FECHADURA ELETRÔNICA COM INTERFACE WEB EMBARCADA: Implementação de um Sistema Autônomo e Persistente de Controle de Acesso com Gerenciamento de Usuários e Logs

Raquel Silva Coelho[1]; Priscila Lima Rocha[2]; Diego Dutra Sampaio[3];

Resumo

Este trabalho apresenta o desenvolvimento de uma fechadura eletrônica com controle de acesso baseado em autenticação via interface web embarcada. O sistema utiliza uma fechadura solenóide acionada pela interface web, liberando o acesso mediante autenticação do usuário e fornecimento da senha padrão da fechadura. Para garantir segurança, as senhas são armazenadas em formato hash utilizando o algoritmo SHA-256, enquanto os dados de usuários e logs são persistidos em arquivos de texto gerenciados pela biblioteca LittleFS, diretamente na memória flash do dispositivo, assegurando a integridade dos dados mesmo após desligamentos. A interface web permite o gerenciamento de usuários, a visualização dos registros de acesso, a alteração de senhas e a operação da fechadura, distinguindo entre usuários comuns e administradores, tudo de forma local, sem dependência de sistemas externos ou bancos de dados. A implementação foi realizada em uma plataforma embarcada Raspberry Pi Pico W, destacando a viabilidade de soluções autônomas para controle de acesso em ambientes residenciais e comerciais. Os resultados demonstram um sistema funcional, seguro e eficiente para monitoramento e controle de acesso em fechaduras eletrônicas, com potencial aplicação em portas, armários, gavetas e outros compartimentos que demandem autenticação eletrônica e registro confiável de eventos.

Palavras-Chave: Fechadura eletrônica. Controle de acesso. Interface web embarcada. Persistência de dados. Segurança.

Financiamento: Este trabalho foi desenvolvido com apoio do Ministério da Ciência, Tecnologia e Inovação (MCTI), no âmbito do programa Embarcatech, executado pelo IFMA Campus Monte Castelo e coordenado pela Softex.

[1] Estudante do Curso Residência Tecnológica em Sistemas Embarcados (EmbarcaTECH) do IFMA - Campus Monte Castelo; E-mail: raquelcoelho@acad.ifma.edu.br
[2] Doutora em Engenharia Elétrica - UFMA; E-mail: priscila.rocha@ifma.edu.br
[3] Mestre em Engenharia Elétrica - UFMA;

Introdução

O avanço das tecnologias embarcadas tem ampliado a aplicação de soluções inteligentes em diversos setores, especialmente na área de segurança. Nesse contexto, sistemas de controle de acesso vêm se destacando por oferecerem maior praticidade, rastreabilidade e confiabilidade quando comparados às fechaduras mecânicas tradicionais. Apesar disso, muitas soluções comerciais ainda dependem de servidores externos ou de conexão constante com a internet, o que limita sua viabilidade em ambientes com infraestrutura reduzida ou conectividade instável.

Diante dessa lacuna, este trabalho propõe o desenvolvimento de uma fechadura eletrônica com interface web embarcada, projetada para operar de forma autônoma e segura em ambientes residenciais e comerciais. O sistema foi implementado no microcontrolador Raspberry Pi Pico W, utilizando uma fechadura solenóide acionada mediante autenticação de usuários. A solução diferencia usuários comuns de administradores, permitindo não apenas a abertura da fechadura, mas também o gerenciamento de usuários, alteração de senha e consulta de registros de acesso com data e hora.

Como diferenciais, destacam-se o uso do sistema de arquivos LittleFS, que assegura o armazenamento persistente de dados diretamente na memória flash, e a aplicação do algoritmo SHA-256 para garantir a segurança no armazenamento das credenciais. Essas características possibilitam um sistema independente de bancos de dados externos e capaz de manter sua integridade mesmo após desligamentos.

O objetivo principal deste estudo é demonstrar a viabilidade de uma solução embarcada de controle de acesso que combine praticidade, baixo custo e segurança, oferecendo autenticação diferenciada, registro de eventos e gerenciamento local de usuários. Acredita-se que a proposta contribua para ampliar as possibilidades de aplicação de sistemas embarcados na área de segurança, atendendo especialmente a contextos que demandam autonomia e confiabilidade sem dependência de infraestrutura complexa.

Metodologia

O controle de acesso eletrônico tem se consolidado como alternativa mais segura

e prática em relação às fechaduras mecânicas tradicionais, oferecendo funcionalidades adicionais como registro de acessos e gerenciamento diferenciado de usuários. Diversas tecnologias são utilizadas nesses sistemas, incluindo cartões RFID, biometria e autenticação via rede. Nesse contexto, microcontroladores assumem papel central por possibilitarem soluções compactas, de baixo custo e altamente customizáveis, especialmente quando associados a interfaces web embarcadas que permitem interação direta com o usuário em tempo real (LUZERNA, 2018).

O Raspberry Pi Pico W, adotado neste projeto, apresenta recursos relevantes para esse tipo de aplicação, como conectividade Wi-Fi integrada e capacidade de atuar como servidor web. Para garantir armazenamento local e persistente dos dados, foi utilizada a biblioteca **LittleFS**, projetada para memória flash em dispositivos embarcados. Essa solução assegura confiabilidade mesmo após desligamentos inesperados. Quanto à segurança, as senhas foram protegidas com o algoritmo de hash **SHA-256**, amplamente reconhecido por sua robustez criptográfica (CALLAGHAN, 2022). Por fim, o uso do módulo **RTC DS1307** viabilizou a geração de registros com data e hora precisas, elemento essencial para auditoria e rastreabilidade em sistemas de controle de acesso (NIST, 2006).

Trabalhos anteriores apresentam propostas de fechaduras eletrônicas baseadas em microcontroladores, mas muitas vezes sem contemplar de forma integrada todos esses recursos, como persistência local de dados, autenticação diferenciada e interface web embarcada. Assim, este estudo se propõe a desenvolver uma solução completa que reúna tais elementos em um único sistema, visando maior autonomia, segurança e aplicabilidade prática.

Tendo isso em vista, o desenvolvimento deste projeto caracterizou-se como uma pesquisa aplicada, com abordagem experimental, voltada à criação de uma solução embarcada de controle de acesso eletrônico. O objetivo foi elaborar um protótipo funcional, seguro e autônomo, capaz de gerenciar usuários, registrar acessos e operar sem dependência de infraestrutura externa, validado em ambiente controlado.

Componentes de hardware e protótipo

A montagem do sistema foi realizada com base no microcontrolador Raspberry Pi Pico W, conectado a uma fechadura solenóide e periféricos auxiliares. O módulo RTC

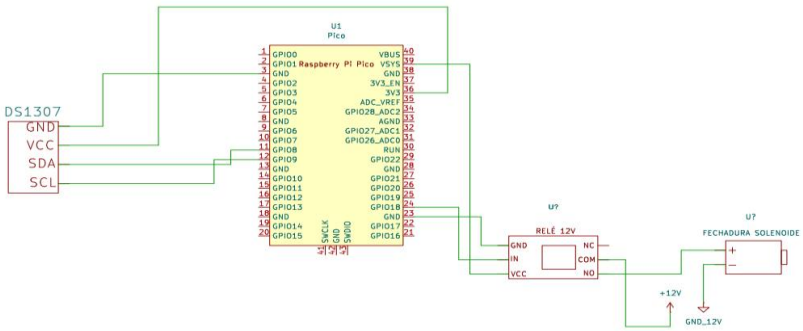
DS1307 foi utilizado para a obtenção de data e hora, permitindo registros precisos de eventos. Um relé eletrônico atuou no chaveamento da fechadura, enquanto LEDs integrados à placa forneceram feedback visual do estado do sistema (trancado ou destrancado). A fonte de 12V garantiu a alimentação da solenóide.

Tabela 1 – Componentes de Hardware utilizados

Componente	**Função**
Raspberry Pi Pico W (Placa BitDog Lab)	Microcontrolador principal já integrado em uma placa de prototipação (BitDog Lab)
USB	Alimentação do circuito via entrada da placa BitDog Lab e comunicação com monitor serial
Módulo RTC DS1307	Fornece data e hora precisas para os registros de eventos. Comunicação via I²C com o Pico.
Fechadura solenóide	Dispositivo de travamento acionado por GPIO via relé.
Relé	Atua como chave eletrônica para controlar com segurança a alimentação 12V
Fonte 12V	Fornece a alimentação necessária para a abertura da fechadura solenóide.

Fonte: Elaborado pela Autora

Figura 1 – Diagrama Elétrico do Protótipo Desenvolvido



Fonte: Elaborado pela Autora via KiCad

Ambiente de desenvolvimento e bibliotecas

O firmware foi desenvolvido em linguagem **C**, utilizando o **Pico SDK** e ferramentas de compilação baseadas em CMake no ambiente Visual Studio Code. A interface web embarcada foi construída em **HTML e CSS** e integrada diretamente ao código, servida por um servidor leve no microcontrolador. Foram empregadas bibliotecas internas do SDK, externas de código aberto e serviços de rede disponibilizados pela residência tecnológica.

Durante a implementação foram utilizadas bibliotecas do próprio SDK, como hardware/i2c.h para comunicação com o RTC, cyw43_arch.h para gerenciamento da rede Wi-Fi, lwIP como pilha de protocolos TCP/IP e pico/stdlib.h para funções básicas de GPIO e temporização. Para armazenamento persistente e segurança, foram empregadas bibliotecas externas: o LittleFS, que implementa um sistema de arquivos confiável na memória flash, e o SHA-256, utilizado para o hashing de senhas. Além disso, serviços de rede como DHCP Server e DNS Server foram incorporados para simplificar a configuração e resolução de nomes na rede local.

Arquitetura do firmware e fluxo de requisições

O sistema foi estruturado de forma modular, garantindo baixo acoplamento e maior facilidade de manutenção.

Tabela 2 – Organização do Firmware

Componente	**Função**
/web	Geração de páginas HTML
/	CRUD em arquivos TXT (LittleFS)
/controle_	Controle de periféricos (RTC, relé)
http	Roteamento de requisições

Fonte: Elaborado pela Autora

O fluxo de funcionamento das requisições segue três etapas:

1. **Requisição HTTP:** recebida via Wi-Fi no endpoint correspondente (ex:

/login).

2. **Callback de rota:** verificação de autenticação, sessão e tipo de usuário, seguida de execução de operações em arquivos locais.
3. **Resposta:** geração de HTML dinâmico ou acionamento físico da fechadura.

Esse processo garante que cada ação passe por autenticação e validação de permissões antes de ser executada.

Armazenamento e segurança

O sistema emprega o LittleFS para gerenciar arquivos em memória flash, estruturados de forma semelhante a CSV.

- **usuarios.txt:** cadastro de usuários com nome, tipo (admin ou comum) e hash da senha.
- **logs.txt:** registro de eventos (logins, trancas e destrancas, alterações de senha) com timestamp do RTC.
- **senha_fechadura.txt:** hash da senha mestra da fechadura.

Para a proteção das credenciais, todas as senhas foram armazenadas utilizando SHA-256, garantindo que não houvesse informações em texto claro. O sistema ainda conta com tokens de sessão, armazenados em cookies, para assegurar a autenticidade do usuário durante a navegação, diferenciando administradores de usuários comuns.

Testes e validação

Os testes foram conduzidos para verificar tanto o funcionamento funcional quanto a robustez do sistema frente a acessos indevidos. Entre eles, destacam-se:

- **Restrição de acesso por tipo de usuário:** usuários comuns não acessaram rotas de administração.
- **Bloqueio de usuários não autenticados:** tentativa de acesso a páginas restritas redirecionou para login.
- **Persistência de sessão:** tokens válidos foram aceitos e corretamente expirados após logout.
- **Dados inválidos:** respostas seguras a credenciais incorretas, sem exposição de informações sensíveis.

- **Integridade de arquivos:** ciclos de leitura/escrita no LittleFS confirmaram a preservação dos dados.

Esses resultados confirmaram que a solução atende aos requisitos de segurança, persistência e autonomia definidos, validando o protótipo como uma alternativa viável para aplicações reais de controle de acesso.

Código implementado

Link: Projeto Fechadura Eletrônica via WEB

Resultados e Discussão

Os resultados obtidos demonstraram a eficácia do sistema como uma solução completa de controle de acesso eletrônico, confirmando sua autonomia e segurança. Todas as funcionalidades essenciais foram validadas em ambiente de teste, evidenciando que a proposta atendeu integralmente aos requisitos definidos.

Tabela 6 – Funcionalidades Validadas

Nome	**Resultados Alcançados**
Interface WEB	Acessível via Wi-Fi Local(AP)
Responsividade	Responsiva em mobile/desktop
Autenticação	Hash-256 para proteção de senhas; Tokens para controle de sessão
Controle de Acesso	Dois níveis de usuário(admin/comum)
Painel do Administrador	Funções específicas para usuário administrador
Acionamento do Hardware	Acionamento remoto da fechadura, após autenticação de senha

Fonte: Elaborado pela Autora

Do ponto de vista funcional, o desempenho do firmware mostrou-se satisfatório. O processo de login, que envolve a aplicação do algoritmo SHA-256 e a verificação nos registros do sistema, ocorreu de forma praticamente instantânea, sem prejuízo à

experiência do usuário. O acionamento da fechadura também foi imediato após a autenticação, confirmando a viabilidade do sistema em aplicações práticas.

O armazenamento persistente, garantido pela biblioteca LittleFS, preservou integralmente os dados de usuários, logs e configurações mesmo após sucessivos ciclos de desligamento e religamento. Essa característica valida a escolha do sistema de arquivos embarcado como solução adequada para ambientes que exigem confiabilidade e persistência de dados, conforme apontado na literatura. Os registros com timestamps fornecidos pelo RTC DS1307 possibilitaram auditoria detalhada das operações, assegurando rastreabilidade e robustez no controle de acessos.

Em termos de segurança, o uso de funções hash criptográficas confirmou-se eficaz. Todas as tentativas de acesso não autorizado foram bloqueadas, respeitando rigorosamente os diferentes níveis de permissão estabelecidos (administradores e usuários comuns). Esse resultado vai ao encontro das boas práticas recomendadas para sistemas de autenticação embarcados, reforçando a proteção das credenciais.

A interface web embarcada mostrou-se responsiva e estável, tanto em dispositivos móveis quanto em computadores, ampliando a acessibilidade e a usabilidade do sistema. Ainda que não tenham sido realizadas medições instrumentais de desempenho, os testes práticos apontaram que os tempos de resposta são adequados e não comprometem o funcionamento do sistema.

Assim, os resultados confirmam que a solução proposta não apenas atende às expectativas levantadas na fundamentação teórica, mas também se destaca por integrar, em um único protótipo, recursos de persistência, segurança criptográfica e interface web embarcada. Como limitação, ressalta-se a ausência de métricas quantitativas mais detalhadas, que poderão ser exploradas em trabalhos futuros.

Conclusão

O desenvolvimento da fechadura eletrônica com interface web embarcada demonstra ser uma solução viável e eficiente para controle de acesso autônomo em ambientes residenciais ou comerciais. O sistema atende plenamente aos objetivos definidos, oferecendo uma interface web responsiva que possibilita o gerenciamento de usuários com diferentes níveis de permissão, o armazenamento persistente de dados por

meio do LittleFS, a proteção de credenciais utilizando o algoritmo SHA-256 e o registro temporal de eventos com o auxílio do módulo RTC DS1307.

Os testes realizados comprovam a confiabilidade do protótipo, que apresenta tempos de resposta satisfatórios tanto na autenticação quanto no acionamento da fechadura, mantendo a integridade dos dados mesmo após múltiplos ciclos de energia. Assim, confirma-se que a proposta integra de maneira equilibrada os requisitos de segurança, autonomia e baixo custo.

Como limitações, identificam-se as restrições da memória flash do Raspberry Pi Pico W, que reduzem a capacidade de armazenamento de usuários e registros, e a complexidade de manutenção da interface web incorporada diretamente ao código C. Essas questões, entretanto, não comprometem a funcionalidade do sistema e indicam oportunidades de aprimoramento.

Entre as melhorias futuras, destacam-se a adoção de armazenamento externo para ampliar o histórico de logs, a separação do código da interface gráfica em arquivos independentes para facilitar atualizações, e a inclusão de recursos avançados de gerenciamento, como filtros e exclusão programada de registros. A integração com outras formas de autenticação, como biometria ou NFC, também representa uma possibilidade de evolução do sistema.

Este trabalho confirma o potencial de soluções embarcadas independentes, de baixo custo e seguras para aplicações em controle de acesso, além de abrir caminho para pesquisas que explorem a ampliação de recursos e a integração com tecnologias da Internet das Coisas.

Agradecimentos

A autora agradece ao IFMA Campus Monte Castelo pela execução do projeto Embarcatech (Residência Tecnológica em Sistemas Embarcados), ao Ministério da Ciência, Tecnologia e Inovação pelo apoio financeiro e à Softex pela coordenação do programa

Referências

CALLAGHAN, Peter. **SHA-256 benefits: Evidence & Authentication. PageFreezer,** 2022. Disponível em: https://blog.pagefreezer.com/sha-256-benefits-evidence-authentication. Acesso em: 30 set. 2025.

LUZERNA, Ricardo Kerschbaumer. **Microcontroladores**. 2018. Apostila. Disponível em: https://professor.luzerna.ifc.edu.br/ricardo-kerschbaumer/wp-content/uploads/sites/43/2018/02/Apostila-Microcontroladores.pdf. Acesso em: 30 set. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Guide to Computer Security Log Management. NIST Special Publication 800-92, 2006.** Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf. Acesso em: 30 jul. 2025.