Fechadura Eletrônica Inteligente com Gerenciamento por Aplicativo e Teclado Numérico

Isadora Barroso Passos[1], **Rian Knupp Verly** [1]

[1]Bacharelado em Sistemas de Informação -
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo Brasil

{isadora.passos,rian.verly}@aluno.cefet-rj.br

Abstract. *The security of residential and commercial spaces still relies on traditional locks, which limit access control and traceability. This work proposes the automation of an electronic lock with local and remote control, using Arduino UNO, a matrix keypad, an electric lock, and a mobile application. The system enables authentication, scheduled password management, and remote unlocking via MQTT. Existing physical structures can be reused, lowering costs. Tests showed effective performance in multiple scenarios, including offline access using an emergency password, confirming the feasibility of the proposal.*

Resumo. *A segurança de ambientes residenciais e comerciais ainda depende de fechaduras tradicionais, com limitações no controle de acesso e rastreabilidade. Este trabalho propõe a automatização de uma fechadura eletrônica com controle local e remoto, utilizando Arduino UNO, teclado matricial, tranca elétrica e um aplicativo móvel. A solução permite autenticação, gerenciamento de senhas com horários definidos e abertura remota via MQTT. A estrutura física existente pode ser reaproveitada, reduzindo custos. Os testes demonstraram funcionamento eficaz em diferentes cenários, incluindo modo offline por senha de emergência, validando a viabilidade da proposta.*

1. Introdução

A Internet das Coisas (IoT, do inglês Internet of Things) representa uma das mais significativas transformações tecnológicas da era digital, conectando objetos físicos à internet e possibilitando a coleta, troca e análise de dados em tempo real. Essa convergência entre o mundo físico e digital vem revolucionando setores como indústria, saúde e segurança residencial [Santos et al. 2016]. No Brasil, a perspectiva futura neste cenário depende da superação de obstáculos como infraestrutura, regulação e capacitação profissional, mas também revela um grande potencial para promover inclusão digital, sustentabilidade e inovação. [Correa et al. 2020].

Sistemas de fechaduras tradicionais, com uso exclusivo de chaves físicas, apresentam limitações tanto em termos de controle de acesso quanto de rastreabilidade. Perder uma chave ou compartilhá-la com terceiros compromete a integridade do ambiente, exigindo soluções mais inteligentes e flexíveis para o gerenciamento de entradas e saídas [Andreas et al. 2019].

Diante desse cenário, a crescente popularização da Internet das Coisas (IoT) abre espaço para soluções que integram tecnologia embarcada e conectividade para automa-

tizar tarefas cotidianas com baixo custo [Santos et al. 2016]. A IoT permite que dispositivos físicos interajam com redes e aplicativos digitais, favorecendo o surgimento de sistemas inteligentes acessíveis para o controle de ambientes [Santos 2018]. A possibilidade de adaptar tecnologias simples, como trancas elétricas já usadas em portões, com dispositivos como o Arduino e sensores de entrada torna viável o desenvolvimento de mecanismos automatizados de segurança [Andreas et al. 2019], sem a necessidade de reformas invasivas ou substituição completa de estruturas existentes [Shinohara 2022].

Neste contexto, este trabalho propõe a automatização de uma fechadura eletrônica utilizando um Arduino UNO, teclado matricial de membrana e uma tranca elétrica acionada por relé, além de um aplicativo móvel para autenticação, gerenciamento de senhas e abertura remota. O diferencial da proposta está na possibilidade de reutilização da estrutura física já instalada na porta, além de permitir a adaptação da tranca elétrica a diferentes tipos de dispositivos, como gavetas, armários e similares, e na redução de custos, promovendo uma solução prática, econômica e escalável para usuários residenciais. A finalidade é possibilitar que o acesso ao ambiente seja controlado de forma local (via senha digitada) ou remota (via aplicativo), com funções como a criação de senhas e a definição de horários de funcionamento.

Os objetivos do trabalho incluem: desenvolver uma arquitetura funcional de fechadura eletrônica de baixo custo com controle local e remoto; validar o sistema por meio de prototipagem com componentes acessíveis; e demonstrar a viabilidade da solução em cenários reais ou simulados. Também se busca avaliar a contribuição da proposta em relação ao estado da arte, identificando seus diferenciais diante de outras soluções de automação residencial apresentadas na literatura.

A principal contribuição deste projeto está na sua simplicidade e adaptabilidade. Esta solução se destaca por não exigir substituição de fechaduras já existentes, por possibilitar a sua adaptação em diferentes dispositivos, por operar com componentes de fácil aquisição e por unir funcionalidades locais e remotas em uma interface acessível ao usuário final. Dessa forma, contribui para democratizar o acesso à automação residencial, com enfoque em segurança e controle inteligente de ambientes.

Os testes realizados com o protótipo demonstraram que a solução desenvolvida é funcional e eficaz. A fechadura foi capaz de operar corretamente em diferentes cenários de uso, permitindo o acesso tanto por meio do teclado físico quanto pelo aplicativo móvel. As senhas cadastradas foram validadas com base em regras de horário previamente definidas, e os comandos de abertura foram executados com rapidez e confiabilidade. O sistema também demonstrou resiliência ao possibilitar o uso de uma senha de emergência mesmo sem conexão com a internet, garantindo acesso em situações críticas. Além disso, a aplicação registrou com precisão todas as tentativas de acesso, permitindo ao usuário consultar um histórico detalhado, reforçando o controle e a segurança do sistema. Esses resultados confirmam a viabilidade do projeto e sua adequação como base para futuros aprimoramentos.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta o estado da arte, revisando propostas semelhantes e discutindo seus méritos e limitações; a Seção 3 detalha a arquitetura e o funcionamento do sistema proposto. A Seção 4 descreve a metodologia de testes e os resultados obtidos; por fim, a Seção 5 apresenta as conclusões

e sugestões para trabalhos futuros.

2. Estado da Arte

O trabalho de [Grossmann 2018] apresenta uma solução completa de fechadura inteligente baseada em protocolos como MQTT-SN, 6LowPan e integração com a plataforma Firebase. O sistema envolve um aplicativo Android robusto que permite cadastrar usuários, visualizar relatórios e abrir a fechadura remotamente. Essa proposta se destaca pela integração avançada com serviços de nuvem, pela segurança oferecida pela autenticação via Firebase e pelo bom nível de detalhamento técnico. No entanto, a implementação é mais complexa, exigindo diversos componentes e conectividade constante com a internet, o que pode dificultar sua adaptação em ambientes com recursos limitados.

Já o estudo publicado por [Meier Basso 2024] propõe uma fechadura inteligente que utiliza a placa ESP32 em conjunto com comunicação Bluetooth Low Energy (BLE), permitindo o acionamento de um servo ou solenóide com base na aproximação de um dispositivo autorizado. A proposta é interessante por sua simplicidade de instalação e por dispensar, em muitos casos, a interação direta com aplicativos. Contudo, seu funcionamento depende da intensidade do sinal BLE, o que representa uma limitação em termos de segurança, especialmente em situações de interferência ou perda do dispositivo móvel autorizado.

O trabalho de [Shinohara 2022] apresenta um sistema completo de controle de acesso com fechaduras eletromagnéticas e integração com câmeras IP, autenticação LDAP e banco de dados MySQL. Essa abordagem se destaca pela robustez e pela possibilidade de gerenciamento detalhado de acessos, inclusive com agendamento semanal para múltiplos usuários. No entanto, trata-se de uma solução mais complexa e de custo elevado, além de exigir infraestrutura tecnológica como redes locais, servidores e sistemas de autenticação, o que pode restringir seu uso a ambientes corporativos ou institucionais mais estruturados.

Por fim, o trabalho de [Carniel et al. 2015] apresenta uma proposta de controle remoto de uma fechadura via rede, utilizando Arduino Mega com shield Ethernet. A solução é simples e viável do ponto de vista técnico, oferecendo acesso remoto básico por meio de uma interface funcional. No entanto, a proposta apresenta segurança limitada e por não contemplar funcionalidades mais elaboradas, como autenticação de múltiplos usuários ou registro de acessos, o que compromete sua aplicabilidade em cenários que exigem maior controle e confiabilidade.

Em comparação aos trabalhos apresentados, a proposta deste projeto se diferencia ao permitir a reutilização de fechaduras já existentes com a adição de uma tranca elétrica simples e de baixo custo, acionada por um Arduino UNO. O uso de um teclado matricial para entrada de senha, em conjunto com um aplicativo móvel para gerenciamento de acessos, oferece um equilíbrio entre segurança, praticidade e acessibilidade. Enquanto outras propostas focam em tecnologias de ponta ou soluções sofisticadas, que exigem infraestrutura complexa, o projeto atual se destaca por sua adaptabilidade e o custo reduzido, facilitando sua adoção em ambientes residenciais sem necessidade de grandes modificações. Com isso, contribui de forma relevante para a disseminação de soluções de automação residencial acessíveis.

3. Apresentação da Proposta

Em consonância com o que foi apresentado anteriormente, este trabalho propôs automatizar uma fechadura utilizando tecnologias como Arduino UNO, ESP8266 (Wi-Fi), transistor, relé, resistores, protoboard e fechadura elétrica, garantindo o funcionamento no nível físico.

No âmbito de software, foi implementado um banco de dados local para armazenar senhas cadastradas, usuários e horários de funcionamento, além da geração de uma senha de emergência válida mesmo sem conexão. O sistema utiliza o broker MQTT como intermediário na comunicação entre a fechadura e os demais componentes. A aplicação móvel desenvolvida com Expo/React Native permite gerenciar senhas, usuários e horários, além de interagir em tempo real com o sistema via WebSocket.

O fluxo de comunicação implementado, ilustrado na Figura 1, consiste em:

1. **Teclado físico → broker → app → fechadura**
   O Arduino monitora o teclado e, ao detectar a tecla "#", formata a senha e a envia via Serial ao ESP-01 com Tasmota. O módulo publica a senha no tópico MQTT `tele/<device-id>/RESULT`. O app, conectado ao broker via WebSocket, detecta essa mensagem, valida localmente a senha e horário no SQLite. Se autorizada, o app publica `"ABRIR"` no tópico `cmnd/<device-id>/SerialSend1`. O ESP-01 recebe e repassa via Serial ao Arduino, que aciona o relé para liberar a tranca por 5 segundos.
2. **Senha de emergência (modo offline)**
   Em caso de falha na conexão Wi-Fi, o app gera uma senha de emergência, armazena-a no banco SQLite e envia ao Arduino via MQTT. Quando digitada no teclado, o Arduino reconhece a senha de emergência localmente e aciona a fechadura sem depender de conexão, garantindo acesso em situações críticas.
3. **Senha via aplicativo (controle remoto)**
   O usuário pode inserir uma senha diretamente no app, que realiza validação local. Se válida, o app publica `"ABRIR"` no mesmo tópico MQTT utilizado anteriormente. O ESP-01 repassa ao Arduino, que libera a tranca. Este fluxo permite controle remoto da fechadura com a mesma segurança aplicada no modo local, sem uso do teclado físico.

3.1. Ferramentas e Componentes Utilizados

Para o desenvolvimento deste projeto foram utilizadas diversas ferramentas e bibliotecas externas que possibilitaram uma integração eficiente entre hardware e software.

O Tasmota foi empregado como firmware no módulo ESP-01, simplificando a comunicação via MQTT sem a necessidade de programar diretamente o ESP. O aplicativo móvel foi desenvolvido com Expo e React Native, facilitando a criação multiplataforma. A biblioteca `MQTT.js` foi utilizada para implementar a interação MQTT via WebSocket no app. Para armazenamento local das senhas e do log de acessos, foi utilizado SQLite via `expo-sqlite`, enquanto a interface foi construída com componentes do `React Native Paper`. Toda a lógica de backend local foi implementada em JavaScript/TypeScript.

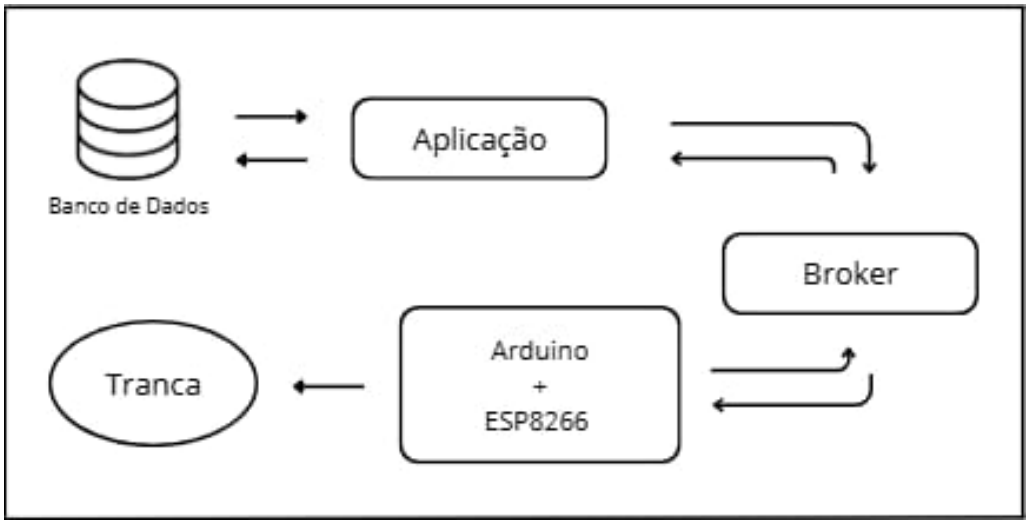

Figura 1. Arquitetura do Sistema Proposto

Componentes Físicos Utilizados

- 1 × Arduino Uno R3
- 1 × Módulo Wi-Fi ESP-8266 (ESP-01)
- 1 × Teclado matricial 4×4
- 1 × Transistor TIP 102
- 1 × Relé 5 V
- Resistores: 2 de 1 kΩ, 1 de 1,8 kΩ
- 1 × Fechadura elétrica 12 V com fonte
- Fios e protoboard

A montagem iniciou-se conectando as oito linhas do teclado matricial, olhando o teclado de frente e começando da esquerda para a direita, aos pinos digitais 9–2 do Arduino. Na protoboard, o transistor TIP 102 teve sua base ligada ao pino 13 do Arduino via resistor de 1 kΩ; seu emissor foi conectado ao GND e o coletor ao relé, com a outra extremidade do relé conectada ao pino 5 V do Arduino. Os contatos do relé (normalmente abertos) foram usados para interligar a fechadura à fonte de 12 V.

Em seguida, utilizou-se o Arduino IDE para carregar o programa `tranca-wifi.ino`, disponível no GitHub[1], que faz uso da biblioteca `Keypad` para mapear o teclado e controlar o relé de forma lógica.

A atualização do firmware do ESP-01 para Tasmota foi necessária para habilitar comunicação Wi-Fi com facilidade, seguindo os passos descritos em [kcow3 2025]. A conexão serial foi estabelecida entre o TX do Arduino e o TX do módulo ESP-01; o RX do ESP-01 foi ligado ao pino RX do Arduino através do divisor resistivo (1 kΩ + 1,8 kΩ) para garantir compatibilidade de tensão. Também foram conectados os pinos GND entre as placas e o CH_PD e 3,3 V do ESP-01 ao 3,3 V do Arduino, assegurando seu funcionamento. *Nota: durante uploads de código para o Arduino, as portas TX e RX devem ser desconectadas*. A Figura 2 mostra o projeto montado.

[1]https://github.com/IsadoraPassos/app-fechaduraIOT.git

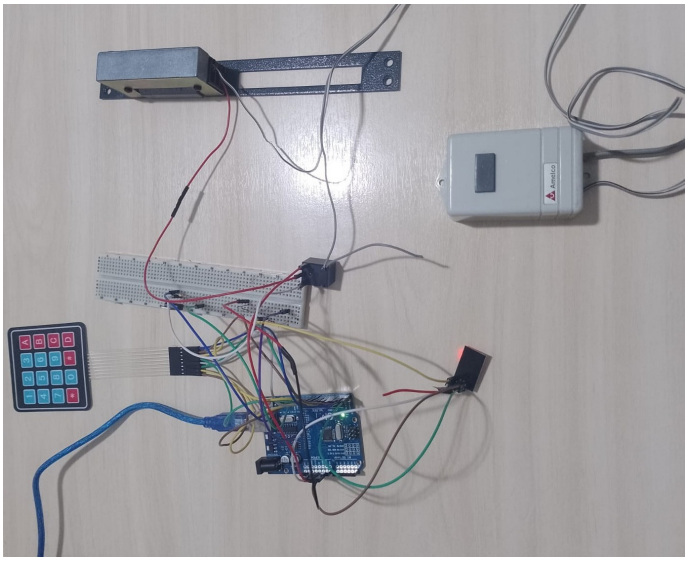

Figura 2. Projeto Físico

3.2. Funcionamento do Sistema

A aplicação móvel desenvolvida para esta solução foi projetada como uma versão demonstrativa dos recursos essenciais para gerenciamento e controle de acesso por fechadura elétrica. Ela oferece uma interface intuitiva que permite ao usuário cadastrar senhas de entrada com validade temporal, além de interagir com o sistema de abertura da fechadura tanto remotamente quanto offline.

As principais funcionalidades implementadas até este momento são: o cadastro de senhas com nome, senha numérica e horário permitido; a validação local utilizando banco SQLite; o envio de comandos MQTT para abertura da fechadura; a recepção de senhas digitadas no teclado físico por meio de tópico MQTT; a geração de senha de emergência no aplicativo e seu envio ao firmware para uso offline; e o registro de um histórico de acessos, com paginação e cores diferenciadas de acordo com o tipo de acesso. O código-fonte e as instruções de execução também estão disponíveis no GitHub[2].

3.3. Segurança Implementada e Pontos a Aprimorar

Neste protótipo, foram adotadas diversas medidas para reforçar a segurança do sistema. A validação de senhas (teclado físico, app ou emergência) ocorre no dispositivo, evitando o envio de credenciais via rede sem tratamento adequado. A comunicação entre o app e o broker MQTT é realizada via WebSocket, o que permite futura migração para WSS com TLS, protegendo dados sensíveis e credenciais de acesso. O armazenamento local utiliza o banco SQLite via *expo-sqlite*, com convenção de consultas parametrizadas para prevenir injeções de SQL. Já o lançamento da senha de emergência segue formato prefixado (*senha:*), reduzindo risco de *spoofing*.

Por se tratar de um protótipo demonstrativo, algumas limitações foram aceitas temporariamente: atualmente não há criptografia no banco, nem uso de armazenamento seguro (como `SecureStore`), e as credenciais MQTT estão presentes no código. Esses

[2]https://github.com/IsadoraPassos/app-fechaduraIOT.git

pontos foram documentados como necessidades a serem resolvidas em uma versão de produção.

4. Resultados de Testes

4.1. Cenários de Teste

O cenário testado envolveu três modalidades principais de uso da fechadura: o acesso presencial via teclado físico com a rede Wi-Fi ativa; o acesso de emergência offline, por meio de uma senha especial gerada no aplicativo; e o acesso remoto via aplicativo, utilizando senha e conexão MQTT. As etapas foram realizadas em um ambiente doméstico, com o Arduino acoplado ao módulo ESP-01 conectado a uma rede Wi-Fi comum, e o smartphone executando o app Expo via WebSocket.

Cenário 1 – Acesso presencial via teclado físico

Para realizar os testes, iniciou-se o servidor Expo com `npm start` e escaneou-se o QR code usando o aplicativo Expo Go no celular. Após abrir o app, o usuário fez login no sistema. Em seguida, acessou-se a tela *Cadastrar Nova Senha*, onde foi criado o usuário Bob, com senha `B123`, válida entre 14:00 e 21:00, como pode ser visto na Figura 3. Ao salvar, a tela exibiu um pop-up informando "Senha cadastrada!", confirmando o armazenamento no banco SQLite, exemplificado na Figura 4.

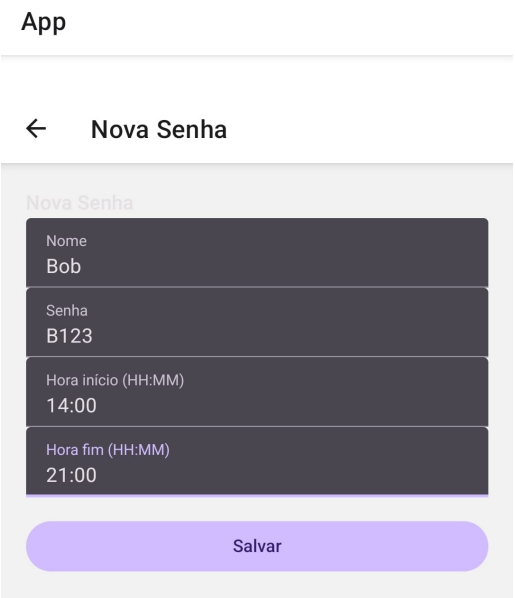

Figura 3. Tela de Cadastro de Senha

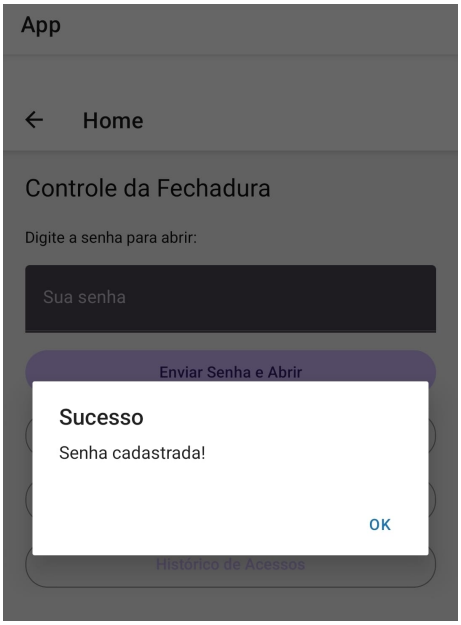

Figura 4. Confirmação do Cadastro de Senha

Com a senha cadastrada, o teste foi realizado no teclado físico conectado ao Arduino. Ao digitar `B123#`, o Arduino enviou a sequência via Serial para o ESP8266 com firmware Tasmota, que publicou a mensagem no tópico MQTT `tele/<device-id>/RESULT`. O app, inscrito neste tópico via WebSocket, capturou a mensagem, extraiu a senha, validou-a no banco de dados e confirmou que estava correta

e dentro do horário permitido. Em seguida, o aplicativo publicou o comando `"ABRIR"` no tópico `cmnd/<device-id>/SerialSend1`, acionando o relé que destravou a fechadura. Como comprovação, o app exibiu o evento no histórico de acessos, com o nome "Bob", status "Acesso permitido" e o timestamp da operação, como mostrado na Figura 5.

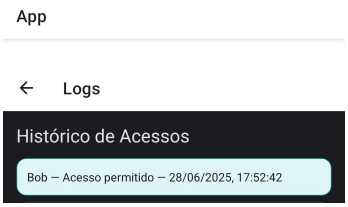

Figura 5. Tela de Logs

Durante o teste, foi possível verificar todas as senhas cadastradas clicando em *Ver Senhas Cadastradas*, onde Bob e outros códigos podem ser visualizados e excluídos conforme necessário, como pode se visto na Figura 6.

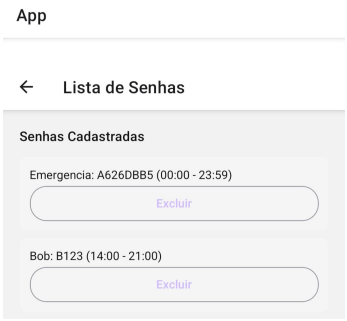

Figura 6. Tela de Listagem das Senhas

Resultado: O protótipo demonstrou-se totalmente funcional, atendendo aos objetivos propostos, como a inserção e validação de senhas via teclado físico, o controle por horário com bloqueio automático fora do período definido, a geração, visualização e exclusão ilimitada de senhas cadastradas, além da disponibilização de um histórico detalhado com nome, status (permitido/negado), data e hora exatas em tempo real.

Cenário 2 – Acesso de emergência offline

Nesse cenário, foi simulada a ausência de Wi-Fi ou broker MQTT, ativando o modo offline. Primeiramente, no aplicativo, acessou-se a funcionalidade de geração de senha de emergência. O sistema gerou automaticamente uma senha aleatória (ex.: `E123456`) e a enviou via MQTT no tópico `cmnd/<device-id>/SerialSend1`, sendo recebida pelo Arduino.

Com o dispositivo desconectado da internet, a senha foi digitada no teclado físico em modo offline. Assim que a sequência `E123456#` foi confirmada, o Arduino a reconheceu localmente, acionou o relé e destravou a fechadura, sem qualquer comunicação com o broker. A aplicação, ao detectar o tópico `tele/.../RESULT` com informação *Emergência: abertura offline*, registrou corretamente no histórico como emergência.

Resultado: A senha de emergência garantiu acesso confiável mesmo na ausência de rede, comprovando a resiliência do sistema. O app registrou o evento com marcação visual de emergência, nome e horário, demonstrando eficácia na funcionalidade offline.

Cenário 3 – Acesso remoto via aplicativo (modo online)

Para testar esta forma de acesso, o Wi-Fi e o broker MQTT estavam ativos, mas o teclado físico não foi utilizado. No app, o usuário inseriu a senha previamente cadastrada (ex.: `B123`) na tela principal e pressionou *Abrir Fechadura*. O app realizou a validação local via SQLite e, ao confirmar o horário e a existência da senha, publicou o comando `"ABRIR"` no tópico `cmnd/<device-id>/SerialSend1`.

O ESP-01 com Tasmota recebeu esse comando e enviou via Serial ao Arduino, que acionou o relé liberando a fechadura. O evento foi gravado no histórico do aplicativo como "Acesso permitido", exibindo o nome associado à senha, data e hora.

Resultado: O acesso remoto demonstrou-se eficiente e seguro, com todas as funcionalidades operando conforme planejado, sem necessidade de teclado físico.

Resultado Geral

Os testes realizados demonstraram que o protótipo da fechadura eletrônica, integrando o aplicativo móvel e o teclado físico, atingiu plenamente os objetivos propostos. O sistema se mostrou funcional, sendo capaz de receber senhas digitadas tanto diretamente no teclado quanto no próprio aplicativo, validando-as com base nas informações armazenadas localmente no banco de dados.

Além da verificação da senha, também é realizada a checagem do horário de validade configurado no momento do cadastro, permitindo ou negando o acesso conforme as regras definidas. O protótipo permite o cadastro de múltiplas senhas, cada uma com nome, valor e faixa de horário específicos, e possibilita ainda sua exclusão.

A interface da aplicação, acessada facilmente pelo Expo Go, oferece uma navegação simples e eficiente, com destaque para a tela de histórico de acessos, onde o usuário pode acompanhar todas as tentativas realizadas, incluindo data, hora, nome associado à senha e o status da tentativa (permitida, negada ou emergência).

5. Conclusões e Trabalhos Futuros

Este artigo apresentou o desenvolvimento de um protótipo funcional de uma fechadura eletrônica de baixo custo, que integra recursos de hardware e software utilizando tecnologias como Arduino Uno, ESP8266 com firmware Tasmota, protocolo MQTT, e um aplicativo móvel criado com React Native via Expo. A proposta teve como finalidade oferecer um sistema de controle de acesso seguro, flexível e acessível, permitindo o gerenciamento de senhas com validade horária e a abertura remota ou presencial da fechadura. Foram implementadas três formas de acesso: via teclado físico, via aplicativo, e por meio de uma senha de emergência capaz de funcionar mesmo sem conexão com a internet. Os testes realizados demonstraram a eficácia da solução, com comunicação fluida entre os dispositivos e correto registro das ações no histórico da aplicação. Dessa forma, o

protótipo atendeu plenamente aos objetivos propostos, validando sua viabilidade técnica e funcional.

Como trabalhos futuros, destaca-se a possibilidade de aprimorar a segurança do sistema com a adoção de autenticação por usuário e senha no aplicativo, uso de tokens JWT e armazenamento seguro das credenciais. Também se propõe a substituição do SQLite por uma base de dados remota com sincronização em nuvem, além da inclusão de uma bateria ao protótipo para solucionar o problema de falta de luz. A comunicação MQTT poderá ser atualizada para uso do protocolo WSS (WebSocket seguro) com TLS, garantindo a confidencialidade dos dados em trânsito. Por fim, podem ser integrados sensores ou câmeras para reforçar a segurança física, bem como um painel web administrativo para gerenciamento remoto dos acessos e dispositivos.

Referências

Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., and Wibisurya, A. (2019). Door Security System for Home Monitoring Based on ESP32. *Procedia Computer Science*, 157:673–682.

Carniel, G., Borsoi, B. T., Brito, R. C., and Favarim, F. (2015). Projeto e Desenvolvimento de Fechadura Eletrônica controlada pela Internet. *Anais do Computer on the Beach*, 6:031–040.

Correa, J. S., Sampaio, M., Barros, R. d. C., and Hilsdorf, W. d. C. (2020). IoT and BDA in the Brazilian future logistics 4.0 scenario. *Production*, 30:e20190102.

Grossmann, G. H. (2018). IoT Smart Lock (ISL): sistema de fechadura inteligente, utilizando protocolos de Internet das Coisas.

kcow3 (2025). Easy ESP-01 Tasmota Programming.

Meier Basso, C. A. (2024). PROPOSTA DE FECHADURA INTELIGENTE USANDO TÉCNICAS DE IOT, VISANDO A CONVERSÃO DE FECHADURAS TRADICIONAIS. *Revista Mundi Engenharia, Tecnologia e Gestão (ISSN: 2525-4782)*, 9(2).

Santos, B. P., Silva, L., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N., and Loureiro, A. (2016). Internet das coisas: da teoriaa prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos*.

Santos, S. (2018). *Introdução à IoT: Desvendando a Internet das Coisas*. SS Trader Editor. Google-Books-ID: EmVaDwAAQBAJ.

Shinohara, F. T. D. (2022). *Desenvolvimento de sistema baseado em IoT para controle de acesso com fechaduras eletromagnéticas*. bachelorThesis, Universidade Tecnológica Federal do Paraná.