

SISTEMA DE CONTROL DE ACCESO DISTRIBUIDO Y EN LA NUBE

DATOS DE CONTACTO:

Relaciones con la Empresa
Oficina de Transferencia de Resultados de la Investigación-OTRI
Universidad de Alicante
Tel.: +34 96 590 99 59
Email: areaempresas@ua.es
<http://innoua.ua.es>

RESUMEN

Investigadores de la Universidad de Alicante han desarrollado un sistema de control de acceso de nueva generación, basado en una arquitectura de Internet de las cosas (IoT) y soportado en la nube, que permite gestionar de forma segura y flexible los accesos a estancias físicas en cualquier tipo de organización.

La solución ofrece interoperabilidad con dispositivos y plataformas de distintos fabricantes, soporte de múltiples tecnologías de identificación (tarjetas, biometría, móviles), monitorización en tiempo real y administración centralizada de permisos.

Su carácter modular y abierto facilita la incorporación de nuevas tecnologías y la conexión con sistemas existentes, garantizando un despliegue escalable, seguro y más económico que los sistemas convencionales.

La tecnología es especialmente adecuada para corporaciones, infraestructuras críticas, centros de investigación, hospitales, universidades, edificios de oficinas o espacios comerciales.



INTRODUCCIÓN

El control de accesos constituye un elemento esencial en la gestión de la seguridad de cualquier organización. Su objetivo es asegurar que únicamente las personas autorizadas puedan entrar en determinadas áreas, al tiempo que se garantiza un registro continuo de los movimientos.

En el mercado actual existen diferentes soluciones, que van desde sistemas sencillos de carácter local hasta plataformas centralizadas dirigidas a grandes empresas o instituciones. No obstante, estas soluciones presentan limitaciones notables.

En muchos casos, se trata de arquitecturas cerradas, desarrolladas por fabricantes que restringen la interoperabilidad y encarecen las ampliaciones futuras. La inversión inicial y los costes de mantenimiento suelen ser elevados, lo que dificulta su implantación en organizaciones de tamaño medio o reducido. Asimismo, el uso exclusivo de credenciales físicas, como tarjetas o llaveros, limita la comodidad de los usuarios y genera riesgos de pérdida, robo o suplantación.

Por otra parte, la escasa integración de estos sistemas con las plataformas de gestión empresarial impide extraer todo el potencial de la información generada en el control de accesos.

La tecnología desarrollada por los investigadores nace como respuesta a las limitaciones de los sistemas tradicionales. Su planteamiento se apoya en la lógica de las arquitecturas IoT, capaces de interconectar dispositivos de distinta naturaleza mediante protocolos estándar y abiertos, y en la gestión en la nube, que permite centralizar la administración de permisos y el análisis de datos.

De este modo, se consigue un sistema más flexible, seguro y económico, que ofrece a las organizaciones un control de accesos completamente adaptado a los retos actuales y a las necesidades futuras.



Fig 1. Dispositivo lector instalado

El sistema propuesto se estructura en distintas capas funcionales que trabajan de manera integrada.

- **Capa de dispositivos IoT.** Esta reúne los equipos de identificación y sensorización. Estos dispositivos incluyen lectores de tarjetas inteligentes, sensores biométricos, sistemas de reconocimiento facial y de huella, así como soluciones basadas en NFC, RFID, Bluetooth o WiFi. A ellos se suman los mecanismos de apertura y cierre de puertas, diseñados para actuar de manera automática en función de las credenciales detectadas, con posibilidad de intervención manual cuando sea necesario.
- **Capa de red.** Esta capa garantiza la comunicación entre los dispositivos y los servidores centrales. Se utiliza tecnologías inalámbricas y protocolos estándar, lo que facilita la interoperabilidad y elimina la necesidad de infraestructuras adicionales complejas. Gracias a ello, el sistema puede conectarse directamente con la nube, aumentando su eficiencia y reforzando la seguridad al reducir los puntos vulnerables de acceso.
- **Capa de apoyo a servicios y aplicaciones.** Esta capa presta capacidades genéricas y específicas a la ejecución de los servicios y aplicaciones, por ejemplo, capacidades de almacenamiento, de control de datos o de procesamiento.
- **Capa de negocio IoT.** Esta capa proporciona las aplicaciones IoT que presenta los servicios finales a los usuarios. Entre estos servicios se encuentran los servicios de administración, que gestiona los permisos de acceso a las distintas estancias y controlan el comportamiento ante situaciones de contingencia como incendios o evacuaciones, y los servicios de monitorización que ofrece cuadros de mando configurables que permiten visualizar la actividad registrada, generar informes históricos y establecer políticas de acceso basadas en perfiles de usuario.

La arquitectura prevé la integración con sistemas de gestión empresarial, tales como plataformas ERP, sistemas de control horario o soluciones de recursos humanos.

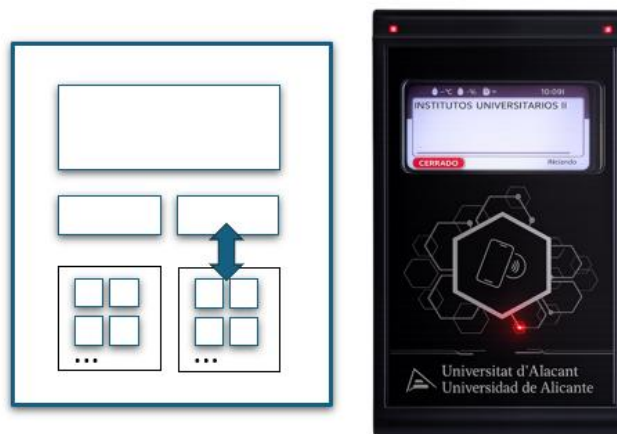


Fig 2. Dispositivo Sensor de Identidad (DI)



Fig 3. Arquitectura IoT para control de acceso distribuido

VENTAJAS Y ASPECTOS INNOVADORES

VENTAJAS DE LA TECNOLOGÍA

La tecnología presenta las siguientes ventajas:

- Permite interoperar con **sistemas y dispositivos de distintos fabricantes**, evitando la fragmentación y facilitando la integración en infraestructuras existentes.
- Soporta **múltiples tecnologías de identificación** (RFID, NFC, biométricos, móvil) y permite añadir nuevas sin modificar la arquitectura.
- La gestión centralizada en la nube actualiza **permisos en tiempo real**, reduciendo la necesidad de intervención manual en cada punto de acceso.
- Equipado con **batería de respaldo**, el sistema sigue funcionando al menos 15 minutos tras un corte de energía, garantizando la continuidad operativa.
- Al ser **modular y abierto**, el **coste** de despliegue y mantenimiento **se reduce** respecto a soluciones cerradas de fabricantes.
- Proporciona **datos en tiempo real** sobre accesos, mejorando la seguridad y permitiendo análisis estadísticos y auditorías eficientes.
- Se integra con **sistemas ERP** y de **gestión de recursos humanos**, facilitando la sincronización de permisos y registros de asistencia.

- Los dispositivos utilizan **modos de reposo y bajo consumo**, optimizando el gasto energético y prolongando la vida útil de la batería.

ASPECTOS INNOVADORES DE LA TECNOLOGÍA

El sistema combina una **arquitectura IoT abierta y modular** que integra dispositivos de apertura motorizada, control local y remoto, y una base de datos local para operar sin conexión.

Permite **múltiples modos de identificación** (tarjeta, etiqueta, biométrico, móvil con app y PIN) y soporta comunicación por RFID, NFC, Bluetooth, Wi-Fi y Wi-Fi Direct, lo que facilita la interoperabilidad con equipos de distintos fabricantes.

La solución incluye **baterías de respaldo, sincronización temporal y gestión de fallos**, y permite actualizaciones remotas y la integración de nuevas tecnologías sin reconfigurar la infraestructura.

Esta **flexibilidad, seguridad reforzada** y la capacidad de **monitorizar en tiempo real** distinguen la tecnología de los sistemas de control de acceso tradicionales.

ESTADO ACTUAL

La tecnología se encuentra desarrollada a escala de prototipo funcional y se han evaluado la operatividad del sistema, las conexiones con distintos dispositivos y la integridad de los datos comunicados.

APLICACIONES DE LA OFERTA

El sistema de control de acceso es aplicable en entornos laborales de cualquier tipo y tamaño independientemente del número de trabajadores y de estancias que deban ser controladas.

Por tanto, es de interés para empresas de construcción y arquitectura que puedan incorporar este tipo de tecnologías a sus soluciones constructivas. Y es de interés para su uso en empresas, edificios de oficinas, espacios comerciales o edificaciones de la administración como, por ejemplo, en el ámbito de la educación, la salud o instalaciones críticas.

COLABORACIÓN BUSCADA

Se buscan empresas interesadas en adquirir esta tecnología para su explotación comercial mediante acuerdos de licencia y acuerdos de desarrollo de proyectos de I+D (cooperación técnica) para emprender proyectos relacionados con la tecnología.

DERECHOS DE PROPIEDAD INTELECTUAL

Esta tecnología se encuentra protegida mediante **solicitud de patente**.

- *Título de la patente: "Sistema de control de acceso".*
- *Número de solicitud: P202530602*
- *Fecha de solicitud: 27/06/2025*

SECTORES DE APLICACIÓN (3)

