Development of a Modular and Low-Cost Electronic Lock System for the Academic Environment

Marcos Vinicius S. Melo[1*], Felipe C. Leal[2], Rubens de S. Matos Junior[1], Alfredo M. Vieira[1]
[1]Federal Institute of Sergipe; Lagarto, Sergipe; [2]Federal University of Sergipe; São Cristóvão, Sergipe, Brazil

Security in educational institutions is paramount, and electronic access control solutions play a crucial role in enhancing the protection of these environments. However, commercially available systems often lack cost-effectiveness for large-scale deployment in public institutions. This article presents the development of a modular, adaptable, and low-cost electronic lock prototype designed for access control in academic settings. The prototype leverages microcontrollers and simple electronic components to deliver an efficient and affordable solution. Key features include remote control, multiple authorization methods, and seamless integration with other systems, making it a practical option for schools with limited budgets.

Keywords: IoT. Smart Campus. Electronic Lock. Security.

Security is a sensitive topic, addressed in various aspects ranging from cybersecurity, also known as logical security, to the physical security of people, environments, and equipment. Ensuring security is a challenge in many scenarios. However, with the notable expansion of technologies aligned with the Internet of Things (IoT) paradigm, numerous network-connected devices, such as surveillance cameras, motion sensors, and electronic locks, have been employed for security purposes. However, limited financial resources can be a significant obstacle to achieving such an innovative scenario in public organizations, where budgets for these matters are often restricted.

Flexible and modular authorization systems for environments are uncommon; however, they offer various applications in shared spaces. The availability of multiple authorization methods is also crucial, particularly in organizations with a diverse range of individuals who may or should have access to a given environment, depending on schedules and contextual needs. This is often the case in universities, institutes of education, science and technology, and schools, which comprise students, faculty members, laboratory technicians, administrative staff, and other occasional academic community members. In different situations, these individuals may or may not be granted access to classrooms, laboratories, offices, and other environments, each of which may have specific access rules.

Microcontrollers with Wi-Fi connectivity integrated into a management system can ensure efficient access control for various environments. To achieve this, it is also essential to guarantee the logical security of the systems involved in such physical access control mechanisms. Encryption of network communications and protection schemes against attacks such as "man-in-the-middle," among others, should be incorporated into the design of such systems, even those with limited computational resources.

This article presents a prototype developed for a door access control system using typical IoT technologies. The main benefits of this approach include (1) Flexible Access Control, (2) Low Cost, (3) Detailed Reports, (4) Solution Modularity with Multiple Authorization Methods, and (5) Protection Against Cyber Attacks. This system was specifically designed for public educational institutions due to its low cost and high adaptability to their unique requirements. However, it can also be adapted for other types of organizations.

Theoretical Foundation

According to Geepalla (2013) [1], digital access control models are often inadequate

Received on 27 September 2024; revised 30 October 2024.

Address for correspondence: Marcos Vinicius S. Melo. Estr. da Barragem - Jardim Campo Novo. Lagarto – Sergipe - Brasil. Zipcode: 49400-000. Lagarto, Sergipe, Brazil. E-mail: marcos.melo089@academico.ifs.edu.br.

for representing the specifications of physical access control. It is crucial to consider the unique characteristics of real-world environments to adapt the corresponding digital strategies. According Bindra and colleagues [2] and Kaur and colleagues [3] provide examples of studies that explore the characteristics of modern access control systems for smart buildings and their various possibilities. Encryption is essential for protecting data and ensuring information confidentiality in an increasingly digital world. According to Kaur and colleagues [3], it uses mathematical algorithms to transform readable data into an encrypted format, making it accessible only to those with the correct decryption key. This technique has been employed since ancient times but has evolved significantly in the digital era. Its primary goal is to secure communication against unauthorized access, ensuring that information remains protected.

The lack of encryption has led to numerous significant data breaches, exposing sensitive information from both companies and individuals. A recent example is the Tangerine Telecom breach 2024, where over 200,000 customer access records were exposed due to inadequate database security [4]. Another case involved Spoutible, which had a vulnerability in its API exploited [5], allowing access to users' personal information and encrypted passwords. These incidents highlight the direct risks of the absence of encryption and robust security measures. Reports like the one from the OAIC (Office of the Australian Information Commissioner) have also exposed severe security flaws in Australian government agencies, such as misconfigured security settings and the lack of proper encryption. In 2024 alone, the Australian government reported 63 data breaches in the first half of the year, leaving personal information vulnerable to unauthorized access [6].

These examples represent just a fraction of what is happening globally. A 2024 study by IBM revealed that 60% of organizations that suffered cyberattacks attributed the root cause to the lack of encryption in their systems [7]. Furthermore, the IBM report indicated that the average cost of a data breach without encryption could reach $4.35 million, factoring in reputational damage, financial losses, and mitigation costs.

These figures reinforce the need for proper encryption as a best practice and a critical factor for business continuity and security.

Therefore, implementing encryption should be considered an essential component for any company or organization. In addition to preventing data breaches and protecting sensitive information, encryption is also necessary for compliance with data protection regulations such as the GDPR (General Data Protection Regulation) in Europe [8] and the LGPD (Lei Geral de Proteção de Dados) in Brazil [9]. Failing to invest in proper data protection exposes organizations to cyberattacks and severe regulatory penalties, highlighting the need for a proactive and integrated approach to information security.

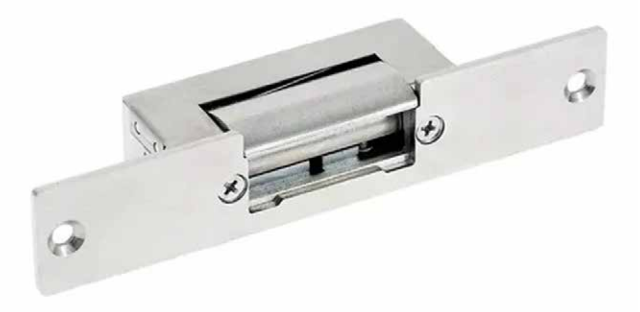
Materials and Methods

The proposed solution is built on the ESP-32 NodeMCU development platform, which enables Wi-Fi integration and connectivity with components such as an RFID reader. For device and permission management, a web application was developed using Django, a Python-based framework for building full-featured web applications. This system manages users, devices, and permissions, allowing for the seamless integration of the involved technologies and providing a robust solution to the proposed problem.

The device includes a relay connected to an embedded electric lock, as shown in Figure 1. This electric lock allows device integration without rendering the original door system unusable. As a result, the remote access control system can be used without losing the traditional key-based access option. Additionally, this solution ensures system security in cases of power outages or device connectivity issues.

To ensure secure requests from the device to the server, authentication is performed using the device's MAC address and IP address, assigning a temporary

Figure 1. Electric lock used in the device.



token to each device at the time of authentication. On its first use, the device remains in standby mode until a system administrator authorizes it, allowing it to make requests to the system. The assigned tokens are based on the UUID4 standard, ensuring system security. Additionally, all requests are made using the HTTPS method, guaranteeing that all packets are encrypted. Once authorized, the device must include the token in all subsequent requests. Every device authentication is logged, including its MAC address, IP, ID, and authentication timestamp. The web platform enables user registration with specific permissions, allowing administrators to manage which environments each user can access. Furthermore, every user's access attempt to an environment is recorded, including details such as user ID, environment, and timestamp.

There are multiple ways to access environments through the platform:

Direct Application Access: The user logs into the application, selects the device and sends a request to unlock the environment.

QR Code Authentication: A QR Code associated with the device can be scanned, which opens an application page and verifies the user's permissions before granting or denying access.

Temporary PIN Access: A 4-digit temporary password with a customizable expiration time can be generated. This PIN is linked to the device and allows non-registered users to access the environment via an authorization page in the application. All accesses using temporary passwords are logged with the user who generated the PIN. An RFID module can also be connected to the device, enabling quick access through an RFID tag scan. Before using RFID tags, they must be registered in the web application, which stores the hexadecimal tag code. The tag is then linked to the user's account, allowing access management and deactivation. The RFID tag's permissions are directly tied to the account permissions of its owner.

Results

The final device measures 84x79x42mm in external dimensions, as shown in Figure 2. The enclosure housing all prototype components was designed and 3D-printed, ensuring durability and meeting the necessary resistance requirements for the device.

The device was assembled as shown in Figure 3 and is powered by a 12V power supply, which provides energy to both the electric lock and a 12V-to-5V voltage converter. This setup allows the remaining system components to function properly.

The final model also features a human-machine interface (HMI) separate from the main device. This interface includes three LEDs:

Figure 2. Device assembly diagram.

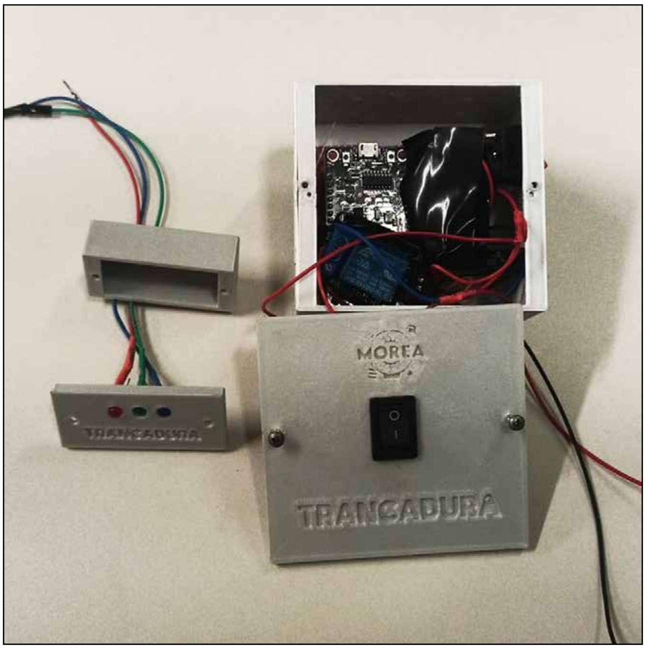
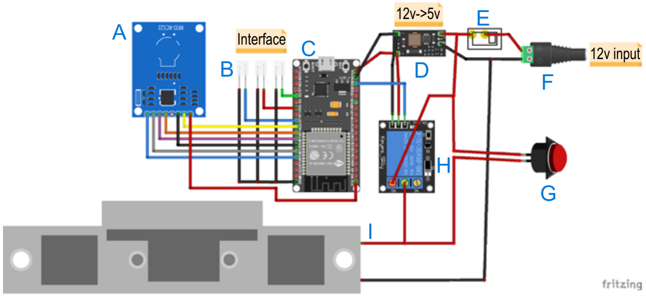


Figure 3. Device Wiring Diagram.



Blue LED: Indicates internet connection status.
Green LED: Signals that entry is unlocked.
Red LED: Signals that entry is locked.

This interface is designed to be installed outside the controlled environment. It allows users to verify the device's operational status before use and connects to the main system via a 4-pin connector. Since the RFID sensor is an optional module, it can be connected via a 6-pin connector. Additionally, the device includes a physical button directly linked to the power supply, serving the same function as the relay in the circuit. This allows users to manually unlock the door from inside the environment without requiring access to the web application, enabling a quick exit when necessary.

Web Application Development

The web application includes the following main sections:

- User and Permission Management
- Device Management
- RFID Tag Management

Each section provides basic CRUD (Create, Read, Update, Delete) operations and specific functionalities.

For example, user management includes permission control, while device management includes authentication approval.QR Codes, one of the authentication methods, are generated using external applications. These QR codes direct users to the device-specific page, allowing access authorization based on the user's account permissions or an active temporary password for that environment.

Conclusion

The electronic lock prototype passed all tests, demonstrating its effectiveness in access control for research laboratories within a federal institution.

- Future developments include:
- New authentication modules, such as numeric keypads and fingerprint sensors.
- Size reduction of the prototype for improved integration.
- Enhancing security features to strengthen protection against cyber threats.

To maximize impact, the project has been released as an open-source solution on GitHub: https://github.com/Morea-IFS. This enables the community to collaborate, improve, and expand its functionalities, fostering more competent environment management.

References

1. Geepalla E, Bordbar B, Du X. Spatio-temporal role based access control for physical access control systems. In 2013 Fourth International Conference on Emerging Security Technologies 2013:39–42.
2. Bindra L, Lin C, Stroulia E, Ardakanian O. Decentralized access control for smart buildings using metadata and smart contracts. In 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS) 2019:32–38.
3. Kaur G, Singh A, Singh D. A comprehensive review on access control systems amid global pandemic. In 2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS) 2022:15–19.
4. ITnews. Tangerine telecom says customer data of 232000 affected by 'cyber incident'. 2024. Available at: https://www.itnews.com.au/news/tangerine-telecom-says-customer-data-of-232000-affected-by-cyber-inciAcesso em: 2024-09-30.
5. Jornalismo N. Falha na rede social spoutible coloca contas em risco. 2024. Available at: https://nucleo.jor.br/curtas/2024-02-05-falha-spoutible-contas-em-risco/.
6. TechRepublic. 2024 exposed: The alarming state of australian data breaches. Available at: https://

www.techrepublic.com/article/state-of-data-breach-australia-2024/.

7. IBM.Adopting security AI and automation can cut breach costs. 2024. Available at: https://www.ibm.com/reports/data-breach#:˜:text=The%20global%20average%20cost%20of,and%20the%20highest%20total%20ever.&text=Share%20of%20breaches%20that%20involved,harder%20to%20track%20and%20safeguard.

8. EU (2016). Regulation (EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

9. Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de protecção de dados pessoais (LGPD). Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

10. Terada, R. Segurança de dados: criptografia em rede de computador. In Segurança de dados: criptografia em rede de computador. Editora Blucher 2008:15-25.