# **Análisis de la solución: Estado del arte y novedad de la propuesta**

**Estado del Arte**

Los sistemas de seguridad y control de acceso tradicionales se suelen basar en el uso de tarjetas, llaves o códigos PIN. Sin embargo, estos métodos están limitados, ya que se pueden perder, ser robados o incluso compartidos, poniendo en riesgo la seguridad​.

Para solucionar estos problemas, se han desarrollado sistemas biométricos que utilizan rasgos únicos de cada persona, como la huella dactilar, el reconocimiento facial o el escaneo del iris. Los lectores de huellas son de los más utilizados gracias a su fiabilidad y facilidad de uso​. No obstante, la mayoría de ellos requieren contacto físico con el sensor, lo que genera inconvenientes en términos de higiene y mantenimiento, especialmente en entornos con gran afluencia de personas​.

**Novedad de la Propuesta**

La tecnología propuesta en esta patente introduce un sistema de captura de huellas dactilares sin contacto, lo que supone una mejora significativa en términos de higiene, comodidad y durabilidad​. Sus principales innovaciones son:

* **Escaneo sin contacto:** Permite identificarse sin necesidad de tocar el sensor, evitando la acumulación de suciedad y reduciendo el desgaste del dispositivo​.
* **Alta precisión y seguridad:** Utiliza algoritmos avanzados para mejorar la calidad de la imagen y verificar que la huella corresponde a una persona real, evitando intentos de suplantación​.
* **Sistema multicanal:** No solo reconoce huellas dactilares, sino que también permite el acceso mediante tarjetas RFID y teléfonos móviles con NFC o Bluetooth®​.
* **Aprendizaje adaptativo:** Integra un sistema que ajusta y actualiza automáticamente los patrones biométricos con el tiempo, evitando que el usuario tenga que volver a registrar su huella si esta cambia debido al envejecimiento o condiciones externas​.

Diagrama

El contenido generado por IA puede ser incorrecto.

# **Diseño de la solución (detalles técnicos que la diferencian).**

Para capturar la huella dactilar en el aire, la cerradura hace uso de un sensor CMOS de 1 a 3 MP con una distancia focal fija y apertura ajustable, además de unos LED de diferentes longitudes para la mejor calidad de imagen.

El dispositivo hace uso de infrarrojos para la detección de la posición del dedo, pudiendo indicar al usuario la realización de los ajustes necesarios para la detección adecuada mediante señales acústicas y lumínicas, además se implementan algoritmos de segmentación, detección de vivacidad y análisis de huella para la comprobación de la calidad de la huella, actualizando la base de datos automáticamente para poder adaptarse a cambios en la piel del usuario.

La cerradura puede ser abierta además de con la huella, usando tarjetas RFID o dispositivos con diversas interfaces de comunicación, tales como Bluetooth, NFC, RFID, TCP/IP, RS-485. Finalmente se pueden adaptar los protocolos de seguridad, para que pida al usuario introducir tres huellas dactilares si se necesita más seguridad.

# **Desarrollo de la solución a través de prototipos**.

Diseño y Componentes

1. Módulo mecánico: Responsable del sistema de bloqueo, con un diseño optimizado para garantizar una durabilidad de hasta 500,000 ciclos de apertura y cierre, superando las opciones actualmente disponibles en el mercado.

2. Módulo electrónico: Gestiona el control del motor de apertura y cierre, así como la monitorización de la posición del pestillo mediante optoacopladores de ranura. Este módulo permite una respuesta rápida y precisa ante comandos de desbloqueo y bloqueo.

3. Módulo de comunicaciones: Facilita la gestión centralizada de las cerraduras a través de múltiples interfaces de conexión, tanto cableadas (RS-485) como inalámbricas (NFC, Bluetooth®).

Esto permite la integración de la solución con plataformas externas y su control remoto desde sistemas centralizados.

Software y Gestión Inteligente

El desarrollo de la solución también incluye la creación de una plataforma de software avanzada, diseñada

para optimizar la administración de accesos. Entre sus principales funcionalidades destacan:

• Registro y gestión de usuarios, con alta y baja de credenciales de acceso.

• Control en tiempo real del estado de las cerraduras y monitoreo de eventos de apertura/cierre.

• Configuración de horarios y calendarios de acceso para optimizar la seguridad y el uso eficiente de

los recursos.

• Generación de informes de eventos y auditorías para un control detallado de la actividad del sistema.

Proceso Iterativo de Desarrollo y Validación

La solución se desarrolla mediante un enfoque iterativo basado en la creación y validación de prototipos funcionales. Cada iteración incluye:

• Diseño y fabricación de prototipos: Se producen modelos funcionales para evaluar el desempeño de los componentes mecánicos y electrónicos.

• Pruebas de resistencia y durabilidad: Se realizan ensayos de ciclos repetitivos de apertura y cierre para evaluar la longevidad de los componentes y detectar posibles mejoras en el diseño.

• Pruebas funcionales: Se integran las cerraduras con la plataforma de software para verificar su correcto funcionamiento y compatibilidad con distintos sistemas de gestión.

• Validación de seguridad: Se realizan pruebas de vulnerabilidad para garantizar que el sistema no pueda ser vulnerado mediante ataques físicos o electrónicos.

Diagrama

El contenido generado por IA puede ser incorrecto.

# **4. Pruebas (Evaluación de los prototipos y probadores)**

Para asegurarnos de que la solución de seguridad para taquillas funciona bien, hemos diseñado un plan de pruebas.

Primero, hacemos pruebas de resistencia y durabilidad, sometiendo la cerradura a miles de aperturas y cierres seguidos. Queremos comprobar que aguanta hasta 500,000 usos sin fallar. También la probamos en condiciones difíciles, como humedad, temperaturas extremas y vibraciones.

En la parte electrónica, usamos equipos automáticos para revisar que los circuitos y sensores funcionen bien en situaciones reales. Además, hacemos pruebas de interferencias para evitar problemas con otros dispositivos.

Las pruebas funcionales nos ayudan a comprobar que la cerradura se conecta bien con el software, gestionando accesos, monitoreo remoto y diferentes tipos de comunicación (RS-485, NFC, Bluetooth® y OSDP). También analizamos su seguridad frente a intentos de hackeo o manipulación física.

Por último, probamos el sistema con usuarios reales en gimnasios, oficinas y otros lugares. Así obtenemos comentarios y hacemos mejoras antes de lanzarlo al mercado.

Para definir las interacciones entre los distintos actores del sistema de seguridad de taquillas, hemos creado un diagrama de casos de uso UML que representa las funciones principales del sistema.

**Diagrama de Casos de uso**

1. Actores del Sistema
2. Usuario (Empleado/Cliente): Persona que utiliza la taquilla y necesita autenticarse para acceder a ella.
3. Administrador del Sistema: Responsable de la gestión de usuarios, configuración de credenciales y supervisión del sistema.
4. API de Terceros: Sistemas externos que pueden controlar accesos mediante la API REST.
5. Casos de Uso Identificados:
   1. Casos de Uso del Usuario:
      1. Autenticarse en la taquilla: El usuario se identifica con una tarjeta RFID, biometría o su dispositivo móvil.
      2. Abrir taquilla: Si la autenticación es válida, el sistema desbloquea la cerradura.
      3. Cerrar taquilla: El usuario puede cerrar la taquilla tras su uso, registrando el evento en el sistema.
      4. Solicitar soporte: En caso de problemas con el acceso, el usuario puede pedir asistencia.
   2. Casos de Uso del Administrador:
      1. Gestionar usuarios: Dar de alta o baja a los usuarios en la plataforma.
      2. Asignar credenciales: Configurar tarjetas RFID, datos biométricos o credenciales móviles.
      3. Monitorear accesos: Consultar registros de apertura/cierre y detectar posibles incidencias.
      4. Configurar horarios: Establecer horarios de acceso y restricciones según políticas de seguridad.
      5. Consultar bloqueos: Revisar taquillas bloqueadas o accesos fallidos por intentos no autorizados.
   3. Casos de Uso del API:
      1. Validar credenciales: Comprobar la autenticidad de los datos de acceso.
      2. Registrar eventos: Guardar en la base de datos cada apertura y cierre.
      3. Enviar alertas: Notificar al administrador en caso de intentos de acceso fallidos o actividades sospechosas.
      4. Actualizar cerraduras: Aplicar nuevas configuraciones de software y firmware a los dispositivos.

Diagrama

El contenido generado por IA puede ser incorrecto.

# **Conclusión**

Esta solución de cerradura biométrica sin contacto mejora la seguridad y comodidad en comparación con los sistemas tradicionales. Al eliminar la necesidad de tocar el sensor, se evitan problemas de higiene y desgaste, mientras que la integración con tarjetas RFID y dispositivos móviles hace que el acceso sea más versátil.

El diseño combina tecnología mecánica, electrónica y de software para garantizar un funcionamiento eficiente y seguro. Con pruebas rigurosas de resistencia, funcionalidad y seguridad, se ha validado su rendimiento en distintos entornos y condiciones.

Gracias a la retroalimentación de usuarios en escenarios reales, se han hecho mejoras para optimizar su uso antes de lanzarlo al mercado. En resumen, esta solución es una alternativa moderna y práctica para la gestión de accesos.