

Solución innovadora para la gestión integral de seguridad de equipamientos de taquillas

1.Análisis de la solución.

Esta solución pretende, innovar las cerraduras electrónicas. Tiene el objetivo de superar las capacidades de las cerraduras ya existentes, para brindar al mercado un modelo con mayor duración, mayor seguridad y flexibilidad para su control desde el software ofrecido por la desarrolladora o de terceros.

Novedades de la propuesta:

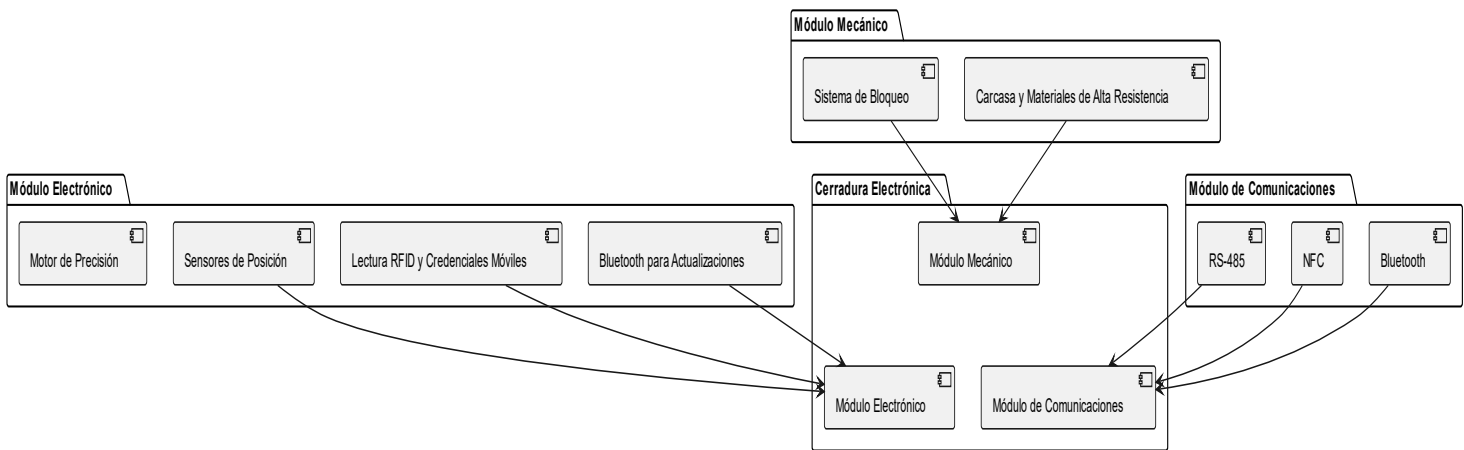
Su diseño mecánico garantiza una durabilidad de hasta 500.000, mayor a las capacidades del mercado actual. Las cerraduras cuentan con un modulo de comunicaciones el cual permite la gestión remota de la cerradura (pudiendo elegir entre diferentes tecnologías, tanto cableado como inalámbricas) facilitando la integración a un sistema centralizado de gestión. Además, se incorporaron módulos avanzados de lectura RFID y biometría, así como un sistema de actualización vía Bluetooth para la garantizar las mejoras y adaptabilidad a nuevos estándares de seguridad.

2.Diseño de la solución.

La cerradura electrónica incorpora un diseño mecánico y electrónico capaz de garantizar hasta 500.000 ciclos de uso. Entre sus componentes clave se encuentran tres módulos principales.

- Módulo mecánico: Este responsable del sistema de bloqueo, con materiales de alta resistencia y un mecanismo optimizado para reducir el desgaste y garantizar una vida útil prolongada.
- Módulo electrónico: Incluye un motor de precisión y sensores de posición mediante optoacopladores de ranura, permitiendo un control exacto del estado de la cerradura y una respuesta inmediata a comandos de apertura o cierre. Además, integra módulos avanzados para la lectura de tarjetas RFID, credenciales móviles mediante teléfonos y su modulo bluetooth para actualizaciones y notificaciones.
- Módulo de comunicaciones: Compatible con tecnologías tanto cableadas como inalámbricas (RS-485, NFC o Bluetooth), facilitando la gestión centralizada de accesos y la sincronización con plataformas digitales.

Las cerraduras operan con baterías de larga duración y cuenta con un sistema de alertas para notificar el estado de carga y mantenimiento.



3.Desarrollo de la solución.

El proceso de desarrollo contempla todas las fases de diseño, desde la selección de materiales hasta la implementación de firmware y software. En la fase inicial, se realiza un análisis de los requisitos técnicos y operativos, seguido de la creación de prototipos y pruebas de validación. Se han incorporado módulos avanzados de lectura RFID y biometría, así como un sistema de actualización vía Bluetooth para garantizar mejoras continuas y adaptabilidad a nuevos estándares de seguridad.

El diseño mecánico se optimiza mediante simulaciones de resistencia estructural y pruebas de desgaste, asegurando la fiabilidad del sistema de bloqueo. Paralelamente, el desarrollo del firmware incluye algoritmos de gestión de energía para maximizar la autonomía de la cerradura y mejorar la eficiencia operativa.

Para garantizar la compatibilidad con distintos entornos de uso, el software de gestión se desarrolla con interfaces flexibles que permiten su integración con plataformas de terceros a través de API REST. Asimismo, el sistema se diseña para operar en entornos con conectividad variable, ofreciendo modos de funcionamiento tanto en línea como fuera de línea.

4.Pruebas.

Prueba nº1: Prueba de Captura en Ambientes con Iluminación Variable

Objetivo: Evaluar el rendimiento del sistema de captura de huellas dactilares sin contacto en diferentes condiciones de iluminación.

Procedimiento:

1. Configurar el dispositivo en una habitación con iluminación controlada.
2. Realizar capturas de huellas bajo las siguientes condiciones:
 - Luz intensa (5000+ lux): Simulando luz solar directa o iluminación de oficinas bien iluminadas.
 - Luz media (1000-3000 lux): Condiciones típicas de interiores.
 - Luz baja (100-500 lux): Simulando una habitación con poca luz.
 - Oscuridad total (0 lux): Evaluar la efectividad de la iluminación interna del dispositivo.
3. Capturar múltiples huellas por usuario y medir la tasa de éxito en cada escenario.
4. Comparar la calidad de las imágenes obtenidas, evaluando el contraste, el nivel de ruido y la precisión de las características biométricas extraídas.

Criterios de éxito:

- El sistema debe mantener una tasa de captura exitosa superior al 95% en todas las condiciones.
- Las imágenes deben ser lo suficientemente nítidas para la identificación, sin pérdidas de detalle en entornos oscuros o sobreexpuestos.
- Se evaluará la capacidad del dispositivo para ajustar automáticamente los parámetros de captura en función de la iluminación ambiental.

Prueba nº2: Prueba de Resistencia a Manipulación y Spoofing

Objetivo: Comprobar la capacidad del sistema para detectar intentos de falsificación o suplantación mediante huellas artificiales.

Procedimiento:

1. Preparar réplicas de huellas dactilares utilizando distintos materiales:
 - Impresiones en papel con tinta conductiva.
 - Modelos en silicona y látex que simulen la textura de la piel.

- Huellas fotográficas en alta resolución mostradas en pantallas OLED.
- 2. Intentar acceder al sistema con cada tipo de falsificación.
- 3. Medir la tasa de aceptación de huellas falsas y comparar con la tasa de aceptación de huellas legítimas.
- 4. Evaluar la efectividad del algoritmo de detección de vitalidad (liveness detection), verificando si identifica correctamente los intentos de engaño.

Criterios de éxito:

- El sistema debe rechazar todas las huellas falsas sin afectar la precisión en huellas reales.
- Se analizará si el uso de luz multiespectral y algoritmos de aprendizaje profundo mejora la detección de huellas fraudulentas.
- Se revisará el tiempo de procesamiento del análisis de vitalidad para garantizar que no retrase el acceso.

Prueba nº3: Prueba de Experiencia del Usuario y Ergonomía

Objetivo: Evaluar la facilidad de uso del dispositivo en diversos escenarios y con distintos perfiles de usuarios.

Procedimiento:

1. Reclutar 50 participantes de diferentes edades, habilidades y condiciones de movilidad.
2. Pedirles que realicen múltiples intentos de captura de huellas en condiciones normales de uso.
3. Medir el tiempo promedio de registro e identificación para cada usuario.
4. Registrar observaciones sobre dificultades en la colocación de los dedos y analizar la utilidad del sistema de señalización acústica-luminosa.
5. Aplicar encuestas para evaluar la percepción de facilidad de uso, comodidad y confianza en el sistema.

Criterios de éxito:

- El tiempo promedio de captura debe ser inferior a 1 segundo por intento exitoso.
- Al menos un 90% de los usuarios deben calificar el proceso como "fácil" o "muy fácil".
- Se debe garantizar que el sistema funcione correctamente para personas con discapacidad o limitaciones físicas.

Prueba nº4: Prueba de Precisión y Velocidad de Identificación en Escenarios de Alto Tráfico

Objetivo: Evaluar el desempeño del sistema en entornos con un alto flujo de usuarios, midiendo la rapidez y precisión en la identificación biométrica.

Procedimiento:

1. Instalar el dispositivo en una entrada de acceso masivo, como un edificio corporativo o universidad.
2. Configurar la base de datos con 10,000 registros de huellas para simular una implementación realista.

3. Hacer que 100 usuarios ingresen de manera continua, replicando condiciones de tráfico elevado.
4. Medir los siguientes parámetros:
 - Tiempo de identificación promedio: Desde que el usuario coloca la mano hasta que recibe la validación.
 - Tasa de éxito de identificación: Porcentaje de huellas correctamente reconocidas en el primer intento.
 - Tasa de rechazo falso (FRR): Casos en los que el sistema rechaza una huella válida.
 - Tasa de aceptación falsa (FAR): Casos en los que el sistema acepta una huella incorrecta.
5. Evaluar la capacidad del sistema para mantener la velocidad de respuesta sin ralentizaciones ni fallos bajo carga de trabajo alta.

Criterios de éxito:

- Tiempo de respuesta inferior a 1 segundo en al menos el 95% de los intentos.
- Tasa de éxito superior al 98% en el primer intento de identificación.
- FRR menor al 1% y FAR menor al 0.01% para garantizar la seguridad y precisión.
- El dispositivo debe funcionar sin interrupciones durante al menos 4 horas de uso continuo en tráfico intenso.

5.Conclusión.

La solución innovadora para la gestión integral de seguridad en cerraduras electrónicas para diferentes usos representa un avance significativo en el sector. Su diseño modular permite una combinación óptima de seguridad, durabilidad y conectividad, facilitando su integración con plataformas digitales de terceros. Las mejoras en la estructura mecánica y electrónica aseguran un rendimiento superior al de las cerraduras convencionales, ofreciendo una vida útil prolongada y mayor eficiencia operativa.

Las rigurosas pruebas de validación han demostrado que el sistema mantiene una alta precisión en la autenticación biométrica y una respuesta rápida incluso en entornos de alto tráfico. La implementación de tecnologías como Bluetooth, NFC y RFID permite un control centralizado y una experiencia de usuario más ágil y segura. Además, el enfoque en la actualización continua del firmware y la adaptabilidad a nuevos estándares de seguridad refuerzan su carácter innovador.

En conclusión, esta cerradura electrónica no solo mejora la seguridad y la gestión de accesos, sino que también optimiza la operatividad en diversos sectores. Su capacidad para integrarse con infraestructuras existentes y su facilidad de uso la convierten en una solución clave para entornos que requieren una seguridad avanzada y un control eficiente.