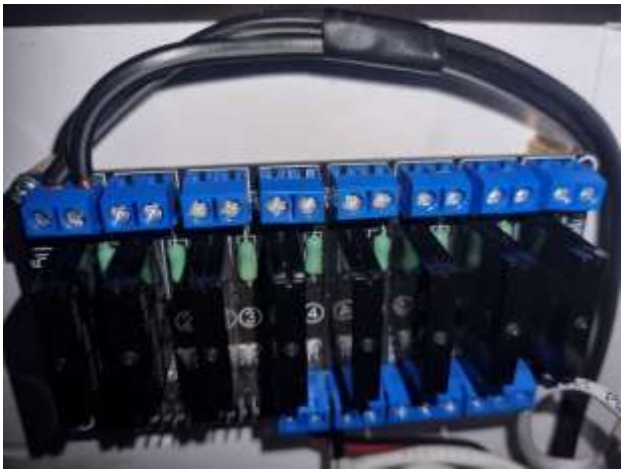


2.1.13. Módulo de Actuadores con Relés de Estado Sólido

Para este sistema se selecciona un módulo comercial de 8 canales con relés de estado sólido. La decisión de comprar este módulo se basa en la facilidad y economía que representa adquirirlo en lugar de fabricarlo desde cero. Existen muchas opciones en el mercado, pero se ha optado por un módulo que cuenta con relés de estado sólido con activación en DC y control en AC. Este tipo de módulo es más adaptable para controlar dispositivos como lámparas o la apertura de un portón, que suelen operar con corriente alterna (AC).

Figura 12

Módulo de relés



2.1.13.1. Características del Módulo. El módulo de relés de estado sólido ofrece versatilidad para controlar dispositivos con señales de corriente continua (DC) y corriente alterna (AC), siendo adecuado para aplicaciones como lámparas o motores de portones. Con 8 canales disponibles, proporciona flexibilidad para futuras expansiones. Inicialmente, se utilizará el primer canal del módulo para activar la sirena del sistema de seguridad.

2.1.13.2. Integración con el PIC16F628A. El módulo se controla mediante un PIC16F628A, que proporciona 8 pines disponibles para manejar cada uno de los canales del módulo de relés.

2.1.13.3. Programación de Rutinas.

- **Advertencia**: Una rutina programada en el PIC16F628A hace que la sirena suene brevemente una sola vez para indicar cuando la placa central recibe una orden de activación o desactivación del sistema.
- **Intrusión**: Otra rutina mantiene activo el canal correspondiente cuando se detecta una intrusión, activando la sirena de manera continua hasta que se resuelva la situación.

2.1.13.4. Conexión y Montaje. La placa central del sistema de seguridad incorporará el controlador PIC16F628A de manera integrada. Además, esta placa está equipada con conectores diseñados específicamente para facilitar la conexión con el módulo de relés de estado sólido.

Nota

Revisar código de programación control de módulo de relés en anexos

2.1.14. Configuración Servidor Web en Raspberry Pi 3B+

Requisitos de Hardware y Software

- Hardware: Raspberry Pi 3B+
- Sistema Operativo: Raspbian (basado en Linux)
- Software a instalar:
  - Apache
  - MySQL / MariaDB
  - Python3
  - PHP

Al momento de instalar los programas y bibliotecas, se debe tener en cuenta las versiones que se instalan, debido a que los scripts que se alojan en este servidor fueron desarrollados previamente en Windows y se tuvieron problemas con las versiones de las bibliotecas de *OpenCV Contrib* y *Speech Recognition* que se usarán. También es importante instalar las bibliotecas de

manera global usando ***sudo apt install*** y no solo ***pip install***, ya que este último solo instala las bibliotecas para el entorno de IDLE de Python y el entorno de Apache no reconoce las bibliotecas.

En la segunda fase se profundizará el tema sobre los scripts alojados en este servidor. En esta etapa, solo se configura el servidor para pruebas iniciales. Estas pruebas se realizan enviando variables numéricas al servidor mediante el método POST. El objetivo es verificar que se logra la conexión con el servidor desde los distintos módulos antes de implementar un programa más complejo para el envío de archivos.

2.1.15. Desarrollo y Funcionamiento de la PCB Central

Esta PCB central es la encargada del manejo de los distintos módulos, tales como módulos de multiplexación, módulo de actuadores, módulo de biometría, y el manejo de datos tanto del control inalámbrico como del envío de datos a internet. En esta placa se encuentra embebido un SoC ESP32 WROOM32, el cual se encarga de la comunicación con el servidor a través de internet. Esta comunicación se realiza a través de WiFi, el cual el SoC ya trae incorporado, o por medio de un cable UTP mediante el módulo ENC28J60, el cual se comunica con la ESP32 a través del protocolo SPI.

El ESP32 también recibe señales tanto del control inalámbrico mediante ESP-NOW, como datos de comprobación desde el módulo de biometría, igualmente mediante ESP-NOW. Además, se encarga de dar órdenes a dos microcontroladores PIC16F628, de los cuales uno controla el módulo de multiplexación y el otro controla el módulo de actuadores.

El primer microcontrolador recibe la orden de empezar la lectura desde el ESP32 mediante un pin digital que cambia de un estado bajo a un estado alto. Este PIC debe informar al ESP32 si se detecta movimiento o apertura de alguno de los sensores mediante otro pin digital que cambia de un estado bajo a un estado alto. El segundo microcontrolador se encarga de controlar el módulo de actuadores, comunicándose con el ESP32 mediante el protocolo de comunicación serial a través

del puerto serie número cero. La ESP32 le envía un número entero que determina las distintas rutinas a ejecutar.

Además, esta placa central cuenta con el módulo SIM7000G, que envía mensajes de texto en caso de emergencia si no se logra una comunicación a internet. Este módulo SIM7000G se conecta a través del puerto serial número dos del ESP32, utilizando comandos AT para configurar el módulo y enviar mensajes. La SIM card debe contar con saldo suficiente para el envío de mensajes. El mensaje puede contener el estado del sistema o el código de error de conexión al servidor.

La PCB central está diseñada de manera que los módulos de actuadores y multiplexación sean controlados por microcontroladores PIC, dejando al ESP32 la tarea de manejar la comunicación y procesamiento de datos sin sobrecargar sus recursos de memoria RAM y ROM.

2.1.15.1. Cálculo de Consumo de los Elementos de la PCB Central. Para asegurar el correcto funcionamiento de la PCB central y evitar caídas de tensión, es crucial calcular el consumo de corriente de cada uno de los componentes. A continuación, se presenta el cálculo del consumo de los principales componentes de la PCB central.

ESP32 WROOM32

- Voltaje de operación: 3.3V
- Consumo promedio: 160 mA (durante la transmisión WiFi puede llegar a picos de hasta 500 mA)

Módulo ENC28J60 (Ethernet)

- Voltaje de operación: 3.3V
- Consumo promedio: 120 mA

SIM7000G (GSM/GPRS)

- Voltaje de operación: 3.3V
- Consumo promedio: 20 mA (puede alcanzar picos de hasta 2A durante la transmisión)

Microcontroladores PIC16F628 (x2)

- Voltaje de operación: 5V
- Consumo promedio: 1.2 mA (cada uno)

Consumo total (promedio):

$$Consumo\ total = 160\ mA + 120\ mA + 20\ mA + 2.4\ mA$$
$$Consumo\ total = 160\ mA + 120\ mA + 20\ mA + 2.4\ mA$$
$$Consumo\ total = 302.4\ mA$$
$$Consumo\ total = 0.3024\ A$$

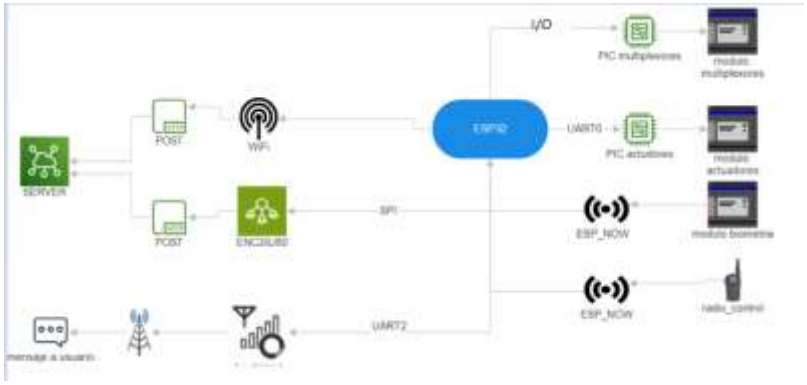
Adicionales

Picos de corriente del SIM7000G: Durante la transmisión, el SIM7000G puede alcanzar picos de hasta 2A. Por lo tanto, se debe considerar un margen de seguridad adicional para la fuente de alimentación que alimenté el SIM7000G se usa el circuito de potencia de los optoacopladores.

Dimensionamiento de la fuente de alimentación: La fuente debe ser capaz de manejar al menos 3A para cubrir los picos de corriente y asegurar un funcionamiento estable del sistema.

Figura 13

Diagrama funcionamiento placa central



Con esta información, se procede al diseño de la PCB en Eagle. El diseño incluirá:

ESP32 WROOM32 para la comunicación y procesamiento de datos.

Módulo ENC28J60 para la conexión Ethernet.

Módulo SIM7000G para el envío de mensajes de texto en caso de emergencia.

Microcontroladores PIC16F628 para el control de los módulos de actuadores y multiplexación.

La distribución de los componentes y el ruteo de las pistas se realizarán de manera que se minimicen las interferencias y se asegure una alimentación adecuada para cada componente. La fuente de alimentación se dimensionará para manejar picos de hasta 2.5A, garantizando así la estabilidad del sistema.

Figura 14

PCB central

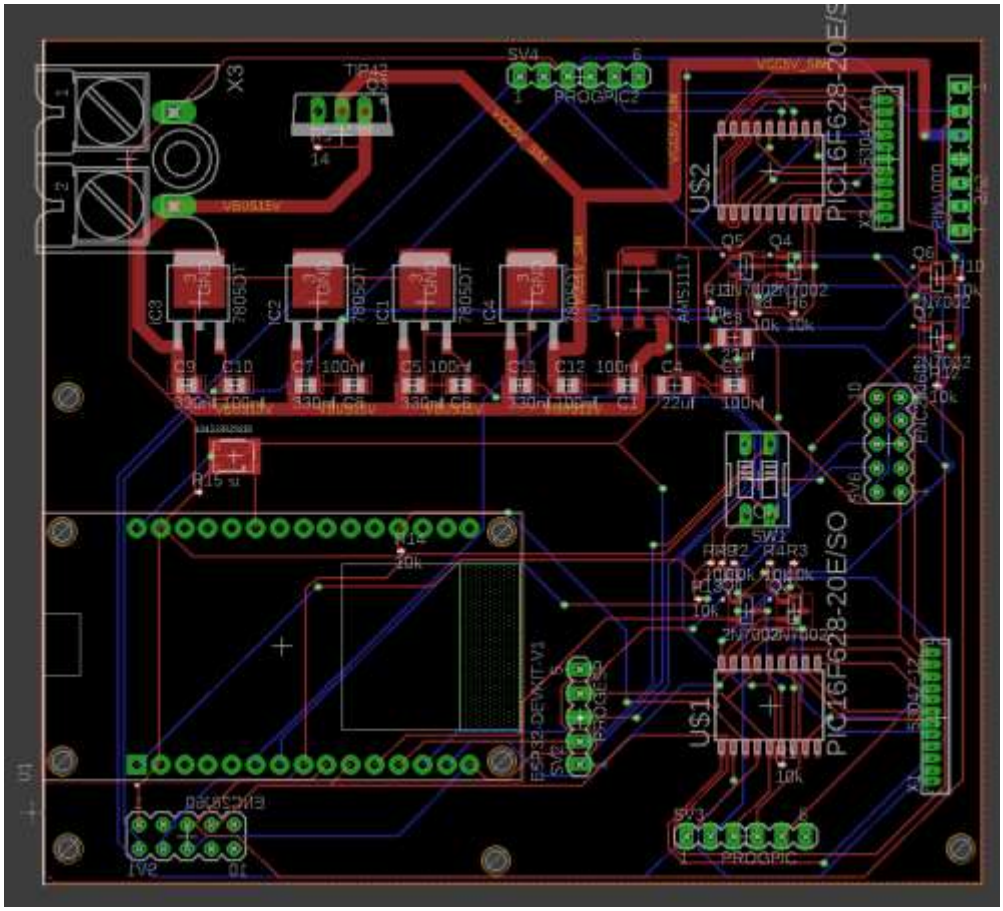
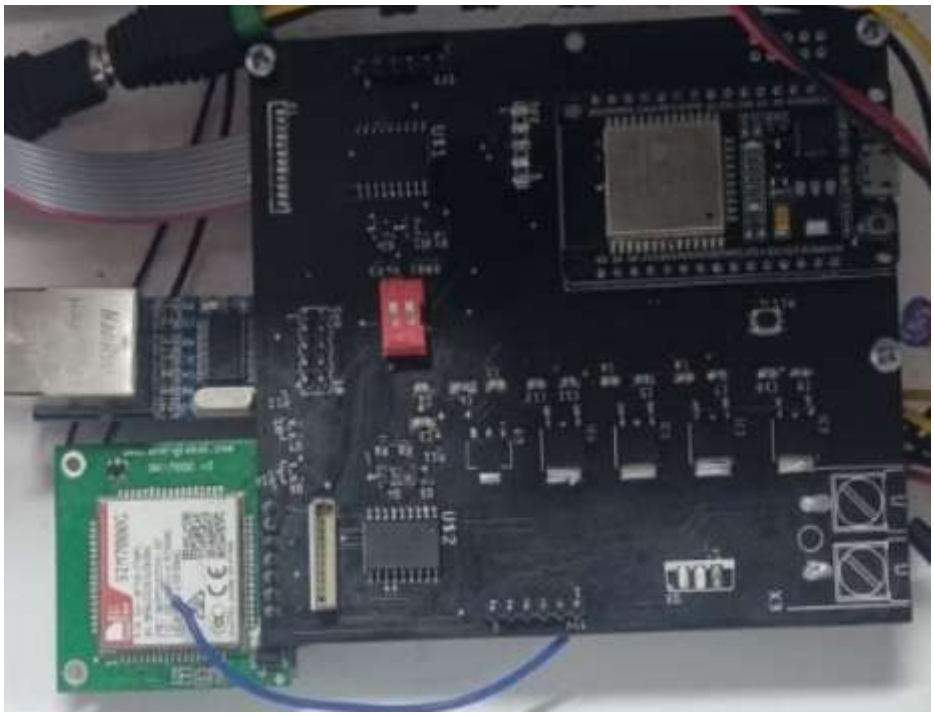


Figura 15

placa central con sus componentes soldados



Una vez que se tiene la placa central ya funcionado se utiliza un código ejemplo de Arduino para enviar variables numéricas al servidor mediante el método POST, en el servidor se tiene un código simple en PHP para recibir estos datos y mostrarlo, esta prueba ser hace con fin de hacer pruebas de conexión al servidor

Figura 16

prueba visualización de datos de la placa centra

Nota: Revisar en anexos la validación en página web la recepción de datos de esta prueba.

2.1.16. Módulo de biometría

Este módulo es el encargado de procesar la información de los periféricos que obtienen los datos biométricos como el sensor de huella dactilar, el micrófono y la cámara. Este módulo cuenta con dos Soc:

- **ESP32-S3**: Encargado de controlar el micrófono y el sensor de huella.
- **ESP32 AI Thinker**: Diseñado para soportar la conexión de una cámara y procesar y almacenar imágenes.

El objetivo es capturar y guardar los archivos de audio y video para posteriormente enviarlos al servidor, el cual cuenta con un hardware más potente que permite ejecutar scripts para el reconocimiento facial y de voz.

2.1.16.1. Funcionamiento del Módulo

1. **Recepción de Órdenes**:

- El módulo de biometría recibe órdenes mediante ESP-NOW desde la placa central cuando el sistema entra en modo de desactivación.
- Si el módulo de biometría confirma que los datos biométricos son correctos, envía una respuesta a la placa central.

2. **Captura y Procesamiento de Datos**:

- **Sensor de Huella**: Utiliza el sensor FPM10A, que se alimenta con una fuente de voltaje de 3.6-6V y tiene un consumo de 150 mA. Este sensor se comunica mediante UART TTL y utiliza la librería *Adafruit_Fingerprint* para Arduino.
- **Micrófono**: Utiliza el micrófono INMP441, que trabaja bajo el protocolo I2S. Los archivos de audio, en formato WAV, se guardan en una memoria SD utilizando la librería SD_MMC.
- **Cámara**: Utiliza la cámara OV2640 conectada al ESP32 AI Thinker. La captura de imágenes se realiza con la librería ESP-CAM.

3. **Envío de Datos al Servidor**:

- Los archivos de audio y video se fragmentan y se envían al servidor mediante el método POST.
- El servidor procesa los datos y envía una respuesta de confirmación.

Nota

Revisar en anexos parte del código de programación donde se evidencia esta fragmentación y envió de los archivos al servidor, la recepción de archivos se explica más claramente en la fase 2.

2.1.16.2. Diagrama de Funcionamiento

Figura 17

Diagrama de funcionamiento del módulo de biometría.

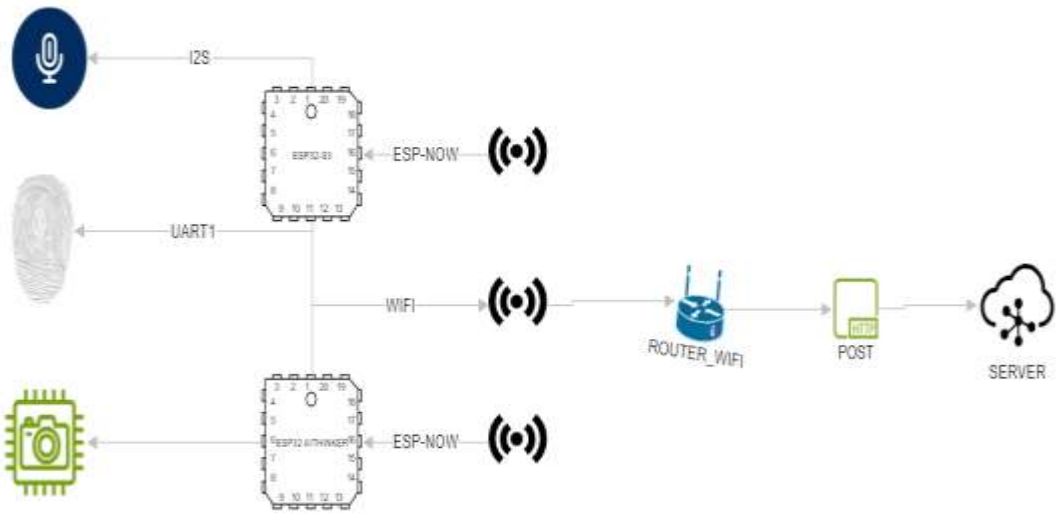
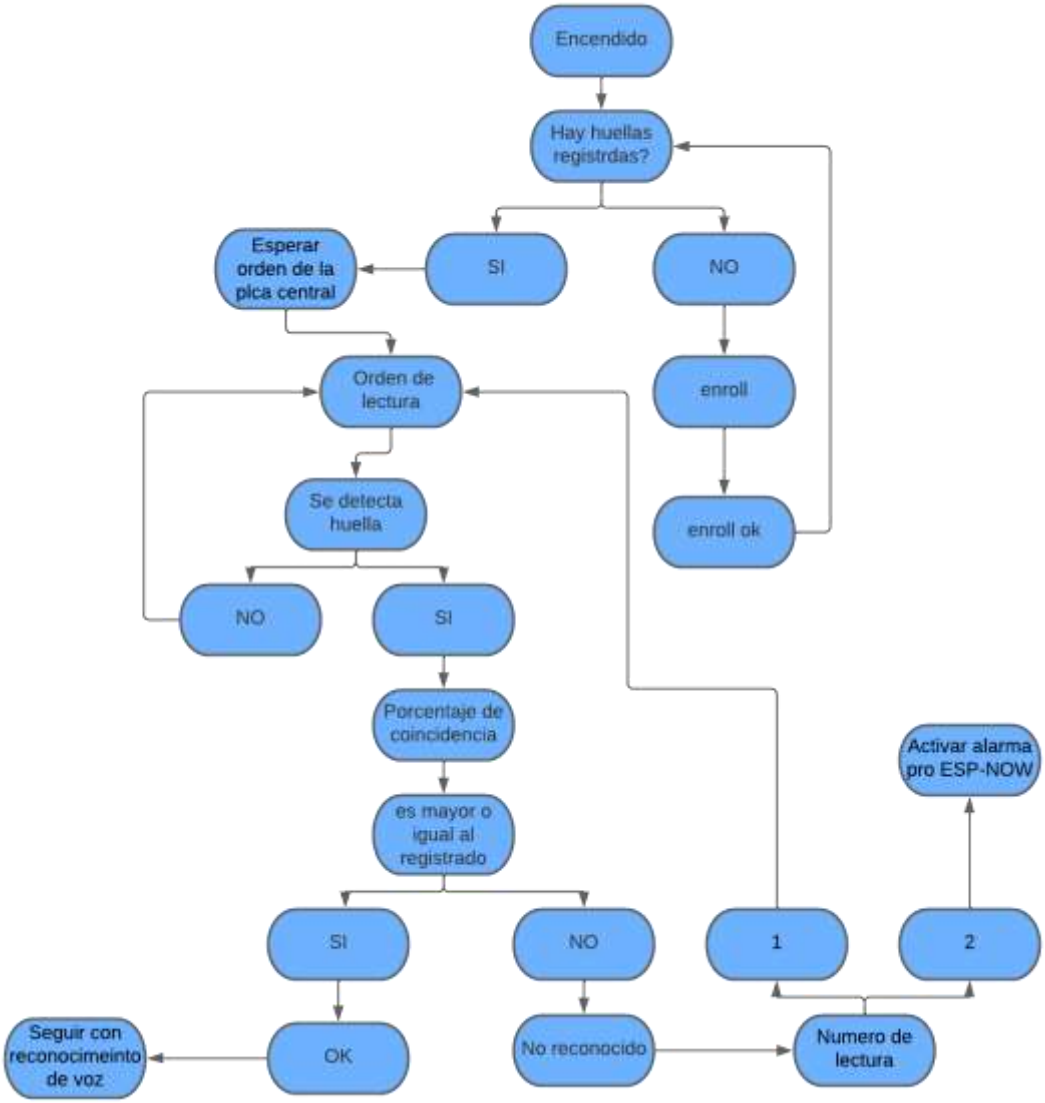


Figura 18

Diagrama código de programación control sensor de huella

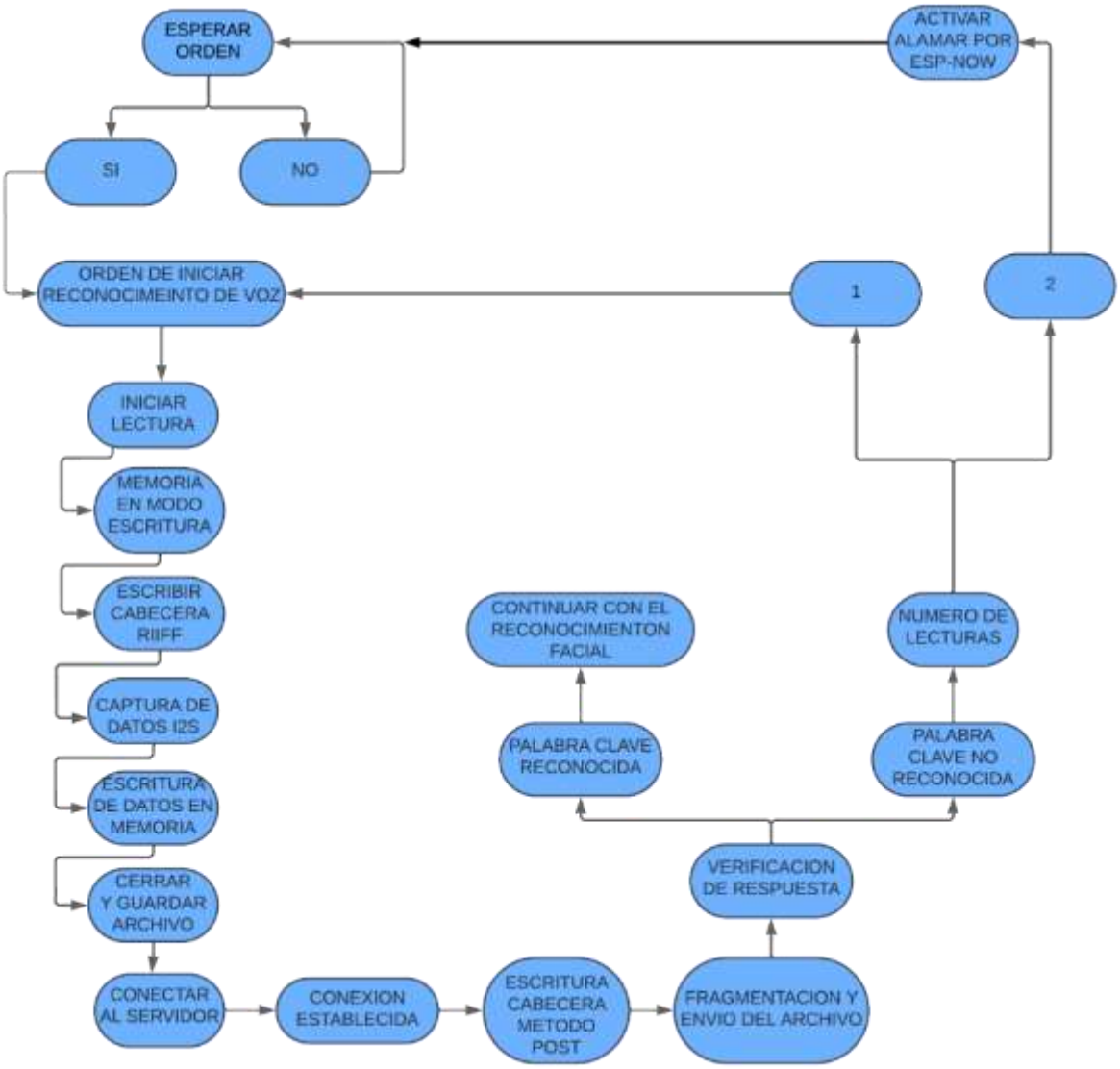


2.1.16.3. Captura de Audio y Envío al Servidor. El micrófono INMP441 graba audio en formato WAV, que se guarda en una memoria SD. El archivo se envía al servidor

fragmentado mediante POST. En el servidor se reconstruye el archivo y ejecuta un script en Python para el reconocimiento de voz.

Figura 19

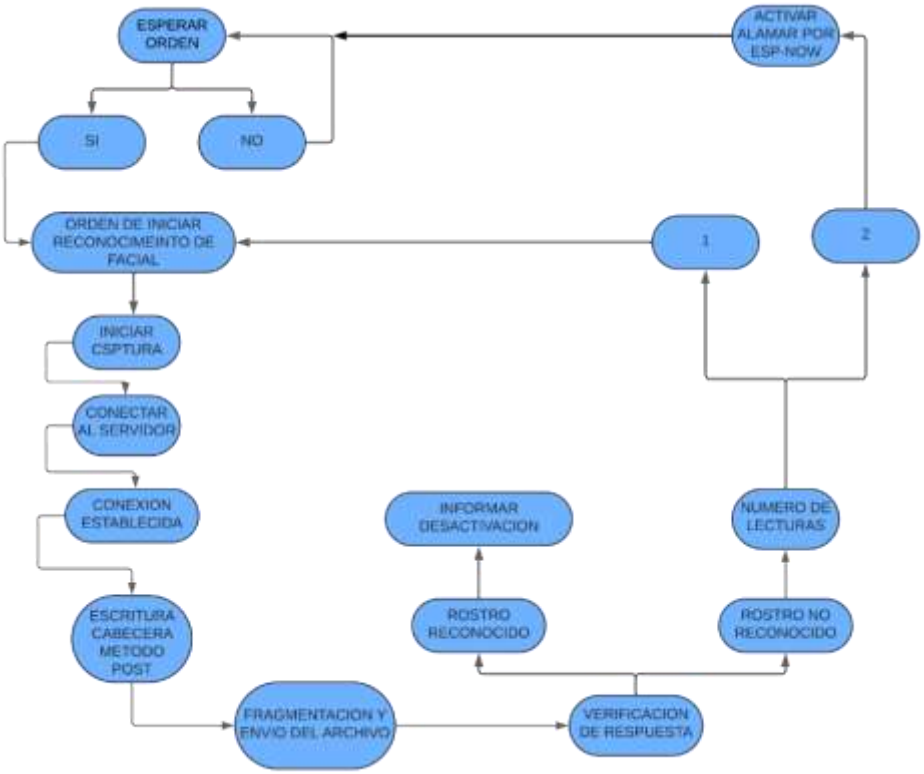
Diagrama de código de programación para envió de archivo de audio al servidor



2.1.16.4. Captura de Imagen y Envío al Servidor. La cámara OV2640 captura imágenes que se almacenan temporalmente en la RAM de la ESP32 AI *Thinker*. Las imágenes se envían al servidor fragmentadas y, tras la verificación, la placa central se desactiva si el reconocimiento es exitoso.

Figura 20

Diagrama de código de programación para el reconocimiento facial



Nota: En la captura de la imagen se debe trabajar en la distancia e iluminación al momento de la captura ya que se presentaron fallas en esta parte ya que la imagen no era clara o el rostro estaba muy alejado no era posible su reconocimiento, sin embargo, cuando se lograr una buena captura el sistema lograba reconocer el rostro.

2.1.16.5. Cálculo de Consumo de Corriente del Módulo de Biometría

Componentes y Consumo

1. **ESP32-S3**
    - Voltaje de operación: 3.3V
    - Consumo promedio: 150 mA (picos de hasta 500 mA)
2. **ESP32 AI Thinker**
    - Voltaje de operación: 3.3V
    - Consumo promedio: 200 mA (picos de hasta 400 mA)
3. **Sensor de Huella FPM10A**
    - Voltaje de operación: 3.6-6V
    - Consumo promedio: 150 mA
4. **Micrófono INMP441**
    - Voltaje de operación: 3.3V
    - Consumo promedio: 50 mA
5. **Cámara OV2640**
    - Voltaje de operación: 3.3V
    - Consumo promedio: 250 mA

Suma de los Consumos

- ESP32-S3: 150 mA
- ESP32 AI *Thinker*: 200 mA
- Sensor de Huella: 150 mA
- Micrófono: 50 mA
- Cámara: 250 Ma

Consumo total (promedio):

$$Consumo\ total = 150\ mA + 200\ mA + 150\ mA + 50\ mA + 250\ mA$$

$$Consumo\ total = 150\ mA + 200\ mA + 150\ mA + 50\ mA + 250\ mA$$

$$Consumo\ total = 800\ mA$$

$$Consumo\ total = 0.8\ A$$

Consideraciones Adicionales

Se recomienda una fuente de alimentación capaz de manejar al menos 1.5A para cubrir los picos de corriente y asegurar un funcionamiento estable del sistema, estos picos de corriente no se

los toma en cuenta en el cálculo de la UPS ya que estos no son constantes sino momentáneos lo que no requerirán mucha potencia de la UPS

2.1.16.6. Diseño de la PCB en Eagle. Con esta información, se procede al diseño de la PCB en Eagle, incluyendo:

ESP32-S3 para el control del micrófono y el sensor de huella.

ESP32 AI Thinker para la conexión y procesamiento de la cámara.

Componentes adicionales como el sensor de huella, el micrófono y la cámara.

La distribución de los componentes y el ruteo de las pistas se realizarán para minimizar interferencias y asegurar una alimentación adecuada para cada componente.

Figura 21

PCB módulo de biometría

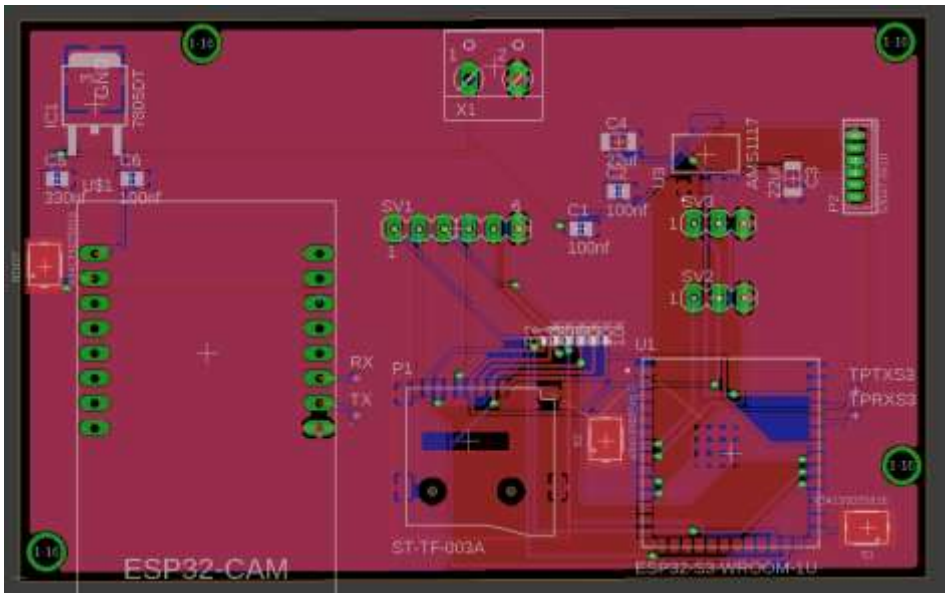
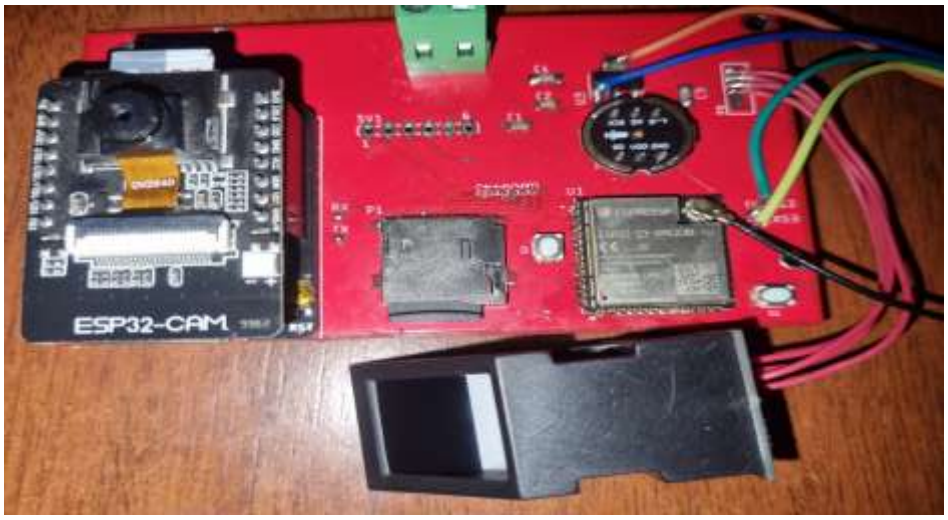


Figura 22

módulo de biometría con sus componentes



2.1.17. Control Remoto con Comunicación ESP-NOW para Sistema de Seguridad

El control remoto utiliza la tecnología ESP-NOW para comunicarse con la placa central y cuenta con cuatro botones, cada uno asignado a una función específica. Las dos funciones principales son la activación y desactivación del sistema de seguridad, mientras que los otros dos botones están reservados para funciones futuras, como la apertura de un portón de garaje o la activación de otros actuadores.

2.1.17.1. Funciones del Control Remoto.

1. **Activación del Sistema**:

   Acción: Presionar el botón de activación.

   Procedimiento: Al presionar este botón, se envía una señal a la placa central para iniciar la secuencia de activación del sistema de seguridad.

   Resultado: La placa central recibe la señal y comienza a monitorear los sensores conectados.

2. **Desactivación del Sistema**:

   Acción: Presionar el botón de desactivación.

Procedimiento: Al presionar este botón, se envía una orden a la placa central para desactivar el sistema.

Resultado: La placa central deja de considerar las lecturas de los sensores PIR y tamper mientras se realiza la verificación biométrica.

3. **Funciones Futuras**:

Acción: Presionar los botones reservados.

Aplicaciones Posibles: Apertura de un portón de garaje para el ingreso de vehículos o la activación de otros actuadores.

Configuración: Estas funciones pueden ser configuradas en el futuro según las necesidades específicas del usuario.

2.1.17.2. Configuración Electrónica del Control Remoto.

Soc: El control remoto está basado en el ESP32-S3.

Pulsadores: Equipado con cuatro pulsadores, cada uno con resistencias en configuración *pull-up* para detectar la pulsación del botón.

Antena Wifi: El ESP32-S3 no tiene una antena Wifi incorporada, pero cuenta con un conector coaxial que permite la conexión de una antena externa. Dependiendo de la referencia de la antena, se puede aumentar la distancia de cobertura del control remoto.

2.1.17.3. Diagrama y Código de Funcionamiento.

Figura 23

Diagrama de Funcionamiento del Control Remoto

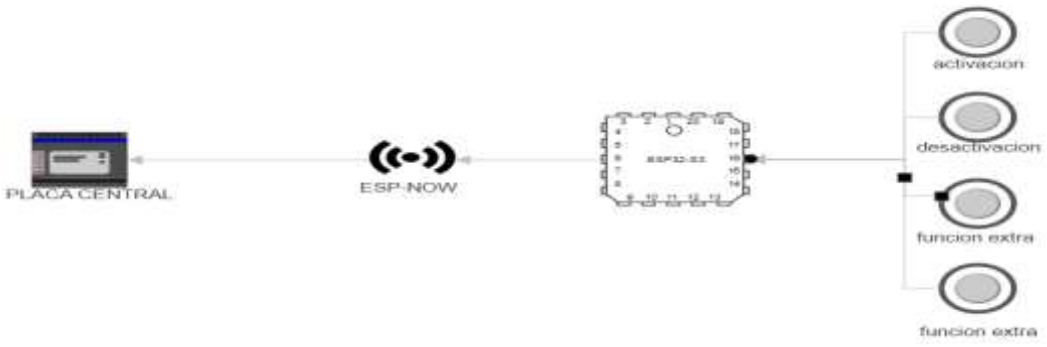
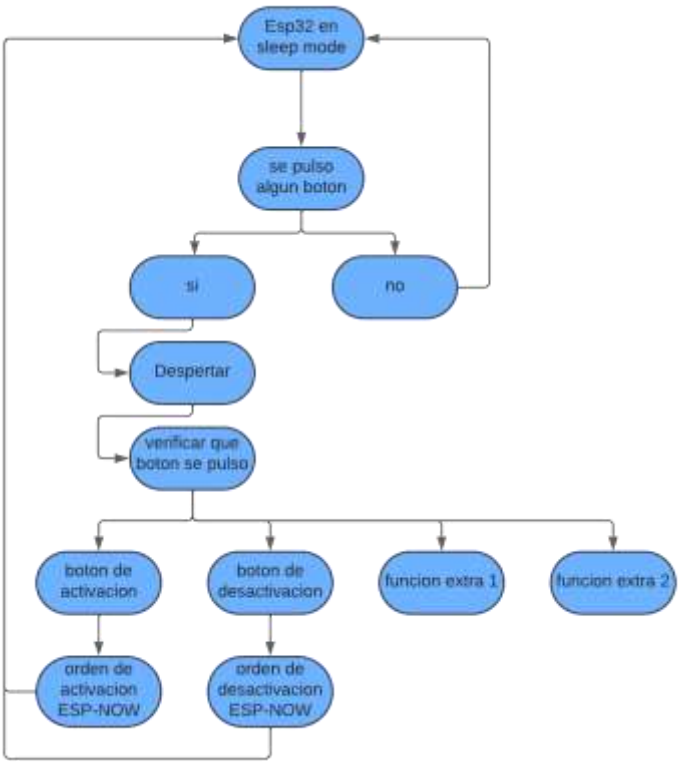


Figura 24

Diagrama del Código de Programación del Control Remoto



(Diagrama mostrando el flujo del código de programación utilizado en el ESP32-S3 para gestionar las funciones del control remoto)

2.1.18. Cálculo de UPS

Para calcular la capacidad de la UPS adecuada con los nuevos datos proporcionados y considerando un tiempo de respaldo de 24 horas, sigue los siguientes pasos:

1. **Consumo total en amperios (A)**:
    - Consumo módulo de multiplexación: 3,84 A
    - Consumo módulo de biometría: 0,8 A
    - Consumo placa central: 0,8 A
    - Consumo módulo de relés: 0,2 A

Consumo total:

Consumo total=3,84*A*+0,8*A*+0,8*A*+0,2*A*=5,64*A*

Consumo total=3,84*A*+0,8*A*+0,8*A*+0,2*A*=5,64*A*

2. **Potencia total en vatios (W)**:

   Asumiendo que el sistema funciona a 12V:

   Potencia (W)=12*V*×5,64*A*=67,68*W*Potencia (W)=12*V*×5,64*A*=67,68*W*

3. **Energía necesaria en vatios-hora (Wh)** para 24 horas:

   Energı´a necesaria (Wh)=67,68*W*×24*h*=1624,32*Wh*Energı´a necesaria (Wh)=67,68*W*×24 *h*=1624,32*Wh*

4. **Factor de carga (20-25%)**:

   - Para asegurar que la UPS no esté funcionando constantemente al 100% de su capacidad, se agrega un margen de seguridad.
   - Multiplicamos la energía necesaria por 1.25 (25% de margen de seguridad):

   Energı´a total con margen (Wh)=1624,32*Wh*×1.25=2030,4*Wh*Energı´a total con margen (Wh)=1624,32*Wh*×1.25=2030,4*Wh*

Revisando estos pasos:

1. **Consumo total (A)**:

   3,84*A*+0,8*A*+0,8*A*+0,2*A*=5,64*A*3,84*A*+0,8*A*+0,8*A*+0,2*A*=5,64*A*

2. **Potencia total (W)**:

   12*V*×5,64*A*=67,68*W*12*V*×5,64*A*=67,68*W*

3. **Energía necesaria (Wh)**:

   67,68*W*×24*h*=1624,32*Wh*67,68*W*×24*h*=1624,32*Wh*

Nota: Debido a que una UPS con la capacidad necesaria tiene un costo significativo en el mercado, solo se presentarán los cálculos para su evaluación. Este cálculo está realizado para el caso más extremo de consumo, y su implementación real se planteará según las necesidades y posibilidades del cliente.

2.2. Resultados del objetivo 2

2.2.1. Explicación del Proceso para la Recepción y Guardado de Archivos en PHP

Estos scripts en PHP son responsables de procesar las solicitudes HTTP utilizando el método POST para recibir y manejar archivos desde el sistema de seguridad. A continuación, se describen los pasos y funcionalidades de estos scripts, cada uno especializado en un tipo de archivo: uno para archivos de audio en formato WAV y otro para archivos de imagen en formato JPG.

.

2.2.1.1. Script para Recepción de Archivos de Audio (WAV).

1. Recepción del Archivo:

El script recibe el archivo de audio mediante una solicitud POST.

2. Reconstrucción del Archivo:

Si el archivo se envía por partes, el script debe ensamblar todas las partes para formar el archivo completo.

3. Determinación del Tipo de Archivo:

Verifica que el archivo recibido es de tipo WAV.

4. Verificación y Almacenamiento:

Verifica si un archivo con el mismo nombre ya existe en el directorio de almacenamiento.

Si existe, el archivo antiguo se elimina.

Guarda el nuevo archivo en la ubicación designada.

5. Ejecución del Script de Reconocimiento de Voz:

Ejecuta el script de reconocimiento de voz en el archivo de audio guardado.

2.2.1.2. Script para Recepción de Archivos de Imagen (JPG).

1. Recepción del Archivo:

El script recibe el archivo de imagen mediante una solicitud POST.

2. Reconstrucción del Archivo:

Si el archivo se envía por partes, el script debe ensamblar todas las partes para formar el archivo completo.

3. Determinación del Tipo de Archivo:

Verifica que el archivo recibido es de tipo JPG.

4. Verificación y Almacenamiento:

Verifica si un archivo con el mismo nombre ya existe en el directorio de almacenamiento.

Si existe, el archivo antiguo se elimina.

Guarda el nuevo archivo en la ubicación designada.

5. Ejecución del Script de Reconocimiento Facial:

Ejecuta el script de reconocimiento facial en el archivo de imagen guardado.

Figura 25

Diagrama de Código de Programación del Script de Recepción de Archivo de Audio

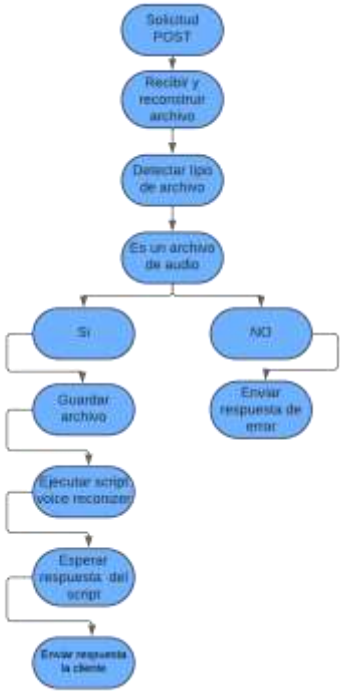
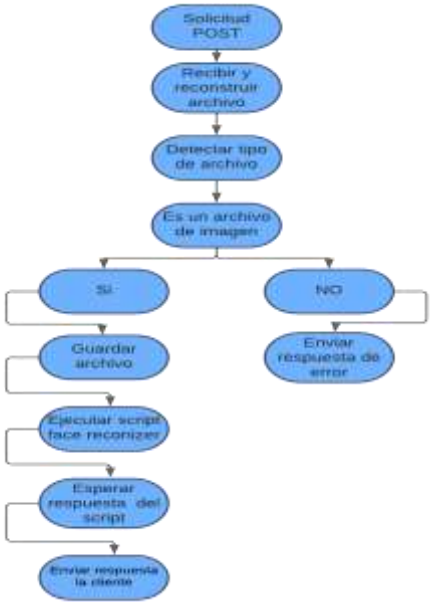


Figura 26

Diagrama de Código de Programación del Script de Recepción de Archivo de Imagen



Estos procesos aseguran que los archivos sean recibidos, almacenados y procesados correctamente, proporcionando una integración eficiente con el sistema de seguridad.

2.2.2. Script reconocimiento de voz

Este script se ejecuta bajo la orden del script de recepción y guardado, se toma el archivo de audio previamente guardado y se lo carga al script. mediante la librería *speech recognition* se llama a la función de convertir voz a texto de Google se extrae las palabras del audio y se guardan en un arreglo de strings, la palabra clave se encuentra guardada en una variable tipo string, con la cual se compara con cada posición del vector, si encuentra una coincidencia se envía una respuesta afirmativa al script de recepción y una respuesta negativa si no se encuentra ninguna coincidencia. Figura 24 Diagrama código de programación reconocimiento de voz

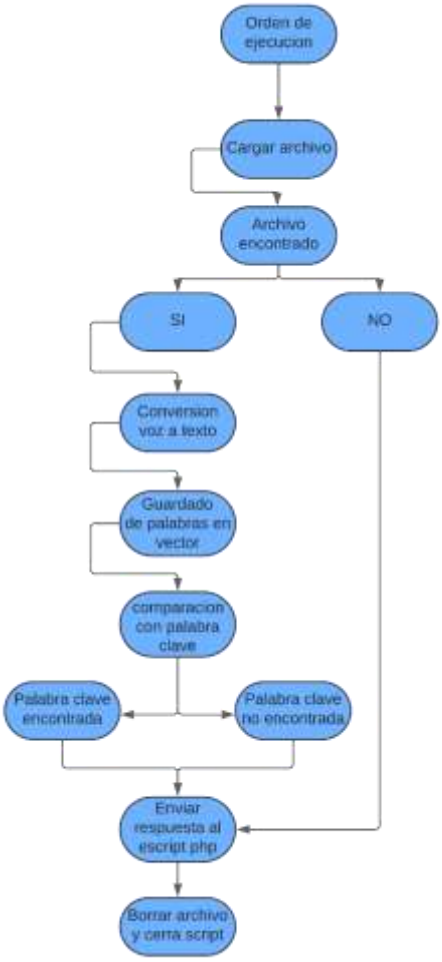
2.2.2.1. Explicación del Script de Reconocimiento de Voz. Este script de reconocimiento de voz se ejecuta después de que el archivo de audio ha sido recibido y guardado. Utiliza la librería *speech_recognition* para convertir el audio en texto. Luego, busca una palabra clave específica en el texto transcrito y envía una respuesta basada en si la palabra clave se encuentra o no.

Descripción del Proceso

1. Recepción del Archivo de Audio:
   El script toma el archivo de audio previamente guardado por el script de recepción.
2. Inicialización del Reconocedor:
   Utiliza la librería speech_recognition para inicializar un reconocedor de voz.
3. Carga del Audio:
   El archivo de audio se carga utilizando *AudioFile.*
4. Conversión de Voz a Texto:
   El método *recognize_google* de la librería speech_recognition se utiliza para convertir el audio en texto. Este método llama a la API de Google para realizar la transcripción.
5. Procesamiento del Texto:
   El texto transcrito se divide en palabras y se guarda en un arreglo de strings.
6. Búsqueda de la Palabra Clave:
   La palabra clave, almacenada en una variable tipo string, se compara con cada palabra en el arreglo de strings.
7. Envío de la Respuesta:
   Si se encuentra la palabra clave, se envía una respuesta afirmativa al script de recepción.
   Si no se encuentra la palabra clave, se envía una respuesta negativa.

Figura 27

Diagrama código de programación reconocimiento de voz



2.2.3. Scripts de Reconocimiento Facial

Esto es un poco complejo debido a la necesidad de crear un modelo de reconocimiento facial. A continuación, se describen los pasos necesarios para la creación del modelo y su uso para el reconocimiento de rostros.

2.2.3.1. Captura de Imágenes. Se captura una serie de imágenes del rostro de la persona realizando diferentes gestos y con diferentes accesorios (lentes, sin lentes).

Creación del Modelo:

- Se ejecuta un script de entrenamiento que utiliza las imágenes capturadas.
- El script utiliza *OpenCV* y el método *Eigenface* para crear un modelo.
- El modelo se guarda en un archivo XML.

Reconocimiento Facial:

- Se recibe una imagen desde el módulo de biometría.
- El script carga el modelo desde el archivo XML.
- La imagen recibida se compara con el modelo.
- Se determina si hay una coincidencia.

Envío de la Respuesta:

- Se envía una respuesta al script PHP indicando si el rostro fue reconocido o no.

Eliminación del Archivo de Imagen:

- El archivo de imagen procesado se elimina para evitar conflictos futuros con los archivos nuevos.

Figura 28

Diagrama de Código de Programación Captura de Imágenes

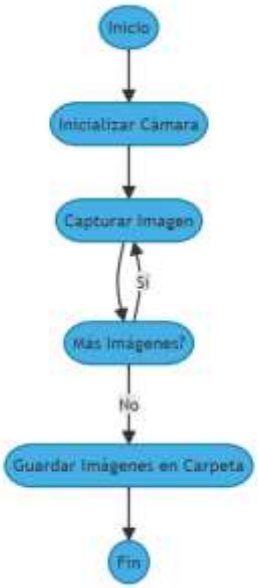


Figura 29

Diagrama de Código de Programación Creación del Modelo

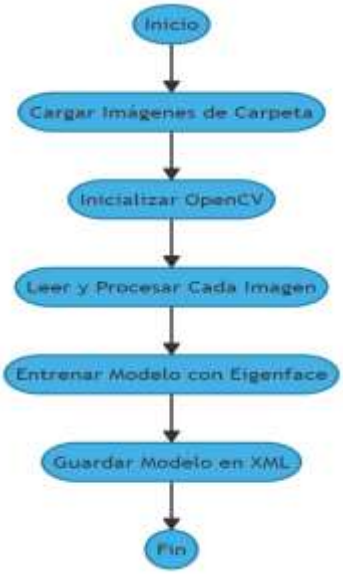
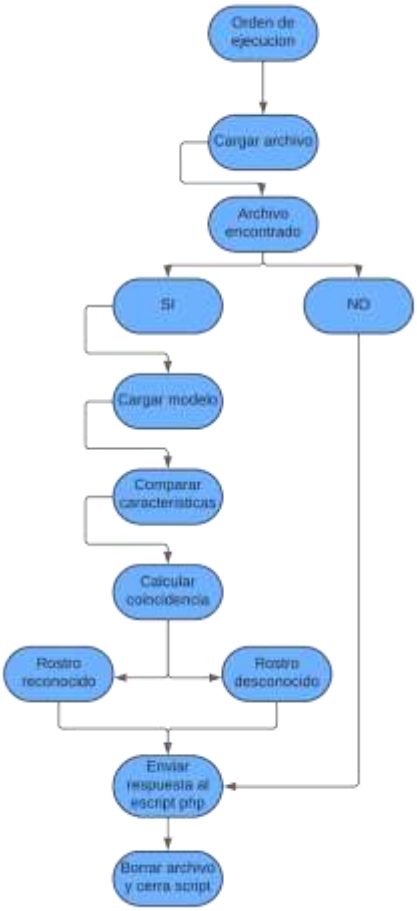


Figura 30

Diagrama código de programación reconocimiento facial



Nota sobre el Proceso de Creación del Modelo: Actualmente, el proceso de creación del modelo se realiza en una computadora y el modelo se sube al servidor para su ejecución. Sin embargo, en el futuro, se podría desarrollar un sistema más dinámico para registrar rostros de manera más eficiente y automática, revisar en anexos los códigos de programación de cada una de las fases de reconocimiento facial.

2.2.4. Script Guardado de Estados de Alarma

Este script se encarga de recibir el estado de la alarma enviado desde la placa central. La placa central envía valores numéricos (1, 2 y 3), donde:

1 indica activación,

2 indica desactivación, y

3 indica que la alarma se ha disparado al detectar un intruso.

El script está desarrollado en PHP y utiliza el método POST para recibir los datos.

2.2.4.1. Descripción del Proceso

1. **Recepción de Datos:**
   El script PHP recibe los datos del estado de la alarma mediante el método POST.
2. **Conexión a la Base de Datos:**
   Se establece una conexión con una base de datos MySQL.
3. **Almacenamiento de Datos:**
   Los datos recibidos se almacenan en una tabla específica de la base de datos.
4. **Confirmación de Almacenamiento:**
   Se verifica si los datos se han almacenado correctamente.

Figura 31

Diagrama de código almacenamiento variables de estado

2.2.5. Script Visualización de Estado de Alarma

Este script se encarga de recuperar los datos de la base de datos y mostrarlos en una página web. La visualización se realiza en el navegador y, por ahora, está diseñada para funcionar de manera local.

Descripción del Proceso

1. Conexión a la Base de Datos:

   El script se conecta a la base de datos MySQL para recuperar los datos.

2. Recuperación de Datos:

   Los datos del estado de la alarma se recuperan de la base de datos.

3. Visualización en Página Web:

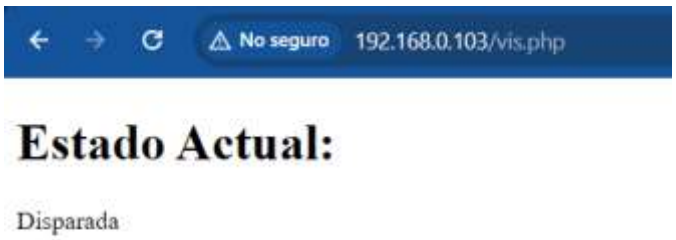
   - Los datos recuperados se muestran en una página web utilizando HTML.

Figura 32

diagrama código de visualización de datos de estado

Figura 33

página de visualización de estados de alarma



Nota: Esta aplicación estaba planeada como una aplicación móvil, pero debido a la complejidad del proyecto y el tiempo de desarrollo, se desarrolla como una página web. A partir

de este punto, se puede crear una aplicación móvil para visualizar estos datos, además de mejorar el auto actualizado de la página para mostrar los datos actualizados en tiempo real. Esto proporcionará una mayor flexibilidad y accesibilidad, permitiendo a los usuarios monitorear el estado de la alarma desde cualquier lugar.

2.3. Resultados del objetivo 3

2.3.1. Instalación de la placa central y módulos en gabinete para prueba de funcionamiento

La instalación del sistema de seguridad en el gabinete implica varios pasos importantes para garantizar un funcionamiento adecuado. Primero, es crucial asegurarse de que el gabinete tenga el espacio y la ventilación necesarios para alojar todos los componentes de manera segura. Luego, se debe colocar la fuente de alimentación en una posición estable dentro del gabinete y conectarla correctamente a la placa central y los módulos adicionales.

El montaje de la placa central y los módulos debe hacerse de manera cuidadosa para evitar daños y garantizar un acceso fácil a las conexiones. Una vez que todos los componentes están instalados, es importante verificar visualmente que todas las conexiones estén seguras y que no haya cables sueltos.

Después de encender la fuente de alimentación, se deben realizar pruebas exhaustivas para asegurarse de que todos los componentes del sistema respondan correctamente. Esto incluye verificar que la placa central pueda enviar y recibir señales de manera efectiva, así como asegurarse de que los módulos adicionales funcionen según lo esperado.

Finalmente, cualquier ajuste necesario en la configuración o disposición de los componentes debe realizarse antes de considerar la instalación completa. Mantener un registro detallado de los pasos realizados y cualquier problema encontrado durante el proceso de instalación puede ser útil para futuras referencias y solución de problemas.

Figura 34

Montaje de módulos y placa central en gabinete

2.3.2. Acoplamiento del Sistema de Seguridad al Servidor

El servidor se encuentra localmente para facilitar las pruebas, ya que inicialmente se planeaba usar un túnel mediante ngrok. Sin embargo, debido a un problema con las solicitudes desde el sistema al servidor, se opta por realizar pruebas de manera local. Este problema se planea solucionar en el futuro.

1. Configuración del Servidor
2. Conexión Local:

   El servidor se encuentra localmente en la red.
3. Obtención de la IP Local:

Se obtiene la dirección IP local del servidor. Esta IP es un parámetro importante para la comunicación del sistema.

4. Configuración del Sistema de Seguridad

1. Conexión a la Red del Servidor:

   El sistema y cada uno de sus módulos deben conectarse a la misma red que el servidor.

2. Modo Desactivado:

   Una vez conectado el sistema a la red, entra en modo desactivado y espera la orden de activación desde el control inalámbrico.

Nota: El acoplamiento del sistema de seguridad al servidor se realiza localmente para facilitar las pruebas. Se espera solucionar los problemas de comunicación para poder implementar el sistema en un entorno remoto en el futuro. Una vez que se establezca la conexión adecuada, el sistema estará listo para su implementación en un entorno de producción.

2.3.3. Modo de Activación del Sistema de Seguridad

Cuando el sistema recibe la instrucción de activarse desde el control, se inicia una secuencia de eventos diseñada para garantizar la efectividad del sistema. Aquí están los pasos clave:

Advertencia de Activación:

En primer lugar, el sistema emite un sonido corto de advertencia en la sirena para indicar que la alarma se ha activado. Esta advertencia sirve como una notificación inicial para cualquier persona en el área protegida.

Inicio de Lectura de Sensores:

El ESP32 en la placa central envía una señal al PIC que controla los multiplexores para que comience la lectura de los sensores. Esto asegura que el sistema esté preparado para detectar cualquier actividad sospechosa una vez que esté activado.

Actualización del Estado al Servidor:

Simultáneamente, el sistema envía al servidor el estado de activación. Esta información permite que el servidor registre el estado actual del sistema y esté al tanto de cualquier cambio.

Permanencia del Estado de Activación:

El estado de activación permanece activo hasta que se reciba la orden de desactivación del sistema. Durante este tiempo, el sistema está preparado para detectar intrusiones y responder de manera apropiada.

Detección de Intrusión:

Si se detecta una intrusión mientras el sistema está activado, el PIC informa al ESP32 de este evento. A continuación, el ESP32 activa la sirena y envía al servidor el estado de intrusión para su registro y posible acción posterior.

Este modo de activación del sistema garantiza una respuesta rápida y eficiente ante cualquier intento de intrusión, proporcionando así una protección efectiva para el área vigilada.

Se realizaron pruebas exitosas de este modo de activación del sistema, lo que confirma su eficacia y funcionamiento adecuado en situaciones reales. Esta validación es crucial para garantizar la fiabilidad del sistema y su capacidad para responder de manera efectiva ante posibles amenazas.

2.3.4. Modo de Desactivación del Sistema de Seguridad

Cuando el sistema recibe la orden de desactivación desde el control, se inicia un proceso diseñado para garantizar la seguridad y la autenticación del usuario. Aquí están los pasos clave:

Informar al Servidor:

En primer lugar, el sistema informa al servidor que se ha recibido la orden de desactivación. Esta comunicación asegura que el servidor esté al tanto del cambio de estado del sistema.

Inicio de Verificación Biométrica:

A continuación, se envía una orden al módulo de biometría para que comience la verificación biométrica del usuario. Esto implica la captura de la huella dactilar, el reconocimiento facial y la voz del usuario para su autenticación.

Respuesta del Módulo de Biometría:

La placa central espera la respuesta del módulo de biometría para determinar si la desactivación del sistema es válida. Si la verificación biométrica es exitosa, se procede con la desactivación del sistema

Acciones según Resultado:

Si la verificación biométrica es satisfactoria, el sistema se desactiva completamente y se detiene cualquier alerta o activación de la sirena. En caso contrario, si la verificación biométrica falla o no es concluyente, el sistema puede activar la sirena como medida de seguridad adicional.

Este modo de desactivación garantiza que solo los usuarios autorizados puedan desactivar el sistema, proporcionando así una capa adicional de seguridad y protección.

Tras llevar a cabo pruebas exhaustivas, se confirma el éxito del modo de desactivación del sistema. Sin embargo, durante estas pruebas, se identificaron problemas significativos con la verificación facial. La captura del rostro puede verse afectada por cambios en el entorno o un enfoque inadecuado, lo que resulta en fallas recurrentes en la verificación facial. Estos desafíos subrayan la necesidad de trabajar en la optimización del proceso de captura del rostro para garantizar su fiabilidad y precisión en diversas condiciones. Esta validación es crucial para asegurar la integridad y la efectividad del sistema de seguridad en situaciones reales.

3. Conclusiones

El desarrollo de módulos para el control de sensores ha sido exitoso, permitiendo gestionar una cantidad considerable de sensores con un número limitado de pines en el controlador. Este logro cumple parte del primer objetivo, que era la conexión de hasta 32 sensores. Además, se ha conseguido el control de actuadores, específicamente el manejo de la sirena de la alarma. En cuanto al módulo de biometría, que representaba el mayor desafío, se logró la funcionalidad necesaria para la captura y envío de archivos al servidor.

En resumen, el proyecto ha avanzado significativamente, con la mayoría de sus funciones desarrolladas con éxito tanto en software como en hardware. No obstante, aún enfrenta desafíos que deben abordarse para lograr su plena realización. Aunque se han identificado avances notables, como el éxito en las pruebas de activación y desactivación del sistema, es crucial reconocer las fallas significativas encontradas durante las pruebas, especialmente en la captura de rostros para la verificación facial. Estas dificultades se atribuyen a la variabilidad del entorno y a un enfoque inadecuado durante la captura, lo que resulta en fallas recurrentes en la verificación facial. Además, se destaca la necesidad de completar aspectos pendientes del proyecto, como la implementación de la visualización en la aplicación móvil.

Abordar estos desafíos con un enfoque dedicado permitirá fortalecer la seguridad y la efectividad del sistema en su conjunto. Si bien el proyecto actual establece una base sólida, es importante reconocer su potencial de desarrollo futuro. Esto podría implicar la exploración de nuevas funcionalidades, la integración de tecnologías emergentes o la adaptación del sistema a diferentes contextos de aplicación. Al mantener una visión orientada hacia el futuro y un compromiso con la mejora continua, el sistema tiene el potencial de evolucionar y satisfacer las necesidades cambiantes del usuario y del entorno tecnológico.

4. Recomendaciones y trabajos futuros

4.1. Mejorar la Captura de Imágenes

Se recomienda mejorar la captura de imágenes utilizando una ESP-CAM o una cámara de mejor resolución para obtener resultados más claros y nítidos.

4.2. Seguridad del Servidor

En este trabajo no se abordó la seguridad del servidor. Este aspecto es fundamental y debe ser trabajado en futuras implementaciones para garantizar una solución completa y segura.

4.3. Visualización y Configuración del Sistema

Se debe trabajar en la parte de visualización utilizando una aplicación más dinámica,

Esta aplicación también debería permitir la configuración del sistema, incluyendo parámetros como la IP, la red Wifi y la dirección MAC, para evitar la necesidad de cargar el código cada vez que estos parámetros cambien.

Referencias Bibliográficas

Alexander, J., Colimba, A., Stheven, J., & Cabrera, M. (n.d.). *Sistema de Acceso RFID*.

Andrés, C., Godoy, G., José, O., & Parra, S. (n.d.). *Sistema de seguridad para locales comerciales mediante Raspberry Pi, cámara y sensor PIR **. http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/851/1369

Augusto, C., & Gil, P. (2016). *Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT*. http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/794/1314

Barillaro, S., De Luca, G., Valiente, W., Carnuccio, E., García, G., Volker, M., Giulianelli, D., Casas, N., & Pérez, M. (n.d.). *Diseño de sistema IoT de monitoreo y alarma para personas mayores*.

¿Cómo funciona un servidor web? 【Características】. (n.d.). Retrieved April 27, 2024, from https://axarnet.es/blog/como-funciona-servidor

etiampro Pir Sensor With Double Twin Optics User Manual - Manuals+. (n.d.). Retrieved October 8, 2022, from https://manuals.plus/etiampro/pir-sensor-with-double-twin-optics-manual#axzz7hEnVbV98

KARINA DOLORES GAIBOR CARRILLO, F. A. L. M., Matemáticas, C., Físicas, Y., Bajo, D. E., Económicos, R., La, D. E., De, C., & Proyecto De Titulación, G. (n.d.). *DISEÑAR UN SISTEMA DE ALARMA INALÁMBRICO DE BAJO COSTO PARA LA PROTECCIÓN DE VIVIENDAS TIPO, EN SECTORESDE BAJO RECURSOS ECONÓMICOS DE LACIUDAD DE GUAYAQUIL*.

Lector De Huella Digital Arduino : 7 Steps (with Pictures) - Instructables. (n.d.). Retrieved May 7, 2022, from https://www.instructables.com/Lector-De-Huella-Digital-Arduino/

Mélany, C., Alayo, P., Zoe, P., Celis, A., Dionicio Guzmán, D. A., & Alarcon, J. A. (2019). Sistema de alarma doméstica a escala controlado por un aplicativo móvil Scale domestic alarm system controlled by a mobile application. *PUEBLO CONTINENTE*, *30*(1), 93–99. https://doi.org/10.22497/PuebloCont.301.30110

¿Qué es un detector magnético de apertura? (n.d.). Retrieved October 8, 2022, from https://www.tecnoseguro.com/faqs/alarma/que-es-un-detector-magnetico-de-apertura

¿Qué son los servidores web y por qué son necesarios? - Duplika. (n.d.). Retrieved April 27, 2024, from https://duplika.com/blog/que-son-los-servidores-web-y-por-que-son-necesarios/

Rodríguez, R., Vera, P., Giulianelli, D., & Cammarano, P. (n.d.). *Implementación con Raspberry PI de un Servidor Portátil de Contenidos*.

Rufino, C., Antonio, M., Manuel, J., Arreguín, R., Rivas-Araiza, E. A., Hurtado, E. G., Carlos, J., & Ortega, P. (2020). *Sistema de monitoreo y servidor WEB con Raspberry Pi para el control de un robot neumático* (Vol. 9, Issue 3). www.mecamex.net/revistas/LMEM

Swann Security. (2019, March 25). *Put the Heat on Crime with PIR Motion & Heat Sensor Cameras – New from Swann*. Recuperado de https://blog.swann.com/put-the-heat-on-crime-with-pir-motion-heat-sensor-cameras

HomeProtex. (n.d.). *An In-Depth Guide to PIR Technology: How It Works*. Recuperado de https://homeprotex.com/an-in-depth-guide-to-pir-technology

Electricity & Magnetism. (n.d.). *Passive infrared (PIR) sensor | How it works, Application & Advantages*. Recuperado de https://www.electricity-magnetism.org/passive-infrared-pir-sensor

Anexos

A.1. **Montaje sistema de seguridad**

A continuación, se muestra evidencia fotografías de cada uno de los módulos y del montaje del sistema

Figura 35

Módulo de multiplexación 8 canales

Figura 36

Control remoto

Figura 37

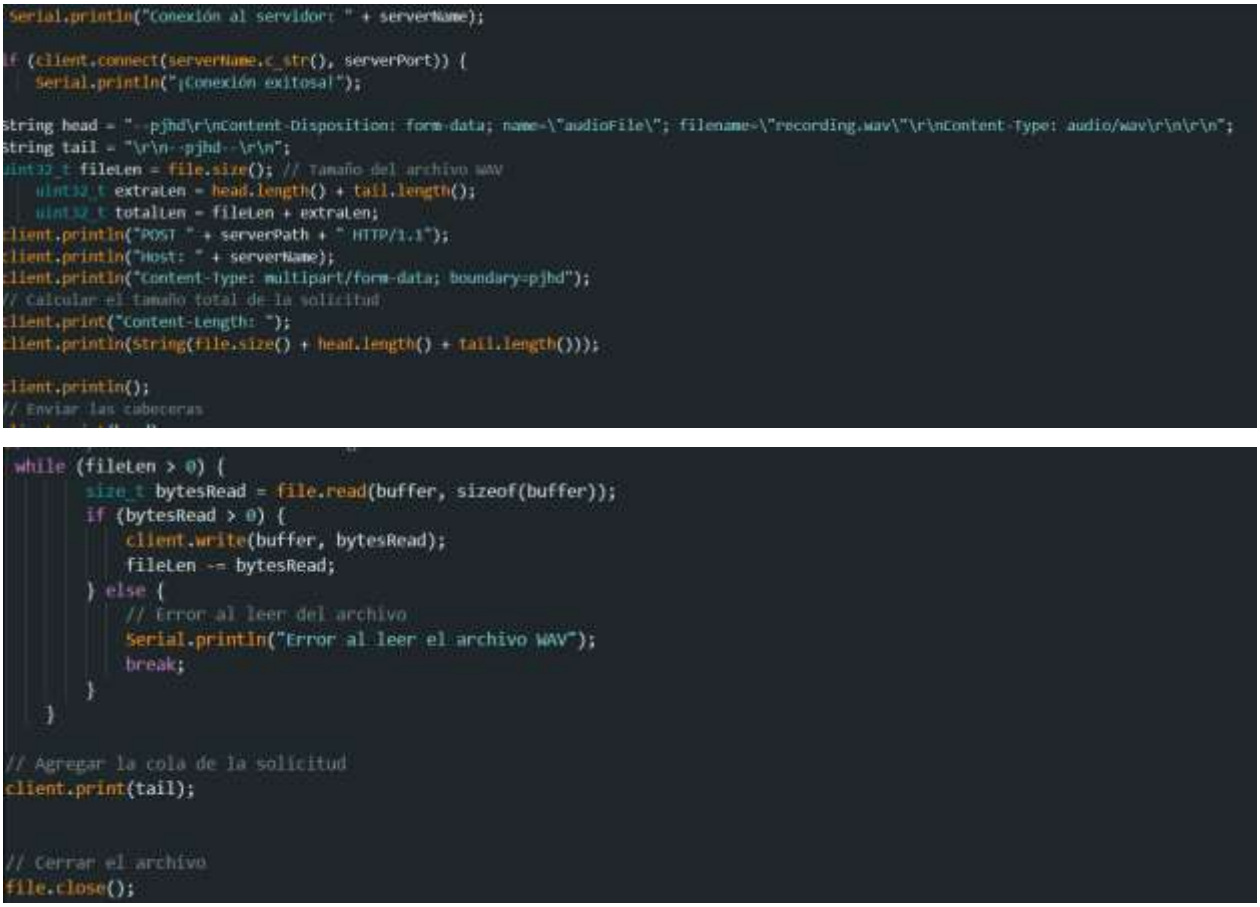
Servidor raspberry pi b+

A.2 Códigos envió de archivos de audio e imagen al servidor

En este parte se cargan las evidencias de parte de los códigos de programación para envió de archivos al servidor.

Figura 38

Código de envío de archivo WAV al servidor



```
Serial.println("Conexión al servidor: " + serverName);

if (client.connect(serverName.c_str(), serverPort)) {
    Serial.println("¡Conexión exitosa!");

String head = "--pjhd\r\nContent-Disposition: form-data; name=\"audioFile\"; filename=\"recording.wav\"\r\nContent-Type: audio/wav\r\n\r\n";
String tail = "\r\n--pjhd--\r\n";
uint32_t fileLen = file.size(); // Tamaño del archivo WAV
    uint32_t extraLen = head.length() + tail.length();
    uint32_t totalLen = fileLen + extraLen;
client.println("POST " + serverPath + " HTTP/1.1");
client.println("Host: " + serverName);
client.println("Content-Type: multipart/form-data; boundary=pjhd");
// Calcular el tamaño total de la solicitud
client.print("Content-Length: ");
client.println(String(file.size() + head.length() + tail.length()));

client.println();
// Enviar las cabeceras
```

```
while (fileLen > 0) {
        size_t bytesRead = file.read(buffer, sizeof(buffer));
        if (bytesRead > 0) {
            client.write(buffer, bytesRead);
            fileLen -= bytesRead;
        } else {
            // Error al leer del archivo
            Serial.println("Error al leer el archivo WAV");
            break;
        }
    }

// Agregar la cola de la solicitud
client.print(tail);


// Cerrar el archivo
file.close();
```

Nota: En este código se realiza la conexión al servidor y se fragmenta el archivo WAV para enviarlo al servidor.

Figura 39

Condigo envío de archivo JPG al servidor

```
if (client.connect(serverName.c_str(), serverPort)) {
  Serial.println("Connection successful");
  String head = "--hdmzpj\r\nContent-Disposition: form-data; name=\"imageFile\"; filename=\"hernan.jpg\"\r\nContent-Type: image/jpeg\r\n\r\n";
  String tail = "\r\n--hdmzpj--\r\n";
  uint32_t imageLen = fb->len;
  uint32_t extraLen = head.length() + tail.length();
  uint32_t totalLen = imageLen + extraLen;

  client.println("POST " + serverPath + " HTTP/1.1");
  client.println("Host: " + serverName);
  client.println("Content-Length: " + String(totalLen));
  client.println("Content-Type: multipart/form-data; boundary=hdmzpj");
  client.println();
  client.print(head);

  uint8_t *fbBuf = fb->buf;
  size_t fbLen = fb->len;
  for (size_t n=0; n<fbLen; n=n+1024) {
    if (n+1024 < fbLen) {
      client.write(fbBuf, 1024);
      fbBuf += 1024;
    }
    else if (fbLen%1024>0) {
      size_t remainder = fbLen%1024;
      client.write(fbBuf, remainder);
    }
  }
  client.print(tail);
```

Nota: En este código realiza la conexión al servidor y la fragmentación del archivo JPG para enviarlo al servidor.

A.3 **Scripts de recepción de archivos de audio e imagen en el servidor**

Figura 40

recepción de archivo de WAV

```php
<?php
$target_dir = "audio/";
$target_file = $target_dir  . basename($_FILES["audioFile"]["name"]);
$uploadOk = 1;
$audioFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
if (file_exists($target_file)) {
  echo "Sorry, file already exists.";
  $uploadOk = 0;
}
if ($_FILES["audioFile"]["size"] > 500000) {
  echo "Sorry, your file is too large.";
  $uploadOk = 0;
}
if($audioFileType != "wav" ) {
  echo "Sorry, only wav";
  $uploadOk = 0;
}
if ($uploadOk == 0) {
  echo "Sorry, your file was not uploaded.";
}
else {
  if (move_uploaded_file($_FILES["audioFile"]["tmp_name"], $target_file)) {

    echo "The file ". basename( $_FILES["audioFile"]["name"]). " has been uploaded??\n";
  }
  else {
    echo "Sorry, there was an error uploading your file.";
  }
}
echo exec("cd /var/www/html/audio && python3.9 reco.py");
?>
```

Nota: Este código recibe el archivo de audio y lo guarda en una carpeta en el servidor, posterior a esto ejecuta el script de reconocimiento de voz y captura la respuesta para enviarla al cliente

Figura 41

Recepción de archivo JPG

```php
<?php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["imageFile"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["imageFile"]["tmp_name"]);
  if($check !== false) {
    echo "File is an image - " . $check["mime"] . ".";
    $uploadOk = 1;
  }
  else {
    echo "File is not an image.";
    $uploadOk = 0;
  }
}
if (file_exists($target_file)) {
if ($_FILES["imageFile"]["size"] > 500000) {
 if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"
&& $imageFileType != "gif" ) {
  echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
  $uploadOk = 0;
}
if ($uploadOk == 0) {
else {
  if (move_uploaded_file($_FILES["imageFile"]["tmp_name"], $target_file)) {
    echo "The file ". basename( $_FILES["imageFile"]["name"]). " has been uploaded.";
  }
  else {
    echo "Sorry, there was an error uploading your file.";
  }
}
echo exec("python /var/www/html/uploads/reconocimiento.py");
```

A.4 C**aptura de imágenes y creación de modelo *eigenface***

Figura 42

Código captura de imágenes para creación de modelo

```
import cv2
import os
import imutils

personName = 'hernan'
dataPath = 'C:/Users/H&G Technologies/Documents/TESIS/reconoximiento facial/reconoximiento facial/data'
personPath = dataPath + '/' + personName
if not os.path.exists(personPath):
        print('Carpeta creada: ',personPath)
        os.makedirs(personPath)

cap = cv2.VideoCapture(0,cv2.CAP_DSHOW)
#cap = cv2.VideoCapture('Video.mp4')

faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_default.xml')
count = 0

while True:

        ret, frame = cap.read()
        if ret == False: break
        frame =  imutils.resize(frame, width=640)
        gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
        auxFrame = frame.copy()

        faces = faceClassif.detectMultiScale(gray,1.3,5)

        for (x,y,w,h) in faces:
                cv2.rectangle(frame, (x,y),(x+w,y+h),(0,255,0),2)
                rostro = auxFrame[y:y+h,x:x+w]
                rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
                cv2.imwrite(personPath + '/rotro_{}.jpg'.format(count),rostro)
                count = count + 1
        cv2.imshow('frame',frame)

        k =  cv2.waitKey(1)
        if k == 27 or count >= 300:
                break

cap.release()
cv2.destroyAllWindows()
```

Nota: Este código abre la cámara de la computadora y capturas las imágenes del rostro para el guardado en la carpeta donde le scripts de creación del modelo las extraerá.

Figura 43

Código creación de modelo Eigenface

```
import cv2
import os
import numpy as np

dataPath = 'C:/Users/H&G Technologies/Documents/TESIS/reconoximiento facial/reconoximiento facial/data'
peopleList = os.listdir(dataPath)
print('Lista de personas: ', peopleList)

labels = []
facesData = []
label = 0

for nameDir in peopleList:
        personPath = dataPath + '/' + nameDir
        print('Leyendo imagenes')

        for fileName in os.listdir(personPath):
                print('Rostros: ', nameDir + '/' + fileName)
                labels.append(label)
                facesData.append(cv2.imread(personPath+'/'+fileName,0))

        label = label + 1
# Selccion métodos para entrenar el reconocedor
face_recognizer = cv2.face.EigenFaceRecognizer_create()
# Entrenando modelo
print("Entrenando...")
face_recognizer.train(facesData, np.array(labels))
# Almacenando el modelo
face_recognizer.write('modeloEigenFace.xml')
print("Modelo guardado")
```

Nota: Este código crea el modelo Eigenface y lo guarda en formato XML, este archivo es esencial para el reconocimiento de rostros.

A.5 **código de programación controladores PIC para control de módulo de relés y multiplexores.**

Figura 44

Código de control multiplexores

```
#include <16f628a.h>
#fuses xt, nowdt , put, noprotect, nomclr
#use delay(internal=4000000)

#USE STANDARD_IO(B)

//#USE I2C(master,fast, sda=PIN_b0, scl=PIN_b1,slow,FORCE_HW, stream=H2)
/*#use rs232(baud=9600, xmit=PIN_c6,rcv=PIN_c7,  bits=8,  STREAM=H1)*/
//#use rs232(baud=9600, xmit=PIN_b,cv=PIN_b1,parity=N, bits=8,  STREAM=H2)
int dec=0;
int senvec[31];
int senlec[31];
INT I;
INT J;
INT NUMSEN=0;
INT CONTE=0;
INT R=1;
INT L=0;
INT CONTA=0;
INT g=0;
VOID LEC_SEN()

{
OUTPUT_A(15);
FOR(I=1;I<5;I=I*2)
{
OUTPUT_B(0);
OUTPUT_A(~I-16);
FOR(J=0;J<128;J=J+16)
{

OUTPUT_B(J);
if(INPUT(PIN_b7)==0)|INPUT(PIN_B2)==0)
{
if(senvec[dec]==1)
{
OUTPUT_A(0);
```

```
OUTPUT_A(0);
OUTPUT_B(0);
OUTPUT_HIGH(PIN_B0);
 g=g+1;
}

}
dec=dec+1;
DELAY_MS(50);
}
}
dec=dec*0;
}

VOID NUMBER_SENSOR()
{
OUTPUT_A(15);
WHILE(CONTE==0){
FOR(R=1;R<9;R=R*2)
{

OUTPUT_A(~R);
OUTPUT_B(0);
FOR(L=0;L<128;L=L+16)
{
OUTPUT_B(L);
IF(INPUT(PIN_b2)==1)
{
 NUMSEN=NUMSEN+1;
 senvec[CONTA]= 1;


}
else
{
 senvec[CONTA]=0;
```

```
}
CONTA = CONTA+1;
DELAY_MS(50);


}

CONTE=1;
}

}
void main()
{
delay_ms(5000);
NUMBER_SENSOR();

while(true)
{

if(INPUT(PIN_B1)==1){
int g=g+1;
if(g==1)
{
LEC_SEN();
}
}
if(INPUT(PIN_B1)==0)
{
OUTPUT_LOW(PIN_B0);
}
}
}
```

Nota: Este código se encarga del control de multiplexores y lectura de las señales de los sensores

Figura 45

Código de control de módulo de relés

```
#include <16f628a.h>
#fuses xt, nowdt , put, noprotect, nomclr
#use delay(internal=4000000)

/*#use rs232(baud=9600, xmit=PIN_c6,rcv=PIN_c7,  bits=8,  STREAM=N1)*/
#use rs232(baud=9600, xmit=pin_b2,rcv=pin_b1,bits=8,parity=N)

#USE STANDARD_IO(B)

#USE STANDARD_IO(A)

 char c;
 int ent;
#INT_RDA
RDA_isr()
{
c=getc();

}


void main(){

 enable_interrupts(INT_RDA); //Activa interrupción serial
 enable_interrupts(GLOBAL);

while(true)
{
//putc(c);
if(c=='A')
{
OUTPUT_HIGH(PIN_A0);
delay_ms(500);
OUTPUT_LOW(PIN_A0);
delay_ms(500);

```

Nota: Este código se encarga del control de los canales del módulo de actuadores.

A.6 **Códigos de reconocimiento de voz y rostro**

Figura 46

Código de reconocimiento de voz

```
import sys
sys.path.append("/lib/python3.9")
import speech_recognition as sr
import os
ruta_archivo = "/var/www/html/audio/recording.wav"

r = sr.Recognizer()
archivo = sr.AudioFile('recording.wav')
with archivo as source:
    audio = r.record(archivo)

L=r.recognize_google(audio, language='es-CO')
clave = "archivo"
##print(type(L))
test = L.split()
##print(test)
##print(type(test))
if clave in test:
    print("correcto")
else:
    print("fail")
if os.path.exists(ruta_archivo):
    # Eliminar el archivo
    os.remove(ruta_archivo)
```

Nota: Este código se encarga del reconocimiento de voz usando el API de *recognize_google.*

Figura 47

Código de reconocimiento facial

```
import cv2
import os
dataPath = "/var/www/html/uploads/data"
imaPath= "/var/www/html/uploads/hernan.jpg"
imagePaths = os.listdir(dataPath)
#print('imagePaths=',imagePaths)
face_recognizer = cv2.face.EigenFaceRecognizer_create()
# Leyendo el modelo
face_recognizer.read('modeloEigenFace.xml')
frame= cv2.imread(imaPath)
faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_default.xml')
gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
auxFrame = gray.copy()

faces = faceClassif.detectMultiScale(gray,1.3,5)

for (x,y,w,h) in faces:
        rostro = auxFrame[y:y+h,x:x+w]
        rostro = cv2.resize(rostro,(150,150),interpolation= cv2.INTER_CUBIC)
        result = face_recognizer.predict(rostro)

        cv2.putText(frame,'{}'.format(result),(x,y-5),1,1.3,(255,255,0),1,cv2.LINE_AA)

        #EigenFaces
        if result[1] < 5700:
                cv2.putText(frame,'{}'.format(imagePaths[result[0]]),(x,y-25),2,1.1,(0,255,0),1,c
                cv2.rectangle(frame, (x,y),(x+w,y+h),(0,255,0),2)
                print('correcto')
        else:
                cv2.putText(frame,'Desconocido',(x,y-20),2,0.8,(0,0,255),1,cv2.LINE_AA)
                cv2.rectangle(frame, (x,y),(x+w,y+h),(0,0,255),2)

                break

if os.path.exists(imaPath):
    # Eliminar el archivo
    os.remove(imaPath)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

Nota: Este código se encarga del reconocimiento de rostro usando el modelo de *Eigenface*