Trancadura 2.0: Fechadura Eletrônica Modular de Baixo Custo para Ambientes Educacionais

Victor A. Lima[1], Genisson E. dos Santos[1], Guilherme da I. Santos[1], Felipe C. Leal[2], Marcos Vinicius S. Melo[1], Silas S. de Jesus[1], Rubens de S. Matos Júnior[1] Alfredo M. Vieira[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia de Sergipe - Campus Lagarto

[2]Universidade Federal de Sergipe - Campus São Cristóvão

{victor.lima091, silas.jesus097}@academico.ifs.edu.br
{felipecarvalho5520, gui.inven, esgenisson}@gmail.com
marcosvinicius.sm@icloud.com
{rubens.junior, alfredo.vieira}@ifs.edu.br

Abstract. *This paper presents the evolution of an open-source project for a low-cost modular electronic lock, designed for access control in educational institutions. The new version introduces a modern architecture based on web technologies, with a backend developed in NestJS and a frontend built with Next.js, both written in TypeScript. Key improvements include support for Over-The-Air (OTA) updates, a Telnet interface for remote diagnostics, secure HTTPS communication, authentication using JWT tokens, and a responsive web application for managing users, devices, and permissions. The embedded system is based on the ESP32 microcontroller, integrating multiple authentication methods such as RFID reading, physical button, and remote API commands. This proposal aims to democratize access to physical security technologies by offering a viable and scalable alternative for public institutions with limited resources.*

Resumo. *Este artigo apresenta a evolução de um projeto open-source de fechadura eletrônica modular de baixo custo, voltado para o controle de acesso em instituições educacionais. A nova versão da solução incorpora uma arquitetura moderna baseada em tecnologias web, com backend desenvolvido em NestJS e frontend em Next.js, ambos escritos em TypeScript. As melhorias incluem suporte a atualizações remotas Over-The-Air (OTA), interface Telnet para diagnóstico remoto, comunicação segura via HTTPS, autenticação com tokens JWT e uma aplicação web responsiva para gerenciamento de usuários, dispositivos e permissões. O sistema embarcado é baseado no microcontrolador ESP32, integrando diversos modos de autenticação, como leitura RFID, botão físico e comandos remotos via API. A proposta busca democratizar o acesso a tecnologias de segurança física, oferecendo uma alternativa viável e escalável para instituições públicas com recursos limitados.*

1. Introdução

A segurança física de ambientes educacionais representa um desafio constante para gestores de instituições públicas e privadas. Laboratórios, bibliotecas, salas de servidores e outros espaços de acesso restrito exigem mecanismos confiáveis de controle de acesso para garantir a integridade de equipamentos, materiais e informações sensíveis. Contudo, soluções comerciais de

controle de acesso, como sistemas biométricos ou fechaduras inteligentes proprietárias, costumam ter custos elevados, o que inviabiliza sua adoção em larga escala em instituições de ensino com orçamentos limitados.

A crescente disseminação de tecnologias baseadas no paradigma da Internet das Coisas (IoT) tem aberto novas possibilidades para o desenvolvimento de soluções acessíveis e personalizáveis. Microcontroladores com conectividade Wi-Fi, como o ESP32, permitem a criação de dispositivos inteligentes que integram hardware e software para o gerenciamento eficiente do acesso físico a ambientes. Além disso, a adoção de práticas de desenvolvimento open-source tem fomentado a colaboração e o compartilhamento de soluções entre instituições, comunidades acadêmicas e desenvolvedores independentes.

Este trabalho descreve o desenvolvimento e a evolução de um sistema de fechadura eletrônica modular, iniciado em 2024 como uma solução experimental e aprimorado em 2025 com a incorporação de novas tecnologias. A solução foi projetada com foco na modularidade, permitindo a integração de diferentes métodos de autenticação, como cartões RFID, senhas temporárias, comandos via aplicação web e até mesmo controle físico por meio de botões. Além disso, aspectos relacionados à segurança digital, como criptografia de comunicações, autenticação por tokens e logs de auditoria, foram tratados de forma prioritária.

2. Fundamentação Teórica

De acordo com [7], os modelos de controle de acesso digital muitas vezes não são adequados para representar as especificações do controle de acesso físico. Como demonstrado em nosso trabalho anterior [1], soluções modulares e de baixo custo podem ser eficazes para ambientes educacionais. É importante considerar características próprias dos ambientes reais, para adaptar as estratégias digitais correspondentes. Em [8] e [9], temos exemplos de trabalhos que abordam as características de sistemas modernos de controle de acesso para prédios inteligentes e suas diversas possibilidades.

A criptografia é uma técnica essencial para proteger dados e garantir a confidencialidade das informações em um mundo cada vez mais digital. Segundo [2], ela utiliza algoritmos matemáticos para transformar dados legíveis em um formato cifrado, tornando-os acessíveis apenas para aqueles que possuem a chave correta para a decodificação. Essa técnica tem sido empregada desde a antiguidade, mas evoluiu significativamente na era digital. O principal objetivo é proteger a comunicação contra acessos não autorizados, garantindo que as informações permaneçam seguras.

A falta de criptografia tem causado uma série de vazamentos de dados significativos, expondo informações sensíveis de empresas e cidadãos. Um exemplo recente é o vazamento no Tangerine Telecom, em 2024, na qual mais de 200 mil registros de acesso dos clientes foram expostos devido à segurança não ser adequada em um banco de dados [3]. Outro caso envolve o Spoutible, que teve uma vulnerabilidade em sua API explorada [4], permitindo acesso a informações pessoais e senhas criptografadas de usuários. Esses incidentes ilustram os riscos diretos da ausência de criptografia e de medidas de segurança robustas. Em relatórios como o da OAIC (*Office of the Australian Information Commissioner*), vazamentos em agências governamentais australianas também revelaram falhas graves, como configurações incorretas de segurança e a falta de criptografia adequada. Em 2024, o governo australiano registrou 63 vazamentos de dados apenas no primeiro semestre, tornando informações pessoais suscetíveis a acesso não autorizado [5].

Estes exemplos são apenas uma pequena amostra do que vem ocorrendo globalmente. Um estudo conduzido pela IBM em 2024 revelou que 60% das organizações que sofreram ata-

ques cibernéticos atribuíram a origem do problema à falta de criptografia em seus sistemas [6]. Além disso, o relatório da IBM aponta que o custo médio de um vazamento de dados sem criptografia pode chegar a US$ 4,35 milhões, considerando os danos à reputação, perdas financeiras e custos relacionados a mitigações. Estes números reforçam que a adoção de criptografia adequada não é apenas uma prática recomendada, mas um fator crítico para a continuidade e a proteção dos negócios.

Portanto, a implementação da criptografia deve ser considerada um componente essencial para qualquer empresa ou organização. Além de evitar vazamentos e proteger dados sensíveis, a criptografia também é necessária para estar em conformidade com normas regulatórias de proteção de dados, como o **GDPR** (*General Data Protection Regulation*) na Europa [10] e a **LGPD** (Lei Geral de Proteção de Dados) no Brasil [11]. Não investir na proteção adequada de dados não só expõe organizações a ciberataques, mas também a severas penalidades regulatórias, enfatizando a necessidade de uma abordagem proativa e integrada em termos de segurança da informação.

3. Evolução Tecnológica do Projeto

A primeira versão do sistema, desenvolvida em 2024, baseava-se em um backend construído com o framework Django, utilizando o banco de dados SQLite e oferecendo funcionalidades básicas de controle de acesso. O dispositivo embarcado, centrado no microcontrolador ESP32, realizava a leitura de cartões RFID e enviava requisições ao servidor via HTTPS. Embora funcional, essa abordagem apresentou limitações significativas, principalmente no que se refere à escalabilidade do backend, à capacidade de atualização remota dos dispositivos e à integração com novas tecnologias.

Em resposta a essas limitações, a equipe de desenvolvimento iniciou, em 2025, uma reestruturação completa da arquitetura do sistema. A transição para um backend em NestJS, com banco de dados PostgreSQL gerenciado por Prisma ORM, permitiu um gerenciamento mais eficiente dos registros e uma maior flexibilidade na criação de novas APIs. Paralelamente, o frontend foi migrado para Next.js com React e TailwindCSS, resultando em uma interface mais responsiva, amigável e acessível em diferentes dispositivos, incluindo smartphones e tablets.

No âmbito do software embarcado, foram implementadas melhorias substanciais no código do ESP32. Destacam-se a adoção de um sistema de autenticação robusto por meio de tokens JWT, a implementação de atualizações OTA com autenticação por senha, e a inclusão de uma interface Telnet que permite diagnósticos remotos e monitoramento em tempo real. Essas mudanças reduziram drasticamente o tempo de manutenção, facilitando atualizações sem necessidade de acesso físico aos dispositivos.

Além disso, o firmware foi otimizado para utilizar a abordagem baseada em temporizadores não bloqueantes (`millis()`), aumentando a responsividade do sistema e evitando travamentos decorrentes de funções de espera ativa (*delay*). Essa reestruturação também contemplou melhorias na detecção e leitura de cartões RFID, aumentando a confiabilidade do sistema mesmo em ambientes com alta taxa de uso.

Por fim, um novo gabinete foi projetado utilizando impressão 3D, proporcionando melhor acabamento, maior resistência e possibilidade de replicação fácil por outras instituições interessadas.

4. Materiais e Métodos

A solução desenvolvida é composta por dois principais componentes: o dispositivo físico responsável pelo controle da fechadura e o sistema web de gerenciamento.

O hardware central é baseado no microcontrolador ESP32, conhecido por sua capacidade de processamento e conectividade Wi-Fi. O circuito eletrônico inclui um módulo RFID RC522 para leitura de cartões, um relé para acionamento da fechadura elétrica, um buzzer para sinais sonoros, três LEDs indicativos (conexão, sucesso e erro), além de um botão físico que permite a abertura local da porta. A alimentação do sistema é feita por uma fonte de 12V, com um conversor buck para fornecer os 5V necessários ao ESP32 e seus periféricos.

No lado do software embarcado, o firmware foi desenvolvido em C++ utilizando o framework do Arduino, com bibliotecas como `ArduinoOTA`, `TelnetStream`, `ESPAsyncWebServer`, `WiFiClientSecure` e `MFRC522`. A arquitetura do código foi projetada para manter o funcionamento assíncrono de suas principais tarefas, utilizando controle de tempo baseado em `millis()` para evitar bloqueios.

O backend da aplicação web utiliza o framework NestJS, com banco de dados PostgreSQL gerenciado via Prisma ORM. A autenticação de usuários e dispositivos é realizada com JWT, garantindo segurança nas requisições. O frontend, por sua vez, foi desenvolvido em Next.js com React, proporcionando uma interface responsiva e de fácil utilização.

Entre as funcionalidades da plataforma web estão o cadastro e gerenciamento de usuários, dispositivos e cartões RFID, além da geração de senhas temporárias para acesso emergencial e visualização de logs detalhados de acessos. As comunicações entre o dispositivo físico e o servidor ocorrem via HTTPS, com validação de token em todas as requisições.

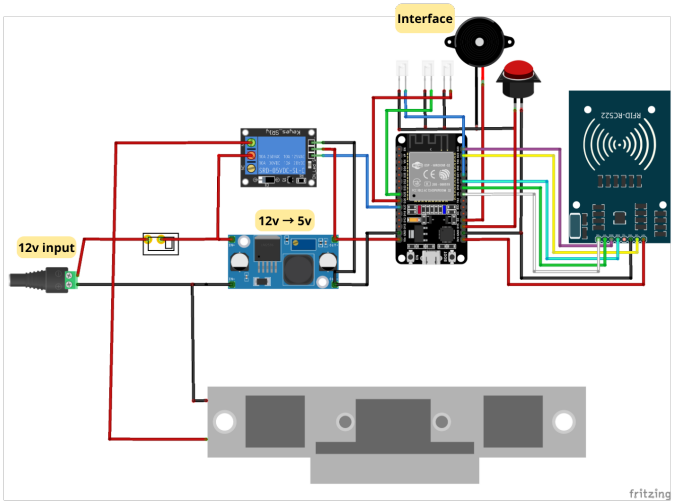

Figura 1. Esquema elétrico do dispositivo.

5. Resultados

Após a finalização do desenvolvimento, foram realizados testes práticos em um ambiente educacional real, especificamente nos laboratórios de informática do Instituto Federal de Sergipe. Os testes contemplaram cenários de uso intensivo, incluindo múltiplas tentativas de acesso simultâneo, quedas de conexão Wi-Fi e operações de atualização OTA.

O sistema demonstrou desempenho satisfatório, com tempo médio de resposta inferior a

3 segundos para a leitura e autenticação de cartões RFID. O módulo OTA permitiu atualizações remotas sem a necessidade de intervenção física, reduzindo o tempo de manutenção. A interface Telnet se mostrou uma ferramenta útil para o diagnóstico remoto de problemas, permitindo comandos diretos de debug em tempo real.

Os registros de acesso foram devidamente armazenados no banco de dados, com informações completas de data, horário, identificação do usuário e do dispositivo. A interface web apresentou boa responsividade, com carregamento eficiente em dispositivos móveis e desktops.

Além dos testes técnicos, foi conduzida uma avaliação qualitativa com usuários finais, incluindo técnicos de laboratório e equipe administrativa, que relataram facilidade de uso e confiabilidade do sistema.

Figura 2. Protótipo físico montado.

6. Conclusão e Trabalhos Futuros

A evolução da fechadura eletrônica modular demonstrou ser uma solução eficiente, segura e de baixo custo para o controle de acesso em ambientes acadêmicos. As melhorias implementadas, incluindo a integração de OTA, Telnet, autenticação JWT e uma interface web moderna, permitiram alcançar um novo nível de robustez e usabilidade.

Como próximos passos, pretende-se incorporar novos métodos de autenticação, como leitores biométricos e teclados numéricos, além de desenvolver um aplicativo mobile para facilitar ainda mais o gerenciamento remoto do sistema. Também está prevista a integração com sistemas acadêmicos existentes, possibilitando, por exemplo, que o acesso aos ambientes seja vinculado automaticamente à matrícula ou ao vínculo institucional dos usuários.

Baseando-se nos objetivos do projeto e visando sua ampliação e melhoria contínua, o código-fonte foi disponibilizado como open-source, permitindo que outras instituições possam replicar, adaptar e contribuir com a evolução da solução.

`https://github.com/Morea-IFS/`

Referências

[1] Leal, F. C., Melo, M. V. S., Matos Júnior, R. S., & Vieira, A. M. (2024). *Um protótipo de fechadura eletrônica modular de baixo custo para ambientes acadêmicos*. Trabalho não publicado, Instituto Federal de Sergipe.

[2] Terada, R. (2008). *Segurança de dados: criptografia em rede de computador*. Blucher. Acesso em: 18 jun. 2025.

[3] ITnews. (2024). Tangerine Telecom says customer data of 232000 affected by 'cyber incident'. Disponível em: https://www.itnews.com.au/news/tangerine-telecom-says-customer-data-of-232000-affected-by-cyber-inci Acesso em: 18 jun. 2024.

[4] Núcleo Jornalismo. (2024). Falha na rede social Spoutible coloca contas em risco. Disponível em: https://nucleo.jor.br/curtas/2024-02-05-falha-spoutible-contas-em-risco/. Acesso em: 18 jun. 2025.

[5] TechRepublic. (2024). 2024 Exposed: The Alarming State of Australian Data Breaches. Disponível em: https://www.techrepublic.com/article/state-of-data-breach-australia-2024/. Acesso em: 18 jun. 2025.

[6] IBM. (2024). Adopting security AI and automation can cut breach costs. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 19 jun. 2025.

[7] Geepalla, E., Bordbar, B., Du, X. (2013). Spatio-temporal Role Based Access Control for Physical Access Control Systems. In: *Fourth International Conference on Emerging Security Technologies*, pp. 39–42. IEEE. DOI: 10.1109/EST.2013.13. Acesso em: 19 jun. 2025.

[8] Bindra, L., Lin, C., Stroulia, E., Ardakanian, O. (2019). Decentralized Access Control for Smart Buildings Using Metadata and Smart Contracts. In: *IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, pp. 32–38. DOI: 10.1109/SEsCPS.2019.00013. Acesso em: 19 jun. 2025.

[9] Kaur, G., Singh, A., Singh, D. (2022). A Comprehensive Review on Access Control Systems amid Global Pandemic. In: *International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*, pp. 15–19. DOI: 10.1109/ICETEMS56252.2022.10093551. Acesso em: 19 jun. 2025.

[10] União Europeia. (2016). Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 20 jun. 2025.

[11] Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jun. 2025.