IoT-Based Anti-Theft Alarm Using Reed Switch and MQTT Protocol

Paula Luiza Rocha de Oliveira, Guilherme Pinto Weil Bastos, Gabriel Lacerda da Fontoura, Maria Giulia Pessanha, William Fagundes, and Rigel P. Fernandes, and Clayton J. A. Silva

***Abstract*— The objective of this project is to design an intelligent anti-theft system. The system employs a magnetic sensor to detect unauthorized openings. When the system is activated and an opening is detected, the system interprets this as a potential theft attempt and triggers an alarm using MQTT protocol. The user can disable the alarm using an RFID card or the front-end interface, ensuring it is only active when desired. The system detects openings with distances of 2 cm.**

***Keywords*— Anti-Theft, Alarm, Embedded Systems, Internet of Things, MQTT, Reed Switch, SBrT 2025.**

I. Introduction

Concerns regarding patrimonial security have grown significantly in recent decades, especially in large urban centers and public environments such as universities, workplaces, transportation systems, gyms, and events. Personal belongings such as handbags, suitcases, backpacks, lockers, and even work equipment have become increasingly vulnerable to theft, which has driven the demand for practical, affordable, and efficient protective solutions [1].

Although there are some anti-theft devices available on the market, many of these solutions are designed for specific applications, involve high costs, are bulky, or require complex infrastructure for installation and maintenance [2]. As a result, they are often unsuitable for users who seek simple, portable, and adaptable solutions for different contexts.

In this context, advances in the Internet of Things (IoT) and embedded systems offer new possibilities for the development of intelligent security solutions. IoT enables the integration of sensors, microcontrollers, and communication protocols, allowing for real-time monitoring and remote user notifications [3], [4]. Additionally, the miniaturization of electronic components and the widespread availability of platforms such as the ESP8266 make it possible to build portable, cost-effective, and easy-to-deploy systems.

Similar solutions have been explored in the literature. The study in [5] demonstrates the feasibility of embedded systems that combine RFID, magnetic sensors, and alert notifications through social media platforms such as Telegram. The work proposed in [6], advocates the use of an IoT-based solution to improve road safety and reduce traffic accidents. The system integrates multiple sensors (GPS, infrared, reed switch and alcohol detection sensors) into a vehicle onboard module that interacts with the road infrastructure through ESP32 microcontrollers. The work in [7], explores the creation of a modular relay protection system designed with open architecture and Industrial IoT integration. The study addresses the limitations of proprietary relay systems, which hinder module replacement and adaptability. The proposed solution uses reed switches, ESP32 microcontrollers, and open communication protocols to build a flexible, low-cost, and interoperable device with applications to power protection infrastructures.

In this project, we propose a generic anti-theft system that can be adapted to various scenarios, such as backpacks, handbags, drawers, lockers, and other personal storage compartments. Although the system was developed with a backpack use case in mind, its architecture is flexible and applicable to a wide range of situations. The solution uses a *reed switch* positioned near the closure to detect unauthorized openings. This event is processed by an ESP8266 microcontroller, which sends a real-time alert via the MQTT protocol to a remote device, while simultaneously activating a red LED and a buzzer for local signaling. An RFID module is also included, allowing authorized users to discreetly disable the alarm and prevent false positives.

The rest of this work is organized as follows. Section II gives an insight on anti-theft systems, focusing on reed switches and the MQTT protocol, while Section III details the system's implementation. Section IV describes the results found, and Section V concludes the work.

II. Anti-Theft Systems

Anti-theft systems are widely employed in various contexts, such as vehicle security, protection of doors and windows, and more recently, for personal belongings like backpacks and suitcases. These systems range from simple solutions using audible alarms to more sophisticated ones incorporating sensors and remote connectivity. The main types of anti-theft systems include: (1) Conventional audible alarms: trigger loud sounds when suspicious movement or unauthorized access is detected. (2) Magnetic sensors (reed switches): detect the separation between two parts (e.g., lid and base), commonly used in doors and windows. (3) Motion sensors (PIR): identify movement within monitored areas and are commonly used in residential environments. (4) RFID or smart tag systems: recognize authorized users and manage access control. (5) IoT-

Paula Luiza Rocha de Oliveira, Guilherme Pinto Weil Bastos, Gabriel Lacerda da Fontoura, Maria Giulia Pessanha, William Fagundes, and Rigel P. Fernandes, and Clayton J. A. Silva are affiliated with the Computer and the Software Engineering programs at the (Centro Universitário IBMEC, Rio de Janeiro, Brazil). Emails: paulalro8@gmail.com, gui.weil90@gmail.com, gabriellacerdadafontoura@gmail.com, mgpessanh@gmail.com, @gmail.com, rigelfernandes@gmail.com, clayton.silva@ibmec.edu.br.

based solutions (Wi-Fi, Bluetooth, LoRa, MQTT): send real-time alerts to remote devices, enabling monitoring via internet-connected applications [8]. (6) GPS-based systems: primarily used for tracking vehicles or valuable items, providing location data in case of theft.

A. Reed switch

The reed switch is a special type of electrical switch that operates using magnetic forces instead of direct physical contact to open or close an electrical circuit. It functions in two states: one when the magnet is close and the switch is closed, and the other when the magnet moves away, causing the switch to open.

The switch consists of two ferromagnetic blades enclosed in a small glass tube. When a magnet approaches, the blades attract and close the circuit. When the magnet is removed, the blades separate and the circuit opens.

Reed switches integrated with microcontrollers are frequently employed in low-cost residential security systems, particularly as sensors for doors and windows. Their key advantages include extremely low power consumption, high durability under environmental exposure, and zero mechanical wear due to the absence of direct physical contact [9].

B. MQTT Protocol

MQTT (Message Queuing Telemetry Transport) is a lightweight communication protocol designed for low-bandwidth and high-latency environments, widely used in IoT applications. Unlike HTTP, which is optimized for web browsing, MQTT is ideal for asynchronous communication between devices, such as smart lights and motion sensors.

In this project, MQTT is used to send real-time notifications to the user when the backpack is opened, enabling prompt response. Its low overhead and efficient publish/subscribe model make it well-suited for embedded systems focused on security and responsiveness.

III. The Method

To develop an efficient and low-cost solution for preventing the theft of personal belongings, a system based on magnetic sensors and MQTT communication was designed. This section outlines the methodology adopted to conceive and implement the system, detailing both the operational logic and the construction of the physical prototype.

The approach integrates simple sensors—such as reed switches and RFID—with embedded connectivity technology via the ESP8266 module, enabling real-time notifications and RFID-based control. The following subsections describe the system operation and the prototype configuration.

A. Proposed System

The system is designed to detect potential theft by identifying unauthorized opennigs. Although the current implementation targets backpacks, the system can be adapted for other applications such as doors and drawers. In this setup, a magnet is placed on one side of the zipper and a reed switch on the other. When the zipper is opened, the magnet moves away from the switch, triggering a notification via MQTT and activating a buzzer. The system is armed and disarmed using an RFID card held by the authorized user.

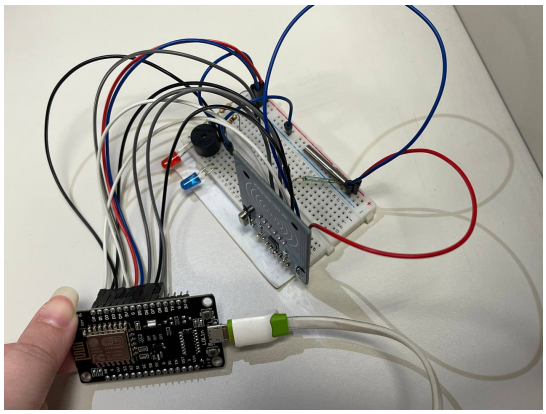


Fig. 1: Image of the assembled prototype.

B. Prototype

Figure 1 depicts the prototype that is composed of the following components: 1x Reed switch (magnetic sensor), 1x Small permanent magnet, 1x Red LED, 1x Blue LED, 1x 220Ω resistor, 1x Buzzer, 1x Breadboard, 1x ESP8266 microcontroller, 1x RFID-RC522 module, 1x RFID card, Jumper wires, USB power supply

As the system is activated using the RFID card, the blue LED turns on, indicating that the system is armed. With the magnet close to the reed switch, the red LED remains off, meaning the circuit is closed. If the magnet is moved away from the reed switch, the red LED turns on, indicating the backpack has been opened, the buzzer is triggered, and an MQTT message is sent to the broker. To disarm the system, the user must present the RFID card again, which turns off the blue LED and sends a disarm notification to the broker.

The microcontroller's embedded C code for the system comprises 157 lines. Based on current Brazilian market prices for the prototype components, including a 3.7V LiPo battery, the estimated system cost ranges from US20toUS45.

For prolonged operation, the ESP8266—the system's primary power consumer—utilizes two distinct modes: active and Deep Sleep. In active mode, particularly when Wi-Fi is enabled, current consumption ranges from 80mA to 150mA. Conversely, Deep Sleep mode offers significantly reduced power draw, consuming approximately 20µA (0.02mA). In a practical scenario where the system remains active for 12 continuous hours (e.g., when the user is away from home) and then transitions to Deep Sleep for the subsequent 12 hours, a 3.7V, 2000mAh LiPo battery is estimated to power the system for approximately 2.5 days.

C. Interface

To enable direct communication with the user, a graphical user interface was developed using JavaScript, allowing real-time monitoring of the device's status. Figure 2 shows the

interface that enables users to activate or deactivate the system without requiring the RFID card, provides immediate alerts when a security breach is detected, and displays a comprehensive log of violations, including the date and time of each unauthorized attempt to open the backpack. Additionally, the system offers an option to export the violation history for further analysis, thereby enhancing its practical utility and contributing to more rigorous monitoring of security events.

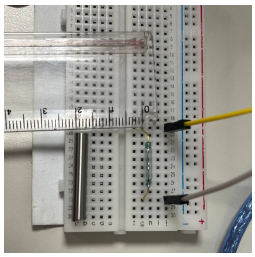
(a) Software interface when the system is activated.

(b) Software interface when the system is violated.

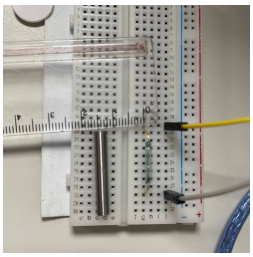
Fig. 2: Software interface for the prototype.

IV. Results

To evaluate the system's performance, two types of tests were conducted. The first test aimed to determine the minimum distance between the magnet and the reed switch required to trigger a change in the circuit state. It was observed that when the reed switch is initially closed, it opens as the magnet is moved approximately 2 cm away, as shown in Figure 3 (a). Conversely, when the circuit is open, it closes when the magnet is brought to approximately 1.5 cm from the sensor (Figure 3 (b)). These values indicate a slight difference in sensitivity between the opening and closing states, which may be attributed to magnetic hysteresis in the reed switch behavior.



(a)



(b)

Fig. 3: Behavior of the reed switch at different distances from the magnet.

V. Conclusion

While this anti-theft solution offers a low-cost approach, its practical application is limited; it isn't a guaranteed daily defense. For instance, the monitored object could easily be removed from the owner's line of sight, or even opened by other means (like a backpack being sliced), rendering any notification irrelevant. Nevertheless, this work serves as a valuable foundational model for future improvements and presents a budget-friendly solution applicable in specific, though not all, scenarios.

This project demonstrated the viability of an embedded anti-theft system using low-cost components such as reed switches, RFID, and the ESP8266 microcontroller, integrated with the MQTT protocol for real-time notifications. The tests confirmed that the system is capable of reliably detecting unauthorized access and triggering audible and visual alarms. Additional improvements include circuit miniaturization, the integration of more precise sensors, and adaptation to commercial backpack designs. Overall, the project presents a promising step toward a portable, intelligent, and adaptable personal security solution suitable for various everyday scenarios.

References

[1] L. Wang, F. Xu, and T. Wang, "Design of multifunctional anti-theft backpack based on microcomputer," in *8th International Conference on Management and Computer Science (ICMCS 2018)*. Atlantis Press, 2018, pp. 507–510. [Online]. Available: https://doi.org/10.2991/icmcs-18.2018.104

[2] S. Omer, K. Sohelrana, A. Tamkeen, M. A. Rasheed *et al.*, "Real time application of vehicle anti theft detection and protection with shock using facial recognition and iot notification," in *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2020, pp. 1039–1044. [Online]. Available: https://doi.org/10.1109/ICCMC48092.2020.ICCMC-000194

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things (iot): A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. [Online]. Available: https://doi.org/10.1109/COMST.2015.2444095

[4] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "Iot based smart security and home automation system," in *2016 international conference on computing, communication and automation (ICCCA)*. IEEE, 2016, pp. 1286–1289. [Online]. Available: https://doi.org/10.1109/CCAA.2016.7813916

[5] S. N. Mustika, E. Noerhayati, P. Gunawirawan, Y. D. Mahandi *et al.*, "Development of an iot-based door security system using reed switch sensor with rfid and telegram notification," in *2023 8th International Conference on Electrical, Electronics and Information Engineering (ICEEIE)*. IEEE, 2023, pp. 1–4. [Online]. Available: https://doi.org/10.1109/ICEEIE59078.2023.10334803

[6] N. Saranya, S. S. Priya *et al.*, "Intelligent vehicle management system using iot," in *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2024, pp. 493–497. [Online]. Available: https://doi.org/10.1109/ICESC60852.2024.10689810

[7] A. Neftissov, I. Kazambayev, L. Kirichenko, A. Aubakirova, D. Urazayev, and K. Zhakupova, "Development of microprocessor device of relay protection based on open architecture using industrial internet of things technology," *Procedia Computer Science*, vol. 231, pp. 672–677, 2024. [Online]. Available: https://doi.org/10.1016/j.procs.2023.12.163

[8] S. Ramadhani and D. P. Putri, "Design of a home door security system based on nodemcu esp32 using a magnetic reed switch sensor and telegram bot application," *Sinkron: jurnal dan penelitian teknik informatika*, vol. 7, no. 4, pp. 2059–2068, 2023. [Online]. Available: https://doi.org/10.33395/sinkron.v8i4.12688

[9] T. Nguyen, "Low-cost residential security system," Bachelor's Thesis, 2018. [Online]. Available: https://urn.fi/URN:NBN:fi:amk-2018122022579