DISTRIBUTED AND CLOUD-BASED ACCESS CONTROL SYSTEM

DATOS DE CONTACTO:

Research Results Transfer Office-OTRI
University of Alicante
Tel.: +34 96 590 99 59
Email: areaempresas@ua.es
http://innoua.ua.es

RESUMEN

Researchers at the University of Alicante have developed a new-generation access control system based on Internet of Things (IoT) architecture and supported in the cloud, which allows secure and flexible management of access to physical spaces in any type of organization.

The solution offers interoperability with devices and platforms from different manufacturers, support for multiple identification technologies (cards, biometrics, mobile devices), real-time monitoring, and centralized permission management.

Its modular and open nature facilitates the incorporation of new technologies and integration with existing systems, ensuring a scalable, secure, and more cost-effective deployment compared to conventional systems.

The technology is particularly suitable for corporations, critical infrastructures, research centers, hospitals, universities, office buildings, or commercial spaces.



INTRODUCCIÓN

Access control is an essential element in the security management of any organization. Its purpose is to ensure that only authorized individuals can enter specific areas, while also guaranteeing continuous logging of movements.

The current market offers a wide range of solutions, from simple local systems to centralized platforms designed for large companies or institutions. However, these solutions present significant limitations.

In many cases, they rely on closed architectures developed by manufacturers that restrict interoperability and increase the cost of future expansions. Initial investment and maintenance costs are often high, making their adoption difficult for small and medium-sized organizations. Additionally, the exclusive use of physical credentials, such as cards or key fobs, limits user convenience and introduces risks of loss, theft, or impersonation.

Furthermore, the limited integration of these systems with enterprise management platforms prevents organizations from fully exploiting the potential of the data generated by access control systems.

DESCRIPCIÓN TÉCNICA

The technology developed by the researchers was conceived in response to the limitations of traditional systems. Its approach is

based on IoT architectures capable of interconnecting devices of different natures through standard and open protocols, combined with cloud-based management that enables centralized permission administration and data analysis.

This results in a more flexible, secure, and cost-effective system that provides organizations with access control fully adapted to current challenges and future needs.



Fig. 1. Installed reader device

The proposed system is structured into several functional layers that operate in an integrated manner:

- **IoT Device Layer.** This layer includes identification and sensing equipment such as smart card readers, biometric sensors, facial and fingerprint recognition systems, as well as solutions based on NFC, RFID, Bluetooth, or Wi-Fi. It also incorporates door opening and locking mechanisms designed to operate automatically according to detected credentials, with the possibility of manual intervention when required.

- **Network Layer.** This layer ensures communication between devices and central servers. It relies on wireless technologies and standard protocols, facilitating interoperability and eliminating the need for complex additional infrastructures. As a result, the system can connect directly to the cloud, improving efficiency and enhancing security by reducing vulnerable access points.

- **Service and Application Support Layer.** This layer provides generic and specific capabilities to support the execution of services and applications, such as data storage, data control, and processing capabilities.

- **IoT Business Layer.** This layer delivers the IoT applications that present end-user services. These include administration services that manage access permissions to different areas and control system behavior in contingency situations such as fires or evacuations, as well as monitoring services that provide configurable dashboards for visualizing recorded activity, generating historical reports, and establishing access policies based on user profiles.

The architecture foresees integration with enterprise management systems such as ERP platforms, time and attendance systems, and human resources solutions.

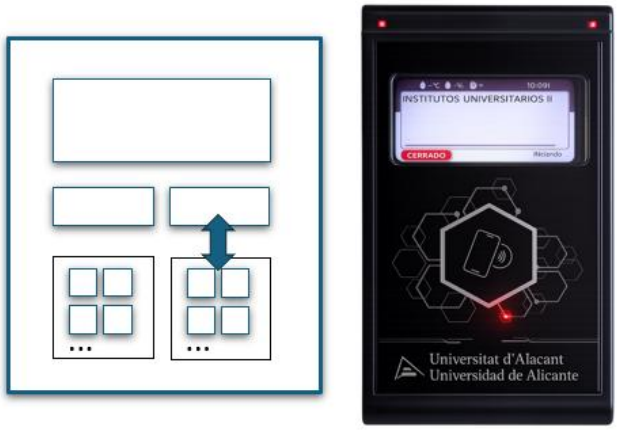


Fig 2. Identity Sensor Device (ID)



Fig 3. IoT architecture for distributed access control

VENTAJAS Y ASPECTOS INNOVADORES

MAIN ADVANTAGES OF THE TECHNOLOGY

The technology offers the following advantages:

- Enables interoperability with **systems and devices from different manufacturers**, avoiding fragmentation and facilitating integration into existing infrastructures.
- Supports **multiple identification technologies** (RFID, NFC, biometrics, mobile devices) and allows new technologies to be added without modifying the architecture.
- Centralized cloud-based management updates **permissions in real time**, reducing the need for manual intervention at each access point.
- Equipped with **backup batteries**, the system continues operating for at least 15 minutes after a power outage, ensuring operational continuity.
- Its **modular and open** design **reduces** deployment and maintenance **costs** compared to closed proprietary solutions.
- Provides **real-time access data**, improving security and enabling efficient statistical analysis and audits.
- Integrates with **ERP and human resources management systems**, facilitating synchronization of access permissions and attendance records.

- Devices operate in **sleep and low-power modes**, optimizing energy consumption and extending battery life.

INNOVATIVE ASPECTS

The system combines an **open and modular IoT architecture** integrating motorized opening devices, local and remote control, and a local database that allows offline operation.

It supports **multiple identification modes** (card, tag, biometric, mobile app with PIN) and communication via RFID, NFC, Bluetooth, Wi-Fi, and Wi-Fi Direct, enabling interoperability with equipment from different manufacturers.

The solution includes **backup batteries, time synchronization, and fault management**, and allows remote updates and the integration of new technologies without reconfiguring the infrastructure.

This **flexibility**, **enhanced security**, and **real-time monitoring** capability clearly differentiate the technology from traditional access control systems.

ESTADO ACTUAL

The technology has been developed at the level of a functional prototype. System operability, connectivity with different devices, and the integrity of transmitted data have been evaluated.

APLICACIONES DE LA OFERTA

The access control system is applicable to work environments of any type and size, regardless of the number of employees or controlled areas.

It is therefore of interest to construction and architecture companies seeking to incorporate this type of technology into their building solutions, as well as for use in companies, office buildings, commercial spaces, or public administration facilities, such as those in education, healthcare, or critical infrastructure environments.

COLABORACIÓN BUSCADA

The researchers are seeking companies interested in acquiring this technology for commercial exploitation through licensing agreements, as well as R&D project development agreements (technical cooperation) to undertake projects related to the technology.

DERECHOS DE PROPIEDAD INTELECTUAL

This technology is protected through a **patent application**.

- *Patent title: "Sistema de control de acceso"."*
- *Application number: P202530602*
- *Application date: 27/06/2025*

SECTORES DE APLICACIÓN (3)

Construction and Architecture
Computer Science, Language and Communication
Engineering, Robotics and Automation