UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN

TELEMÁTICA

RPC-SO-01-NO.025-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

DESARROLLO DE UN SISTEMA DE VIGILANCIA RESIDENCIAL MEDIANTE LA INTEGRACIÓN DEL INTERNET DE LAS COSAS PARA MEJORAR LA SEGURIDAD DOMÉSTICA

AUTOR(ES)

MAURO JAVIER PERALTA CORAQUILLA

DIRECTOR:

MÓNICA KAREL HUERTA

QUITO – ECUADOR

2025

Autor(es):

MAURO PERALTA
Ingeniero en Electrónica Digital y Telecomunicaciones.
Candidato a Magíster en Telemática por la Universidad Politécnica Salesiana - Sede Quito.
mperaltac1@est.ups.edu.ec

Dirigido por:

MÓNICA HUERTA
Ingeniero Electrónico.
Doctora en Ingeniería Telemática, Universidad Politecnica de Cataluña, España.
mhuerta@ups.edu.ec

DESARROLLO DE UN SISTEMA DE VIGILANCIA RESIDENCIAL MEDIANTE LA INTEGRACIÓN DEL INTERNET DE LAS COSAS PARA MEJORAR LA SEGURIDAD DOMÉSTICA.

Dedicatoria

Quiero dedicar este logro a mi esposa, mis hijos, a mi madre, mi hermano y a mi padre que siempre fue mi inspiración en lograr este objetivo.

Agradecimientos

Agradezco infinitamente a Dios por darme la salud y la sabiduría para lograr este sueño que hoy se convierte en realidad, a mi familia por apoyarme, a la PhD. Mónica Huerta por su apoyo incondicional en todo este proceso.

Índice General

Índice de Figuras

Índice de Tablas

Resumen

En la actualidad, la seguridad residencial se ha convertido en una prioridad debido al aumento de incidentes delictivos, lo que pone de manifiesto la necesidad de soluciones tecnológicas avanzadas. Este proyecto aborda esta problemática mediante el desarrollo de un sistema de vigilancia basado en Internet de las Cosas (IoT), diseñado para ofrecer monitoreo en tiempo real y alertas automáticas, incrementando la tranquilidad y seguridad de los residentes. El objetivo principal fue desarrollar un sistema que integre sensores de vibración con el microcontrolador ESP32-CAM, permitiendo la detección temprana de intrusiones y la notificación inmediata a los usuarios a través de Google Drive y Telegram. Para llevar a cabo este proyecto, se seleccionaron dispositivos IoT, se diseñó y ensambló el circuito eléctrico, y se realizaron pruebas en hogares reales. Los resultados fueron positivos, con un 95 % de efectividad en la detección, un tiempo promedio de respuesta de 2 segundos y un alto nivel de satisfacción entre los usuarios. Este sistema ofrece una opción innovadora, práctica y adaptable para mejorar la seguridad en el hogar en un mundo cada vez más digital.

Palabras clave: Sensores inteligentes, ESP32 CAM, Telegram, monitoreo, seguridad residencial, IoT.

Abstract

In today's digital age, residential security is a growing priority due to the increase in criminal incidents, highlighting the need for advanced technological solutions. This project seeks to improve home protection through an Internet of Things (IoT)-based surveillance system. The importance of this system lies in its ability to provide real-time monitoring and automatic alerts, increasing residents' peace of mind.

The objective of the project was to develop a system that integrates vibration sensors and the ESP32-CAM microcontroller, allowing early detection of intrusions and notification to users via Google Drive and Telegram. The methodology included the selection of IoT devices, the design of the electrical circuit, and the implementation of pilot tests in real residential environments. To carry out this project, IoT devices were selected, the electrical circuit was designed and assembled, and tests were carried out in real homes. The results were positive, with 95 % detection effectiveness, an average response time of 2 seconds, and a high level of satisfaction among users. This system offers an innovative, practical, and adaptable option to improve home security in an increasingly digital world.

Keywords: Smart sensors, ESP32 CAM, Telegram, monitoring, residential security, IoT.

Capítulo 1

Introducción

En el año 2023, se registraron 7,592 muertes violentas, lo que resultó en una tasa de homicidios superior a 40 por cada 100,000 habitantes. Entre los factores que contribuyen a estas cifras se encuentran los altos niveles de desigualdad económica, el desempleo juvenil, la presencia de bandas delictivas organizadas y el narcotráfico. Primicia [2023].

De acuerdo con la Policía, se registraron 2.156 informes de robos a domicilios en el Distrito Metropolitano de Quito (DMQ) y el Distrito Metropolitano de Guayaquil (DMG), que incluye Durán y Samborondón, durante el año 2022. De estos incidentes, el 89 % (1.919) ocurrieron en villas y casas, mientras que el 11 % (246) sucedieron en departamentos dentro de casas o edificios. Esta tendencia se ha mantenido en 2023.Historia [2023].

Varios invetigadores diseñaron un dispositivo de seguridad comunitaria basado en Internet de las cosas para registrar evidencias y alertar a la Policía. Este dispositivo busca registrar pruebas y alertar a las autoridades policiales de manera oportuna. Mediante un enfoque metodológico mixto, se identificaron los factores que contribuyen a la inseguridad en el cantón Esmeraldas y se evaluó de manera experimental el rendimiento de las herramientas tecnológicas para el diseño del dispositivo de vigilancia. La tecnología Raspberry Pi se adecuó a las necesidades de la comunidad, mientras que el uso de WhatsApp facilitó la interacción con el sistema, resultando en beneficios para la comunidad y motivando a la Policía a promover proyectos similares con el fin de reducir la criminalidad en el país Toledo et al. [2019].

Los dispositivos de seguridad electrónica inteligentes conectados a una red IoT recogen distintos tipos de datos de sensores que miden variables físicas. Estos datos se integran a través de protocolos de comunicación y luego se

envían a una base de datos para su análisis. Tras el análisis, se utilizan para activar o desactivar sistemas inteligentes con funciones específicas, como abrir puertas, activar cámaras y enviar alertas al usuario mediante aplicaciones. Por otro lado, varios estudios se han enfocado en el uso de la tecnología para minimizar los robos en distintos ambitos como en las universides, en Venezuela se diseñó un sistema de seguridad basado en tecnología RFID para rastrear equipos dentro de edificios. Simulaciones demostraron la efectividad del sistema, incluso frente a interferencias, gracias a las características de salto de frecuencia del RFID Huerta et al. [2017]. Aqeel-ur-Rehman y su equipo presentaron diversas aplicaciones prácticas de la tecnología RFID, tales como la identificación de empleados y estudiantes, el seguimiento de equipos personales, la automatización de salas, el registro inteligente de asistencias y la prevención de robos de equipos. Abbasi et al. [2008]. Por otro lado, Ying Chen presentó un sistema que combina RFID con la tecnología de comunicación ZigBee para rastrear activos y generar alarmas tempranas con el fin de reducir el robo de equipos Alkhateeb et al. [2010].

En el ámbito de la seguridad doméstica, en 2017, Sruthy y Sudhish desarrollaron un sistema de monitoreo residencial empleando Internet de las Cosas y Raspberry Pi. Este sistema utiliza un acceso Wi-Fi y establece nodos de sensores inalámbricos con una estructura de control para supervisar el entorno. Consta de dos nodos de sensores: uno de detección de movimiento por infrarrojos pasivos y otro para la detección de incendios. Se utiliza un módulo NodeMCU ESP8266 para procesar los eventos generados por los sensores y transmitirlos al controlador. Al recibir la notificación, el sistema activa una cámara para capturar el evento y envía alertas al usuario mediante correo electrónico, mensajes de texto o llamadas telefónicas. Esta plataforma da acceso a los operadores para monitorear sus viviendas y recoger avisos, mientras visualizan transmisiones en vivo de su residencia a través de una página web. Chicaiza Guachi [2020].

Por otro lado, en Bulla Rojas et al. [2020] se plantea la creación de un modelo inicial de supervisión y vigilancia residencial, enfocado principalmente en la ciudad de Bogotá, utilizando la tecnología IoT. Este prototipo será completamente operativo, ya que enviará notificaciones al usuario a través de la aplicación de mensajería WhatsApp y correos electrónicos. Esto brindará a los usuarios la capacidad de activar o desactivar el sistema según su conveniencia.

1.1. Justificación

La creciente preocupación por la seguridad residencial, reflejada en el incremento de incidentes delictivos en los hogares en años recientes, subraya la necesidad de sistemas de seguridad más sofisticados y adaptables a las particularidades de cada vivienda. La tecnología (IoT) se presenta como una elección prometedora para desarrollar un sistema de monitoreo inteligente, conectado en red, que emplee dispositivos como cámaras y sensores para la detección temprana de eventos y la rápida respuesta ante los mismos, mejorando la protección del hogar. La implantación del sistema propuesto contribuirá a elevar la calidad de vida de los habitantes al permitirles monitorear y controlar su entorno desde cualquier ubicación, sino que también se encuentra alineada con las tendencias tecnológicas. Además, esta solución no solo optimizará la gestión de recursos energéticos y contribuirá a la sostenibilidad ambiental, sino que también será diseñada teniendo en cuenta las necesidades específicas y la infraestructura local, garantizando su eficacia y durabilidad. En última instancia, este enfoque innovador en seguridad residencial mediante IoT ofrecerá una comunicación instantánea con las autoridades pertinentes, como las Unidades de Policía Comunitaria (UPC) barriales, para proporcionar seguridad de manera eficiente y accesible a todas las familias.

1.2. Objetivos

1.2.1. Objetivo general

Desarrollar un Sistema de Vigilancia Residencial mediante la Integración del Internet de las Cosas para Mejorar la Seguridad Doméstica.

1.2.2. Objetivos Específicos

- Estudiar los Sistemas de Seguridad y Vigilancia basados en IoT, incluyendo su funcionamiento, características y aplicaciones relevantes.
- Seleccionar Dispositivos y Tecnologías IoT Adecuados para el diseño del sistema de vigilancia residencial, considerando factores como la escalabilidad, interoperabilidad y funcionalidades requeridas.
- Diseñar un prototipo electrónico mediante Hardware y Software que cumpla con los requisitos de seguridad y funcionalidad establecidos.

- Diseñar una Interfaz de Usuario que permita a los usuarios controlar y monitorear el sistema de vigilancia desde dispositivos móviles u ordenadores.
- Implementar el prototipo electrónico de seguridad, asegurando su correcto funcionamiento y la integración adecuada de los diferentes componentes.
- Establecer Comunicación Remota con las Autoridades pertinentes facilitando la notificación automática de eventos de seguridad y la respuesta inmediata ante situaciones de emergencia.
- Realizar Pruebas Piloto en Entornos Residenciales Reales, identificando posibles mejoras y ajustes necesarios antes de su implementación a gran escala.

Este documento está organizado en los capítulos siguientes:

- En el Capítulo 2 se lleva a cabo un estudio de los componentes a utilizar en un sistema de vigilancia residencial mediante las plataformas basadas en IoT para una mejorar de la seguridad doméstica.
- En el Capítulo 3 se presenta el diseño del circuito e implementación del mismo.
- En el Capítulo 4 se analiza el funcionamiento como los resultados del circuito implementado y futuras mejoras.
- Finalmente, en el Capítulo 5 se presentan las principales conclusiones y recomendaciones.

Capítulo 2

Marco Teórico

En esta sección, se profundiza los fundamentos teóricos que permitirán el desarrollo de un Sistema de Vigilancia Residencial mediante la Integración del IoT. Se aborda como la convergencia tecnología IoT con los sistemas de seguridad tradicionales puede ofrecer soluciones más efectivas y satisfactorias para proteger los hogares. Se examinan los fundamentos teóricos que respaldan esta iniciativa, así como los conceptos clave relacionados con el IoT y su aplicación en el ámbito de la seguridad residencial. También, se analizan las diversas formas en que el internet de las cosas puede mejorar como la detección, el monitoreo y la respuesta frente a posibles amenazas en el hogar, ofreciendo así una mayor tranquilidad y protección para los residentes.

2.1. Seguridad Residencial

2.1.1. Fundamentos Teóricos de la Seguridad Residencial

La seguridad residencial implica emplear medidas y dispositivos destinados a salvaguardar una vivienda y sus ocupantes frente a posibles intrusiones, robos, accidentes y otros riesgos. Esto abarca desde sistemas de alarmas y cámaras de vigilancia hasta cerraduras más seguras, iluminación exterior adecuada, cercas y otras precauciones diseñadas para disuadir a los intrusos y mantener un ambiente seguro para quienes residen en el lugar. Es importante destacar que la seguridad residencial no se limita únicamente a proteger la propiedad material, además, se enfoca en asegurar la integridad y el bienestar de los residentes.

La seguridad puede verse fácilmente comprometida en diversas situaciones. Por un lado, está la integridad personal, y por otro, los bienes

materiales que tienen un gran valor moral o económico para una persona. Ambos pueden ser vulnerables en muchos casos, lo que hace necesaria la actualización tecnológica mediante la implementación de controles de acceso, alarmas de gases, cámaras de video en vivo, entre otros. Estos sistemas, si se manejan con un protocolo de seguridad riguroso, pueden ser subidos a la web sin temor a ser hackeados. Sin embargo, también existe el riesgo de que la propia red de internet utilizada para la transmisión remota de las cámaras no garantice una total transparencia con el usuario final.

La seguridad doméstica se refiere a las estrategias y a los dispositivos utilizados para proteger el hogar y a los que en él viven contra intrusos, robo, incendio y otros riesgos. Incluye los sistemas de alerta, la videovigilancia, los sistemas de control de acceso, las alarmas de detección y los instrumentos de monitoreo, a fin de crear un ambiente seguro para la vida diaria.

Los sistemas de seguridad que utilizan la tecnología, como Internet de las cosas (IoT), proporcionan una mejora notable en la detección de intrusos en comparación con los sistemas convencionales. Esto es debido a que IoT utiliza cámaras de alta definición, sensores de movimiento y dispositivos de entrada/salida, estos sistemas pueden detectar actividades sospechosas con mayor precisión y en tiempo real. La información recogida por estos dispositivos puede ser analizada al instante, lo que permite emitir alertas inmediatas tanto a los propietarios como a los servicios de seguridad.

2.2. Internet de las Cosas

El Internet de las Cosas (IoT) se refiere a una red que conecta objetos físicos utilizando internet y otros protocolos, principalmente inalámbricos. Estos objetos están equipados con sistemas embebidos o hardware especializado, lo que les permite no solo conectarse a internet, sino también aprovechar la capacidad de microcontroladores y microprocesadores para realizar procesos complejos, análisis de datos, almacenamiento, entre otros.

El Internet de las cosas se refiere a una red de objetos físicos, como dispositivos, vehículos, instrumentos, edificios y otros, que cuentan con electrónica, sensores, software y conexión a la red. Esto les permite recopilar y compartir información entre sí de manera eficiente.Gokhale et al. [2018]. En otras palabras el internet de las cosas (IoT) permite a distancia detectar y controlar objetos aprovechando la infraestructura de red existente, esta tecnología hace posible una mayor relación de nuestro entorno físico con las computadoras, lo que se traduce en una mejor eficiencia y exactitud en

varias actividades, conducta de recursos selectos y toma de decisiones de mejor información.

2.2.1. Historia y Evolución del IoT.

El principio del Internet de las Cosas comenzó gracias al tecnólogo británico Kevin Ashton. A principios de la década de 1990, mientras trabajaba en la empresa Procter and Gamble (P&G), Ashton intentaba persuadir a sus superiores para que implementaran nombres de reconocimiento por radiofrecuencia (RFID) y otros sensores en los productos de la cadena de suministro de la empresa con el fin de automatizar procesos.

No hay una definición única y universalmente aceptada para Internet de las Cosas en la comunidad global de usuarios. Distintos grupos, como académicos, investigadores, profesionales, innovadores, desarrolladores y empresarios, han planteado diversas definiciones del término. No obstante, todas ellas coinciden en que la primera versión de Internet se orientaba hacia datos generados por personas, mientras que la versión actual pone énfasis en los datos producidos por objetos. La definición más adecuada de Internet de las Cosas sería: "Una red abierta e integral de objetos inteligentes que tienen la capacidad de autoorganizarse, compartir información, datos y recursos, reaccionando y actuando ante situaciones y cambios en el entorno" Madakam et al. [2015].

2.3. Seguridad en IoT

La seguridad en IoT es fundamental debido a la extensa y conectada naturaleza de estos dispositivos. Los riesgos vinculados al IoT pueden acarrear consecuencias importantes, afectando tanto la seguridad de los datos como la protección física de las personas.

La seguridad en el hogar ha evolucionado significativamente durante el último siglo y continuará transformándose en los próximos años. En el contexto de las aplicaciones domésticas inteligentes, la seguridad se destaca como una característica fundamental. El concepto emergente de hogares inteligentes proporciona a sus habitantes un entorno más cómodo, práctico y seguro. Mientras que los sistemas de seguridad tradicionales se limitan a proteger a los propietarios y sus bienes mediante alarmas para alertar sobre intrusos, los sistemas de seguridad inteligentes van más allá, ofreciendo una amplia gama de beneficios adicionales. Bangali and Shaligram [2013].

Harbi y otros, identificaron aspectos relevantes en la seguridad de varias Aplicaciones de IoT. Se han desarrollado marcos de modelado de amenazas

aplicables al diseño de seguridad en sistemas IoT. Estos marcos identifican ataques dirigidos a sensores, redes, middleware y capas de aplicación. Además, los investigadores propusieron técnicas de seguridad basadas en criptografía, computación en la niebla, computación en el borde y aprendizaje automático, para mitigar los riesgos y proteger los sistemas IoT frente a estos ataques. Harbi et al. [2021].

En un estudio realizado por Ling et al (Ling et al., 2017), se llevó a cabo un análisis de vulnerabilidad en las cámaras IP Edimax. Los investigadores identificaron que ataques como el escaneo de dispositivos, la fuerza bruta y la suplantación de dispositivos podrían permitir a los atacantes tomar el control de estas cámaras.

Por ejemplo, utilizando un ataque de falsificación de dispositivos, los atacantes pueden obtener la contraseña de una cámara de cualquier longitud y combinación.Sengupta et al. [2020]

También enumerando todas las direcciones MAC posibles, el atacante puede iniciar un ataque de escaneo de dispositivos para encontrar todas las cámaras en línea. Sengupta et al. [2020]

2.4. Elementos de la Arquitectura del Internet de las Cosas

Los elementos que conforman el Internet de las Cosas (IoT) son diversos y van desde los dispositivos físicos hasta las infraestructuras de red y las plataformas de análisis de datos. A continuación, se describen los componentes clave del IoT.

2.4.1. Sensores y Actuadores

Sensores Los sensores en el IoT son dispositivos que permiten la recolección de registros del entorno físico y su transmisión para análisis y toma de decisiones. Los sensores convierten diferentes formas de energía en señales eléctricas que pueden ser procesadas y analizadas.

Los tipos de Sensores y Variables Físicas Medidas son:

1. Sensores de Temperatura: - Variables Medidas: Temperatura ambiente, temperatura de superficies, etc. - Aplicaciones: Control de climatización, monitoreo ambiental, gestión de procesos industriales.

2. Sensores de Humedad: - Variables Medidas: Humedad relativa, humedad del suelo. - Aplicaciones: Agricultura de precisión, sistemas de climatización, almacenamiento de alimentos.

3. Sensores de Presión: - Variables Medidas: Presión atmosférica, presión de fluidos y gases. - Aplicaciones: Meteorología, sistemas hidráulicos, monitoreo de neumáticos.

4. Sensores de Proximidad: - Variables Medidas: Distancia a objetos, presencia de objetos. - Aplicaciones: Seguridad, automatización industrial, dispositivos móviles.

5. Acelerómetros y Giroscopios: - Variables Medidas: Aceleración lineal, velocidad angular. - Aplicaciones: Detección de movimiento, estabilización de cámaras, control de juegos.

6. Sensores de Luz: - Variables Medidas: Intensidad lumínica. - Aplicaciones: Iluminación inteligente, monitoreo ambiental, dispositivos móviles.

7. Sensores de Gas: - Variables Medidas: Concentración de gases específicos (CO2, CO, metano, etc.). - Aplicaciones: Detección de gases peligrosos, calidad del aire, control de procesos industriales.

8. Sensores de Flujo: - Variables Medidas: Tasa de flujo de líquidos o gases. - Aplicaciones: Gestión de recursos hídricos, control de procesos industriales, medición de consumo de gas.

Estos sensores se integran en sistemas IoT para recolectar datos en tiempo real, permitiendo la automatización, monitoreo y optimización de procesos en diversas industrias, Areny [2004].

Actuadores Un actuador es un dispositivo que tiene la capacidad de aplicar una fuerza para alterar la posición, velocidad o estado de un componente mecánico, mediante la conversión de energía. Ramírez et al. [2014]. A continuación, una lista de algunos de los actuadores más utilizados en aplicaciones Iot.

- motores.
- válvulas.
- cerraduras electrónicas.
- cámaras motorizadas.
- luces de seguridad.
- sirenas.

2.4.2. Principales Plataformas de Procesamiento para IoT

Una plataforma de procesamiento en el ámbito del Internet de las Cosas es un sistema tecnológico diseñado para simplificar la gestión, análisis y tratamiento de los datos producidos por dispositivos conectados. Estas plataformas suministran las herramientas y servicios esenciales para enlazar los dispositivos, recolectar datos, examinar la información y tomar decisiones fundamentadas en los datos adquiridos. Las plataformas más comunes utilizadas en IoT son:Amazon Web Services, Microsoft Azure, Google Cloud, and Samsung Smart Things.

Amazon Web Services Amazon Web Services (AWS) es una división de Amazon.com que se encuentra en constante crecimiento y desarrollo. Desde principios de 2006, Amazon Web Services ha estado ofreciendo a empresas de todos los tamaños una plataforma de servicios en la nube para infraestructura web. Millán-Rojas et al. [2014].

Microsoft Azure Microsoft Azure es una plataforma de servicios en la nube que actúa como un entorno para el desarrollo, hospedaje y gestión de servicios en la plataforma Windows Azure. Ofrece a los desarrolladores la posibilidad de acceder a servicios de computación y almacenamiento según lo necesiten, facilitando el alojamiento, la expansión y la gestión de aplicaciones web a través de los centros de datos de Microsoft.

Google Cloud Google Cloud Platform (GCP) se lanzó en 2011 con el fin de ofrecer servicios de computación en la nube. Entre sus opciones, GCP incluye almacenamiento, análisis de grandes datos, bases de datos, inteligencia artificial, redes, herramientas para el desarrollo y gestión, seguridad en la nube, Internet de las cosas y transferencia de datos. Gupta et al. [2021].

Samsung Smart Things Es un sistema de automatización del hogar desarrollado por Samsung que facilita la creación de casas inteligentes. A través de una aplicación en un smartphone Android, permite controlar los dispositivos instalados en el hogar desde cualquier lugar. Moscoso Riera [2023].

2.5. Protocolos de Comunicación en IoT

Los protocolos de comunicación son fundamentales en el Internet de las Cosas ya que facilitan la transferencia de datos entre dispositivos interconectados. A continuación, se detallan algunos de los protocolos de comunicación más comunes en IoT:

Bluetooth

La tecnología inalámbrica Bluetooth se ha establecido como un sistema universal de bajo costo y fácil de usar. En el contexto del Internet de las Cosas (IoT), Bluetooth es especialmente relevante debido a su bajo consumo de energía, ideal para dispositivos IoT con fuentes de energía limitadas.

Bluetooth funciona en la banda de 2.4 GHz según el estándar IEEE 802.15.1, facilitando la conexión de dispositivos a distancias cortas, normalmente hasta 100 metros. La versión Bluetooth Low Energy (BLE) optimiza aún más el consumo de energía, manteniendo alta eficiencia en la transmisión de datos. Además, facilita la implementación de redes de malla (mesh networking), extendiendo el alcance y la robustez de la red IoT.

Bluetooth también incorpora medidas de seguridad avanzadas como cifrado AES-128 y autenticación, asegurando la integridad y confidencialidad de los datos. Su interoperabilidad y facilidad de integración hacen de Bluetooth una tecnología indispensable en la infraestructura IoT moderna Bisdikian [2001].

HTTP (Hyper Text Transfer Protocol ó Protocolo de transferencia de hipertexto)

Es el protocolo de transferencia de hipertexto, el mecanismo que gestiona las solicitudes para acceder a una página web y las respuestas correspondientes, proporcionando la información que se visualizará en la pantalla del ordenador. Avogadro [2007]

HTTP es compatible con la arquitectura web RESTful, que sigue un modelo de solicitud/respuesta. Al igual que CoAP, HTTP emplea un identificador de recursos universal (URI) en lugar de utilizar temas. El servidor envía los datos a través del URI, y el cliente los recibe mediante un URI específico.

HTTP es un protocolo basado en texto que no especifica el tamaño de la carga útil del encabezado ni del mensaje; en cambio, este tamaño está determinado por el servidor web o la tecnología de programación utilizada. Naik [2017]

Wi-Fi (Wireless Fidelity)

Es una tecnología que posibilita la conexión de una amplia gama de dispositivos informáticos sin requerir cables.

Wi-Fi significa "Fidelidad inalámbricaz se utiliza para describir productos de LAN inalámbrica (WLAN) que se basan en los estándares IEEE 802.11. Wi-Fi usa ambos tecnología de radio de espectro ensanchado de secuencia directa de portadora única y tecnología de radio OFDM (multiplexación por división de frecuencia ortogonal) de múltiples portadoras.Nwabueze and Akaneme [2009]

Wi-Fi se basa en el estándar IEEE 802.11 publicado para comunicaciones inalámbricas de corto alcance. Se está implementando para ofrecer cobertura en campus universitarios, hoteles y aeropuertos mediante lo que se conoce como punto de acceso. Un hotspot es el área que cubre uno o varios puntos de acceso (AP). Un punto de acceso inalámbrico conecta varios dispositivos inalámbricos a una red local (LAN) cableada cercana, permitiendo la transmisión de datos entre los dispositivos inalámbricos conectados, además de conectar un único dispositivo cableado. Se basa en la familia de estándares como IEEE 802.11a, 802.11b, 802.11g y 802.11n.Kaushik and Kaushik [2012]

Zigbee

Es uno de los estándares más populares para redes de sensores inalámbricos, caracterizado por su bajo consumo de energía, baja velocidad de transmisión de datos, bajo costo y tiempos de respuesta rápidos. Además, es fácil de desarrollar e implementar, y ofrece una seguridad robusta junto con una alta confiabilidad en la transmisión de datos. Ramya et al. [2011] ZigBee es un protocolo abierto y global basado en paquetes, creado para ofrecer una arquitectura sencilla para redes inalámbricas que sean seguras, fiables y de bajo consumo energético. Tanto ZigBee como el estándar IEEE 802.15.4 están diseñados para redes inalámbricas de baja velocidad de datos, lo que permite evitar el uso de cableado costoso y susceptible a daños en aplicaciones de control industrial.

MQTT (Message Queuing Telemetry Transport)

Uno de los protocolos de comunicación M2M más antiguos es MQTT, que se introdujo en 1999. Fue desarrollado por Andy Stanford-Clark de IBM y Arlen Nipper de Arcom Control Systems Ltd (Eurotech). Naik and Bapat [2020] El protocolo MQTT, que se basa en el patrón de "publicación/suscripción.º "publish/subscribe", es sencillo y ligero, y está diseñado para dispositivos con limitaciones y con ancho de banda limitado para la comunicación, así como para situaciones de alta latencia o condiciones no confiables. Por lo tanto, es particularmente adecuado para aplicaciones

IoT. Escobar Gallardo and Villazón [2018]

MQTT es un protocolo ligero para la comunicación entre máquinas, diseñado especialmente para aplicaciones móviles. Su método de intercambio de información optimiza el uso de recursos y no requiere un formato de datos específico. Además, garantiza que todos los mensajes sean transmitidos, incluso si hay interrupciones breves en la conexión, resolviendo los problemas de las comunicaciones inestables.Luzuriaga et al. [2015]

AMQP (Advanced Message Queuing Protocol)

AMQP (Protocolo avanzado de colas de mensajes) es un protocolo que utiliza colas de mensajes de alto nivel que comenzó a desarrollarse en 2003 por John O'Hara en JPMorgan Chase en Londres. AMQP muestra características sobresalientes en colas de mensajes, distribución de mensajes multifunción a colas en el sistema y buena seguridad. Un corredor AMQP popular es RabbitMQ.Uy and Nam [2019]

Es otro protocolo de tipo publicar/suscribir que originó en el sector financiero. Aunque está presente en las Tecnologías de la Información y Comunicación (TIC), su uso en la industria es bastante limitado. Semle [2016]

El Protocolo Avanzado de Cola de Mensajes (AMQP) es un middleware de mensajería estándar y abierto. Según este estándar, los productos de middleware desarrollados en distintas plataformas y lenguajes de programación pueden intercambiar mensajes entre sí sin problemas. AMQP cuenta con el respaldo de un buen número de actores clave, incluidos Cisco Systems, Credit Suisse, Deutsche Borse Systems, Goldman Sachs, JPMorgan Chase Bank, Red Hat y 29West.Fernandes et al. [2013]

LoRaWAN

Es un protocolo para redes de gran extensión de bajo consumo (LP-WAN) que permite a los dispositivos finales transmitir y recibir datos de forma inalámbrica a bajo consumo.Neumann et al. [2016]

LoRa es la capa física empleada en LoRaWAN. Ofrece un bajo consumo de energía (con una vida útil de la batería de aproximadamente 10 años), una velocidad de datos baja (27 kb/s con un factor de dispersión de 7 y un canal de 500 kHz, o 50 kb/s con FSK), y un alcance de comunicación extenso (de 2 a 5 km en áreas urbanas y hasta 15 km en zonas suburbanas). Este protocolo fue desarrollado por Cycleo, una empresa francesa que fue adquirida por Semtech. Adelantado et al. [2017]

La arquitectura de red LoRaWAN presenta una topología en estrella, en la que los dispositivos finales se comunican únicamente con las puertas de enlace LoRaWAN, sin poder intercambiar datos directamente entre ellos. Múltiples

puertas de enlace están conectadas a un servidor de red central. Las puertas de enlace LoRaWAN tienen la función de retransmitir los paquetes de datos sin procesar desde los nodos finales hacia el servidor de red, encapsulándolos en paquetes UDP/IP para su transmisión.

2.6. Arquitectura de IoT

La estructura para sistemas de IoT se describe como una arquitectura en capas, que fragmenta el sistema en segmentos funcionales para definir y asignar tareas a lo largo de la totalidad del sistema. Esta arquitectura debe cumplir con requisitos específicos, como flexibilidad, escalabilidad, seguridad e interoperabilidad, dada la variedad de dispositivos disponibles en estos sistemas. Otros elementos esenciales de esta arquitectura incluyen la confiabilidad en el almacenamiento y la calidad del servicio.

2.6.1. Capas de la Arquitectura IoT

La estructura de IoT generalmente está formada por múltiples niveles que se comunican entre sí para ofrecer funcionalidad completa al sistema. Algunas de las capas se describen a continuación: Fig. 2.1

Capa Física

La capa física o de percepción recoge información del entorno, de las personas o del propio proceso o sistema en cuestión Sánchez [2018]. Los elementos principales de esta capa son los sensores, que a menudo están integrados en nodos de procesamiento IoT. Estos nodos tienen la capacidad de enviar los datos a la nube mediante servicios como Fiware o Amazon AWS.

Capa de Conectividad

Es la capa responsable de, mediante algoritmos eficientes, gestionar el envío de paquetes seleccionando la ruta más adecuada en cada momento, para que estos sean transmitidos a través de los distintos nodos de la red hasta alcanzar su destino. Esta capa divide los segmentos enviados entre dos equipos en unidades llamadas paquetes, y realiza el proceso inverso al recibirlos en el destino final.

Capa de Procesamiento de Datos

La capa de procesamiento de datos tiene como objetivo diferentes funciones, como la eliminación de ruido de datos, la detección de datos

atípicos, la imputación de datos faltantes y la agregación de datos. Krishnamurthi et al. [2020]

El objetivo de esta práctica es permitir una toma de decisiones y un control inteligentes, fundamentados en la computación en la nube. La información procesada en esta capa garantiza interoperabilidad y escalabilidad, reduciendo amenazas durante el procesamiento y seleccionando la información con el mayor nivel de seguridad. Esto asegura que los datos proporcionen un entorno seguro y servicios eficientes. David Patiño et al. [2021]

Capa de Almacenamiento

Para asegurar la confianza en las operaciones a corto y largo plazo, se utiliza la nube para escalar los datos producidos y garantizar su disponibilidad en cualquier momento. En la nube, se almacenan los datos generados por los dispositivos IoT y se alojan los servidores de aplicaciones web, móviles y de servicios como programas de inserción, consultas y notificaciones de alarmas para los clientes.

Capa de Análisis y Gestión

La Capa de Análisis y Gestión en una arquitectura de IoT se dedica a procesar y analizar los datos que provienen de los dispositivos IoT. Su función principal es convertir datos sin procesar en información útil mediante diversas técnicas de análisis y procesamiento. Además, facilita la visualización de esta información para apoyar la toma de decisiones basada en datos. También se encarga de administrar las políticas de manejo de datos y de optimizar los recursos en función del análisis realizado.

Capa de Aplicación

Esta capa final permite al usuario visualizar la información reunida por los sensores de manera sencilla. Es fundamental que todos los dispositivos sean compatibles para facilitar el intercambio de datos, la conexión y el procesamiento de eventos. Se necesita una interfaz eficiente que simplifique la gestión y la interconexión de los objetos. Todo esto se consigue mediante una interfaz que opera en el frontend de una aplicación a través de una API.

2.6.2. Explicación del uso de las capas en el programa de vigilancia residencial con IoT

El desarrollo del programa de vigilancia residencial con IoT se estructura en seis capas esenciales que colaboran para proporcionar una solución

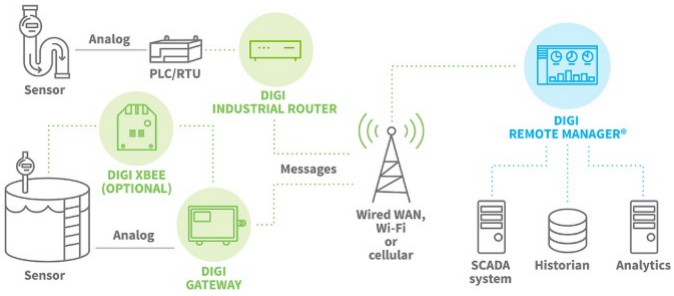

Figura 2.1: Las 4 etapas de la arquitectura IoT, Fuente: https://es.digi.com/blog/post/the-4-stages-of-iot-architecture

completa de seguridad doméstica

1. Capa de Dispositivos: El sistema se inicia cuando el sensor de vibración detecta movimiento en la zona residencial. Este sensor es responsable de captar la información del entorno físico. Al registrar una vibración, envía una señal a la ESP32-CAM, que está lista para realizar la tarea asignada, en este caso, tomar una fotografía.

2. Capa de Conectividad: Tras recibir la señal del sensor de vibración, la ESP32-CAM activa su cámara para tomar una imagen del área monitoreada. A través de una conexión Wi-Fi, la imagen capturada se envía utilizando la API de Google Drive para su almacenamiento. También, se usa la API de Telegram para mandar una alerta que incluye la foto. Adicionalmente, esta capa permite el monitoreo remoto en tiempo real mediante la dirección IP de la cámara, accesible desde cualquier dispositivo conectado a la red.

3. Capa de Procesamiento de Datos: El proceso de datos comienza cuando la ESP32-CAM recibe la señal del sensor de vibración. En función de esa señal, decide si debe o no activar la cámara. Una vez activada, la cámara captura la imagen, la cual se prepara para ser enviada a Google Drive y Telegram. Además, puede realizarse un ajuste como la compresión de la imagen para mejorar el envío.

4. Capa de Almacenamiento: La imagen tomada por la cámara se guarda temporalmente en la memoria interna de la ESP32-CAM antes de transferirse a Google Drive. Este almacenamiento intermedio asegura que la imagen esté disponible hasta que el envío se complete con éxito. Posteriormente, las fotos se guardan en Google Drive.

5. Capa de Aplicación: El usuario recibe una alerta en la aplicación de Telegram, que incluye un mensaje de advertencia y la foto capturada. Esta

notificación es enviada por un bot previamente configurado, lo que permite al usuario reaccionar de inmediato.

2.7. Aplicaciones de IoT

Las aplicaciones del Internet de las Cosas (IoT) son variadas y se extienden por numerosas industrias y aspectos de la vida diaria. A continuación, describo algunas aplicaciones típicas de IoT:

2.7.1. Hogar inteligente

Detección de intrusiones Además, esta aplicación tiene la capacidad de enviar informes detallados que incluyen imágenes o clips de audio/vídeo al usuario, como se muestra en la Fig. 2.2. Su propósito principal es monitorear cualquier actividad sospechosa en el hogar inteligente, notificar al usuario y tomar las acciones necesarias para asegurar la seguridad.

Figura 2.2: Seguridad en Dispositivos IoT, Hogar Inteligente, Fuente: (Hp, 2024)

2.7.2. Salud

Monitoreo escalable y continuo de la frecuencia cardíaca Los datos biométricos de cada paciente se monitorean individualmente mediante el establecimiento de parámetros de umbral específicos del paciente Fig. 2.3. Un sistema de este tipo puede monitorear diversos signos vitales de un paciente, como la frecuencia cardíaca del ECG (incluyendo la variabilidad y la confiabilidad de la frecuencia cardíaca), la frecuencia respiratoria, el nivel

de actividad y la posición del cuerpo. Para realizar un monitoreo remoto de signos vitales adicionales, como la presión arterial y el peso, se pueden utilizar dispositivos complementarios. Uno de los objetivos principales de este sistema es la monitorización del ritmo cardíaco, lo que permite comprender mejor el papel del corazón en síntomas inexplicables, los cuales pueden ser analizados de manera más efectiva utilizando un sistema de monitoreo del ritmo.Kulkarni et al. [2014]

Figura 2.3: Aplicación de Monitoreo de Frecuencia Cardíaca de Reloj inteligente, Fuente: (alamy, 2017)

2.7.3. Transporte

Encontrar espacios de estacionamiento En las grandes ciudades, problemas como la dificultad para encontrar estacionamiento y las largas esperas para el pago de peajes pueden resultar molestos, lo que llevó a la idea de usar la matrícula como una identidad única del conductor (Ren et al., 2012). La matrícula se capturaba mediante un sistema de reconocimiento, mientras que los sensores integrados en ella recolectaban información sobre la superficie de la carretera. Estos datos se reenviaban luego para calcular la ruta óptima y proporcionar direcciones para los vehículos. Este diseño ofrece múltiples beneficios al conductor, como la automatización de la recolección de peajes, la optimización de rutas para evitar tráfico congestionado, la localización de estacionamientos y una mayor seguridad para el vehículo Fig.2.4. Sin embargo, un claro inconveniente es que este diseño lucha por admitir demasiadas funciones que invocan altos costos y dificultades de implementación.Vongsingthong and Smanchat [2014]

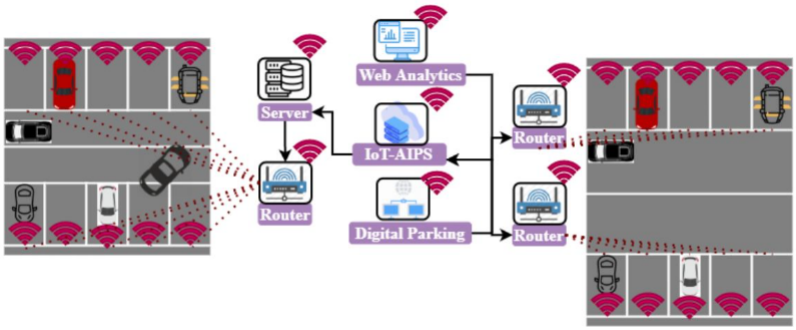

Figura 2.4: Sistema Inteligente de Estacionamiento Asistido por IOT, Fuente: (WWWHATSNEW, 2023)

2.7.4. Agricultura

Maquinaria agrícola La maquinaria agrícola basada en IoT está diseñada para mejorar la productividad y reducir la pérdida de cultivos. El GPS se utiliza para operar el dispositivo en modo piloto automático, mientras que la maquinaria robótica permite el control remoto del dispositivo según la información disponible. Esta información es recopilada por el sistema IoT, como se muestra en la Fig.**??**. La maquinaria agrícola ayuda a los agricultores a recopilar datos esenciales para planificar la siembra de la próxima temporada, como fertilización, riego y nutrición. Mishra et al. [2021]

Figura 2.5: IoT Agricultura Inteligente, Fuente: (alamy, 2016)

Capítulo 3

Marco Metodológico

Este capítulo se detalla la metodología empleada para desarrollar y evaluar un sistema de vigilancia residencial, integrando el IoT con el propósito de mejorar la seguridad en el hogar. Se eligieron componentes de software y hardware función de trabajos relacionados y su compatibilidad con el objetivo del proyecto. El software incluye tanto componentes utilizados para pruebas y validación como para el prototipo final.

3.1. Componentes del Hardware: Dispositivo Electrónico

ESP32-CAM Este módulo de desarrollo utiliza el microcontrolador ESP32 de Espressif Systems, especialmente creado para aplicaciones de cámaras Fig.3.1. Este módulo incorpora una cámara OV2640 y cuenta con conectividad Wi-Fi y Bluetooth integrada, lo que resulta una excelente opción para proyectos IoT que necesiten transmitir imágenes y videos.

Módulo Sensor de Vibración Es un componente esencial en nuestro sistema de seguridad residencial. Diseñado para detectar cualquier movimiento o vibración inusual en la estructura de la propiedad Fig.3.2, este sensor proporciona una capa adicional de protección contra intrusos y actos vandálicos.

Router WI-FI Es un aparato de red que se emplea para gestionar el tráfico de datos entre diversas redes informáticas Fig.3.3. Opera examinando direcciones IP de los paquetes de datos entrantes y salientes y tomando decisiones sobre la mejor ruta para enviarlos. Los routers son fundamentales

Figura 3.1: Dispositivo ESP32-CAM, Fuente: (HackSpace, 2024)

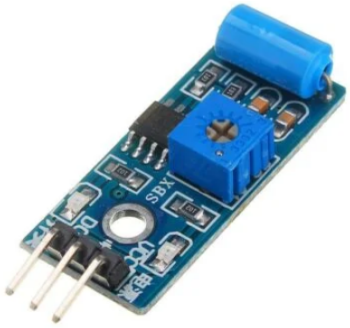

Figura 3.2: Sensor de Vibración SW-420, Fuente: (ElectroStore, 2019)

en la interconexión de redes locales (LAN), redes de área extensa (WAN) e internet.

3.2. Componentes de Software

Se indican los softwares que pueden emplearse en el sistema de control para el desarrollo de un sistema de vigilancia residencial mediante la integración del Internet de las Cosas, con el fin de mejorar la seguridad doméstica y alcanzar los objetivos establecidos

Arduino IDE

El entorno de desarrollo integrado Arduino (IDE) se emplea para programar el microcontrolador ESP32CAM. Incluye un editor de texto, un área de mensajes, una consola de texto y una barra de herramientas

Figura 3.3: Router, Fuente: (LifeWIRE, 2021)

con botones para funciones comunes. Permite escribir, verificar y cargar programas en el hardware. La Fig.3.4 muestra la interfaz del Arduino IDE.

Figura 3.4: Imagen del IDE Arduino, Fuente: (RedHat, 2024)

Google Drive

Es una plataforma de almacenamiento en la nube. Ofrece la posibilidad de guardar archivos en servidores remotos que se pueden alcanzar mediante internet, compartir esos archivos con otros y acceder a ellos desde varios dispositivos. Además de estar disponible como una aplicación web, también cuenta con versiones móviles y de escritorio que hacen más sencillo su uso.

Telegram Es un sistema de servicio de mensajes instantánea que funciona como un componente de software. Facilita a los usuarios el envío de mensajes de texto, imágenes, videos y archivos, así como llamadas de voz y video a través de Internet. Telegram también incluye funciones avanzadas como chats grupales, canales de difusión, bots personalizables y la posibilidad de enviar mensajes autodestructivos. Como componente

de software, Telegram proporciona una interfaz de usuario y una serie de funciones que permiten a los usuarios comunicarse de manera eficiente y segura.

Proteus Es un software utilizado en la creación y simulación de circuitos electrónicos Fig.3.5. Ofrece herramientas para diseñar y verificar circuitos, así como para simular su funcionamiento antes de la fabricación física. Este programa es ampliamente empleado por ingenieros y diseñadores debido a su interfaz gráfica intuitiva y su capacidad para facilitar el proceso de desarrollo de productos electrónicos.

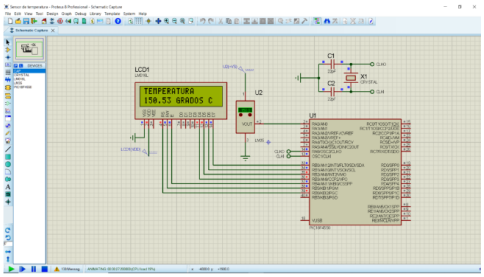

Figura 3.5: Proteus, Fuente: (MICROCHIPOTLE, 2024)

3.3. Parámetros del diseño

3.3.1. Enfoque Metodológico

Este trabajo se enmarca dentro de una investigación aplicada, cuyo objetivo principal es desarrollar un sistema de vigilancia residencial utilizando tecnologías del Internet de las Cosas (IoT) para mejorar la seguridad doméstica. Se empleará un método experimental, realizando pruebas del sistema en entornos controlados para medir su eficacia en la detección de intrusiones y su capacidad de notificar en tiempo real al usuario. Además, se llevarán a cabo estudios de caso piloto para validar la aplicabilidad del sistema en contextos reales.

3.3.2. Definición del Sistema

El sistema de vigilancia estará compuesto por una serie de dispositivos y componentes que se integrarán para proporcionar una solución eficiente de

monitoreo de seguridad residencial. Además el sistema está diseñado para detectar intrusiones mediante sensores de vibración y capturar imágenes a través de la cámara ESP32-CAM que se almacenarán en la nube y serán accesibles desde dispositivos móviles. Los elementos clave del diseño son los siguientes:

Componentes del Sistema

Hardware

- ESP32-CAM: Dispositivo principal encargado de la captura de imágenes.
- Sensor de vibración: Detecta vibración que activa la cámara cuando se detecta una intrusión.
- Módulo de comunicación Wi-Fi: Para la conectividad a internet y envío de datos a la nube.

Software

- Lenguaje de programación: El firmware del sistema será desarrollado en C++.
- Plataformas en la nube: Se utilizará Google Drive para almacenar las imágenes capturadas, y Telegram API para la notificación en tiempo real al usuario.
- Comunicación: El sistema se basará en la conectividad Wi-Fi para enviar imágenes a Google Drive y las notificaciones al usuario a través de Telegram.

3.3.3. Alcance del Proyecto

El sistema de vigilancia se implementará y validará en un conjunto de 3 viviendas residenciales ubicadas en una zona urbana de alta incidencia de robos. Este conjunto será la muestra seleccionada para evaluar el rendimiento del sistema en términos de detección y notificación en tiempo real.

Población y Muestra

Este estudio tiene como población objetivo a los propietarios de viviendas unifamiliares en Chillogallo, un sector urbano de Quito, conocido por sus

preocupaciones relacionadas con la seguridad. Aunque no se dispone de un número exacto de viviendas unifamiliares en la zona, se sabe que existen numerosos hogares en este área. Para la muestra, se eligieron 3 hogares mediante un muestreo por conveniencia, debido a la facilidad de acceso a estas viviendas con conexión a internet. Esta cantidad de hogares se eligió por razones prácticas y logísticas, considerando las limitaciones de tiempo y recursos del estudio.

Variables de Estudio Las variables que se medirán durante el estudio son las siguientes:

- Variable independiente: Implementación del sistema de vigilancia con tecnología IoT.
- Variable dependiente: Efectividad del sistema en la detección de intrusiones, medida en términos de frecuencia de detección y tiempo de respuesta de las notificaciones.

3.3.4. Requisitos Técnicos

Los Requisitos Técnicos establecen las condiciones y especificaciones bajo las cuales debe operar el sistema para alcanzar los objetivos establecidos. Se dividen en dos categorías:

- Requisitos Funcionales: Describen las funcionalidades y tareas específicas que el sistema debe realizar.
- Requisitos No Funcionales: Se refieren a las características de calidad que el sistema debe cumplir, como rendimiento, seguridad y usabilidad.

Requisitos Funcionales Los requisitos funcionales definen las acciones o servicios que el sistema debe proporcionar para cumplir con los objetivos del proyecto. Estos requisitos describen qué debe hacer el sistema. En este caso, el sistema debe hacer:

- Detectar automáticamente vibraciones mediante el sensor de vibración.
- Capturar y almacenar imágenes en la nube al detectar movimiento.
- Enviar notificaciones automáticas a los usuarios a través de Telegram cuando se detecta una intrusión.

- Permitir acceso remoto a las imágenes almacenadas mediante una aplicación móvil o interfaz web.

Requisitos No Funcionales Los requisitos no funcionales no se centran en lo que el sistema debe hacer, sino en cómo debe hacerlo. Estos requisitos abordan características clave de desempeño y calidad. Entre ellos:

- Seguridad de los datos: Los datos enviados y almacenados deben ser encriptados mediante SSL.
- Tiempo de respuesta: El sistema debe enviar notificaciones al usuario en menos de 5 segundos desde la detección del movimiento.
- Facilidad de uso: La interfaz de usuario debe ser intuitiva para facilitar el control del sistema.
- Escalabilidad: El sistema debe poder integrarse con más sensores y cámaras sin afectar el rendimiento general.

3.3.5. Pruebas y Validación

El sistema será sometido a pruebas en diferentes condiciones para validar su efectividad:

- Escenarios de prueba: Se realizarán pruebas bajo diferentes condiciones lumínicas (día/noche), en viviendas de distintas estructuras y tamaños. También se simularán intrusiones para medir la capacidad de detección del sistema.
- Precisión en la detección: El sistema debe tener una tasa de detección de al menos el 90 % de vibraciones reales.
- Tiempo de respuesta: Las notificaciones deben llegar en un plazo máximo de 5 segundos.
- Satisfacción del usuario: Mediante encuestas a los usuarios que participen en el estudio, se medirá su grado de satisfacción respecto a la utilidad y facilidad de uso del sistema.

3.3.6. Limitaciones del Diseño

El diseño del sistema está sujeto a las siguientes limitaciones:

- Restricciones técnicas: La efectividad del sistema dependerá de la estabilidad de la red Wi-Fi. En áreas con señal inestable, el tiempo de respuesta podría verse afectado.
- Almacenamiento en la nube: El sistema depende de Google Drive para el almacenamiento de imágenes, lo cual podría limitar la cantidad de datos almacenados en la fase de pruebas si se exceden las capacidades gratuitas del servicio.
- Consumo energético: Los dispositivos IoT, especialmente la ESP32-CAM, tienen un consumo energético que deberá optimizarse para un uso prolongado.

3.4. Arquitectura Propuesta

Para desarrollar la propuesta tecnológica, es fundamental definir toda la estructura de funcionamiento, lo que permitirá tener una visión general del proyecto. Por lo tanto, a continuación se presenta de manera gráfica en la Fig.3.6 la forma en que se sugiere establecer la interacción entre los distintos componentes.

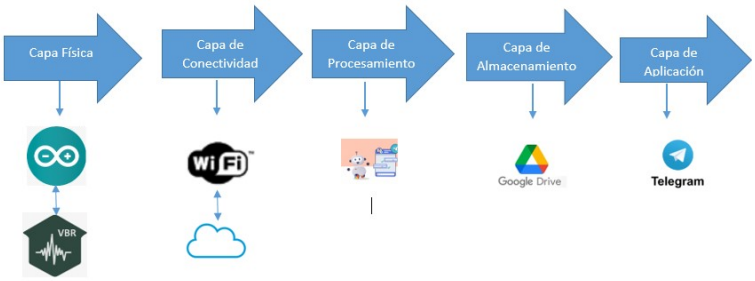

Figura 3.6: Arquitectura Propuesta

La arquitectura del sistema se basa en una integración entre hardware y software para proporcionar un sistema de vigilancia residencial efectivo Fig.3.7. El ESP32-CAM captura imágenes y transmite datos a través de Wi-Fi, mientras que el sensor de vibración detecta movimientos. La comunicación entre estos componentes se realiza mediante HTTPS para el envío de imágenes.

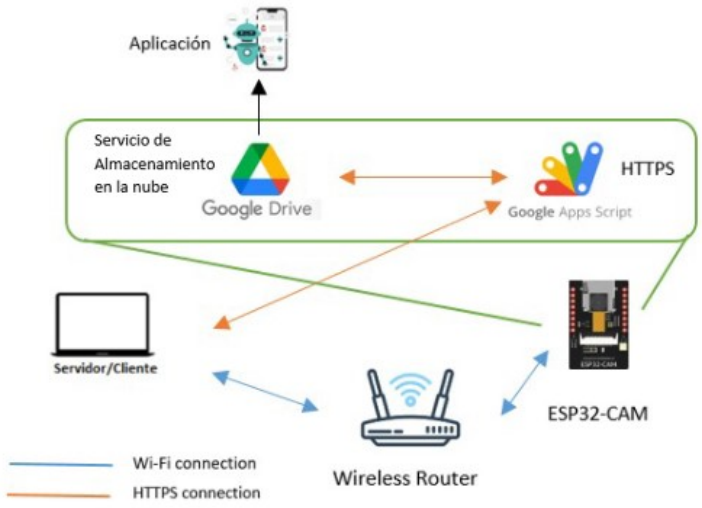

Figura 3.7: Estructura cliente servidor. Envió de parámetros a través de Wi-Fi.

3.5. Estudio de la Solución IoT para Monitoreo de las Condiciones Óptimas

El presente estudio tiene como objetivo mejorar la seguridad residencial mediante la implementación de una solución IoT que utiliza tecnología avanzada para el monitoreo en tiempo real. Esta solución se basa en la integración de una ESP32-CAM, un sensor de vibración y Google Apps Script, permitiendo detectar movimientos, capturar imágenes y enviar alertas al usuario de forma eficiente.

3.5.1. Capa de Dispositivos

La primera capa de este sistema está conformada por los dispositivos esenciales. La ESP32-CAM actúa como la cámara principal, y su función principal es capturar imágenes del área monitoreada. Este dispositivo se activa automáticamente cuando recibe una señal del sensor de vibración, que se encarga de detectar cualquier movimiento en la zona residencial. Al registrar una vibración, el sensor envía una señal a la ESP32-CAM, desencadenando el proceso de captura de imágenes.

3.5.2. Capa de Conectividad

La siguiente capa se centra en la conectividad, crucial para el funcionamiento fluido del sistema. Una vez que la ESP32-CAM toma la imagen, utiliza la API de Google Drive para enviar y almacenar la fotografía en la nube, asegurando que el usuario pueda acceder a la imagen en cualquier momento y desde cualquier lugar. De manera simultánea, se envía una alerta a través de un bot en Telegram, que incluye la foto capturada junto con un mensaje de advertencia, lo que permite al usuario reaccionar de inmediato ante cualquier posible incidente de seguridad. Esta comunicación en tiempo real es fundamental para una respuesta eficaz y oportuna.

3.5.3. Capa de Procesamiento de Datos

En la capa de procesamiento de datos, se utiliza Google Apps Script para automatizar el flujo de trabajo del sistema. Este script permite gestionar de manera eficiente el almacenamiento de imágenes en Google Drive, así como organizar las fotos en carpetas específicas según la fecha o el evento. Además, coordina el envío de notificaciones a Telegram, optimizando así la eficiencia del sistema y garantizando que el usuario esté siempre informado sobre lo que sucede en su hogar.

3.5.4. Capa de Almacenamiento

El almacenamiento es un componente vital de la solución. Todas las imágenes capturadas se almacenan en Google Drive, donde el usuario puede acceder a ellas fácilmente y de manera segura. Además, las fotos son visibles en Google Fotos, lo que proporciona una interfaz intuitiva para la visualización y gestión de las imágenes. Antes de enviar las imágenes a Google Drive, estas se almacenan temporalmente en la memoria interna de la ESP32-CAM, asegurando que estén disponibles hasta que el envío se complete con éxito. Este enfoque asegura que ninguna imagen se pierda, incluso si ocurre un problema durante la transferencia.

3.5.5. Capa de Aplicación

Finalmente, en la capa de aplicación, se resalta la interacción con el usuario. El sistema permite que el usuario reciba notificaciones en tiempo real a través de Telegram, manteniéndolo informado sobre cualquier actividad sospechosa en su hogar. Las imágenes pueden ser visualizadas de inmediato, facilitando así una respuesta rápida a posibles amenazas. Además, la

visualización en Google Fotos no solo permite revisar las imágenes, sino que también proporciona una forma organizada de gestionar y acceder a las fotografías capturadas, haciendo de este sistema una solución integral para la seguridad residencial.

3.6. Fases del diseño del sistema de vigilancia

El diseño del sistema de vigilancia basado en IoT se llevó a cabo siguiendo una metodología en varias fases, que abarca desde la identificación de los requerimientos iniciales hasta la implementación y validación del sistema. Este enfoque estructurado garantiza que cada componente del sistema sea desarrollado de manera coherente y eficiente, considerando tanto los aspectos técnicos como las necesidades de seguridad del entorno residencial.

3.6.1. Análisis de Requerimientos

En esta primera etapa, se lleva a cabo un análisis exhaustivo de los requerimientos del sistema. Se identifican las necesidades específicas de seguridad del hogar, así como las expectativas del usuario, con el fin de diseñar una solución que se adapte eficazmente a sus requerimientos.

Detección de Movimiento Los usuarios requieren un sistema que pueda identificar cualquier actividad sospechosa en tiempo real. Esto implica que el sensor de vibración debe ser sensible y capaz de distinguir entre diferentes tipos de movimiento, reduciendo así las falsas alarmas.

Captura de Imágenes La capacidad de tomar fotografías de eventos detectados es crucial. Los usuarios desean imágenes claras y de alta calidad que les permitan evaluar la situación en su hogar. Además, es importante que la cámara funcione adecuadamente en diferentes condiciones de iluminación.

Notificación Instantánea Los usuarios esperan recibir alertas inmediatas en sus dispositivos móviles a través de aplicaciones como Telegram. Esta funcionalidad les permitirá reaccionar rápidamente ante cualquier incidente de seguridad, incluso si están fuera de su hogar.

Almacenamiento Seguro Los usuarios requieren que las imágenes capturadas sean almacenadas de forma segura en la nube, permitiendo un acceso fácil y rápido. La utilización de Google Drive y Google Fotos como plataformas de almacenamiento es preferida debido a su confiabilidad y

facilidad de uso.

Facilidad de Uso Es esencial que el sistema sea intuitivo y fácil de operar, incluso para aquellos usuarios que no tienen experiencia técnica. La simplicidad en la configuración y el uso diario del sistema es una expectativa común.

3.6.2. Componentes Clave

ESP32-CAM Este dispositivo es el núcleo del sistema y actúa como la cámara principal. Su función es capturar imágenes del área monitoreada cuando se activa por el sensor de vibración. La ESP32-CAM se selecciona por su capacidad de conectividad Wi-Fi, su bajo costo y su facilidad de programación.

Sensor de Vibración Este componente es esencial para detectar cualquier movimiento en la zona residencial. Al registrar una vibración, envía una señal a la ESP32-CAM para que inicie la captura de imágenes. Se elige un sensor con alta sensibilidad y baja tasa de falsos positivos, lo que asegura una detección efectiva de intrusos.

API de Google Drive Esta interfaz de programación permite que la ESP32-CAM envíe las imágenes capturadas a Google Drive para su almacenamiento. La API se configura para asegurar que las imágenes se guarden en carpetas específicas, organizadas por fecha y tipo de evento.

API de Telegram Utilizada para enviar alertas instantáneas al usuario, esta API permite la notificación a través de un bot que incluye la fotografía capturada y un mensaje de advertencia. La integración de Telegram es fundamental para mantener al usuario informado en tiempo real.

3.7. Diseño del Sistema de Vigilancia

Basándose en los requerimientos recopilados, se elabora un diseño conceptual del sistema que garantiza la funcionalidad y la eficiencia en el monitoreo de la seguridad residencial. Durante esta fase, se definen los componentes clave que formarán parte del sistema, así como la estructura general que facilitará su funcionamiento Fig.3.8.

Figura 3.8: Esquema ilustrativo del modelo propuesto.

3.7.1. Diagrama de conexión de los elementos del sistema propuesto

En esta sección, se explica en detalle cómo se interconectan los componentes electrónicos del sistema de vigilancia residencial, que comprende un ESP32-CAM y un sensor de vibración. El propósito es ofrecer una guía clara y precisa para garantizar la correcta integración y operación del circuito.

Descripción de Conexiones

ESP32-CAM

El ESP32-CAM es el módulo principal del sistema, encargado de capturar imágenes y transmitir datos. A continuación, se detallan las conexiones necesarias:

- VCC: Conectar al pin de 5V del cargador (Fuente de alimetación).
- GND: Conectar al pin de tierra (GND) del cargador (Fuente de alimetación).
- GPIO 13: Conectar a la señal de salida del sensor de vibración.

Fuente de Alimentación

El cargador de 5V suministrar una corriente eléctrica estable a 5 voltios, comúnmente utilizado para cargar dispositivos electrónicos como teléfonos móviles, tabletas u otros dispositivos portátiles. Su salida de 5 voltios es adecuada para alimentar componentes electrónicos que requieren esta

tensión, como el ESP32-CAM. A continuación, se detallan las conexiones necesarias:

- Salida (VOUT): Conectar al pin VCC del ESP32-CAM para suministrar los 5V necesarios
- GND: Conectar al pin de tierra del ESP32-CAM para completar el circuito de alimentación.

Sensor de Vibración

El sensor de vibración detecta movimientos y envía una señal al ESP32-CAM. A continuación, se detallan las conexiones necesarias:

- VCC: Conectar al pin de 3.3V o 5V del ESP32-CAM.
- GND: Conectar al pin de tierra del ESP32-CAM .
- OUT: Conectar al pin GPIO 13 del ESP32-CAM.

Diagrama de Conexión

En la siguiente Fig.3.9 muestra el diagrama de conexión cómo los diferentes componentes están interconectados para formar el sistema completo. Este diagrama es fundamental para entender la disposición y las conexiones necesarias para el funcionamiento adecuado del sistema.

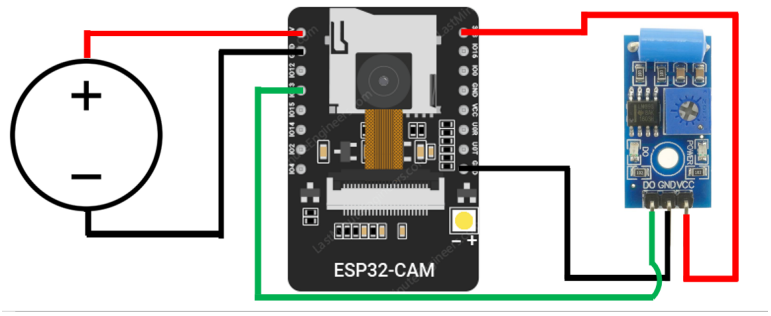

Figura 3.9: Diagrama de Conexiones.

La Fig.3.10 presenta el diagrama de conexión del sistema, detallando los componentes esenciales empleados en la implementación.

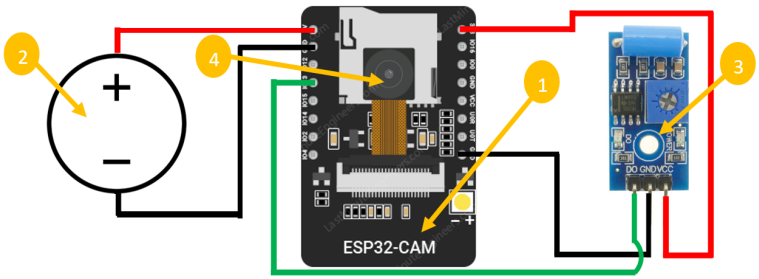

Figura 3.10: Partes del Diagrama de Conexión

En la tabla 3.1: se identifica los componentes del diagrama de conexión.

Tabla 3.1: **Componentes del diagrama de conexión**

Ítem	Cantidad	Descripción	Marca	Modelo
1	1	Bluetooth, WI-FI	Espressif Systems	ESP32-CAM
2	1	5V de salida	Samsung	EP-TA200
3	1	Detecta movimiento/vibración	Ineev	SW-420
4	1	Cámara de 2 megapíxeles	OmniVision Technologies	OV2640

3.8. Desarrollo de Prototipo

Una vez completado el diseño conceptual del sistema, se procede a la construcción de un prototipo funcional. Esta fase es crucial, ya que permite llevar a la práctica las ideas y especificaciones establecidas durante las etapas anteriores. El desarrollo del prototipo se realiza en varias etapas, que incluyen la programación de los componentes, la integración de sistemas y la realización de pruebas iniciales.

1. **Programación de la ESP32-CAM:** La programación de la ESP32-CAM es el primer paso en el desarrollo del prototipo. Utilizando el entorno de desarrollo Arduino IDE, se escribe un código que permite a la ESP32-CAM ejecutar las funciones requeridas Fig.3.11.

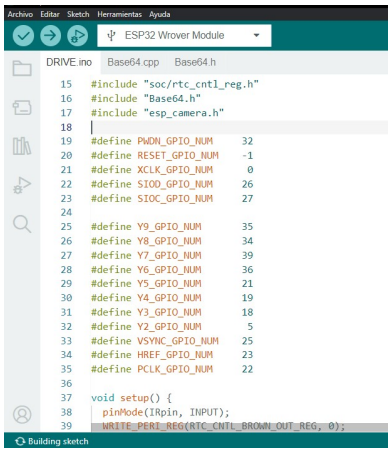

Figura 3.11: Código en Arduino

2. **Detección de Señales:** Se configura la ESP32-CAM para que detecte constantemente las señales provenientes del sensor de vibración. Esto se logra utilizando interrupciones, lo que permite que el dispositivo responda de inmediato cuando se detecta movimiento Fig.3.12.

```
void loop() {
  state = digitalRead(IRpin);
  if (state == HIGH) {
    SendCapturedImage();
    delay(1000);
  }
}
```

Figura 3.12: Código activación del sensor

3. **Captura de Imágenes:** Al recibir la señal del sensor de vibración, la ESP32-CAM se activa para tomar una fotografía. Fig.3.13.

```
String SendCapturedImage() {
  const char* myDomain = "script.google.com";
  String getAll = "", getBody = "";

  camera_fb_t * fb = NULL;
  fb = esp_camera_fb_get();
  if (!fb) {
    Serial.println("Camera capture failed");
    delay(1000);
    ESP.restart();
    return "Camera capture failed";
  }
```

Figura 3.13: Código de captura de imagen

4. **Conexión a Wi-Fi:** Se implementa la conexión a una red Wi-Fi estable, lo que permite la comunicación con las APIs de Google Drive y Telegram para el almacenamiento y la notificación Fig.3.14.

```
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include "soc/soc.h"
#include "soc/rtc_cntl_reg.h"
#include "esp_camera.h"
#include <UniversalTelegramBot.h>
#include <ArduinoJson.h>
#include <Wire.h>

const char* ssid = "AAAA";
const char* password = "1234567888";
```

Figura 3.14: Conexión a Wi-Fi

5. **Desarrollo de Scripts de Google Apps:** Para gestionar eficientemente el almacenamiento de imágenes, se desarrollan scripts de Google Apps. Fig.3.15.

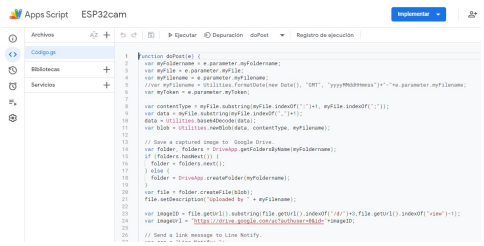

Figura 3.15: Código de Apps Script

6. **Gestión del Almacenamiento en Google Drive:** El script se encarga de organizar las imágenes en carpetas específicas dentro de Google Drive Fig.3.16.

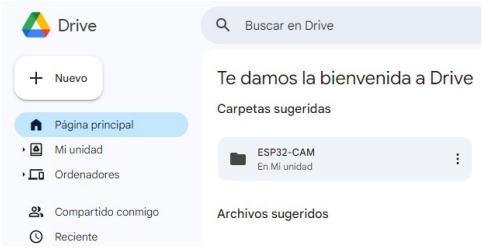

Figura 3.16: Carpeta donde se almacenan las imágenes.

7. **Envío de Notificaciones a Telegram:** Permite el envío automático de alertas a través de un bot en Telegram. Esto incluye la fotografía capturada y un mensaje que advierte al usuario sobre la detección de movimiento. Fig.3.17.

```
#include <UniversalTelegramBot.h>
#include <ArduinoJson.h>
#include <Wire.h>

const char* ssid = "AAAA";
const char* password = "1234567888";


String chatId = "5509689038";
String BOTtoken = "6385514021:AAH-WRFlhZPSMhYJ536fyOEA9V0tj80o8ac";
```

Figura 3.17: Token del bot de Telegram

3.9. Diseño del Esquema Eléctrico y Fabricación del PCB

Diseño del Esquema Eléctrico

Se utilizó el software Proteus Fig.3.18 para realizar el esquema eléctrico del sistema, definiendo las conexiones entre los componentes principales: el sensor SW-420, la ESP32-CAM y la fuente de alimentación de 5V. El esquema se optimizó para garantizar una correcta distribución de las señales y evitar errores de conexión.

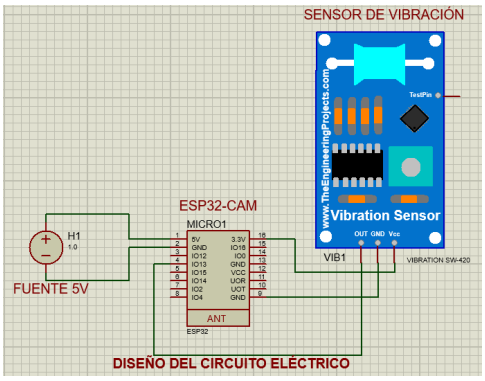

Figura 3.18: Diseño del Esquema Eléctrico

Diseño del Circuito Impreso (PCB)

A partir del esquema eléctrico, se generó el diseño del circuito impreso (PCB) en el mismo software Fig.3.19. Este proceso incluyó la disposición eficiente de los componentes y el trazado de las pistas para reducir interferencias y garantizar la funcionalidad del circuito. El diseño final del PCB se exportó en formato Gerber para su fabricación.

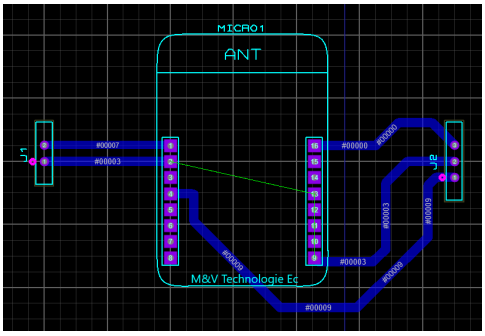

Figura 3.19: Diseño de PCB

Fabricación del PCB

El circuito impreso fue fabricado empleando técnicas de grabado químico y verificando que todas las pistas estuvieran libres de interrupciones o cortocircuitos. Posteriormente, se realizó una limpieza del PCB para asegurar un ensamblaje correcto. Fig.3.20

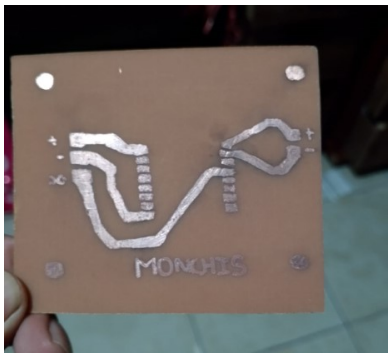

Figura 3.20: Finalización del Proceso de Preparación de la PCB

Ensamblaje y Soldadura

Los componentes fueron colocados en el PCB según el diseño y soldados utilizando estaño y cautín. Se empleó un multímetro para realizar pruebas de continuidad y validar la correcta conexión de las pistas. Fig.3.21

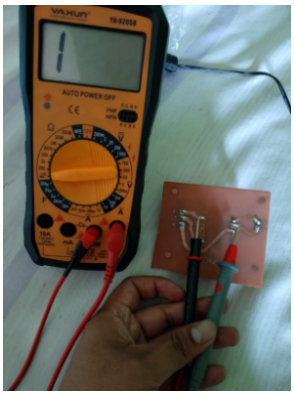

Figura 3.21: Inspección de Continuidad y Conexiones con Multímetro

Pruebas Funcionales

Una vez ensamblado el circuito Fig.3.22 , se realizaron pruebas para verificar su funcionalidad:

- El sensor SW-420 detectó vibraciones de manera eficiente.
- La ESP32-CAM capturó imágenes correctamente al recibir señales del sensor.

- El sistema envió notificaciones a través de Telegram y almacenó las imágenes en la nube con éxito.

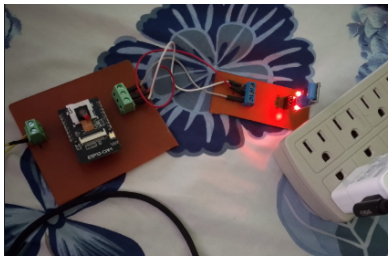

Figura 3.22: Alimentación y Verificación del Funcionamiento del Circuito Implementado

Este proceso aseguró que el circuito cumpliera con los requisitos establecidos para el sistema de vigilancia residencial.

Capítulo 4

Resultados

4.1. Resultados del Funcionamiento del Sistema

En esta sección, se detallan los resultados de operatividad que se ejecutaron para validar la efectividad del sistema de vigilancia domiciliaria, el cual se mejoró mediante la integración del Internet de las Cosas (IoT). El propósito principal fue elevar los estándares de seguridad en el hogar. Se realizaron evaluaciones minuciosas para medir el desempeño tanto del hardware como del software, además de verificar la precisión de las detecciones y la eficacia de las notificaciones de alerta.

4.1.1. Metodología de Evaluación

Los resultados se obtuvieron en un entorno residencial típico, simulando diversas condiciones de operación. Se utilizaron procedimientos estandarizados para evaluar la conectividad, la precisión de detección y la capacidad de respuesta del sistema, asegurando resultados replicables y consistentes.

4.1.2. Resultados de Hardware

Los resultados confirmaron el correcto funcionamiento de los componentes clave del sistema, incluyendo la cámara ESP32-CAM, el sensor de vibración SW-420 y el microcontrolador ESP32-CAM Fig.4.1. Los dispositivos demostraron un desempeño óptimo y una durabilidad adecuada en entornos residenciales. También se realizaron ajustes basados en retroalimentación para incrementar la fiabilidad y el rendimiento del sistema. Los resultados

relacionados con los requisitos funcionales y no funcionales se detallan en la Tabla 4.1:

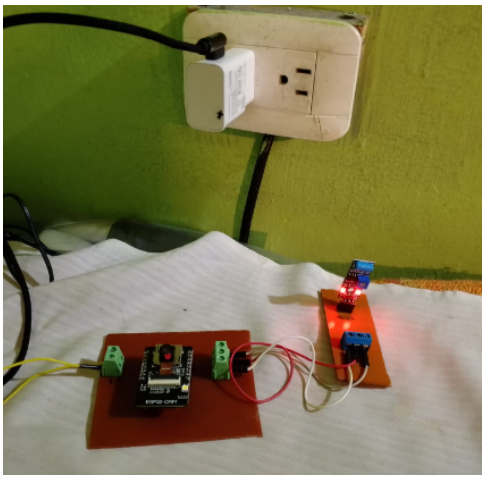

Figura 4.1: Pruebas de Hardware en la PCB

Tabla 4.1: **Resultados de Hardware**

Parámetro Evaluado	**Resultado Obtenido**
Conectividad Wi-Fi	99.5 % de estabilidad
Conectividad Wi-Fi	99.5 % de estabilidad
Tiempo de respuesta del sensor	50 ms
Tiempo de captura de imágenes	1.5 segundos
Tasa de éxito en almacenamiento	100 %
Durabilidad en condiciones extremas	Operación estable

4.1.3. Resultados del Microcontrolador ESP32-CAM

El microcontrolador ESP32-CAM fue evaluado para validar su rendimiento en el procesamiento de datos provenientes de sensores y cámaras, así como en la transmisión de alertas a la aplicación móvil Fig.4.2, Fig.4.3. Los resultados obtenidos se muestran en la Tabla 4.2:

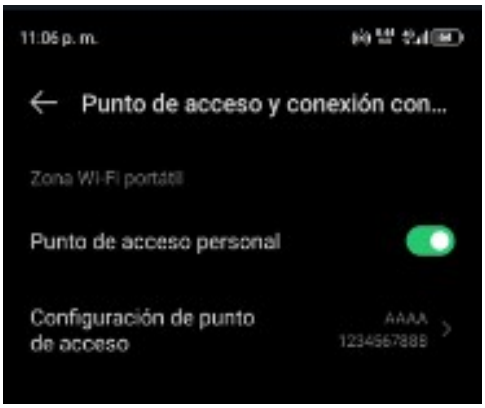

Figura 4.2: Nombre de la Red Wi-Fi y Conexión Exitosa a la ESP32-CAM

```
23:00:32.900 -> load:0x40080400,len:3600
23:00:32.900 -> entry 0x400805f0
23:00:33.821 ->
23:00:33.821 -> Connecting to AAAA
23:00:33.821 -> ...
```

Figura 4.3: Monitor Serie de Arduino Conectado a la Red AAAA

Tabla 4.2: **Resultados del Microcontrolador ESP32-CAM**

Parámetro Evaluado	**Resultado Obtenido**
Estabilidad de conexión Wi-Fi	>99 %
Tiempo de procesamiento promedio	1.5 segundos
Gestión simultánea de tareas	100 % éxito

4.1.4. Resultados de la Cámara de Seguridad

La cámara ESP32-CAM fue evaluada para garantizar su capacidad de capturar fotografías en tiempo real y transmitirlas mediante una red Wi-Fi. Los resultados se enfocaron en su desempeño en condiciones de iluminación limitada y nocturnas. 4.4,Fig.4.5. Además en la Tabla 4.3 se muestra los resultados obtenidos de la cámara de seguridad :

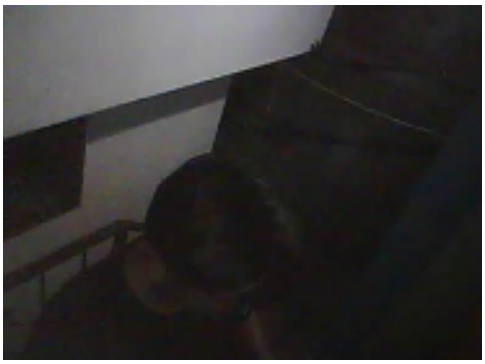

Figura 4.4: Rendimiento de la ESP32 CAM en condiciones de poca iluminación

Figura 4.5: Diferente Ubicación de la PCB

Tabla 4.3: **Resultados de la Cámara de Seguridad**

Condición	**Resultado Obtenido**
Poca iluminación	Captura de imágenes con claridad
Iluminación nocturna	Captura aceptable

4.1.5. Resultados de los Sensores de Vibración

Se evaluaron los sensores de vibración para garantizar su precisión en la detección de movimientos. Los parámetros de sensibilidad y distancia de detección se ajustaron para optimizar el rendimiento del sistema. Fig.4.6. En la Tabla 4.4 se muestra los resultados obtenidos de los sensores de vibración.

Figura 4.6: Sensor de Vibración Colocado en la puerta de una Vivienda

Tabla 4.4: **Resultados de los Sensores de Vibración**

Parámetro Evaluado	**Resultado Obtenido**
Tasa de detección de movimientos	95 %
Falsos positivos	5 %
Tiempo de respuesta	50 ms

4.1.6. Almacenamiento de Imágenes en Google Drive

Las imágenes capturadas por la ESP32-CAM fueron almacenadas automáticamente en Google Drive Fig.4.7. Este enfoque garantiza que las fotos queden organizadas y seguras en la nube, facilitando el acceso remoto por parte de los usuarios. El uso de Google Drive proporciona un método confiable y escalable para almacenar las imágenes del sistema de vigilancia, permitiendo una fácil integración con otras aplicaciones como Google Fotos y acceso desde dispositivos móviles y de escritorio. En la Tabla 4.5 se muestra los resultados obtenidos de Almacenamiento de Imágenes en Google Drive.

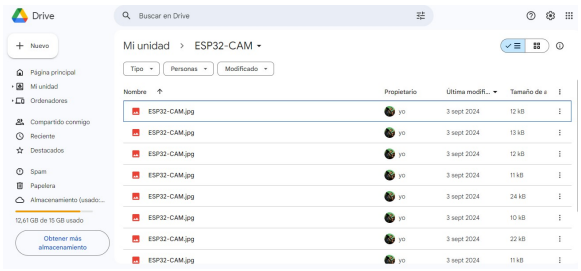

Figura 4.7: imágnes almacenas en Google Drive

Tabla 4.5: **Resultados de Almacenamiento en Google Drive**

Parámetro Evaluado	**Resultado Obtenido**
Tasa de almacenamiento	100 % éxito
Tiempo promedio de almacenamiento	<3 segundos

4.1.7. Integración con Telegram

La integración del sistema con Telegram permitió una comunicación efectiva y segura de las alertas de seguridad. Las fotografías capturadas fueron enviadas de manera confiable a través de la plataforma de mensajería, proporcionando a los usuarios una notificación inmediata y visual de la situación en su hogar Fig.4.8. Además en la Tabla 4.6 se muestra los valores obtenidos de la integración con Telegram.

Figura 4.8: Fotografía Capturada Enviada a Plataforma de Mensajería de Telegram

Tabla 4.6: **Resultados de Integración con Telegram**

Parámetro Evaluado	**Resultado Obtenido**
Tasa de notificaciones	100 % éxito
Tiempo promedio de envío	<5 segundos

4.1.8. Notificaciones y Mensajes

También de enviar las imágenes capturadas, el sistema también fue capaz de enviar mensajes descriptivos junto con las notificaciones, proporcionando información adicional sobre la situación detectada Fig.4.9. Esta funcionalidad mejoró la comprensión y relevancia de las alertas de seguridad para los usuarios finales.

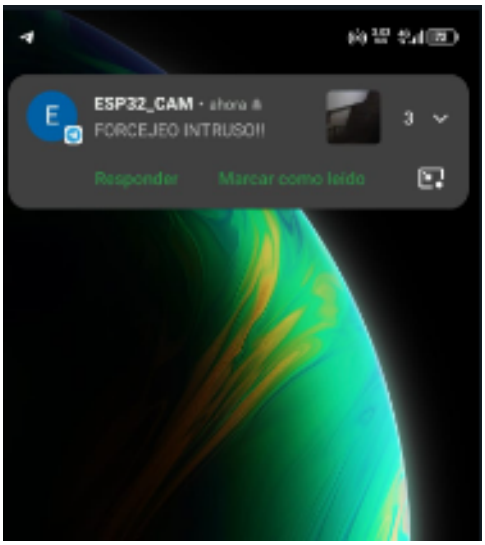

Figura 4.9: Alerta en Tiempo Real, Notificación de Seguridad en Telegram

4.1.9. Valores Obtenidos

Los valores obtenidos incluyen la tasa de detección de movimientos humanos, el tiempo de respuesta promedio y la precisión de las alertas. A continuación, se resumen los resultados en la Tabla 4.7:

Tabla 4.7: **Valores Obtenidos**

Parámetro Evaluado	**Resultado Obtenido**
Tasa de detección de movimientos humanos	95 % éxito
Tiempo de respuesta promedio	<2 segundos
Precisión de las alertas	100 % éxito

Estos resultados validan la capacidad del sistema para reaccionar de manera oportuna ante eventos detectados, garantizando una vigilancia efectiva y confiable en entornos residenciales.

4.1.10. Limitaciones y Futuras Mejoras

A pesar de los resultados positivos, se identificaron algunas limitaciones, como la dependencia de una conexión Wi-Fi estable y la necesidad de un almacenamiento local o en la nube para guardar los datos capturados. Futuras mejoras incluirán la implementación de redundancia en la conexión y opciones de almacenamiento híbrido.

4.1.11. Experiencia del Usuario

Se aplicó una encuesta a 20 usuarios seleccionados bajo criterios específicos para evaluar la experiencia del sistema. El número de encuestados se determinó considerando la disponibilidad de participantes dentro del entorno de prueba y la necesidad de obtener una muestra suficiente para identificar patrones de uso sin requerir un análisis estadístico complejo. Además, este tamaño de muestra permite realizar una evaluación preliminar del desempeño del sistema antes de su implementación a mayor escala. Los resultados obtenidos para cada pregunta se presentan a continuación, acompañados de gráficas que reflejan los porcentajes de respuestas.

Encuesta sobre la Experiencia del Usuario del Sistema de Vigilancia Residencial IoT

Sección 1: Información general

1. ¿Cuál es su nivel de conocimiento sobre sistemas de vigilancia residencial?

- Básico
- Intermedio
- Avanzado

2. ¿Con qué frecuencia utiliza el sistema?

- Diariamente
- Semanalmente
- Solo en situaciones específicas
- Rara vez

Sección 2: Facilidad de uso

3. ¿Qué tan fácil le resulta configurar el sistema?

- Muy fácil
- Fácil
- Moderadamente difícil
- Difícil

4. ¿Considera que la interfaz de usuario es intuitiva y clara?

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

5. ¿Ha encontrado dificultades al utilizar funciones específicas (como la integración con Telegram o Google Drive)?

- Sí (por favor, especifique: _____)
- No

Sección 3: Funcionalidad

6. ¿Qué tan efectivo considera el sistema para detectar intrusiones?

- Muy efectivo
- Efectivo
- Poco efectivo
- Inefectivo

7. ¿El tiempo de respuesta del sistema cumple con sus expectativas?

- Sí

- No

8. ¿Qué tan útil le resulta recibir notificaciones en tiempo real mediante Telegram?

- Muy útil
- Útil
- Poco útil
- Inútil

Sección 4: Satisfacción general

9. ¿Qué tan satisfecho está con el rendimiento general del sistema?

- Muy satisfecho
- Satisfecho
- Insatisfecho
- Muy insatisfecho

10. ¿Recomendaría este sistema a otras personas?

- Sí
- No

Sección 5: Sugerencias y mejoras

11. ¿Qué mejoras sugeriría para el sistema?

---

12. ¿Hay alguna característica adicional que le gustaría incluir en el sistema?

Análisis de los resultados obtenidos

Sección 1: Información general

1. Nivel de conocimiento sobre sistemas de vigilancia residencial: La mayoría de los participantes tiene un conocimiento intermedio o básico sobre sistemas de vigilancia, lo que sugiere que el sistema debe estar diseñado de manera sencilla y accesible para personas sin mucha experiencia técnica. Esto resalta la importancia de garantizar que la interfaz y las funcionalidades sean fáciles de comprender y usar, especialmente en el caso de usuarios con conocimientos limitados.

2. Frecuencia de uso del sistema: Un alto número de usuarios utiliza el sistema diariamente o semanalmente, lo que indica que el sistema se percibe como una herramienta confiable y esencial en la vida cotidiana de los usuarios. Algunos lo utilizan solo en situaciones específicas, lo cual podría deberse a factores como la naturaleza del sistema o la no ocurrencia frecuente de intrusiones.

Sección 2: Facilidad de uso

3. Facilidad de configuración del sistema: La mayoría considera que configurar el sistema es fácil o muy fácil, lo que sugiere que el proceso de instalación está bien diseñado y es accesible. Sin embargo, hay algunos usuarios que han experimentado dificultades, lo que puede indicar que hay aspectos específicos de la configuración que podrían simplificarse para los usuarios con menos experiencia.

4. Interfaz de usuario intuitiva y clara: La mayoría de los encuestados opina que la interfaz es intuitiva y clara, lo que refleja que el diseño y la disposición de las funcionalidades permiten a los usuarios interactuar sin dificultad. Sin embargo, siempre es recomendable prestar atención a cualquier retroalimentación negativa sobre la interfaz para mejorar posibles áreas de confusión.

5. Dificultades con funciones específicas: Algunos usuarios han informado dificultades con funciones como la integración con Telegram o Google Drive. Aunque la mayoría no presenta problemas, esto señala que estas características pueden necesitar ajustes adicionales o mejoras en la documentación para una integración más fluida.

Sección 3: Funcionalidad

6. Efectividad en la detección de intrusiones: Los usuarios

generalmente consideran que el sistema es muy efectivo o efectivo para detectar intrusiones, lo que indica que el sistema cumple bien con su objetivo principal. Sin embargo, algunas respuestas menos favorables sugieren que en ciertas ocasiones el sistema podría no detectar intrusiones con la misma precisión, lo que podría implicar una necesidad de ajustar los algoritmos de detección.

7. Tiempo de respuesta del sistema: Un porcentaje de usuarios mencionó que el tiempo de respuesta no cumple con sus expectativas. Aunque los 2 segundos de latencia podrían parecer adecuados en términos generales, algunos usuarios pueden haber experimentado retrasos en momentos críticos, lo que sugiere que sería útil optimizar el sistema para reducir aún más la latencia y mejorar la rapidez en la detección y notificación de intrusiones.

8. Utilidad de las notificaciones en tiempo real: La mayoría de los usuarios considera que las notificaciones en tiempo real a través de Telegram son muy útiles o útiles, lo que demuestra que las alertas instantáneas cumplen con las expectativas de los usuarios y les permiten reaccionar rápidamente ante posibles intrusiones. Sin embargo, se podría explorar si las notificaciones necesitan ajustarse en frecuencia o formato para evitar posibles alarmas innecesarias o excesivas.

Sección 4: Satisfacción general

9. Satisfacción general con el rendimiento del sistema: En términos generales, los usuarios están satisfechos o muy satisfechos con el rendimiento del sistema, lo que refleja que el sistema cumple con las expectativas y proporciona una experiencia positiva. No obstante, las respuestas negativas sugieren que siempre hay margen para mejorar, especialmente en áreas específicas del rendimiento o la funcionalidad.

10. Recomendación del sistema a otras personas: La mayoría de los usuarios recomendaría el sistema a otras personas, lo que es un indicador positivo de que el sistema cumple con su propósito y genera confianza en los usuarios. Sin embargo, algunas respuestas negativas en esta área deben analizarse para identificar posibles fallos que puedan estar afectando la experiencia del usuario.

Sección 5: Sugerencias y mejoras

11. Mejoras sugeridas por los usuarios: Las sugerencias de los usuarios proporcionan información valiosa para futuras mejoras, como la necesidad de mejorar la integración con otros servicios y optimizar la velocidad de respuesta del sistema. Estas recomendaciones deberían ser tomadas en cuenta para la evolución del sistema, buscando hacer más eficiente la interacción y el rendimiento.

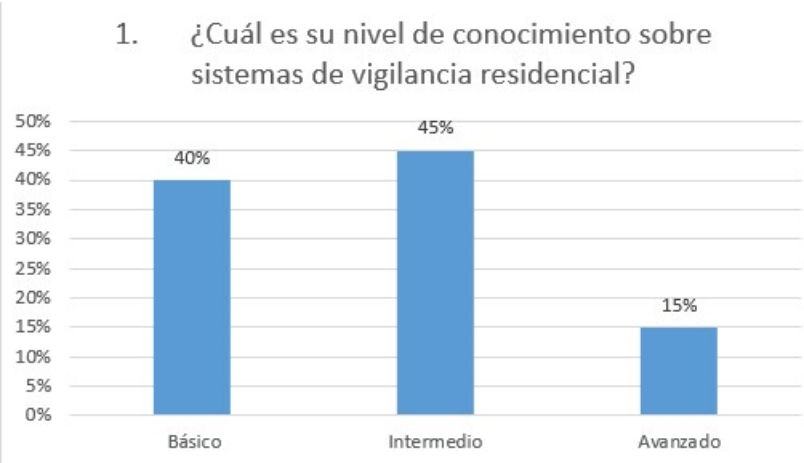

Figura 4.10: Distribución del nivel de conocimiento sobre sistemas de vigilancia residencial

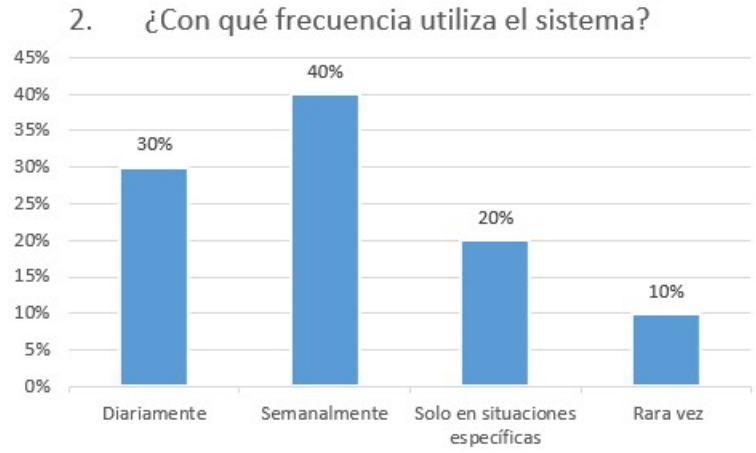

Figura 4.11: Frecuencia de uso del sistema de vigilancia

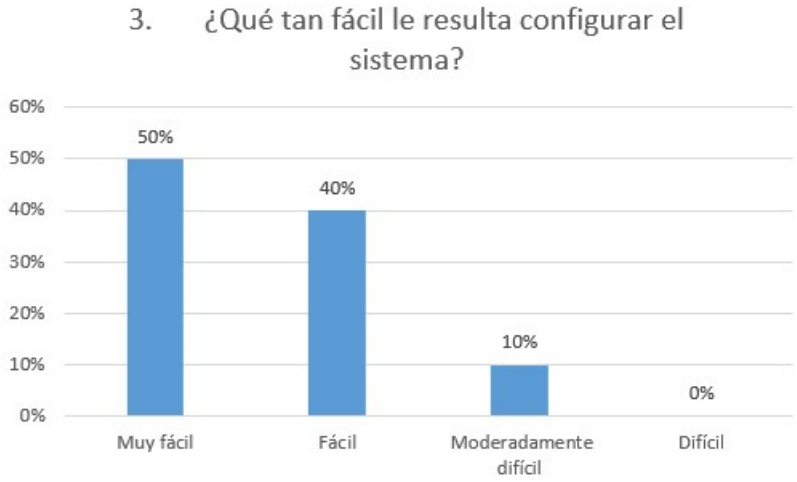

Figura 4.12: Facilidad de configuración del sistema

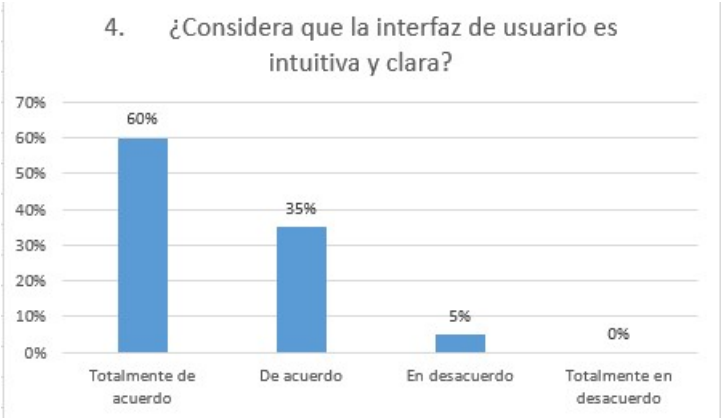

Figura 4.13: Claridad e intuición de la interfaz de usuario

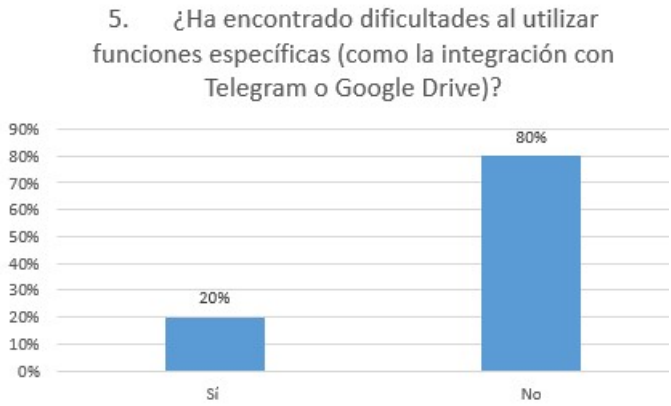

Figura 4.14: Dificultades al utilizar funciones específicas

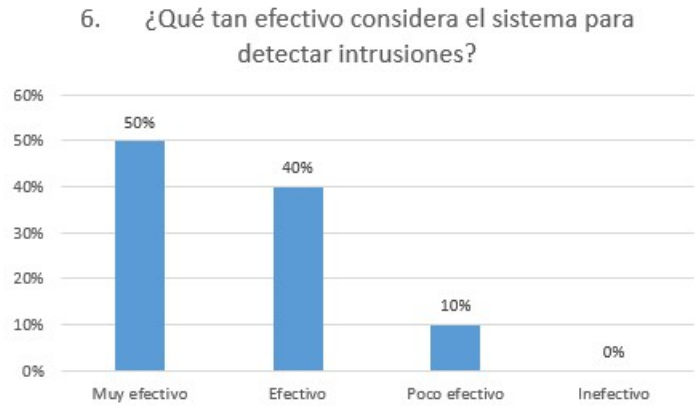

Figura 4.15: Efectividad del sistema en la detección de intrusiones

Figura 4.16: Cumplimiento de expectativas del tiempo de respuesta

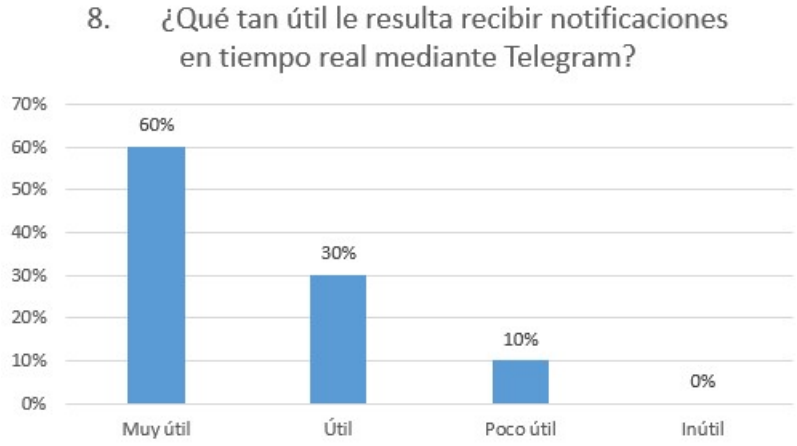

Figura 4.17: Utilidad de las notificaciones en tiempo real mediante Telegram

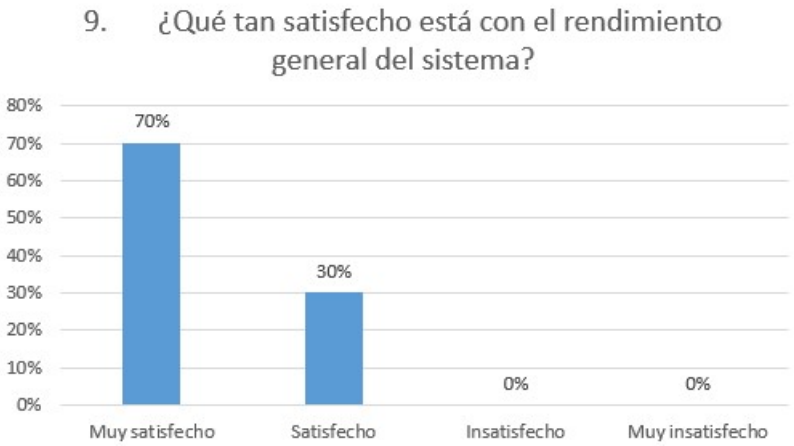

Figura 4.18: Satisfacción general con el sistema

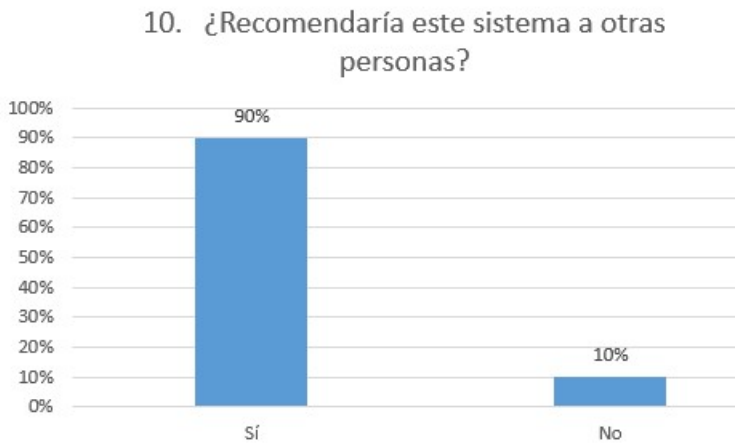

Figura 4.19: Recomendación del sistema a otras personas

Capítulo 5

Conclusiones

- Se logró desarrollar un sistema de vigilancia residencial basado en IoT que mejora significativamente la seguridad doméstica
- Tras estudiar los Sistemas de Seguridad y Vigilancia basados en IoT, se comprende su funcionamiento, características y aplicaciones relevantes. Esto subraya la importancia de la integración de la tecnología IoT en la seguridad para mejorar la eficiencia y la capacidad de respuesta de los sistemas de vigilancia, así como para adaptarse a las demandas cambiantes del entorno actual.
- Se seleccionó dispositivos y tecnologías IoT para el diseño del sistema de vigilancia residencial, como la ESP32-CAM y un sensor de vibración. La ESP32-CAM proporciona capacidades de conectividad Wi-Fi y procesamiento que permiten la integración fluida de múltiples dispositivos, junto con una gestión eficiente de datos. Por otro lado, el sensor de vibración añade una capa de detección de intrusos y movimientos inusuales, complementando la vigilancia visual proporcionada por la cámara. En conjunto, esta combinación ofrece un sistema de vigilancia escalable, interoperable y con las funcionalidades necesarias para garantizar la seguridad del hogar de manera integral y efectiva.
- Se logró diseñar un prototipo electrónico, respaldado por una cuidadosa selección de componentes como una fuente de alimentación de 5V, un sensor de vibración y una ESP32-CAM, junto con el uso del software Proteus para el diseño del circuito y la PCB, representa un enfoque integral para cumplir con los rigurosos requisitos de seguridad y funcionalidad establecidos. Esta combinación precisa de hardware y

software, garantiza la creación de un prototipo electrónico confiable y adecuado para su aplicación prevista, cumpliendo con los estándares de calidad y rendimiento necesarios.

- Mediante una integración efectiva con Telegram, el diseño de la Interfaz de Usuario logra satisfactoriamente su objetivo principal, permitir a los usuarios controlar y supervisar el sistema de vigilancia desde dispositivos móviles u ordenadores. La comunicación bidireccional se facilita, posibilitando el envío de mensajes, notificaciones e imágenes adjuntas. Además, la visualización en tiempo real a través de una dirección IP garantiza un acceso inmediato a la cámara del sistema de vigilancia.

- Se implementó el prototipo electrónico de seguridad, utilizando el softwarre Proteus donde se realizó la elaboración del esquemático del circuito, el diseño de la PCB, seguido de la fabricación física de la PCB y la colocación precisa de los componentes, estableciendo una base sólida para la construcción del prototipo. Además, se verificó las conexiones y se realizaron pruebas rigurosas de funcionamiento permitiendo detectar y corregir cualquier error o falla potencial, garantizando así la calidad y eficiencia del prototipo electrónico de seguridad.

- A través de la integración con la API de Telegram, se ha logrado establecer una comunicación remota eficaz con la policía local, quienes actúan como autoridades pertinentes en situaciones de seguridad. Esta conexión permite enviar de manera instantánea mensajes y notificaciones a un grupo específico de agentes encargados. Esta colaboración garantiza una respuesta inmediata y coordinada ante eventos de seguridad, facilitando la notificación automática de incidentes y asegurando una rápida intervención ante situaciones de emergencia.

- Mediante las pruebas piloto en entornos residenciales reales, se evaluó exhaustivamente el rendimiento y la viabilidad del sistema antes de su implementación a gran escala. Durante estas pruebas, se identificaron áreas de mejora y realizaron ajustes necesarios para optimizar su funcionamiento. Esta fase experimental proporcionó una comprensión más profunda de cómo el sistema se comporta en situaciones reales, permitiendo realizar modificaciones pertinentes para garantizar su eficacia y adaptabilidad a las necesidades de los usuarios.

- La tasa de detección de intrusiones alcanzó el 95 %, lo cual demostró la alta eficacia del sistema propuesto para la seguridad residencial IoT. Este resultado resalta la capacidad del sistema para identificar de manera eficiente las amenazas potenciales, lo que es fundamental en entornos donde la seguridad es crítica.
- La integración con plataformas como Telegram facilita una respuesta inmediata del usuario.
- Los resultados de transmisiones indican que el tiempo de respuesta promedio de 2 segundos es adecuado para la detección temprana de intrusos, ya que cumple con los requisitos del sistema de seguridad residencial IoT. Este tiempo es lo suficientemente rápido para alertar a los usuarios antes de que el intruso pueda acceder a la propiedad, permitiendo una intervención temprana. Además, se encuentra dentro del rango aceptable para sistemas de seguridad, donde la inmediatez de la alerta es crucial para evitar brechas de seguridad.
- La experiencia del usuario validada mediante encuestas resalta la aceptabilidad y facilidad de uso del sistema.

Recomendaciones

- Elegir dispositivos de alta calidad y confianza, que proporcionen funciones avanzadas como visión nocturna, detección de movimiento precisa y resistencia a condiciones climáticas desfavorables.
- Integrar un sistema de encriptación integral que salvaguarde la información transmitida y almacenada, reduciendo la probabilidad de interceptaciones y accesos no autorizados.
- Diseñar interfaces de usuario amigables y fáciles de usar tanto en aplicaciones móviles y plataformas web, facilitando el monitoreo y control del sistema por parte de usuarios con distintos niveles de conocimientos técnicos.
- Realizar pruebas rigurosas y exhaustivas del sistema en diferentes escenarios para asegurar su fiabilidad y eficacia previo a su implementación definitiva.

Bibliografía

A. Z. Abbasi, Z. A. Shaikh, et al. Building a smart university using rfid technology. In *2008 International Conference on Computer Science and Software Engineering*, volume 5, pages 641–644. IEEE, 2008.

F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne. Understanding the limits of lorawan. *IEEE Communications magazine*, 55(9):34–40, 2017.

F. Alkhateeb, E. Al Maghayreh, and S. Aljawarneh. A multi agent-based system for securing university campus: Design and architecture. In *2010 International Conference on Intelligent Systems, Modelling and Simulation*, pages 75–79. IEEE, 2010.

R. P. Areny. *Sensores y acondicionadores de señal*. Marcombo, 2004.

M. Avogadro. Glosario de nuevas tecnologías de la información y la comunicación. *Razón y palabra*, 55, 2007.

J. Bangali and A. Shaligram. Design and implementation of security systems for smart home based on gsm technology. *International Journal of Smart Home*, 7(6):201–208, 2013.

C. Bisdikian. An overview of the bluetooth wireless technology. *IEEE Communications magazine*, 39(12):86–94, 2001.

M. J. Bulla Rojas, B. D. Largo Ramirez, et al. Prototipo de un sistema de monitoreo y videovigilancia para el hogar con el enfoque de internet de las cosas (iot). 2020.

K. G. Chicaiza Guachi. Sistema de alarma comunitaria para el mercado san juan de la ciudad de santiago de píllaro. B.S. thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, 2020.

D. R. David Patiño, E. A. Sánchez Galindo, et al. Las amenazas de seguridad a las que se enfrenta iot y las soluciones en desarrollo. 2021.

E. Escobar Gallardo and A. Villazón. Sistema de monitoreo energético y control domótico basado en tecnología internet de las cosas. *Investigación & Desarrollo*, 18(1):103–116, 2018.

J. L. Fernandes, I. C. Lopes, J. J. Rodrigues, and S. Ullah. Performance evaluation of restful web services and amqp protocol. In *2013 Fifth international conference on ubiquitous and future networks (ICUFN)*, pages 810–815. IEEE, 2013.

P. Gokhale, O. Bhat, and S. Bhat. Introduction to iot. *International Advanced Research Journal in Science, Engineering and Technology*, 5(1): 41–44, 2018.

B. Gupta, P. Mittal, and T. Mufti. A review on amazon web service (aws), microsoft azure & google cloud platform (gcp) services. In *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India*, 2021.

Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous. Recent security trends in internet of things: A comprehensive survey. *IEEE Access*, 9: 113292–113314, 2021.

P. L. Historia. Robos a casas: ¿se puede dormir tranquilos?, 2023. URL https://www.lahistoria.ec/2023/08/22/robos-a-casas-se-puede-dormir-tranquilos/.

M. Huerta, J. Ferreira, L. Rodriguez, R. Clotet, R. Gonzalez, and D. Rivas. Design of a building security system in a university campus using rfid technology. In *2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII)*, pages 1–6. IEEE, 2017.

M. Kaushik and S. Kaushik. An overview of technical aspect for wireless fidelity (wi-fi-wireless network technology). *International Journal of Advances in Electrical and Electronics Engineering (IJAEEE, ISSN: 2319-1112)*, 1(02):173–178, 2012.

R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi. An overview of iot sensor data processing, fusion, and analysis techniques. *Sensors*, 20(21):6076, 2020.

A. Kulkarni, S. Sathe, et al. Healthcare applications of the internet of things: A review. *International Journal of Computer Science and Information Technologies*, 5(5):6229–6232, 2014.

J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni. A comparative evaluation of amqp and mqtt protocols over unstable and mobile networks. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pages 931–936. IEEE, 2015.

S. Madakam, R. Ramaswamy, and S. Tripathi. Internet of things (iot): A literature review. *Journal of Computer and Communications*, 3(5): 164–173, 2015.

E. E. Millán-Rojas, J. N. Pérez-Castillo, et al. Servicio amazon web services de clasificación primaria de imágenes de fuentes hídricas del piedemonte amazónico que usan redes neuronales-service amazon web services primary classification images of the amazon piedmont water sources using neural networks. *Revista científica*, 19(2):104–117, 2014.

K. N. Mishra, S. Kumar, and N. R. Patel. Survey on internet of things and its application in agriculture. In *Journal of Physics: Conference Series*, volume 1714, page 012025. IOP Publishing, 2021.

R. I. Moscoso Riera. La domótica y su impacto en la eficiencia energética en una vivienda de clase media de la ciudad de guayaquil. Master's thesis, Guayaquil: ULVR, 2023., 2023.

G. P. Naik and A. U. Bapat. A brief comparative analysis on application layer protocols of internet of things: Mqtt, coap, amqp and http. *Int. J. Comput. Sci. Mob. Comput*, 9(9):135–141, 2020.

N. Naik. Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http. In *2017 IEEE international systems engineering symposium (ISSE)*, pages 1–7. IEEE, 2017.

P. Neumann, J. Montavont, and T. Noel. Indoor deployment of low-power wide area networks (lpwan): A lorawan case study. In *2016 IEEE 12th international conference on wireless and mobile computing, networking and communications (WiMob)*, pages 1–8. IEEE, 2016.

C. A. Nwabueze and S. Akaneme. Wireless fidelity (wi-fi) broadband network technology: an overview with other broadband wireless networks. *Nigerian Journal of Technology*, 28(1):71–78, 2009.

P. Primicia. Expertos de la onu analizarán la crisis de inseguridad en ecuador, 2023. URL https://www.primicias.ec/noticias/seguridad/expertos-crisis-inseguridad-ecuador-propuestas/#:~:text=El%20%C3%ADndice%20lleg%C3%B3%20a%2047,del%20mundo%2C%20seg%C3%BAn%20el%20Observatorio.

L. G. C. Ramírez, G. S. A. Jiménez, and J. M. Carreño. *Sensores y actuadores*. Grupo Editorial Patria, 2014.

C. M. Ramya, M. Shanmugaraj, and R. Prabakaran. Study on zigbee technology. In *2011 3rd international conference on electronics computer technology*, volume 6, pages 297–301. IEEE, 2011.

V. M. B. Sánchez. Internet de las cosas-horizonte 2050. *bie3: Boletín IEEE*, (11):956–969, 2018.

A. Semle. Protocolos iiot para considerar. *Aadeca Revista*, 34, 2016.

J. Sengupta, S. Ruj, and S. D. Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of network and computer applications*, 149:102481, 2020.

M. R. N. Toledo, W. F. M. Vélez, and V. Y. Ortiz. Sistema de monitoreo delicuencial en viviendas basado en internet de las cosas. *3c Tecnología: glosas de innovación aplicadas a la pyme*, 8(3):24–43, 2019.

N. Q. Uy and V. H. Nam. A comparison of amqp and mqtt protocols for internet of things. In *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, pages 292–297. IEEE, 2019.

S. Vongsingthong and S. Smanchat. Internet of things: a review of applications and technologies. *Suranaree Journal of Science and Technology*, 21(4):359–374, 2014.