# Controlador inteligente de cerradura de puerta con LLM

Integrantes:
Cristiam Loaiza
Jefferson Andrés Durango Argaez
Juan Diego Cabrera Moncada

1. Planteamiento del problema y motivación

En la actualidad, la seguridad en accesos residenciales y comerciales enfrenta desafíos como robos, accesos no autorizados y la dificultad de gestionar cerraduras de forma remota. Los sistemas tradicionales de control de acceso, como llaves físicas o contraseñas fijas, pueden ser vulnerables a pérdidas, robos o ataques. Además, los sistemas de seguridad convencionales no ofrecen una interacción intuitiva ni la capacidad de adaptarse a los patrones de uso de los usuarios, lo que limita su eficiencia y comodidad.

Con la creciente expansión de las casas inteligentes se han incorporado nuevos sistemas en el ámbito de la domótica al punto que las tecnologías inteligentes ahora conforman una parte integral de nuestras vidas. Con ello, recientes estudios [3] plantean que resulta pertinente el análisis de los riesgos de privacidad que conlleva la implementación de sistemas inteligentes en el hogar no solo desde una perspectiva técnica. Así, cuando se trata especialmente de dispositivos centrados en garantizar la seguridad del hogar del cliente, debemos pensar en “soluciones que proporcionen la conveniencia, fiabilidad y control que los usuarios buscan” ([1]).

En Colombia, empresas como Zurich ofrecen servicios que brindan protección al hogar mediante la instalación de cámaras de vigilancia y cerraduras inteligentes e iluminación exterior con sensores de movimiento que complementan el sistema ([4]). Sin embargo, la instalación de un sistema completo avanzado de seguridad que además resulte sencillo de controlar puede resultar costoso para ciertas zonas del país. Por tal razón, en los últimos años la tecnología de seguridad de los hogares se ha visto influenciada fuertemente por la implementación de mecanismos de seguridad biométricos, de control remoto, o con asistentes virtuales basados en inteligencia artificial, con el fin de facilitar al usuario el manejo de un servicio de seguridad avanzado brindando respuestas eficientes ([2]).

Con esto en mente, este proyecto propone un controlador de cerradura inteligente basado en IoT y un modelo de lenguaje de gran escala (LLM), capaz de interpretar comandos en lenguaje natural y proporcionar respuestas adaptativas a eventos de seguridad. Al combinar sensores, conectividad en la nube y procesamiento de datos mediante inteligencia artificial, se busca mejorar la seguridad y accesibilidad en hogares y oficinas. La motivación principal es ofrecer una solución segura, intuitiva y proactiva que no solo permita la gestión remota de accesos, sino que también detecte amenazas en tiempo real y mejore la experiencia del usuario mediante automatización inteligente.

## 2. Propuesta de la arquitectura del sistema

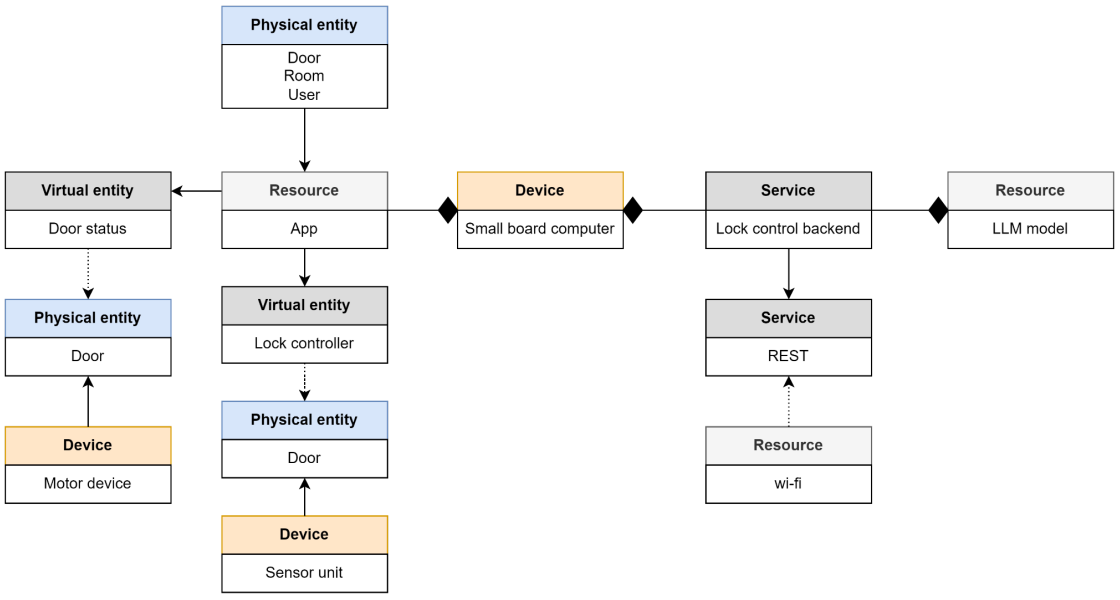
### 2.1. Requerimientos del sistema

Desde el punto de vista operacional del sistema, éste debe establecer como máxima prioridad la garantización de bloqueo y desbloqueo de la cerradura, ya sea que el usuario realice la solicitud de realizar el cambio de estado de la cerradura por medio del uso del LLM incorporado o de forma manual. Como segunda función principal se encuentra la denegación de acceso en un intervalo de tiempo corto en dado caso que se detecte niveles de vibración anormales en la puerta, como indicación de un intento de entrada forzosa o de daño a la cerradura. Asimismo, se considera evaluar el nivel de facilidad de uso de la interfaz de usuario y que el retardo de respuesta del sistema a las órdenes que envía el usuario desde la aplicación no resulte significativo. En caso de falla crítica del sistema, se debe asegurar que el sistema es manipulable manualmente para evitar inconvenientes en el manejo del sistema ya sea por incapacidad del usuario para usar la aplicación o por fallos de la misma.

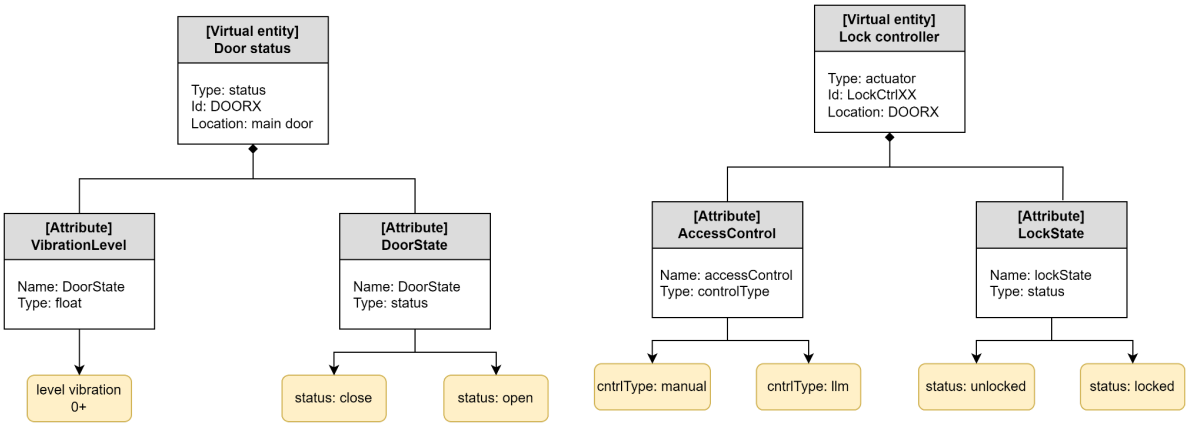
En lo que respecta a los requerimientos no funcionales del sistema, se busca que la interfaz de usuario establecida para el diseño de la aplicación en conjunto con el asistente virtual con LLM incorporado ofrezca al usuario una operación intuitiva, sugiriendo acciones de seguridad según patrones de uso.

En cuanto a la parte técnica, el sistema utiliza un ESP32 para conectividad Wi-Fi y un servidor MQTT en la nube para comunicación segura. Los eventos se almacenan en una base de datos InfluxDB, y la visualización se gestiona mediante una app web o móvil. A partir de ello, los usuarios deben poder interactuar con el sistema por voz o texto para bloquear/desbloquear la puerta, recibir alertas de seguridad y consultar el historial de accesos.

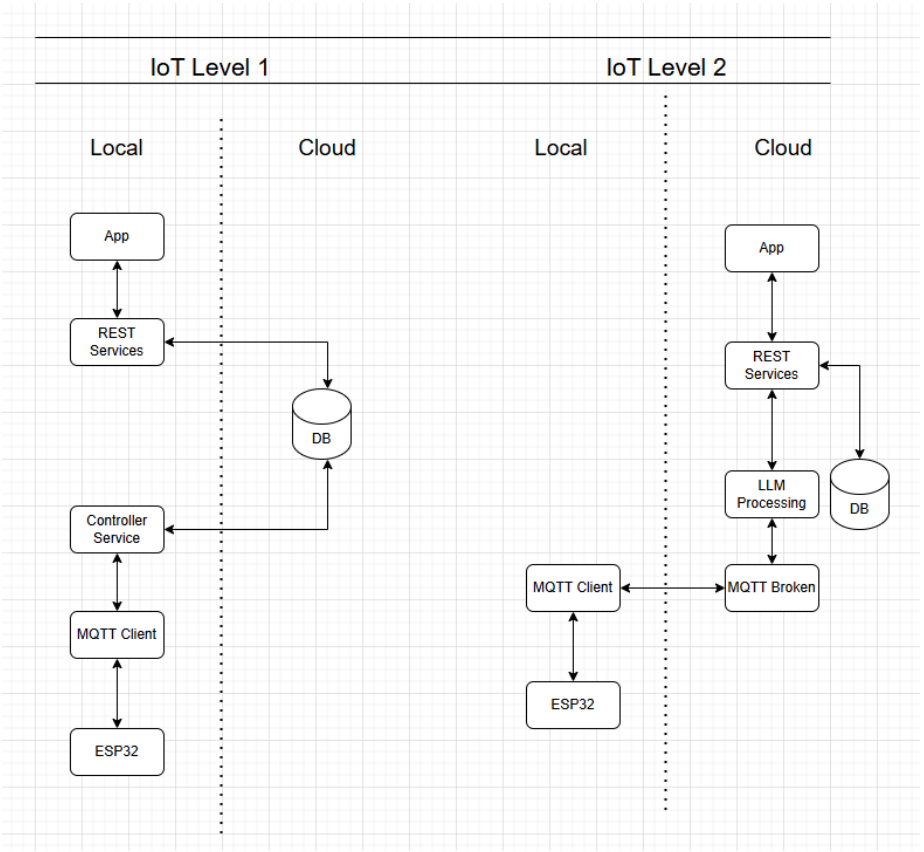
### 2.2. Especificación de Modelo de Dominio



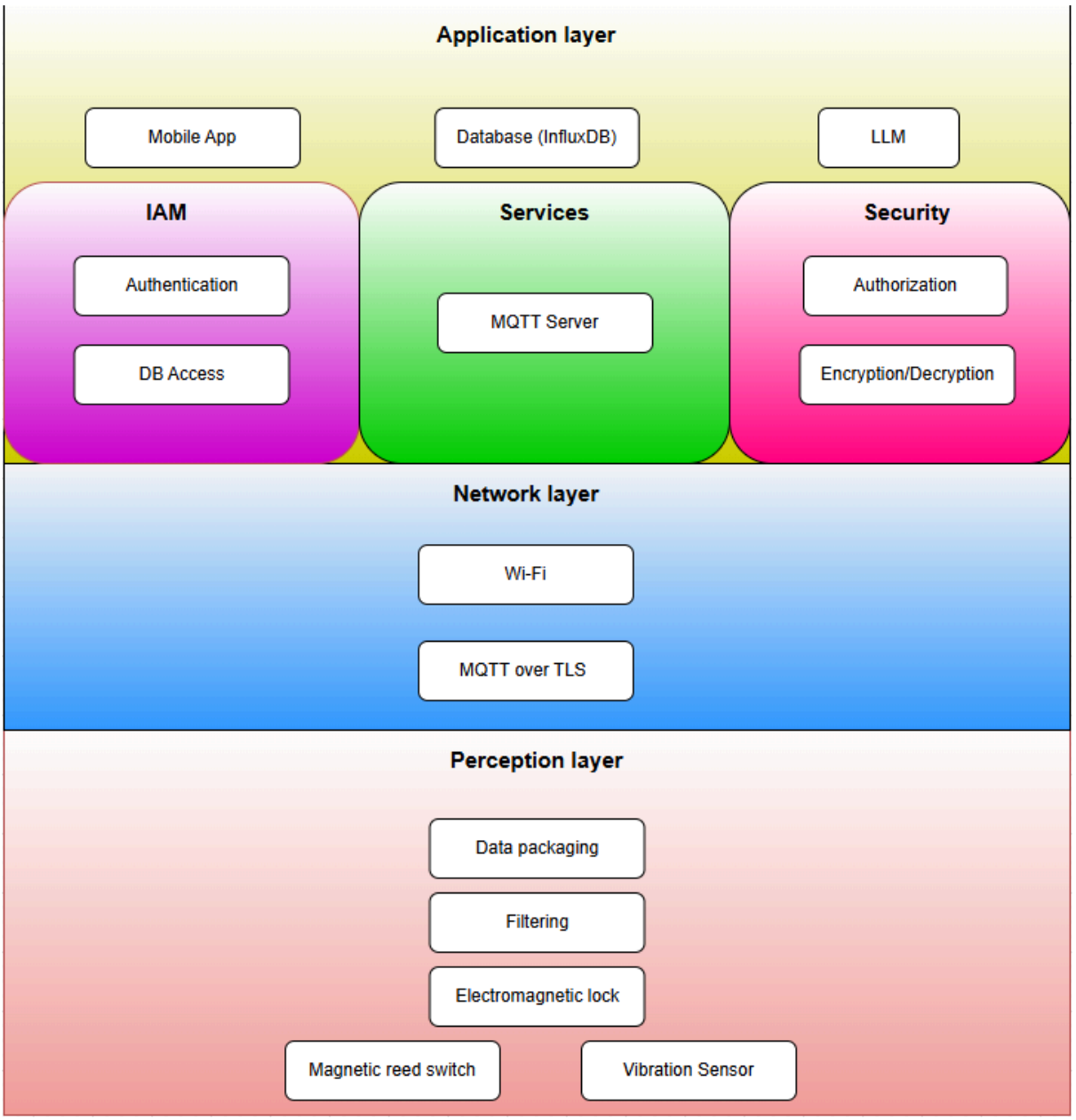
## 2.3. Especificación de Modelo de Información



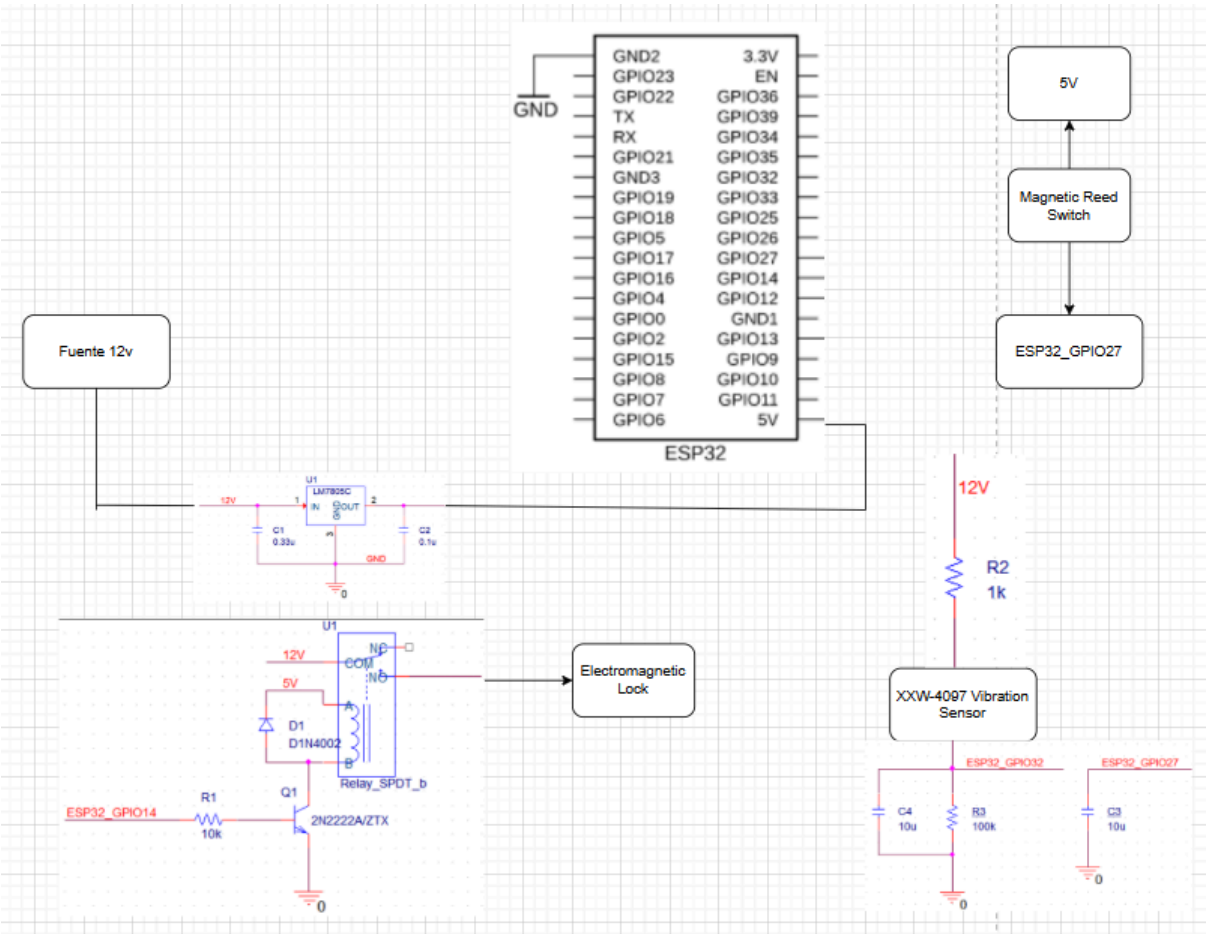

## 2.4. Especificación de Nivel de IoT



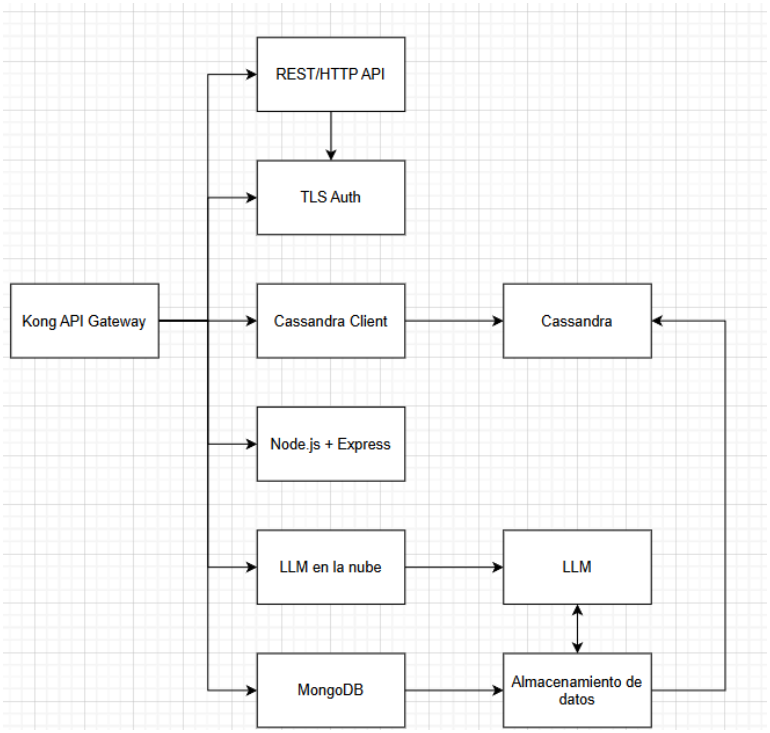

## 2.5. Especificación de Vista Funcional




2.6. Integración de Dispositivo




## 2.7. Integración de Componentes



3. Variables medidas y controladas

A través de la sensórica descrita previamente, se evidencia que las variables medidas corresponden a: Nivel de vibración de la cerradura de la puerta y Estado actual de la puerta (Cerrada o Abierta), las cuales son registradas y guardadas en la base de datos de la app para un mejor desempeño y personalización. A partir de los datos recolectados, se busca controlar el estado de la cerradura (Bloqueada o Desbloqueada) y las alertas de seguridad enviadas al usuario para facilitar la gestión del sistema de seguridad implementado.

4. Cronograma de ejecución del proyecto

| Cronograma de ejecución del proyecto | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Semana 3 (17 - 23 mar.) | Semana 4 (24 - 30 mar.) | Semana 5 (31 mar. - 6 abr.) | Semana 6 (7 - 13 abr.) | Semana 7 (14 - 20 abr.) | Semana 8 (21 - 27 abr.) | Semana 9 (28 abr. - 4 may.) | Semana 10 (5 - 11 may,) | Semana 11 (12 - 18 may.) | Semana 12 (19 - 25 may.) | Semana 13 (26 may. - 1 jun.) |
| Integración Capa de Percepción | | | | | | | | | | | |
| Integración Capa de Red | | | | | | | | | | | |
| Entregable Proyecto Final | | | | | | | | | | | |
| Pruebas de sensórica | | | | | | | | | | | |
| Implementación de tratamiento de datos | | | | | | | | | | | |
| Pruebas de actuadores | | | | | | | | | | | |
| Planteamiento de Propuesta | | | | | | | | | | | |
| Conectividad Wi-Fi con ESP32 | | | | | | | | | | | |
| Gestión de paquetes de datos JSON | | | | | | | | | | | |
| Implementación de MQTT sobre TLS | | | | | | | | | | | |
| Desarrollo de servidor MQTT | | | | | | | | | | | |
| Desarrollo de app móvil | | | | | | | | | | | |
| Almacenamiento en base de datos | | | | | | | | | | | |
| Integración del LLM para control inteligente | | | | | | | | | | | |

REFERENCIAS

[1] C. Paranagama and B. Hettige, “A Review on Existing Smart Door Lock Systems,” 2022. doi: 10.13140/RG.2.2.18892.08325.

[2] J. S. Edu, J. M. Such, and G. Suarez-Tangil, “Smart Home Personal Assistants: A Security and Privacy Review,” ACM Computing Surveys, vol. 53, no. 6, Art. 116, Nov. 2021. doi: 10.1145/3412383.

[3] S. Yu, B. Bentley, and F. Carroll, “Enhancing Smart Home Security: A Privacy Risk Analysis Framework,” 2024. doi: 10.1007/978-981-97-3973-8_18.

[4] Zurich Colombia Seguros S.A. “Seguridad en el hogar: Mejores prácticas para proteger tu casa y a tu familia”. Zurich Seguros. Accedido el 20 de marzo de 2025. [En línea]. Disponible: https://www.zurichseguros.com.co/blog/articulos/2024/05/practicas-para-proteger-tu-hogar