RFID-BASED IoT SYSTEM FOR WIRELESS IDENTIFICATION

Milan Vesković[1], Veljko Ćorić[2], Srđan Nogo[3]

[1]University of Kragujevac, Faculty of Technical Sciences in Čačak, Svetog Save 65, 32000 Čačak, Serbia, milan.veskovic@ftn.kg.ac.rs
[2]Technical School Čačak, cara Dušana, 32000 Čačak, Serbia
[3]University of East Sarajevo, Faculty of Electrical Engineering, Vuka Karadžića 30, 71123 East Sarajevo, Bosnia and Herzegovina

PROFESSIONAL PAPER

Received: 18 September 2026.
Accepted: 12 October 2026.
Published: 16 November 2026.
DOI: https://doi.org/10.63395/STEDConf15022026142V297

Corresponding Author: University of Kragujevac, Faculty of Technical Sciences in Čačak, Svetog Save 65, 32000 Čačak, Serbia, milan.veskovic@ftn.kg.ac.rs

Copyright © 2026 Milan Vesković et al.; published by UNIVERSITY PIM. This work licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.

Citation: Vesković, M. et al. (2026). Rfid-based IoT system for wireless identification. In Kojić, D. & Sredić. D. (eds.) *Conference proceedings, XV International Conference on Social and Technological Development: STED 2026* (pp. 297-306). Trebinje, B&H: University PIM.

ABSTRACT

This paper examines the development and application of integrated circuits for wireless communication in IoT networks, with a particular focus on their role in the design and implementation of practical low-power systems. The theoretical part of the paper addresses the fundamental concepts of IoT architecture, the principles of wireless communication, and the role of integrated communication circuits in device connectivity, data acquisition, and remote system control. Special attention is devoted to the analysis of the characteristics of low-power microcontrollers and communication modules, as well as their application in smart infrastructure solutions.

The practical part of the paper includes the design and implementation of a toll-gate system prototype based on the Arduino UNO R3 platform, representing an example of an IoT device with wireless user identification. The system uses an RFID integrated circuit for contactless communication and authentication, a servo motor for mechanical barrier control, and an LCD display for user interaction. Before the physical prototype was implemented, a system simulation was developed in the Tinkercad environment, enabling verification of the operating logic, sequence of actions, and system behaviour under controlled conditions.

Based on the simulation, a physical prototype was developed, confirming the correctness of communication between the integrated circuits, as well as the functionality of the system under real operating conditions. The obtained results show that it is possible to implement a embedded identification system using simple and widely available integrated circuits. The paper emphasizes the importance of integrating hardware and software components in the development of IoT solutions and indicates the potential application of such systems in smart traffic and automated infrastructure.

Keywords: Internet of Things, low-power integrated circuits, System-on-Chip, duty cycling, energy efficiency.

INTRODUCTION

The rapid evolution of integrated circuits and wireless communication technologies has significantly transformed the development of modern Internet of Things (IoT) systems [1], [3]. IoT represents a paradigm in which physical devices are interconnected through communication networks, enabling data exchange, remote monitoring, and automated control without direct human intervention [1], [2]. This technological concept has become a fundamental foundation for smart environments, including intelligent transportation systems, industrial automation, and security infrastructures [3].

A key aspect of IoT systems is the integration of efficient wireless communication modules and embedded processing units within a single system architecture [2], [3]. These integrated communication circuits, often implemented as system-on-chip (SoC) solutions, enable reliable data transmission while maintaining low power consumption and high scalability [3]. Their role is crucial in sensor networks, where large numbers of devices must operate under energy constraints and limited computational resources [5].

Among various IoT applications, radio frequency identification (RFID) technology has emerged as a widely used solution for automated identification and access control systems [3], [6]. RFID enables contactless communication between a reader and a tag, providing fast and reliable identification of users or objects [6]. Due to its simplicity, low cost, and high efficiency, RFID technology is commonly applied in access control systems such as parking management, toll gates, and secure facility entry systems [6].

This paper presents the design and implementation of an RFID-based IoT system for wireless identification and automated vehicle access control. The developed system integrates a microcontroller-based processing unit, an RFID reader module, a servo motor for mechanical barrier control, and an LCD display for real-time user feedback. The system is designed as a low-cost embedded solution that demonstrates the practical application of integrated communication circuits in IoT environments [3].

A toll gate scenario is implemented as a case study to validate the proposed system architecture. The system was first developed and tested in a simulation environment, followed by the construction of a physical prototype. The results confirm the reliability of the system in performing real-time identification and automated control tasks, demonstrating its potential application in smart transportation and infrastructure systems.

The main contribution of this work is the practical demonstration of how integrated communication circuits can be combined with embedded processing units to develop a functional and cost-effective IoT-based access control solution.

FUNDAMENTALS OF WIRELESS COMMUNICATIONS IN IOT NETWORKS

Wireless communication represents the fundamental enabling technology for modern Internet of Things (IoT) systems. It allows interconnected devices to exchange data without physical wiring, thereby enabling flexible, scalable, and distributed system architectures [1], [3]. In IoT environments, wireless communication is used to connect embedded devices, sensors, and processing units into a unified network capable of real-time monitoring, control, and automation [2].

The IoT concept is based on the integration of physical devices with network connectivity and data processing capabilities. This integration enables systems to operate autonomously with minimal human intervention [1], [2]. As a result, IoT technologies are widely applied in smart environments such as intelligent transportation systems, industrial automation, healthcare monitoring, and security systems [3].

As illustrated in Figure 1, a typical IoT system is organized into four functional layers, each responsible for a specific task in data acquisition, communication, processing, and user interaction [2], [3]. The lowest layer is the sensing layer, which is responsible for data acquisition from the physical environment. This layer includes sensors and identification technologies such as Radio Frequency Identification (RFID). RFID systems enable contactless identification of objects or users through radio frequency signals and are widely used in access control and tracking applications [6]. The communication between the RFID reader and tag is based on electromagnetic

coupling, where the reader generates a radio frequency field that enables energy transfer and data exchange with the RFID tag.

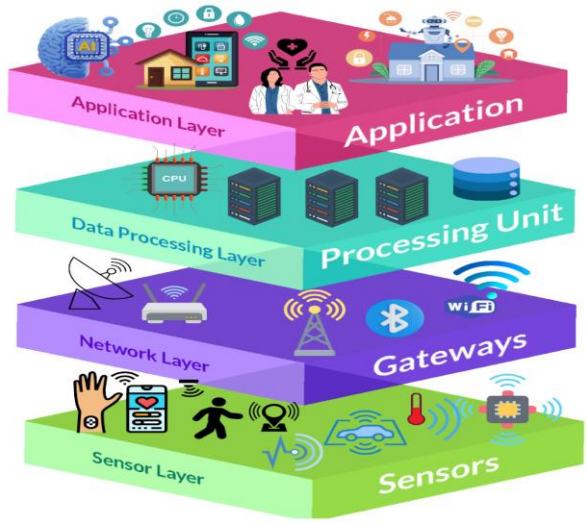


Figure 1. Four-layer architecture of an Internet of Things (IoT) system

In this work, RFID technology is used as the primary method for user identification in automated toll-gate system. Above the sensing layer is the communication layer, which ensures reliable data transmission between devices. Depending on system requirements, different wireless technologies can be applied, such as Wi-Fi, Bluetooth, Zigbee, and other low-power communication protocols [4], [5]. The choice of communication technology depends on factors such as transmission range, data rate, power consumption, and overall system reliability.

The processing layer is responsible for analyzing incoming data and executing appropriate control actions. This layer is typically implemented using microcontrollers or embedded processing units capable of running real-time control algorithms [3]. In the proposed system, a microcontroller processes RFID input data, verifies user authorization, and controls actuators such as servo motors for barrier operation.

The application layer represents the interface between the system and the end user. It provides real-time feedback and system status information through displays or user interfaces. In access control systems, this layer is responsible for displaying messages such as access granted or access denied, thereby improving usability and system transparency [2].

Wireless communication in IoT systems is characterized by several key parameters that directly affect system performance. One of the most important factors is transmission range, which defines the distance over which devices can communicate reliably. Short-range communication technologies are typically used in localized systems such as access control, while long-range technologies are used in wide-area IoT deployments [4], [5].

Another important characteristic is data rate, which determines how much information can be transmitted within a given time interval. IoT systems generally do not require extremely high data rates but rather prioritize stable and efficient communication. Closely related to this is power consumption, which is a critical constraint in embedded and battery-powered IoT devices. Low-power operation is essential for ensuring long-term system functionality and reducing maintenance requirements [5].

Reliability is also a key factor in wireless communication systems, as it ensures consistent data transmission and minimizes errors caused by interference or signal degradation. In practical IoT implementations, reliability is achieved through robust hardware design and communication protocols capable of handling unstable network conditions [3].

In addition to these characteristics, IoT systems must satisfy several fundamental requirements. Massive connectivity is necessary to support many interconnected devices within a

single network. Scalability ensures that the system can be expanded without significant degradation in performance. Security is another essential requirement, as IoT systems often handle sensitive identification and control data. Therefore, proper authentication mechanisms and secure communication strategies are critical for system integrity [3], [6].

INTEGRATED CIRCUITS FOR WIRELESS COMMUNICATION

Integrated circuits (ICs) represent the core hardware components that enable modern wireless communication systems. In the context of Internet of Things (IoT), these circuits integrate processing units, memory, and communication interfaces into compact and energy-efficient modules [3]. Their development has significantly contributed to the miniaturization, reliability, and scalability of embedded systems used in smart applications [1], [3].

In IoT environments, integrated communication circuits are responsible for acquiring, processing, and transmitting data between devices. These circuits are commonly implemented as microcontrollers, communication modules, or system-on-chip (SoC) solutions that combine multiple functional units within a single silicon platform [3]. The integration of such components allows the design of low-cost and energy-efficient systems suitable for large-scale deployment [2], [5].

A widely used example of an embedded processing IC is a microcontroller-based platform, such as the Arduino family. These platforms provide a simple development environment for interfacing sensors, actuators, and communication modules. In this work, an Arduino Uno R3 microcontroller is used as the central processing unit responsible for managing system operations, including RFID data processing and actuator control. A practical example of an integrated processing platform used in IoT applications is shown in Figure 2. The Arduino Uno R3 combines a microcontroller unit with digital and analog interfaces, enabling simple integration with sensors, actuators, and communication modules.



Figure 2. Arduino Uno R3 microcontroller platform used for embedded IoT applications

The Arduino Uno R3 is based on the ATmega328P microcontroller, operating at a clock frequency of 16 MHz and powered by a 5 V supply. It provides 14 digital input/output pins, including six Pulse Width Modulation (PWM) outputs, and six analog input channels with a 10-bit analog-to-digital converter (ADC). The board also incorporates UART, SPI, and I²C communication interfaces, enabling efficient integration with various sensors, actuators, and peripheral communication modules [11]. These features make the Arduino Uno R3 a suitable platform for rapid prototyping and the development of low-cost IoT applications [3]. Due to its open-source architecture, extensive software support, and compatibility with numerous sensors and communication modules, the Arduino Uno R3 is widely used for educational, research, and prototype development purposes.

In the proposed system, the Arduino Uno R3 communicates with the MFRC522 RFID reader through the Serial Peripheral Interface (SPI), a synchronous communication protocol designed for fast and reliable data exchange between embedded devices [11]. The SPI interface supports clock frequencies of up to 8 MHz on the Arduino Uno platform, enabling rapid transmission of RFID identification data with minimal communication latency. This high-speed interface allows the

microcontroller to process authentication requests in real time and control peripheral devices immediately after user identification.

Another important integrated component used in IoT systems is the Radio Frequency Identification (RFID) module. RFID systems consist of a reader and a passive or active tag, where communication is established through electromagnetic induction or radio waves [6]. In the proposed system, the MFRC522 RFID reader operates at a carrier frequency of 13.56 MHz and complies with the ISO/IEC 14443 Type A standard [12]. Under typical operating conditions, the communication range extends up to approximately 5 cm, allowing fast contactless identification within a few milliseconds [12]. Due to its simplicity, reliability, and low implementation cost, RFID technology is widely adopted in access control systems, parking management, and automated identification applications [6]. An example of the RFID reader module used in the proposed system is shown in Figure 3.

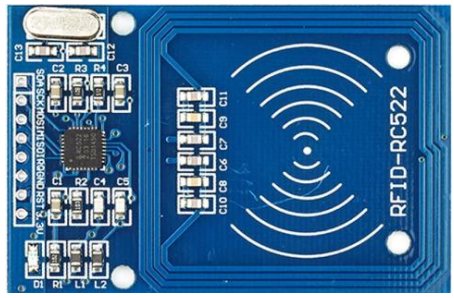


Figure 3. MFRC522 RFID reader module used for wireless identification

After detecting an RFID tag, the MFRC522 reader transfers the unique identification number (UID) to the Arduino Uno through the SPI interface. The microcontroller compares the received UID with the list of authorized identifiers stored in its memory and executes the corresponding control algorithm. If authentication is successful, a control signal is generated to activate the servo motor, while the LCD display simultaneously provides visual feedback to the user regarding the access status. This integration of identification, processing, and actuation represents a typical architecture of embedded IoT-based access control systems [3], [6].

In addition to microcontrollers and RFID modules, modern IoT systems increasingly rely on wireless communication chips such as Wi-Fi and Bluetooth modules [3], [4]. These modules can be integrated directly into microcontroller boards or implemented as standalone communication ICs. They enable connectivity with external networks and cloud-based services, extending the functionality of embedded systems beyond local operation [3].

System-on-chip (SoC) architectures represent a further advancement in integrated circuit design. SoC solutions combine processing units, memory, and communication interfaces into a single chip, significantly improving performance while reducing power consumption and physical size [3]. Such architectures are particularly suitable for large-scale IoT deployments where efficiency and scalability are critical [2], [3]. An example of a System-on-Chip architecture is illustrated in Figure 4, where processing units, memory, communication interfaces, and peripheral modules are integrated into a single semiconductor device.

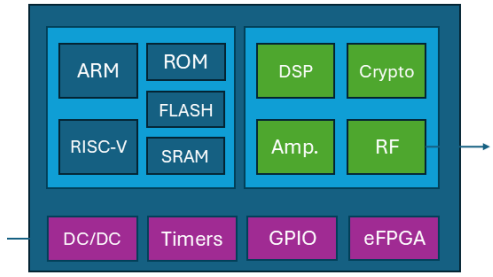


Figure 4. Internal architecture of a System-on-Chip (SoC) device

The selection of appropriate integrated circuits in IoT system design directly affects system performance, including power consumption, processing capability, communication range, and overall reliability. Therefore, careful consideration of hardware components is essential when designing embedded IoT solutions.

DEVELOPMENT AND IMPLEMENTATION OF COMMUNICATION ICs IN IoT DEVICES

The development of IoT systems relies heavily on the practical implementation of integrated communication circuits within embedded platforms. This stage of system design focuses on combining hardware components and software algorithms into a functional architecture capable of performing real-time data acquisition, processing, and control [3].

In modern IoT applications, communication integrated circuits are embedded into sensor nodes and embedded controllers to enable efficient interaction between physical devices and digital systems. These circuits must ensure low power consumption, reliable communication, and fast response times to support real-time applications such as access control, monitoring, and automation [2], [3].

A typical IoT device consists of a processing unit, communication module, input sensors, and output actuators. The processing unit is responsible for executing control logic, while communication modules handle data exchange between devices or external systems. Sensors provide input data from the environment, and actuators perform physical actions based on system decisions [2].

In the implemented system, an Arduino Uno R3 microcontroller serves as the central processing unit responsible for coordinating all system operations. The system uses an RFID reader module for wireless identification, where each RFID tag contains a unique identifier used for user authentication. Once the identifier is read, it is processed by the microcontroller, which determines whether access should be granted or denied based on predefined logic.

If the authentication process is successful, the system activates a servo motor that simulates a barrier mechanism. At the same time, an LCD display provides real-time feedback to the user by displaying system status messages such as “Access Granted” or “Access Denied”. This ensures clear communication between the system and the user.

Before physical implementation, the system logic was verified using a simulation environment. This allowed validation of communication flow, control algorithms, and component interaction without the risk of hardware damage. After successful simulation testing, a physical prototype was constructed and tested under real operating conditions.

The implementation demonstrates how integrated circuits can be effectively combined within IoT architectures to create low-cost, reliable, and scalable embedded systems. The proposed solution highlights the importance of proper hardware-software integration in achieving efficient system performance [3].

EXPERIMENTAL PART – CASE STUDY: TOLL GATE SYSTEM

This section presents the experimental implementation of the proposed IoT-based system for wireless identification and automated access control. The case study is designed to demonstrate the practical application of integrated communication circuits in a real embedded environment [3].

The developed system simulates a toll gate scenario where users are identified using RFID technology, and access is granted or denied based on authorization. RFID-based identification is widely used in automated access control applications due to its contactless operation, reliability, and fast data exchange capabilities [6]. The system is built using an Arduino Uno R3 microcontroller as the central processing unit, which coordinates all input and output operations. The RFID reader module is responsible for detecting and reading unique identifiers from RFID cards, while a servo motor is used to simulate a physical barrier mechanism. An LCD display provides real-time feedback to the user regarding system status.

System Operation Principle

The operation of the system is based on a sequential process. When an RFID card is brought close to the reader, the RFID module captures the unique identifier and sends it to the microcontroller. The Arduino then compares the received identifier with a predefined list of authorized users stored in memory.

If the identifier matches an authorized entry, the system triggers the servo motor to open the barrier, allowing vehicle passage. Simultaneously, the LCD display shows a message indicating successful authentication. After a predefined time interval, the system automatically returns the servo motor to its initial position, simulating barrier closure.

In cases where the RFID tag is not recognized, the system denies access and displays an appropriate message on the LCD screen. This ensures secure and controlled access to the system.

Simulation Environment

Before building the physical prototype, the system was designed and tested using a simulation environment. The simulation allowed verification of system logic, component interaction, and control flow under controlled conditions. This step was essential for identifying potential errors in the system design before hardware implementation.

The simulation confirmed correct operation of RFID-based identification, microcontroller processing, and actuator control. It also demonstrated that the system logic behaves as expected in both authorized and unauthorized access scenarios.

The simulation model was developed in the Tinkercad simulation environment, where the main system components and their interactions were virtually implemented and tested. The developed Tinkercad simulation is presented in the following figure.

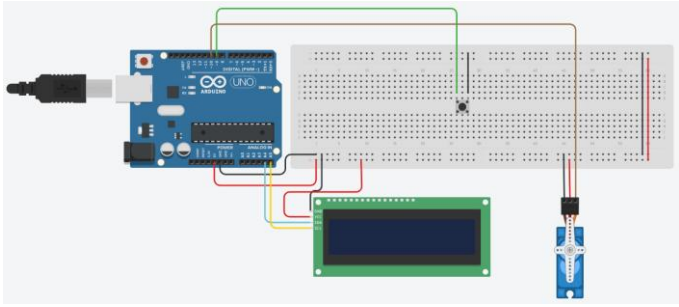


Figure 5. Tinkercad simulation

Physical Prototype and Toll-Gate Implementation

The physical prototype represents the final implementation of the proposed system. It is built using the same architecture validated in the simulation phase. The hardware components are interconnected to form a functional embedded system capable of real-time operation.

The system demonstrates stable performance in detecting RFID tags, processing data, and controlling the servo motor. The LCD display provides clear and immediate feedback to the user, improving system usability and transparency.

The experimental results confirm that the proposed design is suitable for low-cost automated access control applications, such as parking systems, secure facilities, and toll gate infrastructure.

The wiring diagram of the implemented physical prototype, including the connections between the Arduino Uno microcontroller, RFID reader, LCD display, and servo motor, is shown in the following figure.

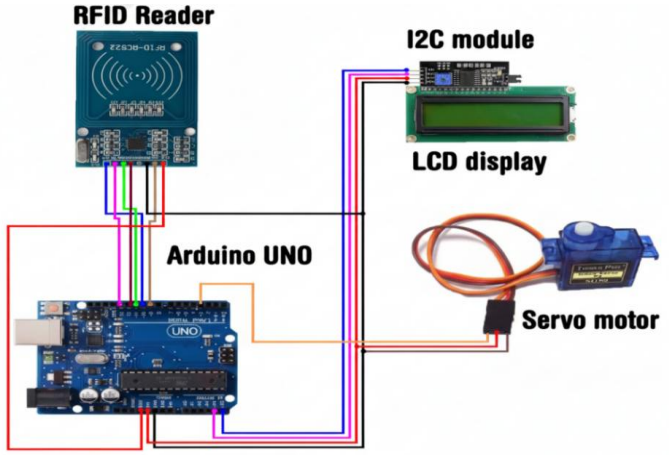


Figure 6. Wiring diagram of the physical prototype

The final physical realization of the proposed RFID-based toll-gate system is presented in Figure 7. The implemented prototype integrates all previously described hardware components, including the Arduino Uno R3 microcontroller, MFRC522 RFID reader, LCD display, and servo motor mechanism. The assembled system demonstrates the practical operation of the proposed IoT architecture, where RFID-based identification is processed by the microcontroller and converted into an automated access control action. The prototype successfully represents the transition from simulation to real hardware implementation and confirms the feasibility of the developed low-cost embedded solution.

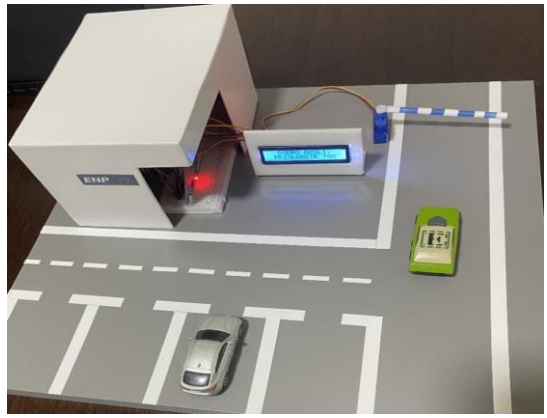


Figure 7. Implemented physical prototype of the RFID-based toll-gate system

DISCUSSION

The implemented RFID-based IoT system demonstrates a functional and efficient approach to automated access control using low-cost embedded components. The combination of an Arduino Uno R3 microcontroller, RFID reader module, servo motor, and LCD display enables a complete closed-loop system capable of real-time identification and response.

One of the key advantages of the proposed system is its simplicity and reliability. The RFID-based identification process is fast and stable, allowing near-instant user recognition. This makes the system suitable for real-time applications such as toll gates, parking systems, and secured entry points [6]. The use of microcontroller-based architecture ensures deterministic behavior and low latency in decision-making processes.

From a performance perspective, the system operates with minimal delay between RFID detection and actuator response. The servo motor provides a clear mechanical representation of

access control, while the LCD display improves user interaction by providing immediate system feedback. This combination of visual and physical response enhances system transparency and usability.

However, the system also has certain limitations. The RFID technology used in this implementation has a limited reading range, typically only a few centimeters, which restricts its use to close-proximity applications. Additionally, basic RFID systems without advanced security mechanisms may be vulnerable to cloning or unauthorized duplication, which represents an important consideration in high-security environments [6].

Another limitation is the absence of a full IoT backend or cloud integration in the implemented prototype. Although the system is conceptually aligned with IoT principles, its current implementation operates locally without remote monitoring or data storage capabilities. This reduces its scalability in large distributed systems.

Despite these limitations, the system provides a strong foundation for future enhancements. Possible improvements include integration with Wi-Fi or cellular communication modules, cloud-based user authentication, and database logging of access events. These upgrades would significantly increase system functionality and enable real-world deployment in smart infrastructure environments [3].

In comparison with traditional manual access control systems, the proposed solution offers improved automation, reduced human involvement, and increased operational efficiency. The use of embedded integrated circuits ensures low-cost implementation while maintaining acceptable levels of performance and reliability.

Overall, the results confirm that RFID-based IoT systems represent a practical and scalable solution for modern access control applications, especially in environments where cost efficiency and simplicity are primary requirements [3], [6].

CONCLUSION

This paper presented the design and implementation of an RFID-based IoT system for wireless identification and automated access control. The proposed system integrates an Arduino Uno R3 microcontroller, an MFRC522 RFID reader module, a servo motor, and an LCD display to achieve a simple and functional model of an automated toll gate system.

The main objective of the work was to demonstrate how integrated communication circuits and embedded systems can be combined to create a low-cost and efficient solution for real-time identification and access control. The implemented system successfully performs user identification through RFID technology, processes authentication data using a microcontroller, and executes physical access control through a servo motor mechanism.

The results obtained from both simulation and physical prototype testing confirm that the system operates reliably under real-time conditions. The system responds quickly to RFID input, provides clear user feedback through the LCD display, and accurately controls the barrier mechanism. This confirms the practicality of using simple embedded IoT architectures for access control applications.

The validation of the proposed system was performed through simulation and physical prototype implementation. During experimental operation, the system successfully detected authorized and unauthorized RFID tags, executed the corresponding access control logic, and provided appropriate feedback through the LCD display. These observations confirm the correct interaction between the RFID communication module, microcontroller-based processing unit, and actuator components, demonstrating the functionality of the proposed embedded IoT solution.

Although the current implementation operates as a standalone system without cloud connectivity, it provides a solid foundation for future improvements. Potential enhancements include integration with wireless communication modules, cloud-based data storage, and real-time monitoring systems. These improvements would enable scalability and deployment in larger smart infrastructure environments.

In conclusion, the developed system demonstrates that RFID-based IoT solutions can provide effective, reliable, and cost-efficient alternatives to traditional access control mechanisms. The

integration of hardware and software components highlights the importance of embedded systems in the development of modern intelligent infrastructure.

ACKNOWLEDGEMENTS
This research was supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under Grant No. 451-03-34/2026-03/200132, implemented at the University of Kragujevac, Faculty of Technical Sciences in Čačak.

DECLARATIONS OF INTEREST STATEMENT

The authors affirm that there are no conflicts of interest to declare in relation to the research presented in this paper.

LITERATURE

1. Univerzitet Crne Gore. (n.d.). *Uvod u Internet stvari i IoT*. PDF dokument. Available at: https://www.ucg.ac.me/skladiste/blog_43268/objava_76411/fajlovi/TM_IoT.pdf [accessed: 8 January 2026].
2. Univerzitet Crne Gore. (2025). *IoT arhitektura*. PDF dokument. Available at: https://www.ucg.ac.me/skladiste/blog_615384/objava_202159/fajlovi/2_IOT_arhitektura_rev2025_.pdf [accessed: 8 January 2026].
3. Bhuiyan, M. Z. A., Hassan, M. F., Abdullah, M., et al. (2023). Internet of Things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions. *Energies*, 16(8), 3465. https://doi.org/10.3390/en16083465.
4. Islam, M., Jamil, H. M. M., & Pranto, S. A. (2023). Future industrial applications: Exploring LPWAN-driven IoT protocols. *arXiv preprint*. Available at: https://arxiv.org/abs/2310.09177 [accessed: 8 January 2026].
5. Raza, U., Kulkarni, P., & Sooriyabandara, M. (2016). Low power wide area networks: An overview. *arXiv preprint*. Available at: https://arxiv.org/abs/1606.07360 [accessed: 8 January 2026].
6. Hossain, M. S., Ghoneim, A., Elgendy, I. H., et al. (2022). Analysis on functionalities and security features of Internet of Things related protocols. *Wireless Networks*. Springer. https://doi.org/10.1007/s11276-022-02999-7.
7. Fakultet elektrotehnike. (2025). *Bežična komunikacija i IoT uređaji*. PDF materijal. Available at: https://elektronika.elfak.ni.ac.rs/wp-content/uploads/2025/07/1.-Bezicna-komunikacija-slajdovi.pdf [accessed: 8 January 2026].
8. CARNET. (n.d.). *Internet of Things priručnik*. IoT PDF vodič. Available at: https://edutorij-admin-api.carnet.hr/api/files/9b9dfb9c-4b85-4c5d-95d8-ea63992497ef/download/4443516/Internet%20of%20Things.pdf [accessed: 8 January 2026].
9. Drajić, D. D. (2017). *Uvod u IoT*. Beograd: Akademska misao. Available at: https://akademska-misao.rs/wp-content/uploads/2021/07/IoT-pregled.pdf [accessed: 25 January 2026].
10. Radenković, B., et al. (2017). *Internet inteligentnih uređaja*. Beograd: Fakultet organizacionih nauka, Univerzitet u Beogradu. Available at: https://id.fon.bg.ac.rs/uploads/documents/empire_plugin/Internet%20inteligentnih%20uredjaja%20preview.pdf [accessed: 8 January 2026].
11. Arduino. (2024). *Arduino Uno Rev3 Technical Specifications*. Arduino Documentation. Available at: https://docs.arduino.cc/hardware/uno-rev3 [accessed: 8 January 2026].
12. NXP Semiconductors. (2016). *MFRC522 Standard Performance MIFARE and NTAG Frontend*, Rev. 3.9. NXP Semiconductors. Available at: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf [accessed: 8 January 2026].