Diseño de un sistema de monitoreo y vigilancia de intrusos para residencia familiar basado en dispositivos IoT

Pedro Nel Torres Castillo

Asesor

Fausto Miguel Castro Caicedo

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Redes de Nueva Generación

2026

Nota de Aceptación

_____

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2026

Resumen

El hurto a la propiedad es una problemática global, y también frecuente en Colombia, donde Bogotá registró más de 3.428 casos de enero a julio de 2025. El factor de oportunidad sigue siendo una de las principales causas, especialmente en robos no planificados. En estos escenarios, la evolución tecnológica y el uso de dispositivos IoT podrían ofrecer soluciones eficientes y accesibles frente a los sistemas tradicionales de seguridad.

El proyecto tiene como objetivo principal diseñar un sistema de monitoreo y detección de intrusos basado en IoT para una residencia familiar, utilizando redes de nueva generación (NGN), que permita supervisión remota, detección en tiempo real y alertas automáticas.

El proyecto contempla diferentes etapas en su desarrollo, como el análisis del estado del arte de los sistemas de monitoreo y vigilancia de intrusos basados en IoT, la identificación y selección de componentes tecnológicos más adecuados y el diseño de la arquitectura conceptual del sistema incluyendo los criterios que permitan su viabilidad en entornos residenciales, mediante el uso de redes NGN.

La propuesta contribuirá a la adopción de diversas tecnologías aplicables a la seguridad residencial, beneficiando a los hogares con una solución accesible y replicable, y fomentando el uso de NGN e IoT en contextos domésticos.

Se espera que el diseño del sistema propuesto pueda contribuir a una futura implementación que a su vez, incida directamente en la reducción de los casos de hurto a residencias familiares.

Palabras clave**:** IoT, detección de intrusos, entorno residencial, NGN.

Abstract

Property theft is a global issue and also a frequent occurrence in Colombia, where Bogotá recorded more than 3,428 cases between January and July 2025. The opportunity factor remains one of the main causes, especially in unplanned robberies. In these scenarios, technological evolution and the use of IoT devices could offer efficient and accessible solutions compared to traditional security systems.

The main objective of this project is to design an IoT-based monitoring and intrusion detection system for a family residence, using Next Generation Networks (NGN), enabling remote supervision, real-time detection, and automatic alerts.

The project includes different development stages, such as the analysis of the state of the art of IoT-based monitoring and intrusion surveillance systems, the identification and selection of the most suitable technological components, and the design of the system's conceptual architecture, including the criteria that ensure its feasibility in residential environments through the use of NGN.

This proposal will contribute to the adoption of various technologies applicable to residential security, providing households with an accessible and replicable solution, and promoting the use of NGN and IoT in domestic contexts.

It is expected that the design of the proposed system may contribute to a future implementation that, in turn, directly helps reduce cases of theft in family residences.

Keywords: IoT, intrusion detection, residential environment, NGN.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Introducción

La evolución de las redes de nueva generación (NGN) ha facilitado el desarrollo de aplicaciones para el monitoreo de variables relacionadas con la seguridad en ámbitos residenciales, en las que se emplea el internet de las cosas (IoT) como columna vertebral (Castaño-Gómez et al., 2021). Estas tecnologías permiten que los dispositivos puedan comunicarse entre sí, en tiempo real y generar notificaciones automáticas ante la detección de eventos que representen amenazas de intrusión en el hogar (Balakrishnan, Ph.D. & Murugan V, 2024).

En este contexto, en el presente proyecto se plantea el diseño de un sistema de monitoreo y detección de intrusos basado en tecnología IoT, haciendo uso de infraestructura NGN, que pueda ser implementado en el ámbito doméstico y en el cual se combinen las capacidades de ambas tecnologías.

En el diseño que consideran elementos clave como Gateway, sensores y aplicaciones que constituyen un ecosistema IoT integrado. Asimismo, considera el uso de herramientas de seguridad en red, incluyendo redes privadas de seguridad (VPN) que contribuyen a garantizar la confidencialidad e integralidad de los datos transmitidos entre dispositivos.

El sistema propuesto busca sentar las bases para futuras implementaciones en las que se aproveche el potencial de las tecnologías IoT.

Planteamiento del Problema

De acuerdo con (World Population Review, 2025), Costa Rica es uno de los países con la tasa de robos más alta del mundo, con 776 casos por cada 100.000 habitantes. Otros países con la tasa de robos más alta fueron Suecia, Luxemburgo y Australia. En Colombia, el hurto a la propiedad no deja de ser una preocupación y se ha convertido en uno de los delitos más recurrentes en los últimos años. Según (Policia Nacional de Colombia, 2025) tan solo desde el día primero de enero hasta el 31 de julio de 2025 se han cometido alrededor de 14.434 de estos delitos en el territorio nacional, siendo la ciudad de Bogotá una de las más afectadas entre las ciudades principales, con más de 3428 de estos delitos reportados.

Tal como se afirma en (Policia Nacional de Colombia, 2025), se evidencia un incremento del delito en la ciudad de Bogotá en comparación con el 2024, pasando de 2109 eventos reportados durante todo el 2024 a 3428 eventos reportados de enero a julio de 2025. Las cifras de Bogotá triplican ampliamente las cifras de la segunda ciudad más importante de Colombia, Medellín, en la que se reportaron 821 delitos de enero a julio de 2025.

Si bien, las causas más probables de este delito, podrían ser de orden educativo, económico, social y cultural, otra condición corresponde al factor de oportunidad que encuentran los practicantes de estas actividades. Si bien, el 88% de las invasiones de vivienda no son planificadas, el uso de sistemas de seguridad más eficaces podría ayudar a reducir este delito en los próximos años, afirma (Pupkevicius, 2024).

¿Cómo puede implementarse un sistema de monitoreo y vigilancia basado dispositivos IoT para detectar y prevenir intrusiones en residencias familiares y que sea un mecanismo efectivo para mejorar la seguridad y reducir el riesgo de hurto a la propiedad?

Justificación

Los problemas de seguridad como hurto a la propiedad e invasión ilegal han estado presentes en las principales ciudades de Colombia y han sido frecuentes durante los últimos años. La percepción de inseguridad ha aumentado entre los ciudadanos, quienes no se sienten seguros incluso en sus propios hogares (RTVC Noticias, 2026).

Si bien, los sistemas de seguridad como los Circuitos Cerrados de Televisión proveen mecanismos para monitorear la propiedad privada, su implementación y supervisión puede llegar a ser costosa (G4S Colombia, 2025) .

La evolución tecnológica en los últimos años ha permitido el desarrollo de redes de comunicación de nueva generación (NGN) y la expansión del Internet de las Cosas (IoT), que ofrecen nuevas oportunidades para la implementación de sistemas de monitoreo y detección de intrusos más eficientes, accesibles y personalizables (Rifa Pous et al., 2019). Estas tecnologías permiten la creación de redes inteligentes de dispositivos conectados que pueden detectar, monitorear y reaccionar ante situaciones de riesgo en tiempo real, brindando a los propietarios la capacidad de supervisar sus hogares de manera remota y recibir alertas instantáneas en caso de intrusiones.

El proyecto propone el diseño de un sistema de monitoreo y detección de intrusos basado en tecnología IoT para una residencia familiar. Este sistema permitirá integrar múltiples sensores conectados a una red que, mediante algoritmos de detección y procesamiento de datos, pueda identificar eventos sospechosos, generar alertas automáticas y activar medidas de seguridad en tiempo real.

Este proyecto no solo responde a una necesidad urgente de mejorar la seguridad residencial, sino que también representa una oportunidad para explorar el potencial de las redes

NGN en la integración de soluciones IoT. La implementación de este tipo de sistemas puede contribuir a la reducción de incidentes de hurto, ofrecer mayor tranquilidad a los residentes y, a largo plazo, fomentar la adopción de estas tecnologías en el ámbito doméstico.

La relevancia de este proyecto radica en su capacidad para proporcionar una solución tecnológica, que combine el uso de las redes NGN con el potencial de los dispositivos IoT para mejorar la seguridad residencial.

Objetivos

Objetivo General

Diseñar un sistema de monitoreo y detección de intrusos basado en tecnología IoT para una residencia familiar, utilizando redes de nueva generación (NGN) que permita la supervisión remota, detección en tiempo real y alertas automáticas para mejorar la seguridad y prevenir el hurto.

Objetivos Específicos

Analizar el estado del arte de los sistemas de monitoreo y vigilancia de intrusos basados en tecnologías IoT, con énfasis en su aplicación en entornos residenciales y su integración con redes de próxima generación (NGN).

Identificar y seleccionar los componentes tecnológicos más adecuados (sensores, protocolos de comunicación, plataformas de gestión, entre otros) para el diseño de un sistema de monitoreo orientado a la seguridad de residencias familiares.

Diseñar una arquitectura conceptual del sistema de monitoreo y vigilancia de intrusos, especificando su estructura funcional, los flujos de comunicación, y los criterios técnicos que permitan su viabilidad en entornos residenciales conectados a redes NGN.

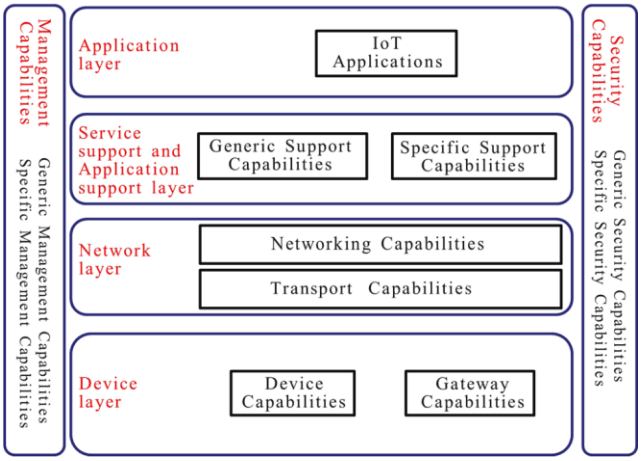
Marco Conceptual y Teórico

Internet de las Cosas (IoT)

(International Telecommunication Union, 2012) Define el Internet de las cosas (IoT por sus siglas en ingles Internet of Things), como una "Una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de objetos (físicos y virtuales) basados en tecnologías de la información y la comunicación interoperables existentes y en evolución" (p. 1). Adicionalmente establece un modelo de referencia similar al modelo TCP/IP, compuesto por cuatro capas, que permite la interacción entre dispositivos y aplicaciones.

Figura 1

Modelo de Referencia para Aplicaciones IoT



Nota. En el modelo de referencia, cada capa incluye capacidades que además de facilitar la comunicación con las capas adyacentes, contempla características específicas de seguridad y administración. Tomado de *ITU-T Y2060 Overview of the Internet of thing* (p.7), por (International Telecommunication Union, 2012).

En la capa de aplicación se encuentran las aplicaciones IoT que permiten al usuario interactuar con los dispositivos. En las capas de soporte de servicio y soporte de aplicación se

encuentra la infraestructura que permite el almacenamiento, procesamiento de datos o satisfacer las necesidades propias de las aplicaciones. En la capa de red, se proporcionan funciones de control de acceso y transporte de recursos, administración de la movilidad o la autenticación, autorización y contabilidad (AAA) y la infraestructura necesaria para proveer el transporte de información entre dispositivos y aplicaciones. En la capa de dispositivos se encuentran los sensores y actuadores que pueden interactuar directamente o no con la capa de red y los equipos que brindan las capacidades de puerta de enlace (Gateway).

Dispositivos

Sensores

Para el monitoreo de intrusos en espacios residenciales, existen varios tipos de tecnologías dentro de las cuales se destacan los siguientes:

Interruptores Magnéticos. Conformados por dos elementos independientes (un imán y un switch magnético), generan una señal discreta cuando son separados. (Garcia, 2006)

Figura 2

Interruptor Magnético

Nota. El switch magnético (en la imagen corresponde al componente con el cable) se instala sobre el marco de la puerta o ventana y el imán sobre la hoja de la puerta o la ventana. Tomado de *https://honeywell.scene7.com/is/image/Honeywell65/hbt-security-943wg-wh-miniature-sized-magnetic-primaryimage*, por Honeywell Building Automation (s.f).

Sensores Infrarrojos Pasivos. Conocidos como PIR (Por sus siglas en inglés Passive Infrared Sensor), son capaces de detectar la presencia de un objeto cuando su campo de visión es bloqueado por un objeto que tiene una temperatura diferente a la del fondo que está siendo sensado. (Garcia, 2006)

Figura 3

Sensor Infrarrojo Pasivo (PIR)

Nota. El sensor de la imagen usualmente se instala en las esquinas de los espacios. Existen modelos que se instalan sobre la superficie de los techos ofreciendo mayor cobertura. Tomado de *https://honeywell.scene7.com/is/image/Honeywell65/hbt-security-is312b-compact-pir-motion-sensor-primaryimage,* por Honeywell Building Automation (s.f).

Cámaras (Cámaras de Video). Las cámaras de video realizan la captura de imágenes y video por medio de un sensor que recibe la luz reflejada por los objetos y la convierte en una señal eléctrica que es almacenada. Estos dispositivos pueden utilizar analíticas de video o IA para detectar eventos de intrusión.

Figura 4

Cámara de Video

Nota. A diferencia de los sensores mencionados anteriormente, estos equipos cuentan con la posibilidad de manejar protocolos IP, TCP, HTTP, lo que les permite integrarse directamente a redes NGN. Tomado de *https://honeywell.scene7.com/is/image/Honeywell65/HBT-SEC-35S-HC35WBxR2,* por Honeywell Building Automation (s.f).

Gateway

Dentro de las soluciones más versátiles y de bajo costo, se destaca la Raspberry Pi, que básicamente es un equipo de cómputo, con procesador, memoria RAM, interfaces para conexión USB, HDMI, Ethernet. Wi-Fi, entre otras. Además de contar con la capacidad para integrar otros periféricos como sensores y actuadores mediante sus entradas y salidas de propósito general (GPIO).

Figura 5

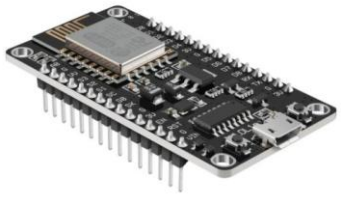
Raspberry Pi

Nota. Tomado de *https://assets.raspberrypi.com/static/8f6eca535dbb23a21eb41a748050e3a0/b0461/16gb.png,* por Raspberry Pi (s.f).

De manera similar, la placa de desarrollo de código abierto NodeMCU ESP8266, además de contar con memorias flash y RAM y una interfaz que permite conectividad Wi-Fi, dispone al igual que la Raspberry Pi de entradas y salidas de propósito general (GPIO) para integrar periféricos como sensores y actuadores.

Figura 6

Placa de Desarrollo Basada en ESP8266



Nota. Tomado de *https://www.steren.com.co/media/catalog/product/cache/0236bbabe616ddcff749ccbc14f38bf2/image/20764b39a/placa-de-desarrollo-nodemcu-esp8266.jpg,* por NodeMCU (s.f).

Por otro lado existen otras soluciones con capacidad para integrar periféricos por medio de protocolos como Zigbee 3.0 como es el caso del Gateway Tuya, que adicionalmente tiene cuenta con interfaces para conexión vía Ethernet y Wi-Fi.

Figura 7

Gateway Tuya

Nota. Tomado de *https://seapromotionstatic.cdn5th.com/static/275611206470062080.png,* por Tuya Inc.(s.f).

Red

Las redes LAN basadas en el estándar IEEE 802 como Ethernet (IEEE 802.3) y Wi-Fi (IEEE 802.11n) suelen ser empleadas en IoT, para el intercambio de datos entre la capa de dispositivos y las capas de soporte de servicio y de aplicaciones. Otras redes son utilizadas en aplicaciones específicas en las que se requiere una baja transferencia de datos como Bluetooth (IEEE 802.15.1).

Las redes móviles basadas en estándares GSM/GPRS/CDMA/EDGE/UMTS/LTE incluso redes 5G son empleadas en la capa de aplicaciones al permitir a los usuarios acceder a los servicios IoT por medio de teléfonos inteligentes.

Soporte de Servicio y Soporte de Aplicación

En la capa de soporte de servicio y soporte de aplicación existen dos modelos (Cirani et al., 2019):

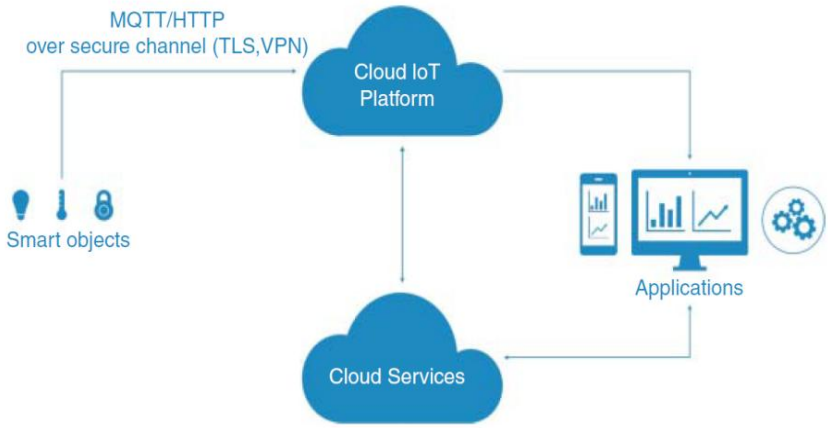
Servicios Basados en la Nube

En un principio, el enfoque de IoT fue conectar dispositivos a internet, bajo la premisa que la nube proporcionaría el almacenamiento de los datos y a través de una interfaz basada en HTTP, los clientes pudieran acceder a aplicaciones (mediante el uso de navegadores o aplicaciones de telefonía móvil), como se muestra en la figura 8.

Gran parte de los proveedores de servicios basados en la nube como Amazon (AWS), Microsoft (Azure), entre otros, han implementado estas soluciones para facilitar la implementación de aplicaciones.

Figura 8

Arquitectura IoT Basada en Servicios en la Nube



Nota. Tomado de *Internet of Things Architectures, Protocols and Standards (p. 94),* por (Cirani et al., 2019).

Sistemas de Mensajería

Estos sistemas emplean mensajería o middleware, los cuales ofrecen una comunicación asíncrona, y en los que se implementa al menos dos de los siguientes enfoques:

Colas de mensajes: El remitente envía un mensaje a una cola en un servidor, donde se almacena y permanece. El mensaje no se borra inmediatamente, sino que se guarda en memoria hasta que un consumidor lo recibe. Solo una vez entregado, el mensaje se elimina de la cola. Este patrón implementa la comunicación asincrónica punto a punto, con total independencia entre el remitente y el consumidor.

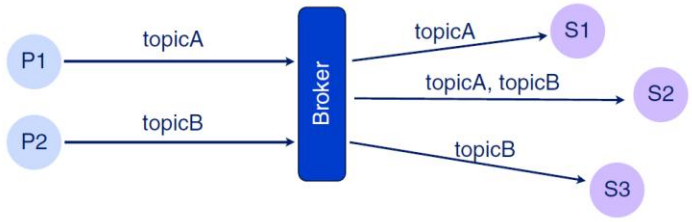
Publicación / Suscripción (Publish/Subscribe): En este enfoque, los publicadores envían mensajes con un "topic[1]" y datos en formato de bytes al servidor. Los clientes (suscriptores) se suscriben al "topic" para recibir una copia del mensaje, lo que implica que puedan existir

[1] El topic es una cadena de texto UTF-8 que se emplea en MQTT como etiqueta para los mensajes y facilita el intercambio de datos entre publicadores y clientes (suscriptores). (Amazon AWS, 2025)

múltiples suscriptores. La separación entre publicadores y suscriptores es posible gracias a nodos intermediarios, llamados broker. Ver figura 9.

Figura 9

Modelo de Mensajería Basado en Publicación / Suscripción (Publish/Subscribe)



Nota. En este modelo, el broker cumple un rol fundamental, al ser el responsable de reenviar los mensajes a los suscriptores. Tomado de *Internet of Things Architectures, Protocols and Standards (p. 99)*, por (Cirani et al., 2019).

Plataformas de Gestión y Entornos de Desarrollo

En el ecosistema IoT intervienen algunos elementos que además de facilitar la conexión entre dispositivos y aplicaciones, son útiles para gestionar el almacenamiento y distribución de la información y el desarrollo de aplicaciones.

(Rajani & Malik, 2025) Consideran, que estos elementos puede clasificarse en:

Plataformas IoT. Las plataformas IoT comúnmente se basan en servicios en la nube que centralizan la conectividad de dispositivos y la integración de aplicaciones. Estas plataformas ofrecen los entornos necesarios para la conexión de dispositivos, seguridad, análisis e interoperabilidad con otros servicios. En esta categoría se destacan Amazon (AWS), Microsoft (Azure), Google IoT, IBM Watson IoT, entre otros.

Entornos de Desarrollo IoT. Estos entornos cuentan con una colección de herramientas y librerías que facilitan el desarrollo de aplicaciones, la interconexión de dispositivos,

almacenamiento y visualización. En esta categoría se destacan alternativas de código abierto como Thingsboard, Blynk, Thinger, Node-Red, entre otros.

Middleware. El middleware es un programa informático que permite uno o varios tipos de comunicación o conectividad entre aplicaciones o componentes de una red distribuida, creando esencialmente un "pegamento de software" que une sistemas diferentes (IBM Technology company, 2025). El middleware provee soluciones de integración de datos, procesamiento y análisis implementando políticas de seguridad.

Protocolos

Los protocolos de comunicación IoT constituyen la columna vertebral del intercambio de datos entre dispositivos.

MQTT. Es un protocolo utilizado en escenarios donde deben producirse comunicaciones bidireccionales entre puntos finales, en redes con recursos limitados. Es la base de modelos de Publicación / Suscripción y emplean “topic” en los mensajes para el intercambio de información.

XMPP. El Protocolo Extensible de Mensajería y Presencia (XMPP), se basa en el intercambio de información entre cliente y servidor. Permite el intercambio de mensajes, chats de grupo, audio y video con servicios de mensajería y correo electrónico compatibles.

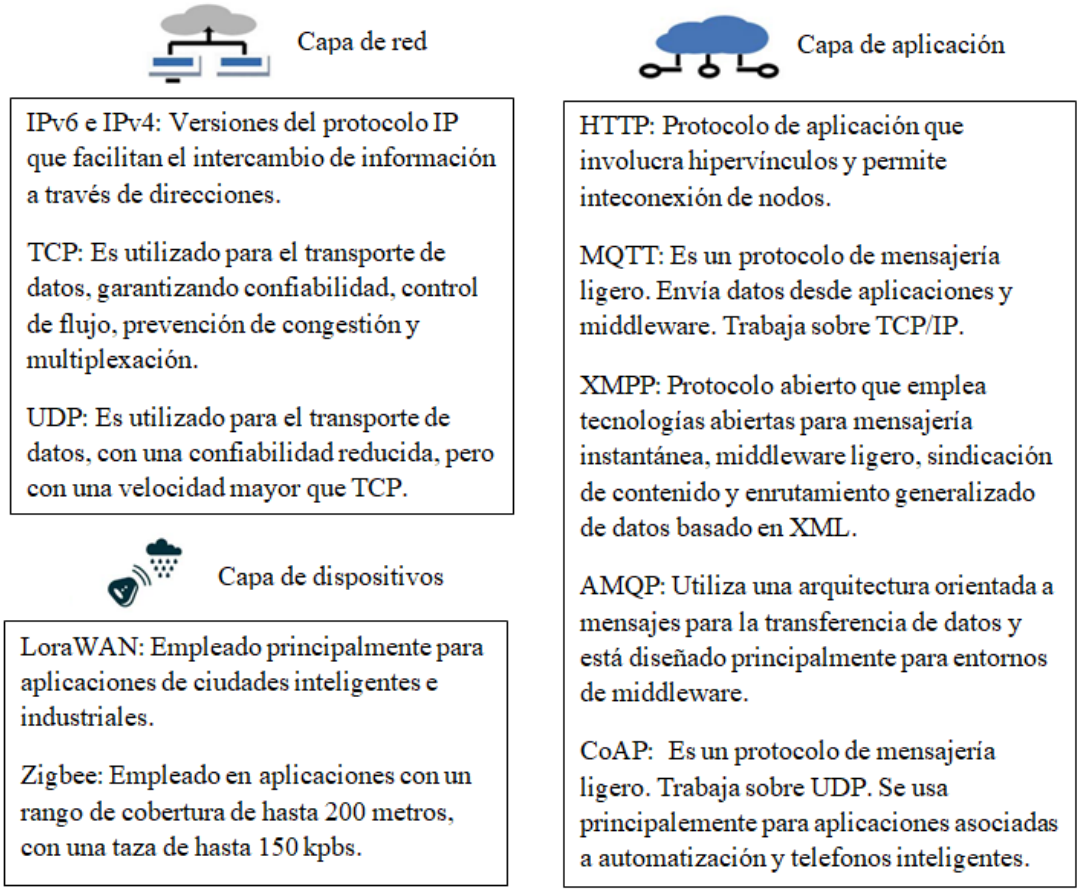
AMQP. El Protocolo de Cola de Mensajes Avanzado (AMQP) es un protocolo orientado a mensajes, que puede ser considerado como un complemento asíncrono de HTTP.

CoAP. El Protocolo de Aplicación Restringida (CoAP) fue diseñado para replicar la experiencia de HTTP, caracterizándose principalemente por manejar paquetes pequeños, bajo consumo de ancho de banda y bajo consumo eléctrico.

En la figura 10 se resumen los protocolos más empleados en aplicaciones IoT.

Figura 10

Protocolos Empleados en Aplicaciones IoT



Nota. Adaptado de *Internet of Things A Hardware Development Perspective (c. 4, p.2),* por (Sharma, 2022)

Adicionalmente existen protocolos enfocados a priorizar la conexión segura entre los dispositivos que hacen parte de IoT, dentro de los cuales se destacan:

SSL. La capa de socket seguro (Secure Sockets Layer) es un protocolo que permite la interconexión segura entre servidores y clientes haciendo uso de comunicaciones cifradas que aseguran la integridad y privacidad de la información transmitida a través de la red. Hace uso de certificados digitales a través de los cuales se verifica la identidad y autenticidad de los

servidores, y emplea llaves públicas y llaves simétricas aleatorias que se comparten entre el servidor y el cliente, permitiendo la encriptación y desencriptación de los mensajes. SSL hace uso de códigos de autenticación de mensaje (MAC - Message Authentication Code) para autenticar el origen y la naturaleza del mensaje.

TLS. El protocolo de Seguridad de la Capa de Transporte (Transport Layer Security) es la versión mejorada de SSL, que emplea algoritmos criptográficos mas seguros y avanzados. TLS hace uso de códigos de autenticación de mensajes con Hash (HMAC Hash-based Message Authentication Code) los cuales utilizan una combinación de una función Hash criptográfica y una clave secreta para la autenticación de mensajes.

Tecnologías VPN

(Cybellium Ltd., 2023) Define una Red Privada Virtual (VPN) como una tecnología que permite que una red privada pueda ser extendida sobre una red pública como internet, creando un "túnel" en el que los datos son encriptados. A Continuación se describen las principales tecnologías VPN.

Tabla 1

Tipos de Protocolos y Tecnologías VPN

Protocolo	Características
PPTP (Point-to-Point Tunneling Protocol)	Descripción: Provee niveles básicos de seguridad y es uno de los más antiguos. Encriptación: A menudo usa cifrado MPPE de 128 bits. Ventajas: Fácil de implementar y ampliamente soportado. Desventajas: Considerado el menos seguro.

Protocolo	Características
L2TP (Layer 2 Tunneling Protocol)	Descripción: Usa un túnel entre dos conexiones L2TP. Encriptación: A menudo usa IPsec para encriptación, empleando AES o 3DES. Ventajas: Más seguro que PPTP. Desventajas: Más lento debido a doble encapsulación.
IPSec (IP Security)	Descripción: Emplea un conjunto de protocolos que encriptan la capa IP. Encriptación: A menudo usa AES o 3DES. Ventajas: Seguro, configurable, usado en aplicaciones “Site-to-Side”. Desventajas: Configuración compleja. Puede ser lento.
Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs	Descripción: Utiliza la misma tecnología que los sitios Web seguros con varias longitudes de clave. Encriptación: A menudo usa AES. Ventajas: Fácil de usar. No es necesario ningún software de cliente especial. Desventajas: Limitado a aplicaciones Web, menos control sobre la seguridad del cliente.
Internet Key Exchange version 2 (IKEv2)	Descripción: Protocolo de tunelización. Encriptación: A menudo usa AES. Ventajas: Ideal para dispositivos móviles, reconexión rápida. Desventajas: No es ampliamente soportado, puede ser bloqueado por Firewalls.

Protocolo	Características
WireGuard VPN	Descripción: Protocolo nuevo, conocido por su simplicidad y velocidad. Emplea configuraciones tipo *Hub and Spoke* (en las que se emplea un Gateway que gestiona la comunicación entre clientes y servidores) y *Mesh* (En las que no se cuenta con un Gateway central y todos los nodos/clientes y servidores se conectan directamente entre si). Encriptación: Utiliza ChaCha20 y Poly1305 para autenticación. Ventajas: Rápido, eficiente y utiliza técnicas criptográficas modernas. Desventajas: Podría ser costoso, al ser relativamente nuevo.

Nota. La información de esta tabla se encuentra basada en (Cybellium Ltd., 2023)

Redes de Nueva Generación

De acuerdo con (International Telecommunication Union, 2004), La red de nueva generación (NGN sus siglas en inglés Next Generation Network), es un "Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta en la movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios."

(Janevski, 2016), Describe los principales componentes de las redes NGN, para el acceso y transporte, según se indica a continuación:

Estratos de Transporte y Servicios de NGN

La separación de los servicios del transporte, que permiten que se ofrezcan por separado y se desarrollen de forma independiente, es una característica de las redes NGN.

El estrato de servicio ofrece las funciones que permiten la transferencia de información relacionada con los servicios como voz, video, datos y multimedia administrando los recursos de servicio y los servicios de red con el objetivo de habilitar aplicaciones y servicios de usuario.

El estrato de transporte se encarga de las funciones que permiten el envío y recepción de los datos del usuario a través de la red. En la red, el estrato de transporte proporciona funciones que controlan y gestionan los recursos de transporte para la transmisión de datos de extremo a extremo.

Acceso en NGN

Respecto a las tecnologías de acceso de banda ancha a Internet, se pueden agrupar en los dos tipos principales siguientes:

Acceso a Internet de Banda Ancha Fijo. Incluye todas las redes de banda ancha que utilizan ya sea cooperación como redes de par trenzado o cable y fibra incluyendo redes ópticas pasivas y activas.

Acceso a Internet de Banda Ancha Móvil e Inalámbrico. Incluye el acceso de banda ancha a través de redes móviles e inalámbricas de banda ancha, que incluyen redes móviles 3G, 4G y 5G y Wi-Fi como WLAN.

Metodología

El presente proyecto se desarrolla bajo un enfoque de proyecto aplicado y está estructurado en tres fases.

Fase 1. Investigación

En esta fase se analiza el estado del arte de los sistemas de monitoreo y vigilancia de intrusos basado en tecnologías IoT, con el propósito de identificar las tecnologías, arquitecturas y componentes necesarios para el desarrollo del diseño del sistema. Asimismo, se lleva a cabo la evaluación y selección de los componentes tecnológicos más adecuados, considerando criterios de funcionalidad, compatibilidad y viabilidad de implementación.

Métodos: Se realiza una revisión del estado del arte relacionado con la detección de intrusos en entornos residenciales. Adicionalmente, se lleva a cabo un análisis comparativo de tecnologías con el fin de seleccionar aquellas que resulten más apropiadas para el sistema de monitoreo y vigilancia propuesto.

Instrumentos: Para el desarrollo de esta fase se emplean matrices comparativas presentadas en forma de tablas. Estas matrices permiten analizar diferentes soluciones de sistemas de seguridad residencial basados en IoT identificadas durante la revisión del estado del arte. Asimismo, se utilizan matrices de evaluación de los componentes tecnológicos considerados para el diseño del sistema de monitoreo, con el fin de facilitar la comparación de sus características y su selección.

Fase 2. Diseño de la Arquitectura del Sistema de Monitoreo y Vigilancia de Intrusos

En esta fase se desarrolla el diseño de la arquitectura del sistema de monitoreo y vigilancia de intrusos, integrando los elementos tecnológicos seleccionados en la fase de investigación. Se define la estructura funcional del sistema, la interacción entre sus componentes

y los criterios técnicos necesarios para garantizar su viabilidad y adecuada operación en entornos residenciales.

Métodos: Se realiza el diseño conceptual de la arquitectura IoT del sistema, estableciendo la interacción entre los dispositivos de captura de información, la infraestructura de red, las plataformas de procesamiento, los servicios de comunicación y las aplicaciones de usuario que permiten la supervisión y gestión del sistema de monitoreo.

Instrumentos: Como instrumento de apoyo para el desarrollo de esta fase se elabora un diagrama de arquitectura conceptual del sistema, el cual representa la organización estructural y funcional de los diferentes componentes y permite visualizar la forma en que estos interactúan dentro de la solución propuesta.

Fase 3. Validación del Diseño Propuesto

En esta fase se realiza la validación del diseño de la arquitectura del sistema de monitoreo y vigilancia de intrusos, con el fin de comprobar su viabilidad técnica y operativa. Para ello, se desarrolla una implementación básica del sistema mediante un prototipo funcional que permita evaluar el comportamiento de los componentes, su integración y capacidad de respuesta ante eventos de intrusión.

Métodos: La validación se realiza mediante la implementación de un prototipo funcional del sistema, a través del cual se ejecutan pruebas orientadas a verificar la comunicación entre los dispositivos, el procesamiento de eventos y la generación de alertas automáticas ante posibles intrusiones.

Instrumentos: Para el desarrollo de esta fase se utilizan diferentes recursos tecnológicos que permiten la implementación y evaluación del sistema. Entre estos se incluyen dispositivos físicos de prueba, como el gateway y sensores simulados o reales, una plataforma de desarrollo

IoT para la configuración de flujos de procesamiento, un broker de mensajería para la gestión de eventos, aplicaciones cliente para el monitoreo remoto del sistema, herramientas de configuración y administración, así como mecanismos de simulación de eventos de intrusión que permiten evaluar el comportamiento del sistema ante diferentes escenarios.

Estado del Arte

La seguridad en entornos residenciales es una preocupación que ha derivado en el desarrollo de diversas propuestas académicas orientadas al diseño de sistemas de detección de intrusos.

Sistemas de Seguridad Física Basados en IoT

Algunos trabajos se han enfocado en identificar los elementos más comunes empleados en sistemas de seguridad física basados en IoT como (Castaño-Gómez et al., 2021), los cuales presentan una revisión sobre el estado del arte en la que además de plantear el sistema de seguridad física como un conjunto de subsistemas, en los cuales se encuentra el sistema de detección de intrusos, desarrollan un diagrama general para soluciones de seguridad soportadas en IoT, en la que se emplea un Gateway que gestiona la información proveniente de los diferentes sensores y actuadores hacia las capas superiores.

Propuestas de Monitoreo y Vigilancia de Intrusos Basados en IoT

A continuación se abordarán las diferentes propuestas que han sido tenidas en cuenta durante el desarrollo del proyecto, tomando como base el modelo de referencia indicado en la Figura 1 y considerando que cada una de las propuestas presentadas de manera general se encuentran alineadas a dicho modelo.

Diferentes autores han propuesto implementaciones específicas que evidencian el potencial de soluciones IoT en la vigilancia de entornos residenciales. Por ejemplo, (Mohammad & Radha, 2017) y (AMSV et al., 2024), desarrollaron una aplicación que notifica eventos de intrusión por medio de SMS y correos electrónicos haciendo uso de redes móviles 2G y 2.5G. Los componentes empleados en cada propuesta se encuentran indicados en la Tabla 2.

Tabla 2

Sistemas de Seguridad Residencial IoT Basados en Redes 2G y 2.5G

Propuesta	Capa de dispositivo	Capa de red	Capa de soporte de servicio y soporte de aplicación	Capa de aplicación
An IOT based Solar Integrated Home Security System by using GSM Module and Raspberry pi (Mohammad & Radha, 2017)	Dispositivos: Sensor PIR, cámara USB Gateway: Raspberry Pi	Red GPRS	Servidor SMS Servidor de correo electrónico	SMS Correo electrónico
Integrated IoT-Based Smart Home Security System: Real-Time Hazard Detection and Alerts Using Multi-Sensor Fusion (AMSV et al., 2024)	Dispositivos: Sensor PIR, cámara, detector de gas, detector de fuego y buzzer. Gateway: Arduino UNO	Red GSM / GPRS	Servidor SMS	SMS

Por otro lado, en otros trabajos se emplean redes Wi-Fi y redes móviles 3G o superior, para enlazar las capas de dispositivos con las capas de soporte de servicio, soporte de aplicaciones y con la capa aplicaciones bajo ciertas particularidades.

Es el caso de (Uthman Azlan & Shamian Zainal, 2024), quienes emplean aplicaciones como Blynk para facilitar la interacción del usuario con el sistema de seguridad y su supervisión en tiempo real y de (Ganesan et al., 2024) quienes además, incorporan elementos para monitorear temperatura, nivel de agua, fuego y fugas de gas. De manera similar (Mohammad et al., 2022), incorporan detección de fugas de gas, Firebase como base de datos y una aplicación web desarrollada en 000webhos, la cual es replicada en un teléfono inteligente para la gestión y monitoreo del sistema en tiempo real.

Otros perspectivas incluyen la captura y almacenamiento de imágenes por medio de cámaras, como (Balakrishnan, Ph.D. & Murugan V, 2024), quienes presentan un sistema cuyo objetivo principal es detectar intrusos, capturar sus rostros y almacenar las imágenes en una tarjeta SD, enviándolas además por correo electrónico al propietario. En un enfoque más avanzado, (Sabit, 2025) incorpora técnicas de inteligencia artificial al procesamiento de video y reconocimiento facial con el fin de aumentar la capacidad de detección en sistemas de seguridad basados en IoT. Su diseño, integra cámaras de CCTV, sensores PIR que interactúan con el Gateway, que a su vez permite la transmisión y recepción de datos desde servidores en la nube y su interacción con aplicaciones de teléfonos inteligentes para asistir al usuario en la identificación de niveles de amenaza. En la Tabla 3, se muestran los componentes usados en cada una de las aplicaciones.

Tabla 3

Sistemas de Seguridad Residencial IoT Basados en Redes Wi-Fi

Propuesta	Capa de dispositivo	Capa de red	Capa de soporte de servicio y soporte de aplicación	Capa de aplicación
IoT Based Home Security for Housing Areas. (Mohammad et al., 2022)	Dispositivos: Sensor PIR, detector de gas y buzzer. Gateway: Arduino Uno y módulo Wi-Fi ESP8266	Wi-Fi Red 3G/4G/5G	Base de datos Firebase	Aplicación web en 000webhost, MIT App Inventor (Smartphone)
IoT Based Home Automation and Security System (Ganesan et al., 2024)	Dispositivos: Sensor de nivel ultrasónico, detector de temperatura y humedad relativa, sensor PIR, sensor de fuego y sensor de gas. Gateway: NodeMCU ESP8266	Wi-Fi Red 3G/4G/5G	Blynk Server	Aplicación Blynk

Propuesta	Capa de dispositivo	Capa de red	Capa de soporte de servicio y soporte de aplicación	Capa de aplicación
Smart Anti-Theft Security System Using IOT (Balakrishnan, Ph.D. & Murugan V, 2024)	Dispositivos: Sensor ultrasónico y cámara. Gateway: NodeMCU ESP8266	Wi-Fi	Servidor de correo electrónico	Correo electrónico
Artificial Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications (Sabit, 2025)	Dispositivos: Sensor PIR, cámara (AI-driven video processing (Object Detection and Face Recognition) Gateway: Raspberry Pi 5	Wi-Fi Red 3G/4G/5G	Google Drive database. Servidor de correo electrónico	Correo electrónico, React Native
An IoT Based Home Security System With ESP32, Video Monitoring, and Blynk Integration (Uthman Azlan &	Dispositivos: Sensor PIR, cámara, sensor infrarrojo Gateway: NodeMCU ESP32	Wi-Fi Red 3G/4G/5G	Blynk Server	Aplicación Blynk

Propuesta	Capa de dispositivo	Capa de red	Capa de soporte de servicio y soporte de aplicación	Capa de aplicación
Shamian Zainal, 2024),				

Por último, algunos autores han optado por emplear redes Ethernet y redes móviles 3G o superior, para establecer conexiones entre las capas de dispositivos y las capas de soporte de servicio, soporte de aplicaciones y capa de aplicaciones.

(Anwar & Kishore, 2016) Desarrollan una solución que integra una cerradura electromagnética, la cual permite controlar remotamente la accesibilidad a las puertas e introduce un componente de autenticación para la gestión del acceso, lo que lo diferencia de propuestas centradas únicamente en la detección de intrusiones. Adicionalmente (Asadul Hoque & Davidson, 2019), emplean un servidor web HTTP configurado con NodeJS y con la base de datos MongoDB que permite la interacción con un teléfonos inteligentes para la supervisión del sistema. En la Tabla 4, se muestran los componentes usados en cada una de las aplicaciones.

Tabla 4

Sistemas de Seguridad Residencial IoT Basados en Redes Ethernet

Propuesta	Capa de dispositivo	Capa de red	Capa de soporte de servicio y soporte de aplicación	Capa de aplicación
IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone (Anwar & Kishore, 2016)	Dispositivos: Sensor PIR, cámara, cerradura de puerta electromagnética y altavoz. Gateway: Arduino Uno y módulo Wi-Fi NodeMCU ESP8266	Ethernet Red 3G/4G/5G	Servidores Linux	Aplicación en Smartphone para enviar comandos de terminal de Linux a través de SSH
Design and Implementation of an IoT-Based Smart Home Security System (Asadul Hoque & Davidson, 2019)	Dispositivos: Interruptor magnético. Gateway: Elegoo Mega 2560 board, Par receptor-transmisor de RF y Raspberry Pi 2.	RF, Ethernet, Internet Red 3G/4G/5G	Servidor Web, Base de datos MongoDB	NodeJS, Aplicación en Android

Tendencias y Oportunidades de Mejora

Es muy común la utilización de redes inalámbricas como Wi-Fi y redes móviles de 3G o superior (considerando que redes móviles de generaciones anteriores se encuentran en periodo de obsolescencia) para la integración de dispositivos hacia servicios y aplicaciones, y el uso de dispositivos electrónicos como la Raspberry Pi y el NodeMCU, debido a su flexibilidad para permitir integrar otros elementos como sensores y/o actuadores a internet.

En las capas de soporte y de aplicación se evidencia una marcada tendencia hacia la adopción de plataformas en la nube y servicios móviles para facilitar la gestión de los sistemas de seguridad residencial basados en IoT. Soluciones como Firebase, Blynk, servidores web HTTP o gestores de bases de datos han permitido integrar la captura de datos con aplicaciones móviles, ampliando las capacidades de interacción en tiempo real entre los usuarios y los dispositivos.

Si bien cada una de las propuestas busca aumentar la seguridad en entornos residenciales a través de tecnologías IoT, a excepción de (Anwar & Kishore, 2016), no se consideran mecanismos enfocados a mitigar las vulnerabilidades que pueden presentar las redes en relación a ataques informáticos.

Selección de Componentes Tecnológicos para el Sistema de Monitoreo

A continuación se presentan las principales ventajas y desventajas de los componentes tecnológicos a ser considerados para el diseño del sistema de monitoreo.

Capa de Dispositivos

Gateway

En la Tabla 5, se exponen las principales ventajas y desventajas de los equipos considerados como Gateway.

Tabla 5

Gateways para Aplicaciones IoT

Dispositivo	Ventajas	Desventajas
Raspberry Pi	Potente y versátil (CPU multi-core, RAM ampliable). Soporta múltiples protocolos (Zigbee, Z-Wave, Matter, Thread, etc. con módulos). Permite trabajar en modo local (sin depender de la nube). Compatible con plataformas abiertas (Blynk, Thinger, Node-RED)	Costo mayor que las otras opciones. Requiere configuración inicial y conocimientos técnicos para desarrollo y programación.
NodeMCU ESP8266	Muy económico. Ideal para prototipos educativos y proyectos simples.	Limitado a Wi-Fi (sin Zigbee/Z-Wave nativos). Muy poca memoria y

Dispositivo	Ventajas	Desventajas
	Permite programación en Arduino, Lua o MicroPython.	capacidad de procesamiento. No apto como Gateway robusto.
Gateway Tuya	Bajo costo y fácil configuración (plug & play). Compatible con aplicaciones como Alexa/Google Home.	Cerrado al ecosistema Tuya. Alta dependencia de la nube. Poca escalabilidad y personalización.

Dentro de las opciones consideradas, la Raspberry Pi es más versátil debido a su capacidad para integrarse con entornos de programación como Node-RED y manejar protocolos como MQTT. Si bien el costo puede ser más elevado y se requieren mayores conocimientos en programación a diferencia de las otras dos opciones, esta alternativa posee un hardware más robusto para el manejo de aplicaciones basadas en IoT.

Dispositivos de Detección de Intrusos

En la Tabla 6, se exponen las principales ventajas y desventajas de los dispositivos de detección de intrusos considerados.

Tabla 6

Sensores para Aplicaciones IoT Enfocadas a Detección de Intrusos

Dispositivo	Ventajas	Desventajas
Interruptor Magnético	Económico y de fácil instalación. Muy confiable para detectar aperturas no autorizadas. Bajo consumo de energía.	Solo detecta apertura/cierre, no presencia.
Sensor PIR (Infrarrojo Pasivo)	Detecta movimiento de personas en interiores. Bajo costo y amplia disponibilidad. Consumo eléctrico reducido.	Puede generar falsas alarmas (mascotas, cambios de temperatura). No distingue entre personas autorizadas y extraños.
Cámara de Video (Ethernet o Wi-Fi)	Proporciona verificación visual en tiempo real. Puede integrarse con analítica de video (detección de movimiento, reconocimiento facial). Permite almacenamiento de evidencia.	Mayor costo y consumo eléctrico. Requiere ancho de banda de red.

Por su principio de funcionamiento, los sensores empleados en aplicaciones de detección de intrusos pueden complementarse entre sí, y constituir una solución más eficiente y robusta. Pueden ser instalados en diferentes espacios del entorno doméstico, donde se consideren condiciones de vulnerabilidad, por lo tanto serán considerados en el desarrollo del diseño.

Capa de Red

Si bien, la mayor parte de los usuarios de internet en Colombia cuentan con una conexión móvil, 8,9 millones de conexiones de internet fijo fueron alcanzadas en diciembre de 2023, de las cuales el 89.9% corresponde al entorno residencial según afirma (Comisión de Regulación de Comunicaciones, 2024).

El punto de acceso para las conexiones de internet fijo en los hogares se realiza a través de un modem suministrado por el proveedor de servicios de internet (ISP – Internet Service Provider). Las redes de transporte emplean medios como cable coaxial, fibra óptica y/o radio enlaces (en entornos rurales con limitado acceso a conexiones físicas).

En el diseño se considerará una red LAN basada en Wi-Fi (IEEE 802.11n), teniendo en cuenta que la mayor parte de los modem cuentan con este tipo de conexión y que al ser una tecnología inalámbrica facilita la ubicación de equipos como el Gateway dentro del hogar.

Para la supervisión remota se hará uso de teléfonos inteligentes, conectados a redes móviles.

Capa de Soporte de Servicios y Soporte de Aplicaciones

A continuación se describen las principales ventajas y desventajas asociadas a los modelos de soporte y aplicación IoT:

Tabla 7

Modelos de Soporte y Aplicación IoT

Modelo	Ventajas	Desventajas
Servicios basados en la nube	Fácil de implementar en aplicaciones web y móviles. Compatible con infraestructura cloud tradicional.	Los servicios basados en la nube, pueden involucrar costos de suscripción o licenciamiento. Menor flexibilidad para personalización.
Sistemas de mensajería – Colas de mensajes	Comunicación asíncrona: remitente y receptor independientes en el tiempo. Fiabilidad: el mensaje se conserva en la cola hasta ser entregado. Útil para procesamiento punto a punto.	Generalmente un mensaje va a un solo consumidor (no múltiples receptores). No es tan eficiente para escenarios donde varios dispositivos requieren la misma información.
Sistemas de mensajería – Publicación/Suscripción	Comunicación asíncrona. Un mensaje puede ser recibido por múltiples suscriptores. Escalabilidad: ideal para sistemas distribuidos con muchos nodos.	Requiere un broker que gestione los tópicos. Mayor complejidad inicial que Solicitud / Respuesta

Modelo	Ventajas	Desventajas
	Los dispositivos permanecen desacoplados (publicador no conoce a los suscriptores). Uso de brokers MQTT/AMQP asegura bajo consumo de ancho de banda. Puede ser desarrollado en entornos de código abierto.	

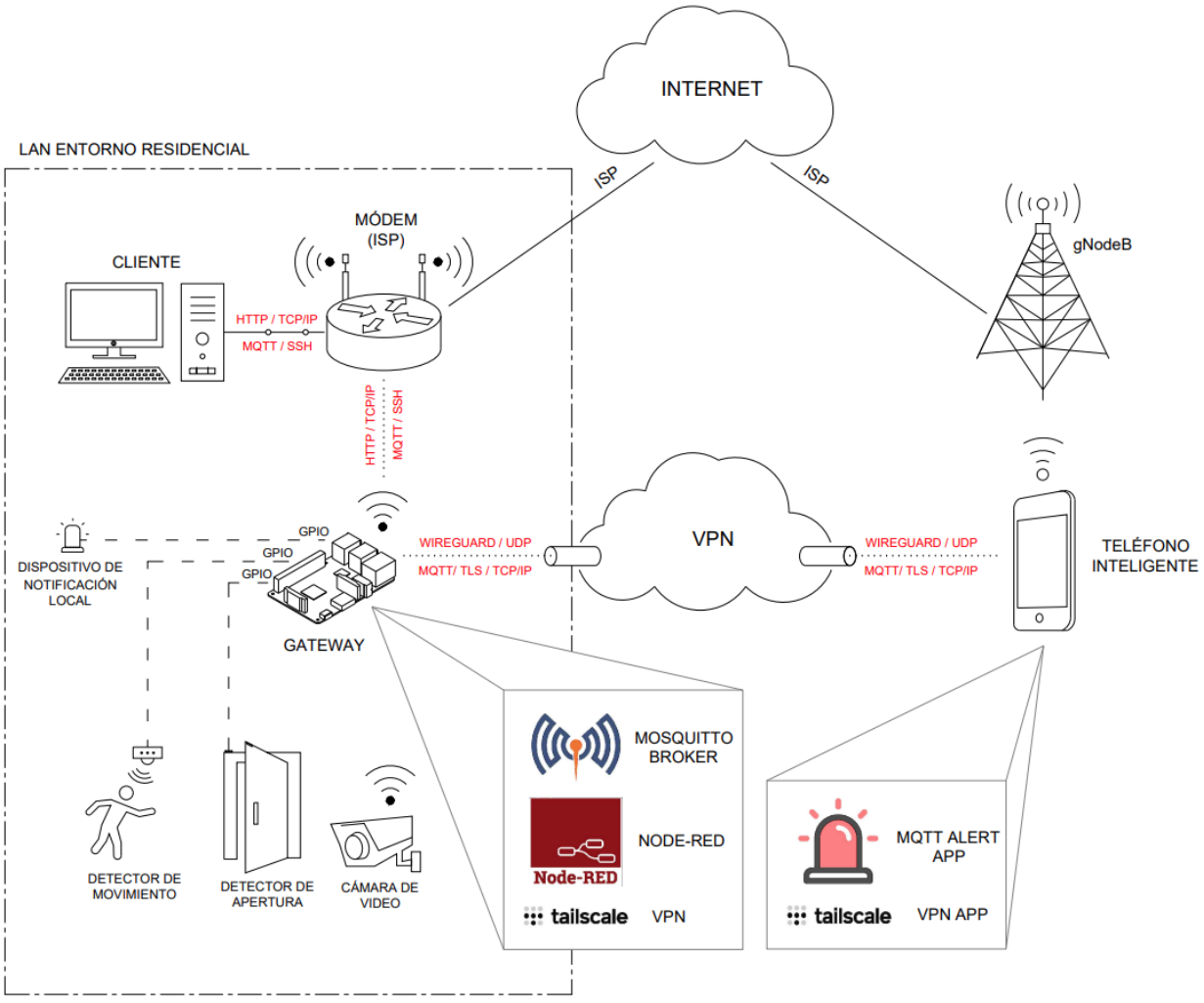
Con base en lo indicado en la tabla 7, el modelo de Publicación/Suscripción resulta ventajoso para la interconexión de sistemas con múltiples nodos (como dispositivos móviles, Gateway, entre otros), ya que demanda un menor consumo de ancho de banda y puede desarrollarse en entornos de código abierto, lo que facilita su implementación. En contraste, el modelo de Solicitud/Respuesta suele estar asociado a plataformas IoT basadas en la nube, cuyo acceso en algunos casos puede estar condicionado a costos de suscripción o licenciamiento y además presenta una menor flexibilidad en la programación y adaptación de aplicaciones.

Arquitectura Propuesta del Sistema de Monitoreo y Vigilancia de Intrusos

Considerando el estado del arte y la selección de componentes tecnológicos para el monitoreo y vigilancia de intrusos, en este capítulo se presenta la arquitectura propuesta para el monitoreo y vigilancia de intrusos basada en dispositivos IoT.

Figura 11

Arquitectura del Sistema de Monitoreo y Detección de Intrusos Basada en Tecnología IoT para Residencia Familiar



Nota. En la figura los protocolos de comunicación empleados se encuentran indicados en color rojo.

Gateway y Sensores

La arquitectura está basada en el modelo de mensajería Publicación / Suscripción y contempla en la capa de dispositivos una Raspberry Pi que cumple la función de puerta de enlace (Gateway) al permitir la integración de los detectores de movimiento, detectores de apertura y dispositivos de notificación local al sistema mediante cableado físico a los GPIO, que para este caso cumplen la función de entradas y/o salidas discretas.

Por otra parte la Raspberry Pi ejerce el rol de servidor de aplicaciones, al permitir la ejecución local de las aplicaciones necesarias para la operación del ecosistema IoT, que incluyen:

Broker. Aplicación necesaria para modelos IoT basados en Publicación / Suscripción. Se emplea como referencia MOSQUITTO BROKER, el cual permite la publicación del "topic" asociado a cada uno de los sensores que hacen parte del sistema.

Entorno de Desarrollo IoT. Se emplea como referencia Node-RED, el cual es una herramienta de programación basada en nodos y flujos, y que incluye una interfaz web que facilita la configuración e implementación. Permite la configuración de los topic y automatizar eventos.

VPN. Teniendo en cuenta que debe establecerse un conexión privada y segura en el Gateway y el teléfono inteligente, bajo la premisa que debe ser posible monitorear el estado de los sensores, aun cuando el usuario no se encuentre en el entorno residencial y por ende, el teléfono móvil no se pueda conectar a la LAN, se hace necesaria la implementación de una Red Privada Virtual (VPN) que permita la comunicación segura entre dispositivos. Se utiliza como referencia Tailscale VPN.

El conjunto de sensores considerados está conformado por un detector de movimiento el cual generará un evento de intrusión ante la presencia de un intruso, un detector de apertura cuya activación derivará en un evento de intrusión en escenarios donde se realice la apertura de la puerta de manera ilegal, un dispositivo de notificación local que tiene como objetivo generar una alarma local ante un evento de intrusión y una cámara de video IP, la cual se conecta directamente al modem del ISP por medio de la red LAN basada en Wi-Fi y tendrá como objetivo generar alarmas ante eventos de intrusión. Los elementos considerados podrán ser instalados en diferentes espacios de la residencia y su ubicación podrá ser definida una vez se realice un análisis de vulnerabilidades o estudio similar previo a la implementación.

Cliente

En la arquitectura se proyecta un computador personal que será empleado como cliente del servidor de aplicaciones de manera temporal para la configuración del sistema y el desarrollo de las aplicaciones necesarias para su operación. Este equipo permitirá acceder al entorno de programación del Gateway y al entorno de desarrollo IoT. Una vez completada la fase de configuración, el sistema operará de manera autónoma.

Modem (ISP)

El Modem es el equipo suministrado por el ISP que tiene como propósito servir como "puente" entre la LAN del entorno residencial e internet. El ISP emplea redes NGN proveer los servicios de conexión a internet fijos, mediante diversos medios de transmisión como cable coaxial, fibra óptica, radio enlaces y/o conexiones satelitales.

Los Modem de conexión fija a internet proveen ciertas ventajas como conexiones confiables, altas velocidades y diversos tipos de conexión de dispositivos con Ethernet y Wi-Fi. Sin embargo, cuando se requiere realizar configuraciones que permitan la implementación de

VPN tradicionales, pueden presentar ciertas desventajas al contar con limitaciones en la administración para redirigir y/o reenviar puertos (Port Forwarding) y para modificar la configuración del NAT. Por esta razón, la utilización de VPNs basadas en WireGuard como Tailscale que permiten la autenticación a través de cuentas de correo y la asignación de IPs privadas dentro su propia red.

Teléfono Inteligente

En la arquitectura propuesta, el teléfono inteligente cuenta principalmente con dos aplicaciones:

Aplicación para Interacción IoT. Esta aplicación le permite al dispositivo, suscribirse y publicar en los "topic". De esta forma es posible realizar el monitoreo de los estado de los sensores del sistema y la activación del dispositivo de notificación local. Se utiliza como referencia MQTT Alert.

VPN. Permite establecer un conexión privada y segura entre el Gateway y el teléfono inteligente.

Flujos de Comunicación

En la arquitectura se emplea una serie de protocolos de comunicación que permiten la comunicación confiable y segura entre los diferentes elementos que componen el sistema, según se indica a continuación:

HTTP. (HyperText Transfer Protocol): Se emplea para el acceso a la configuración y desarrollo del sistema a través de la interfaz web de Node-RED y permite la comunicación entre el cliente y el servidor de aplicaciones (Raspberry Pi).

SSH. Se utiliza para el acceso remoto seguro al Gateway (Raspberry Pi), durante la instalación y configuración del sistema.

MQTT. Es el protocolo principal para la comunicación entre los dispositivos IoT y el servidor de aplicaciones (Broker). Permite que los sensores envíen datos de eventos como detección de movimiento o apertura de puertas, mientras que los clientes suscritos (por ejemplo, la aplicación móvil o Node-RED) reciben las actualizaciones en tiempo real.

TLS. El protocolo TLS es la versión mejorada de SSL, encargada de facilitar la encriptación, autenticación e integridad de los datos que se intercambiarán entre el Gateway (Raspberry Pi) y el telefono inteligente, haciendo uso de certificados TLS instalados en el Gateway y configurados para que el broker pueda acceder a los mismos. Estos certificados tambien son instalados en el teléfono inteligente.

WireGuard. Es el protocolo base empleado por Tailscale para crear la VPN entre el Gateway y el teléfono inteligente, lo que permite la comunicación segura.

TCP y UDP. El sistema emplea protocolos para el transporte como TCP y UDP, según el servicio que se esté ejecutando. Ambos operan bajo la infraestructura IP.

Redes de Nueva Generación

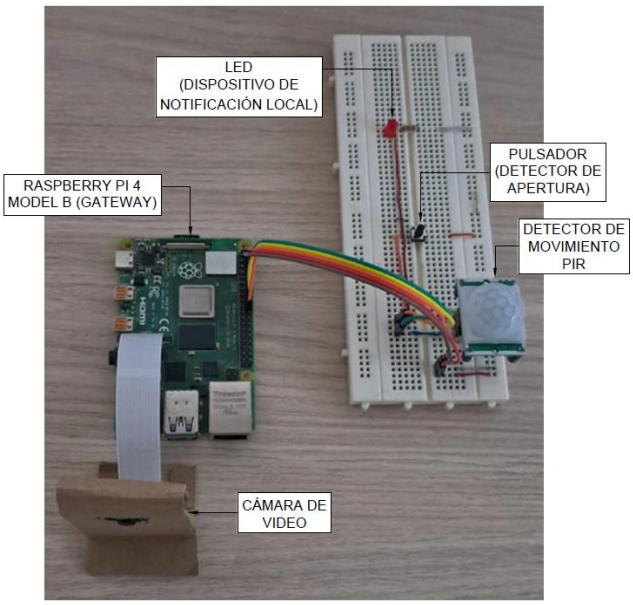
En la arquitectura se proyecta la utilización de redes NGN para proveer acceso a los servicios de internet. Se emplean redes 5G para el acceso del teléfono inteligente, y Wi-Fi para el acceso a internet del Gateway.

Validación del Diseño Propuesto

El proceso realizado para la validación del diseño propuesto, consiste en una implementación básica utilizando algunos de los componentes indicados en la arquitectura de referencia y simulando los otros. Ver figura 12.

Figura 12

Sensores y Gateway Empleados en la Validación del Diseño Propuesto



Nota. Se simula el dispositivo de notificación local a través de un indicador LED, el detector de apertura por medio de un pulsador y la cámara de video IP por medio de la cámara de la Raspberry Pi.

Configuración de la Raspberry Pi

La Raspberry Pi cuenta con sistema operativo Raspbian 10. Previamente se ha configurado la dirección IP fija 192.168.1.30 a fin de establecer una conexión remota que facilite su configuración por medio de comandos enviados vía SSH a través del emulador PuTTY. Se realiza la instalación de las aplicaciones Mosquitto, Node-RED y Tailscale. Ver **Apéndice A** *Configuración de la Raspberry Pi*

.

Figura 13

Mosquitto en Raspberry Pi

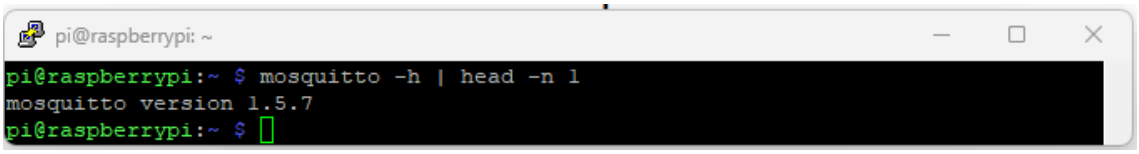


Figura 14

Node-RED en Raspberry Pi

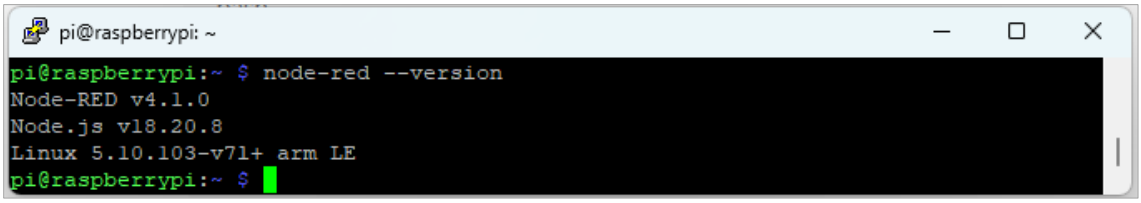
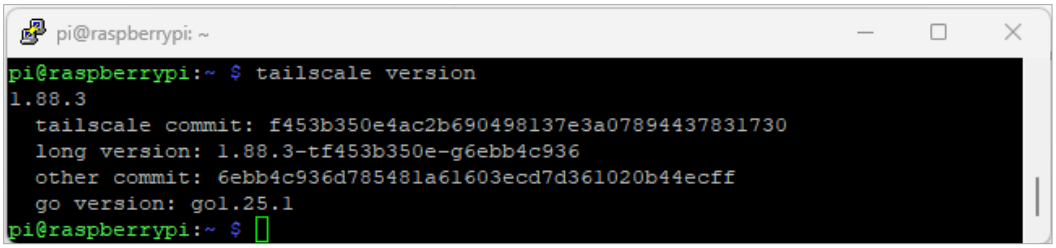


Figura 15

Tailscale en Raspberry Pi



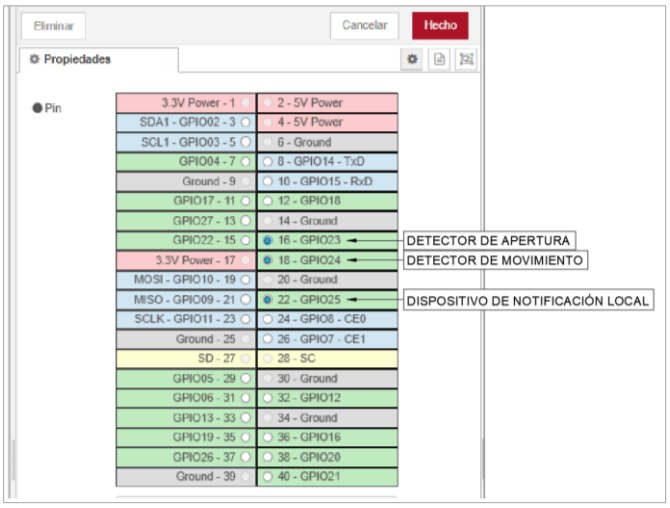
Configuración Node-RED

Se ejecuta el comando *node-red-start* para iniciar el servicio en la Raspberry Pi. Posteriormente es posible acceder a la interfaz Web de Node-RED a través de la dirección IP de la Raspberry, puerto 1880.

En el dashboard de Node-RED se encuentran los nodos asociados a los GPIO de la Raspberry (rpi-gpio in y rpi-gpio out), en los cuales se asignan las entradas y salidas a las que serán conectados los sensores y actuador, según se muestra a continuación:

Figura 16

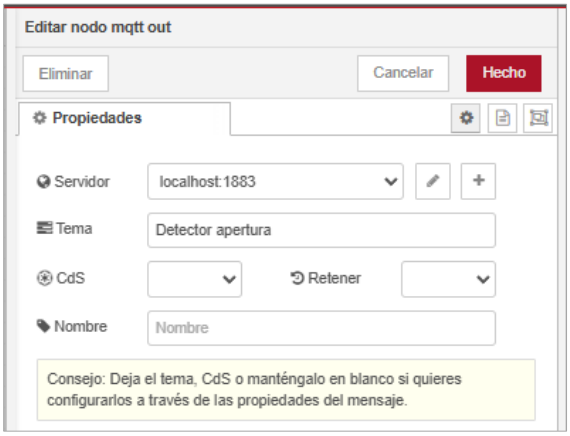
Asignación GPIO en Node-RED



Posteriormente se agregan nodos mqtt in y mqtt out a través de los cuales se configuran los “topics” o temas asociados a cada uno de los sensores (mqtt out) y actuador (mqtt in), por medio de los cuales será posible publicar o suscribirse a los mensajes gestionados por el broker Mosquitto.

Figura 17

Configuración Modo MQTT OUT en Node-RED



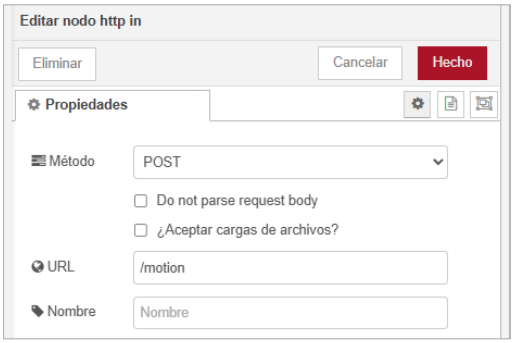
Nota. Teniendo en cuenta que el broker se ejecuta directamente en la Raspberry Pi, el servidor empleado corresponde al localhost.

Considerando que la cámara de video IP es simulada a través de la cámara de la Raspberry, se instala la aplicación motion, la cual permite la visualización del flujo de video por medio de la dirección IP de la Raspberry (puerto 8081) y la detección de movimiento.

La cámara generará un evento de detección de movimiento a través de un nodo http in, empleando el método POST.

Figura 18

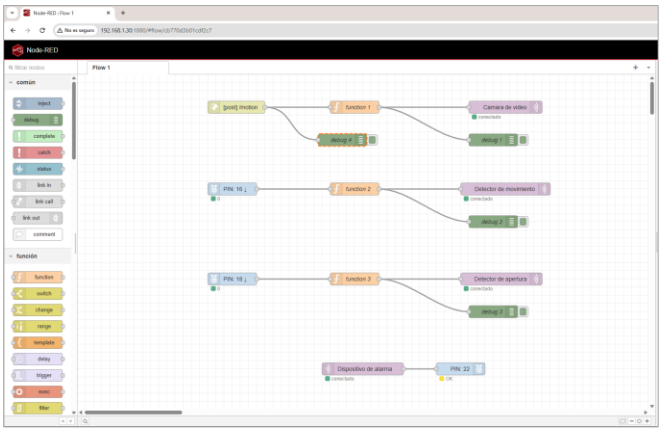
Configuración Nodo HTTP IN en Node-RED



Se emplean nodos tipo function asociados a los nodos mqtt out a través de los cuales se publica el evento de detección generado por los sensores. Se utiliza un nodo debug para validar los eventos en la interfaz Node-RED.

Figura 19

Configuración Flujos en Node-RED



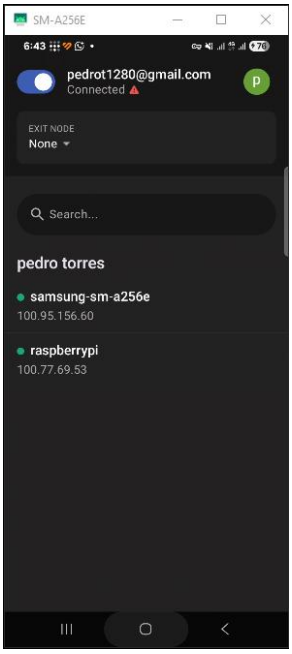
Configuración Teléfono Inteligente

En el Teléfono Inteligente se instalan las aplicaciones Tailscale (VPN) y MQTT Alert. En esta última se realiza la suscripción y publicación relacionada a los topics gestionados a través del Broker Mosquitto.

Tailscale (VPN). Emplea una cuenta de correo electrónico para asociar dispositivos al inicio de sesión, para realizar la conexión a su red privada y asigna de manera automática IPs fijas.

Figura 20

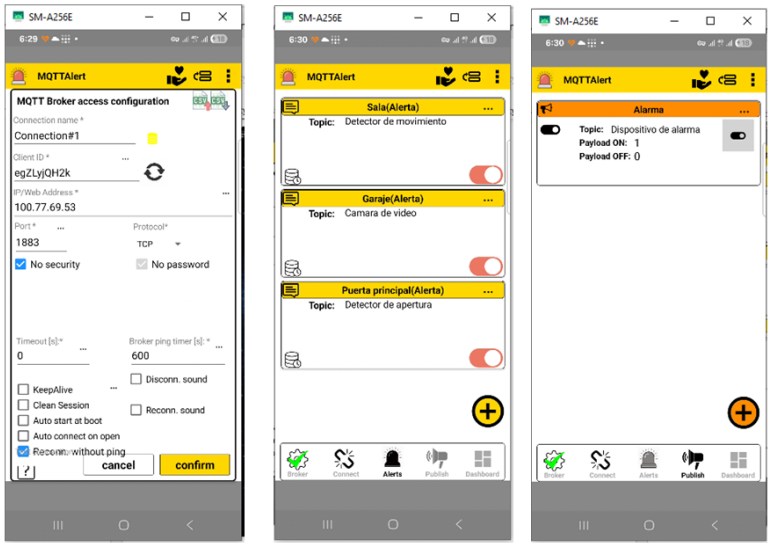
Configuración Tailscale APP



MQTT Alert. Se configura el acceso al broker y a los topics. Las notificaciones asociadas a los sensores, se configuran como alertas, y el dispositivo notificación local como publish. Se establecen varios escenarios como sala, garaje y puerta principal, donde se simulan los dispositivos.

Figura 21

Configuración MQTT Alert



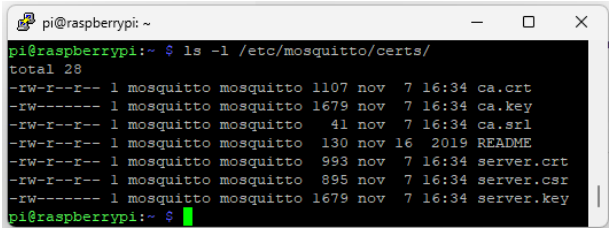
Configuración TLS

Se generan los certificados (CA), certificado del servidor y clave privada y se configura el Broker Mosquitto y los certificados TLS. Ver **Apéndice B**

Configuración TLS

Figura 22

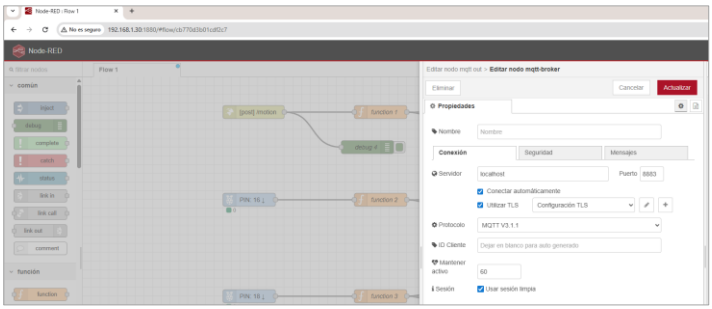
Certificados TLS en Raspberry Pi



En Node-RED se hace uso de la señal asociada al detector de apertura de la puerta, para crear un nuevo nodo con el topic “Detector”, configurado como se muestra a continuación:

Figura 23

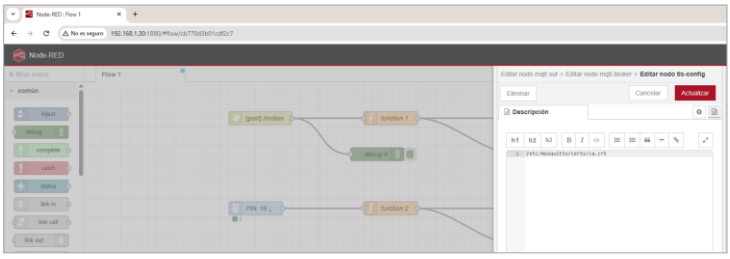
Configuración TLS en Node-RED



Teniendo en cuenta que los certificados se encuentran alojados localmente en el servidor, se configura el acceso a los mismos.

Figura 24

Certificados TLS en Node-RED



A través de la aplicación MQTT Dash (teniendo en cuenta que cuenta con posibilidad de habilitar conexión empleando SSL/TLS), se configura el broker, habilitando SSL/TLS para validar la conexión segura.

Figura 25

Configuración MQTT Dash –TLS / SSL

Pruebas

Durante la ejecución de las pruebas se simulan eventos de intrusos a través de la activación de los diferentes sensores y es posible confirmar que las notificaciones asociadas a eventos de intrusión son notificadas de manera automática, en el teléfono inteligente, a través de *MQTT Alert*. En la figura 26 se evidencia que el teléfono no se encuentra conectado vía Wi-Fi a la LAN.

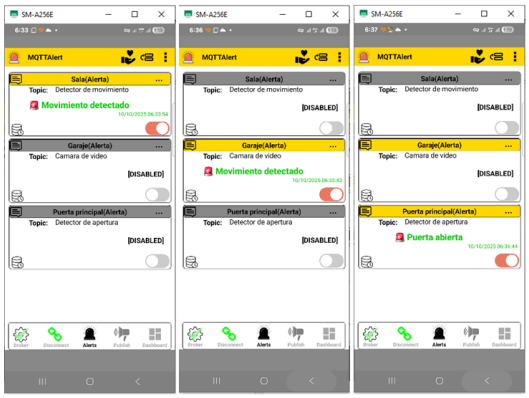
Figura 26

Notificaciones en Teléfono Inteligente

De igual forma, el usuario podrá reconocer los eventos al ingresar a la aplicación, e identificarlos en cada uno de los escenarios previamente configurados, para establecer con precisión el lugar y el tipo de evento. Con el fin de evitar la saturación de alarmas en el teléfono, las alarmas objeto de la prueba son deshabilitadas temporalmente, mientras se simula una de ellas, como se observa en la figura 27.

Figura 27

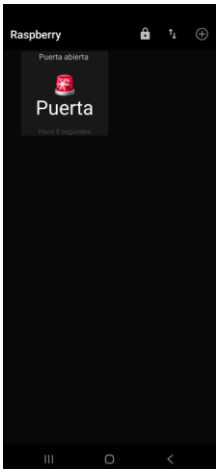
Notificaciones MQTT Alert



También es posible validar que la conexión empleando TLS se realiza de manera exitosa y se notifica el evento de apertura de la puerta a través de MQTT Dash.

Figura 28

Notificación MQTT Dash



Conclusiones

Al analizar el estado del arte relacionado con los sistemas de monitoreo y vigilancia de intrusos basado en tecnologías IoT, se evidencia una marcada tendencia hacia el uso de redes Wi-Fi y redes móviles, la utilización de dispositivos electrónicos como Raspberry Pi y NodeMCU y la preferencia por modelos basados en servicios en la nube para la gestión de la información.

El sistema propuesto emplea la Raspberry Pi como Gateway, aprovechando su versatilidad y capacidad para integrarse con entornos como Node-RED y para gestionar de forma flexible y local los diferentes sensores de detección de intrusos, cuyas tecnologías se complementan entre sí. En la capa de red, el sistema emplea una conexión vía Wi-Fi, facilitando su ubicación dentro del hogar y la conexión al modem del ISP. El modelo de publicación/suscripción, a través del protocolo MQTT garantiza una comunicación eficiente y de bajo consumo de ancho de banda, brindando una solución que puede ser implementada a través de código abierto y que permite la supervisión remota mediante telefonos inteligentes.

La arquitectura conceptual para el monitoreo y vigilancia de intrusos es viable y segura, ya que aprovecha la infraestructura de red provista por los ISP (redes como Wi-Fi y 5G) y emplea VPN como Tailscale (empleando protocolo WireGuard) para el monitoreo remoto a través de telefonos inteligentes y para superar las limitaciones que pueden presentar los modem de los ISP durante la configuración y adicionalmente emplea protocolos como TLS, el cual permite la conexión segura entre el Gateway y el telefono inteligente haciendo uso de comunicaciones cifradas.

Recomendaciones

Se recomienda explorar la implementación de mecanismos automáticos que generen alertas locales (como activación de sirenas, luces o notificaciones en tiempo real) ante la detección de intrusos, mejorando la capacidad de respuesta inmediata.

Se sugiere desarrollar módulos que permitan establecer comunicación automática con entes de seguridad, como la policía o empresas de vigilancia, mediante llamadas o mensajes preconfigurados ante eventos críticos.

Se aconseja evaluar la implementación de métodos de almacenamiento de video que permitan servir como evidencia ante eventos de intrusión.

Referencias Bibliográficas

Amazon AWS. (28 de 09 de 2025). https://aws.amazon.com/es/what-is/mqtt/

AMSV, S., A Aswini, P., ANG, L., Narendra, K., & Harish, S. (2024). Integrated IoT-Based Smart Home Security System: Real-Time Hazard Detection and Alerts Using Multi-Sensor Fusion. *International Conference on Intelligent and Innovative Practices in Engineering & Management (IIPEM 2024)* (pp. 1-6). Singapur: IEEE.

Anwar, S., & Kishore, D. (2016, Diciembre). IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone. *International Journal of Engineering Research & Technology (IJERT), 5*(12), 504-509.

Asadul Hoque, M., & Davidson, C. (2019, Abril). Design and Implementation of an IoT-Based Smart Home. *International Journal of Networked and Distributed Computing, 7*(2).

Balakrishnan, Ph.D., B., & Murugan V, A. (2024, Junio). SMART ANTI-THEFT SECURITY SYTEM USING IOT. *International Advanced Research Journal in Science, Engineering and Technology, 11*(6).

Castaño-Gómez, M., López-Echeverry, A., & Villa-Sánchez, P. (2021). Review of the use of IoT technologies and devices in physical security systems. *Revista Ingeniería y competividad*, 1-19.

Cirani, S., Ferrari, G., Picone, M., & Veltri, L. (2019). *Internet of Things Architectures, Protocols and Standards.* Chennai: John Wiley & Sons Ltd.

Comisión de Regulación de Comunicaciones. (17 de 05 de 2024). *https://www.crcom.gov.co/.* https://www.crcom.gov.co/es/noticias/comunicado-prensa/en-2023-colombia-alcanzo-cerca-54-millones-conexiones-internet

Cybellium Ltd. (2023). *Mastering VPN: A Comprehensive Guide to Learn VPN.* Cybellium Ltd.

G4S Colombia. (2025, 03 06). *https://www.g4s.com*. https://www.g4s.com/es-co/insightsroom/2025/03/06/sistema-de-camaras-de-seguridad#:~:text=Un%20sistema%20de%20c%C3%A1maras%20de%20seguridad%20suelen%20ser%20m%C3%A1s%20econ%C3%B3micos,en%20t%C3%A9rminos%20de%20almacenamiento%20local.

Ganesan, D., Pandian, T., & Ismaeil, H. (2024, Abril). IOT BASED HOME AUTOMATION AND SECURITY SYSTEM. *International Research Journal of Modernization in Engineering Technology and Science*, 9964-9967.

Garcia, M. (2006). *Vulnerability Assessment of Physical Protection Systems.* Burlington: Elsevier.

Honeywell Building Automation. ((s.f)). https://honeywell.scene7.com/is/image/Honeywell65/hbt-security-943wg-wh-miniature-sized-magnetic-primaryimage

Honeywell Building Automation. ((s.f)). https://honeywell.scene7.com/is/image/Honeywell65/hbt-security-is312b-compact-pir-motion-sensor-primaryimage

Honeywell Building Automation. ((s.f)). https://honeywell.scene7.com/is/image/Honeywell65/HBT-SEC-35S-HC35WBxR2

IBM Technology company. (17 de 09 de 2025). *https://www.ibm.com/*. https://www.ibm.com/es-es/topics/middleware

International Telecommunication Union. (2004). *ITU-T Y2001 General overview of NGN.*

International Telecommunication Union. (2012). *ITU-T Y2060 Overview of the Internet of things.*

Janevski, T. (2016). *Internet Technologies for Fixed and Mobile Networls.* Norwood, United States of America: Artech House.

Mohammad, A., & Radha, K. (2017, Diciembre). An IOT based Solar Integrated Home Security. *International Journal of Advanced Engineering Research and Science (IJAERS), 4*(12), 155-199.

Mohammad, S., Mohamad Bakri, M., Abdul Razak, M., Sapari, D., & Abdul Rashid, M. (2022). *Advanced Materials and Engineering Technologies* (Vol. 162). (A. Ismail, W. Mohd Dahalan, & A. Öchsner, Eds.) Springer.

Node MCU. ((s.f)). https://www.steren.com.co/media/catalog/product/cache/0236bbabe616ddcff749ccbc14f38bf2/image/20764b39a/placa-de-desarrollo-nodemcu-esp8266.jpg

Policia Nacional de Colombia. (17 de 08 de 2025). *https://www.policia.gov.co*. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.policia.gov.co%2Fsites%2Fdefault%2Ffiles%2Fdelitos-impacto%2FHurto%2520a%2520residencias_6.xlsx&wdOrigin=BROWSELINK

Pupkevicius, M. (01 de 31 de 2024). *Burglary Statistics & Facts You Need to Be Aware of in 2025*. https://moneyzine.com/buying-a-home/burglary-statistics/

Rajani, & Malik, K. (2025). *Internet of Things: A Basic Approach.* India: Authors Click Publishing.

Raspberry Pi. ((s.f)). https://assets.raspberrypi.com/static/8f6eca535dbb23a21eb41a748050e3a0/b0461/16gb.png

Rifa Pous, H., Gallego Terris, R., & Huertas Garcia , V. (2019, 09). *https://openaccess.uoc.edu.* https://openaccess.uoc.edu/server/api/core/bitstreams/c1d41d6f-c3c1-4d22-b1ae-f9df9ee4db43/content

RTVC Noticias. (2026, 02 16). *https://www.rtvcnoticias.com*. https://www.rtvcnoticias.com/colombia/inseguridad-principales-ciudades-bogota-medellin-cali

Sabit, H. (Febrero de 2025). Artifical Intelligence-Based Smart Security System Using Internet. *Electronics*, 1-25.

Sharma, M. (2022). *Internet of Things A Hardware Development Perspective.* Boca Raton: CRC Press Taylor & Francis Group.

Tuya Inc. ((s.f)). *https://www.tuya.com*. https://seapromotionstatic.cdn5th.com/static/275611206470062080.png

Uthman Azlan, M., & Shamian Zainal, M. (2024). An IoT Based Home Security System With ESP32, Video Monitoring, and Blynk Integration. *Enhanced knowledge in science and technology*, 238-244.

World Population Review. (26 de 08 de 2025). *https://worldpopulationreview.com*. https://worldpopulationreview.com/country-rankings/burglary-rates-by-country

Apéndices

Apéndice A

Configuración de la Raspberry Pi

Comandos de instalación e inicio automático del broker MQTT Mosquitto:

sudo apt install -y mosquitto mosquitto-clients

sudo systemctl enable mosquitto

Comando de instalación y configuración de Node-RED:

bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)

Comando de inicio automático de Node-RED:

Sudo systemctl enable nodered.service

Comandos de instalación y configuración de Tailscale:

curl -fsSL https://tailscale.com/install.sh | sh

Comandos de inicio de sesión e integración de la Raspberry a la red Tailscale:

sudo tailscale up

Comando para obtener dirección IP:

tailscale ip -4

Apéndice B

Configuración TLS

Comandos empleados para la generación de directorio para certificados:

mkdir ~/certs

cd ~/certs

Comandos empleados para generación de certificados CA:

openssl genrsa -out ca.key 2048

openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt

Comando empleado para la generación de clave privada de servidor:

openssl genrsa -out server.key 2048

Comandos empleados para generación CSR del servidor:

openssl req -new -key server.key -out server.csr

Comandos empleados para firmar el certificado del servidor

*openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial *

-out server.crt -days 3650 -sha256

Comando empleado para editar el archivo de configuración:

sudo nano /etc/mosquitto/mosquitto.conf

Se agregan las siguientes líneas en el archivo de configuración:

listener 8883 // Puerto seguro

cafile /mosquitto/pi/certs/ca.crt // Certificado raíz que firmó al servidor

certfile / mosquitto/pi/certs/server.crt // Certificado público del servidor

keyfile / mosquitto/pi/certs/server.key // Clave privada del servidor

require_certificate false// No se exige certificado al cliente