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, low-cost modular electronic lock for access control in educational institutions. The new version adopts a modern web-based architecture, with a NestJS backend and a Next.js frontend, both in TypeScript. Key enhancements include OTA updates, secure HTTPS communication, JWT-based authentication, and a responsive web app for managing users, devices, and permissions. Powered by the ESP32 microcontroller, the system supports multiple authentication methods, including RFID, a physical button, and remote API commands. The project promotes accessible and scalable physical security solutions for resource-limited public institutions.*

Resumo. *Este artigo apresenta a evolução de uma fechadura eletrônica modular open-source e de baixo custo, voltada para controle de acesso em instituições educacionais. A nova versão adota uma arquitetura moderna com backend em NestJS e frontend em Next.js, ambos em TypeScript. As melhorias incluem suporte a OTA, comunicação segura via HTTPS, autenticação JWT e uma aplicação web responsiva para gerenciamento de usuários e permissões. Baseado no ESP32, o sistema integra autenticação por RFID, botão físico e comandos via API, oferecendo uma solução acessível e escalável para ambientes 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 [Leal et al. 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 tags RFID, PinCodes temporários, 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

Os sistemas de controle de acesso físico têm evoluído com o suporte de plataformas embarcadas como o ESP32, que viabilizam a integração com sensores RFID, comunicação segura e interfaces web. Estudos como os de Geepalla et al. (2013) e Bindra et al. (2019) destacam a aplicabilidade dessas soluções em ambientes institucionais. Neste trabalho, a criptografia é aplicada de forma prática com o uso de HTTPS e autenticação via JWT, evitando protocolos inseguros como Telnet em ambientes produtivos.

Segundo [Geepalla et al. 2013], modelos digitais de controle de acesso nem sempre representam adequadamente as exigências do mundo físico, exigindo adaptações às características dos ambientes reais. Trabalhos como os de [Bindra et al. 2019] e [Kaur et al. 2022] demonstram abordagens modernas voltadas a edifícios inteligentes, reforçando a diversidade de estratégias disponíveis.

A criptografia é fundamental para garantir a confidencialidade e integridade das informações. Conforme [Terada 2008], trata-se de uma técnica matemática que transforma dados legíveis em formatos cifrados, acessíveis apenas por quem possui a chave de decodificação. A ausência dessa proteção tem gerado graves incidentes de segurança.

Em 2024, o Tangerine Telecom sofreu a exposição de mais de 200 mil registros de acesso por falhas de segurança em seu banco de dados [ITnews 2024]. O Spoutible também teve vulnerabilidades exploradas em sua API, comprometendo dados pessoais e senhas criptografadas [Jornalismo 2024]. Relatórios da OAIC revelaram que órgãos governamentais australianos sofreram 63 vazamentos apenas no primeiro semestre de 2024, motivados por falhas de configuração e ausência de criptografia [TechRepublic 2024].

Esses casos não são isolados. Um estudo da IBM em 2024 apontou que 60% dos ciberataques ocorreram por falta de criptografia, e que o custo médio de um vazamento pode chegar a US$ 4,35 milhões [IBM 2024]. Isso inclui prejuízos financeiros, danos à reputação e medidas corretivas.

Assim, a adoção de criptografia se torna essencial para qualquer organização, não apenas para prevenir vazamentos, mas também para atender às exigências regulatórias como o GDPR europeu [EU 2016] e a LGPD brasileira [Brasil 2018]. Ignorar essas práticas expõe instituições a riscos operacionais e legais, reforçando a importância de estratégias de segurança da informação bem estruturadas.

3. Materias e Metódos

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 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 para diagnósticos remotos e monitoramento em tempo real. O firmware também passou a utilizar uma arquitetura baseada em temporizadores não bloqueantes (`millis()`), aumentando a responsividade do sistema e evitando travamentos decorrentes de funções de espera ativa (*delay*). Essa reestruturação contemplou ainda melhorias na leitura de cartões RFID e um novo gabinete projetado com impressão 3D, visando melhor acabamento e facilidade de replicação.

O sistema completo é composto por dois elementos principais: o dispositivo físico responsável pela execução do controle de acesso e a plataforma web de gerenciamento.

No hardware, o núcleo do sistema é o ESP32, microcontrolador com conectividade Wi-Fi. Os componentes incluem um módulo RFID RC522, relé de 5V, buzzer piezoelétrico, LEDs indicativos (azul para conexão, verde para sucesso e vermelho para erro), além de um botão físico. A alimentação é feita por uma fonte de 12V com conversor buck para 5V. A fechadura elétrica do tipo solenoide é integrada ao sistema por meio do relé, permitindo acionamento seguro sem inutilizar o sistema mecânico tradicional da porta, como mostra a Figura 1.

Figura 1. Fechadura elétrica utilizada no dispositivo

O firmware foi desenvolvido em C++ utilizando o framework do Arduino, com bibliotecas como `ArduinoOTA`, `TelnetStream`, `ESPAsyncWebServer`, `WiFiClientSecure` e `MFRC522`. A arquitetura do código prioriza o funcionamento assíncrono das tarefas e a segurança nas comunicações.

Para garantir que as requisições dos dispositivos ao servidor sejam feitas de forma segura, a autenticação inicial é baseada no endereço MAC e IP do dispositivo. Quando o ESP32 conecta-se pela primeira vez, ele permanece em modo de espera até ser autorizado por um administrador da plataforma. Ao ser autorizado, recebe um token temporário baseado no padrão UUID4, que deve ser utilizado em todas as requisições subsequentes. Todas as comunicações são feitas via HTTPS, garantindo a criptografia dos pacotes. As autenticações são registradas em logs detalhados, contendo MAC, IP, ID do dispositivo e horário da autenticação.

No backend, o NestJS é responsável pelas rotas e autenticação com tokens JWT. O banco PostgreSQL, acessado via Prisma ORM, armazena os dados dos usuários, dispositivos, permissões e registros de acesso. O frontend desenvolvido com Next.js oferece uma interface moderna para administração do sistema, como mostra a Figura 2.

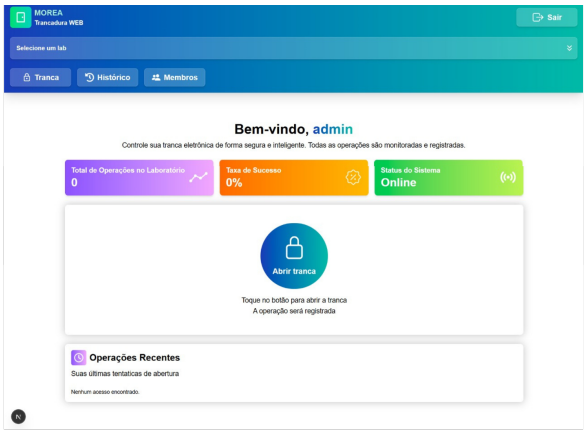

Figura 2. Interface web para gerenciamento de ambientes e permissões.

3.1. Funcionalidades da Plataforma

A plataforma web integra recursos completos de gerenciamento e múltiplos métodos de acesso:

- **Gerenciamento**: Controle de usuários (admin/professor/técnico), logs detalhados e monitoramento em tempo real
- **Acesso Web**: Liberação remota via interface após login
- **QR Code**: Autenticação rápida via código escaneado
- **PinCode**: Senhas temporárias de 5 dígitos para acesso sem cadastro

Do ponto de vista do fluxo de dados, o sistema pode ser dividido em dois principais caminhos:

- **Acionamento via site**: usuário autorizado faz login, solicita abertura de ambiente → o servidor valida a requisição → envia comando via HTTPS ao ESP32 → o ESP32 aciona o relé e libera a fechadura.
- **Acionamento via RFID**: ESP32 realiza a leitura de uma tag → envia o UID para o servidor via HTTPS → o servidor verifica autorização → resposta enviada ao ESP32 → aciona o relé (em caso positivo) ou indica erro com LED vermelho e buzzer.

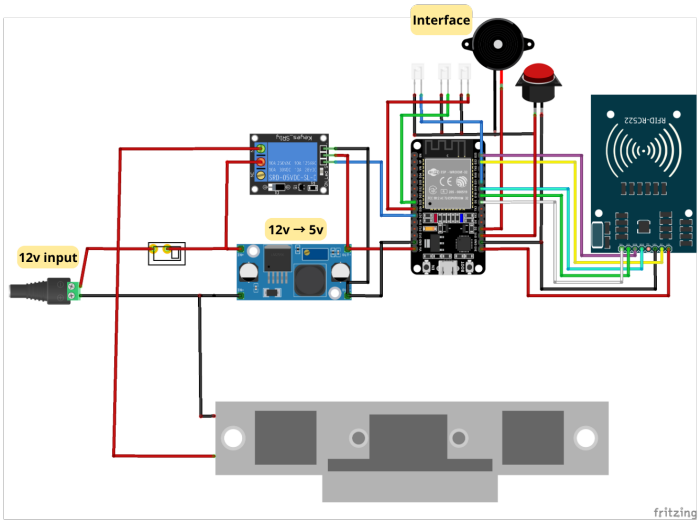

Figura 3. Esquema elétrico do dispositivo.

4. Resultados

O sistema Trancadura 2.0 foi implementado e testado em ambiente real, demonstrando eficácia no controle de acesso em instituições educacionais. Atualmente, duas unidades estão em operação contínua, gerenciando 31 usuários ativos. Os principais resultados obtidos foram:

4.1. Desempenho Operacional

- Taxa de sucesso em leitura RFID: 85% (falhas ocorreram principalmente devido ao posicionamento incorreto do cartão)
- Tempo de recuperação após queda de Wi-Fi: 5-6 segundos
- Taxa de sucesso em atualizações OTA: 90% (9 em 10 tentativas bem-sucedidas)
- Tempo médio de resposta para autenticação: menos de 3 segundos

4.2. Vantagens Financeiras

Uma das principais vantagens da solução desenvolvida é seu baixo custo em comparação com sistemas comerciais equivalentes. Como mostra a Tabela 1, o custo total por unidade é de aproximadamente R$ 212,00, significativamente inferior aos R$ 400-500 cobrados por fechaduras eletrônicas comerciais básicas.

Tabela 1. Tabela de custo da Trancadura 2.0

Item	Trancadura 2.0 (R$)
Dispositivo principal (ESP32)	40,00
Módulo RFID RC522	16,00
Conversor de tensão	12,00
Relé	10,00
Solenoide	120,00
Gabinete com os leds	14,00
Total	**212,00**

Além da economia direta nos custos de hardware, a solução oferece vantagens adicionais:

- Custo de manutenção reduzido devido à capacidade de atualização remota (OTA)
- Flexibilidade para expansão e personalização sem custos adicionais de licenciamento
- Possibilidade de replicação em larga escala com economia de escala

4.3. Testes Práticos

Os testes realizados nos laboratórios do Instituto Federal de Sergipe demonstraram:

- Funcionamento estável mesmo em cenários de uso intensivo
- Eficácia do sistema de logs para auditoria de acessos
- Boa aceitação pelos usuários finais, que destacaram a facilidade de uso
- Confiabilidade do sistema de backup físico (botão e chave mecânica) durante quedas de rede ou energia

Figura 4. Protótipo físico montado em ambiente real.

5. 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, leitores NFC e teclados numéricos, além de desenvolver um aplicativo mobile para facilitar ainda mais o gerenciamento remoto do sistema. Também está prevista a substituição do protocolo Telnet por um modelo de depuração mais seguro, como o SSH. Adicionalmente, planeja-se a integração com sistemas acadêmicos existentes, permitindo, por exemplo, que o acesso aos ambientes seja automaticamente vinculado 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

Bindra, L., Lin, C., Stroulia, E., and Ardakanian, O. (2019). 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)*, pages 32–38.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (LGPD). `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. Acesso em:: 2024-10-01.

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`. Acesso em:: 2024-10-01.

Geepalla, E., Bordbar, B., and Du, X. (2013). Spatio-temporal role based access control for physical access control systems. In *2013 Fourth International Conference on Emerging Security Technologies*, pages 39–42.

IBM (2024). Adopting security ai and automation can cut breach costs. `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`. Acesso em: 2024-09-30.

ITnews (2024). Tangerine telecom says customer data of 232000 affected by 'cyber incident'. `https://www.itnews.com.au/news/tangerine-telecom-says-customer-data-of-232000-affected-by-cyber-inciden` Acesso em: 2024-09-30.

Jornalismo, N. (2024). Falha na rede social spoutible coloca contas em risco. `https://nucleo.jor.br/curtas/2024-02-05-falha-spoutible-contas-em-risco/`. Acesso em: 2024-10-01.

Kaur, G., Singh, A., and Singh, D. (2022). A comprehensive review on access control systems amid global pandemic. In *2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*, pages 15–19.

Leal, F. C., Melo, M. V. S., Matos Júnior, R. S., and Vieira, A. M. (2024). Um protótipo de fechadura eletrônica modular de baixo custo para ambientes acadêmicos. Trabalho não publicado.

TechRepublic (2024). 2024 exposed: The alarming state of australian data breaches. `https://www.techrepublic.com/article/state-of-data-breach-australia-2024/`. Acesso em: 2024-09-30.

Terada, R. (2008). Segurança de dados: criptografia em rede de computador. In *Segurança de dados: criptografia em rede de computador*, pages 15–25. Editora Blucher.