Um protótipo de fechadura eletrônica modular de baixo custo para ambientes acadêmicos

Felipe C. Leal[1], **Marcos Vinicius S. Melo**[2],
Rubens de S. Matos Júnior[2], **Alfredo M. Vieira**[2]

[1]Universidade Federal de Sergipe - Campus São Cristóvão

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

felipecarvalho5520@gmail.com, marcosvinicius.sm@icloud.com

{rubens.junior,alfredo.vieira}@ifs.edu.br

Abstract. *Security in educational institutions is essential and electronic access control solutions can increase the protection of these spaces. However, the available commercial systems are not cost-effective for large-scale implementation in public institutions. This article presents the development of a prototype of a modular, adaptable and low-cost electronic lock for access control in academic environments. The prototype uses microcontrollers and simple electronic components to ensure an efficient and cost-effective system. The solution offers benefits such as remote control, multiple forms of authorization and easy integration with other systems, making it viable for low budget schools.*

Resumo. *A segurança em instituições educacionais é fundamental e soluções de controle de acesso eletrônico podem aumentar a proteção dos espaços. No entanto, os sistemas comerciais disponíveis têm custos inviáveis para uma implementação em larga escala em instituições públicas. Este artigo apresenta o desenvolvimento de um protótipo de fechadura eletrônica modular, adaptável e de baixo custo para o controle de acesso em ambientes acadêmicos. O protótipo utiliza microcontroladores e componentes eletrônicos simples, para garantir um sistema eficiente e econômico. A solução oferece benefícios como controle à distância, múltiplas formas de autorização e facilidade de integração com outros sistemas, sendo viável para instituições com recursos limitados.*

1. Introdução

Segurança é um tema sensível sendo abordado em diversas vertentes, desde a segurança cibernética, também conhecida como segurança lógica até a segurança física de pessoas, ambientes e equipamentos. Garantir a segurança é um desafio em diversos cenários, mas com a expansão notável das tecnologias voltadas ao paradigma da Internet das Coisas (IoT - *Internet of Things*), diversos dispositivos conectados às redes têm sido utilizados para fins de segurança, tais como câmeras de monitoramento, sensores de presença e fechaduras eletrônicas. No entanto, a escassez de recursos financeiros pode ser um fator complicador importante para alcançar tal cenário inovador em organizações públicas, nas quais o orçamento para tais questões é frequentemente limitado.

Sistemas de autorização flexíveis e modulares para ambientes são incomuns, contudo, apresentam diversas aplicações em ambientes compartilhados. A presença de mais

de um meio de autorização também se faz importante, especialmente em organizações com uma grande variedade de perfis de pessoas que podem/devem ter acesso a um determinado ambiente, a depender dos horários e ou contextos em que se encontram. Esse é frequentemente o caso de universidades, institutos de educação, ciência e tecnologia e escolas, compostas por estudantes, docentes, técnicos de laboratório, pessoal administrativo e outros membros eventuais da comunidade acadêmica, que em diferentes situações devem ou não ter seu acesso concedido a salas de aula, laboratórios, escritórios e outros tipos de ambientes, cada uma destes podendo ter regras de acesso específicas.

A utilização de microcontroladores com acesso a redes Wi-Fi e integrados a um sistema de gerenciamento pode assegurar a gestão eficiente de acesso aos mais diversos ambientes. Para tanto, é importante garantir também a segurança lógica dos sistemas envolvidos em tais mecanismos de controle de acesso físico. A criptografia das comunicações em rede envolvidas e esquemas de proteção contra ataques do tipo "*man-in-the-middle*", entre outros, deveria fazer parte do projeto desse tipo de sistema, mesmo daqueles que possuem recursos computacionais mais limitados.

Este artigo apresenta um protótipo que foi elaborado para um sistema de controle de portas utilizando tecnologias típicas de IoT. Os principais benefícios do uso dessa abordagem são: (1) Controle de Acesso Flexível; (2) Baixo Custo; (3) Relatórios detalhados; (4) Modularidade da solução com múltiplas formas de autorização; e (5) Proteção contra ataques cibernéticos. Esse sistema foi projetado para ter especial utilidade em instituições de ensino públicas, por ser de baixo custo e bastante adaptável às particularidades de cada uma, porém adapta-se a outros tipos de organizações.

2. Fundamentação Teórica

De acordo com [Geepalla et al. 2013], os modelos de controle de acesso digital muitas vezes não são adequados para representar as especificações do controle de acesso físico. É importante considerar características próprias dos ambientes reais, para adaptar as estratégias digitais correspondentes. Em [Bindra et al. 2019] e [Kaur et al. 2022], 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 [Terada 2008], 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 [ITnews 2024]. Outro caso envolve o Spoutible, que teve uma vulnerabilidade em sua API explorada [Jornalismo 2024], 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 [TechRepublic 2024].

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 ataques cibernéticos atribuíram a origem do problema à falta de criptografia em seus sistemas [IBM 2024].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 [EU 2016] e a **LGPD** (Lei Geral de Proteção de Dados) no Brasil [Brasil 2018]. 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. Materiais e Métodos

A solução proposta trabalha sobre a plataforma de desenvolvimento ESP-32 NoceMCU, que permite a integração com redes Wi-Fi, além da conexão com componentes como o leitor de RFid. Para o gerenciamento de dispositivos e permissões, foi desenvolvida uma aplicação web baseada em Django, um framework em Python para o desenvolvimento de aplicações web completas, que administra os sistemas de usuários, dispositivos e permissões. Dessa forma, é possível criar sistemas que integram as tecnologias envolvidas e fornecem soluções robustas para o problema proposto.

O dispositivo possui um relé conectado a uma fechadura elétrica de embutir, como a mostrado na figura 1. Esse tipo de fechadura elétrica permite a integração do dispositivo sem inutilizar o sistema original da porta. Dessa forma, é possível utilizar um sistema de controle de acesso remoto sem perder a opção do uso tradicional das chaves. Essa solução também garante a segurança do sistema em casos de queda de energia ou instabilidades nas conexões dos dispositivos.

Figura 1. Fechadura elétrica utilizada no dispositivo

Para que as requisições do dispositivo ao servidor sejam feitas de forma segura, a autenticação é feita utilizando o endereço MAC e IP do dispositivo, atribuindo um *token*

temporário a cada dispositivo no momento de sua autenticação. Na primeira utilização do dispositivo, o mesmo fica em modo de espera até que um administrador do sistema autorize o dispositivo, para que enfim esse dispositivo possa fazer requisições ao sistema. Os tokens atribuídos são baseados no padrão UUID4, garantindo a segurança do sistema. Vale citar também que todas requisições são feitas por meio do método HTTPS, o que garante que todos pacotes sejam criptografados. Depois de autorizado, o dispositivo deverá enviar o token em todas requisições. Toda autenticação de um dispositivo será armazenada nos logs, contendo o endereço MAC, IP, ID e horário de autenticação do dispositivo.

A plataforma web permite o cadastro de usuários com suas determinadas permissões, dessa forma, é possível administrar a quais ambientes cada usuário terá acesso. Além disso, cada acesso a um ambiente realizado por um usuário é registrado, constando o usuário, ambiente e horário do acesso.

Por meio da plataforma é possível realizar o acesso aos ambientes de algumas formas, a primeira delas é entrando na aplicação, selecionando o dispositivo e realizando uma requisição para a liberação do ambiente. A segunda é possível por meio da leitura de um QRCode associado ao dispositivo, que abre uma página da aplicação e verifica as permissões do usuário para liberar ou não o ambiente. A terceira forma possível através da plataforma é gerando uma senha temporária de 4 dígitos, na qual é possível escolher a duração da mesma. Essa senha temporária fica associada ao dispositivo e permite que usuários que não possuem conta acessem o ambiente através da utilização dessa senha em uma página de autorização da aplicação. Todos os acessos realizados com senhas temporárias são registrados com o usuário que gerou a senha.

Além desses meios de autorização, também é possível conectar um módulo RFid ao dispositivo, possibilitando o acesso de forma rápida pela leitura de uma etiqueta RFid. Antes da utilização de etiquetas RFid, é necessário realizar o cadastro da mesma na aplicação web, que realiza o armazenamento do código hexadecimal da etiqueta. Ela ficará associada a conta do usuário que a possui, possibilitando o gerenciamento do acesso a ambientes e da etiqueta, caso se faça necessária a desativação da mesma. Com isso, as permissões da etiqueta também ficam associadas as permissões da conta de seu possuidor.

4. Resultados

O dispositivo obtido apresenta 84x79x42mm de dimensões externas, como mostrado na figura 2. A caixa que comporta todos os componentes do protótipo foi desenvolvida e impressa com o uso de impressoras 3D, o que garantiu qualidade e supriu nossas necessidades em relação à resistência do dispositivo.

O dispositivo foi montado conforme figura 3. É alimentado por uma fonte 12v, que alimenta o fecho elétrico e um conversor de tensão de 12v para 5v, o que nos permite ligar o restante dos dispositivos do modelo.

O modelo final também apresenta uma interface humano-máquina separada do dispositivo principal, que conta com 3 leds, um azul, um verde e um vermelho, através da qual o azul indica o status da conexão com a internet e o verde e vermelho os status do fecho (Entrada liberada/Entrada bloqueada). Essa interface foi construída para ser posicionada do lado de fora do ambiente, permitindo o usuário verificar a integridade e o funcionamento do dispositivo antes da utilização. Essa interface é conectada ao principal por meio de um conector de 4 pinos.

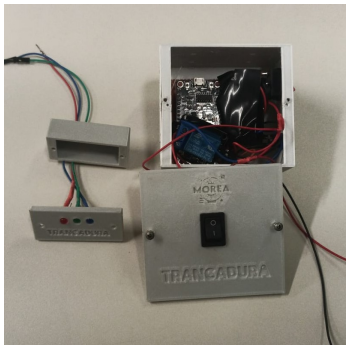

Figura 2. Esquema de montagem do dispositivo

O sensor RFid, por ser um módulo opcional, pode ser conectado ao dispositivo por meio de um conector de 6 pinos. O dispositivo obtido também conta com um botão ligado diretamente a fonte, tendo a mesma função do relé no circuito. Dessa forma, é possível abrir o fecho por dentro do ambiente sem a necessidade de acesso a aplicação web, possibilitando a saída rápida dos ambientes.

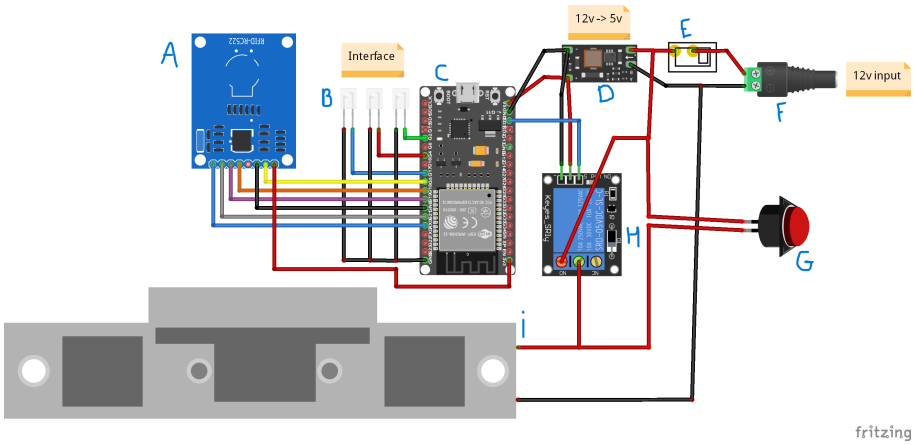

Figura 3. Esquema de montagem do dispositivo

Quanto a aplicação web, foram desenvolvidos os seguintes grupos de páginas: gerenciamento de usuários e permissões, gerenciamento de dispositivos e gerenciamento de etiquetas RFid. Cada grupo de páginas conta com rotas básicas como: criar, ler, editar e deletar, além das específicas de cada grupo, como a de gerenciamento de permissões para usuários e a de liberação de autenticação de dispositivos.

Os QRCodes, um dos meios de autorização, são criados em aplicações externas, e levam o usuário a página referente ao dispositivo, possibilitando a liberação do ambiente pelas permissões da conta do usuário ou senha ativa para o ambiente.

5. Conclusão

O projeto da fechadura demonstrou sucesso nos testes realizados, permitindo o controle de acesso em laboratórios de pesquisa de uma instituição federal. Entre os projetos futuros, destacam-se a criação de novos módulos de autorização, como teclados numéricos e sensores de digitais, além disso, também buscamos reduzir o tamanho do protótipo atual e melhorar os sistemas de segurança presentes.

Baseando-se nos objetivos do projeto, disponibilizou-se o projeto de forma *open-source* (https://github.com/Morea-IFS/), ,já que o mesmo pode ter impacto significativo na gestão inteligente de ambientes e pode ser melhorado e debatido ainda pela comunidade.

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-inci 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.

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.