REVISTA Mundi
Engenharia, Tecnologia e Gestão
INSTITUTO FEDERAL Paraná

UMA PROPOSTA DE FECHADURA INTELIGENTE USANDO TÉCNICAS DE IOT, VISANDO A CONVERSÃO DE FECHADURAS TRADICIONAIS

A SMART LOCK PROPOSAL USING IOT TECHNIQUES, AIMING THE CONVERSION OF TRADITIONAL DOOR LOCKS

Carlos Alberto Meier Basso[1]

Resumo: O presente estudo traz uma proposta de fechadura inteligente para portas que possa dispensar uma pessoa de ter que carregar e gerenciar chaves tradicionais. Tal proposta se baseia em um dispositivo *IoT* que exija um mínimo de adaptações para sua instalação e o mínimo de interações humano/computador para proceder com o bloqueio e desbloqueio da fechadura. Para tal, a referida fechadura inteligente foi desenvolvida usando uma placa ESP32, se comunicando com dispositivos chave por meio de *Bluetooth Low Energy*, com auxílio de uma fechadura por solenóide ou por meio de um servo e peças impressas em 3D para, assim, proceder com o trancamento e abertura de fechaduras tradicionais já presentes na maioria das casas.

Palavras-chave: Internet das Coisas. IdC. fechadura inteligente.

Abstract: The present study introduces a proposal for a smart door lock that can eliminate the need for a person to carry and manage traditional keys. This proposal is based on an IoT device that requires minimal adaptations for its installation and the least amount of human-computer interaction to perform the locking and unlocking of the lock. To achieve this, the aforementioned smart lock was developed using an ESP32 board, communicating with key devices via Bluetooth Low Energy, with the assistance of a solenoid lock or a servo, and 3D-printed parts to facilitate the locking and unlocking of traditional locks already present in most homes..

Keywords: Internet of Things. IoT. Smart Lock.

[1] MSc em Ciência da Computação, IFPR/Foz do Iguaçu, meierbasso@gmail.com.

1 INTRODUÇÃO

A Internet das Coisas (IoT) é uma rede de objetos e dispositivos conectados à internet, permitindo a troca de dados e informações sem a necessidade de interação humana, visando realizar vários processos do cotidiano (MAGRANI, 2018). Em casas inteligentes, a IoT é usada para automatizar tarefas domésticas, tornando a vida mais conveniente e eficiente (MAMONOV e BENBUNAH-FICH, 2019).

Para que o modelo de casas inteligentes possa evoluir adequadamente, é necessário que sejam desenvolvidos dispositivos que fazem a ponte entre controles manuais tradicionais, presentes há muitos anos na maioria das casas, para controles automatizados inteligentes. Dessa forma, criando dispositivos inteligentes que adaptam controles manuais e tradicionais, é possível que a adoção de dispositivos para casas inteligentes aconteça de maneira mais expressiva - ainda que mais suave e orgânica - já que consistem apenas em adaptações que trazem digitalização e inteligência a dispositivos tradicionais (MAMONOV e BENBUNAH-FICH, 2019).

Assim, o presente estudo tem como **objetivo** o desenvolvimento de uma proposta de fechadura inteligente para portas, que possa dispensar uma pessoa de ter que carregar e gerenciar chaves tradicionais[2].

Este estudo visa, também, encontrar formas de utilizar tecnologias de Internet das Coisas (*IoT*) para viabilizar um modelo de fechadura inteligente com as seguintes **características**:

- baixo custo de construção;
- exigir o mínimo possível de adaptações para a instalação (para que a instalação possa ser feita por um leigo);
- funcionar com fechaduras tradicionais (com chave ou com solenóides);
- exigir o mínimo possível de interação entre usuário e fechadura;
- ser rápida (preferencialmente mais rápida que uma fechadura com chaves tradicionais);

[2] Por “chaves tradicionais”, consideramos aquelas fabricadas em metal, sem nenhum tipo de eletrônica.

- ser multiplataforma e compatível com o maior número possível de dispositivos móveis (evitando o uso de um *app*[3] caso possível);
- permitir o desenvolvimento futuro de formas de acesso alternativas (pela internet ou usando biometria);
- código e modelo abertos, para o desenvolvimento da ideia pela comunidade;

Para tal, foi desenvolvido um modelo que usa uma placa ESP32[4], com auxílio de um servo[5] e peças impressas em 3D, e pode ser adaptada às chaves e fechaduras tradicionais já presentes na maioria das casas, ou, ainda, a uma fechadura com solenóide[6]. A fechadura reage quando um dispositivo móvel do usuário, previamente cadastrado, se aproxima da porta, o que é calculado por meio da intensidade de sinal da conexão *Bluetooth Low Energy* (*BLE*)[7] do dispositivo móvel captada pelo ESP32.

Para detalhar os experimentos, o presente artigo é seguido por uma seção de desenvolvimento, que mostra alguns estudos correlatos e ferramentas disponíveis no mercado. Na sequência é apresentada a seção tratando da metodologia aplicada, seguida pela seção com o modelo proposto e resultados obtidos. Ao final, apresentamos conclusões e possibilidades de trabalhos futuros, bem como as referências utilizadas no presente artigo.

2 DESENVOLVIMENTO

Existem alguns estudos que tratam do desenvolvimento de fechaduras eletrônicas e que trazem resultados interessantes. Entre eles, Mamonov e Benbunah-Fich (2019) fazem um estudo sobre os fatores chave que afetam a intenção de adoção de fechaduras inteligentes. Entre os diversos pontos

[3] Aplicativo para dispositivos móveis;

[4] ESP32 são microcontroladores do tipo "sistema em um chip", munidos de formas de conexão de dados, amplamente utilizadas em soluções IoT (BABIUCH; FOLTYNEK; SMUTNY, 2019)

[5] Servo motor é um dispositivo eletromecânico projetado para controlar e realizar movimentos precisos em resposta a sinais de controle (SHANTHINI, et al. 2020), usado, neste trabalho, para movimentar uma chave em uma fechadura tradicional.

[6] Dispositivo eletromagnético que converte energia elétrica em movimento mecânico, neste caso, para destrancar uma fechadura.

[7] BLE é uma tecnologia de rede sem fios de curta distância proeminente em aplicações onde o consumo de energia é crucial (AFANEH, 2022).

avaliados, os autores concluem que as influências mais relevantes para a adoção das fechaduras inteligentes é a “utilidade percebida pelo utilizador” e a “facilidade de uso percebida pelo utilizador".

Yu (2018) faz um estudo sobre fechaduras digitais, no qual trata de vários tipos possíveis de chaves e interações para destrancar a porta. Entre os exemplos, ele apresenta, por exemplo, que o uso de um *PIN*[8] para abrir a porta tem uma vantagem sobre chaves tradicionais pois não é necessário carregá-las. Porém, com o passar do tempo, os números apresentados no teclado numérico começam a ficar marcados, podendo sugerir a uma pessoa mal intencionada quais são os dígitos usados no *PIN*. Assim, seria necessário a troca do *PIN* a cada poucos meses, o que ofereceria uma desvantagem, já que o *PIN* trocado com frequência pode ser esquecido, especialmente quando se está com pressa de entrar em casa. Uma desvantagem também, é que a interação com um teclado não é muito prática para o uso repetitivo de abrir a porta com frequência.

Yu (2018) continua seu artigo apresentando benefícios e problemas dos variados tipos de chaves e chega em um modelo que considera ideal para uma fechadura inteligente: que forneça a possibilidade de chaves carregadas (usando *smart cards*) ou chaves não carregadas (usando uma tela sensível ao toque) e que, além disso, possibilite funcionar quando não há energia elétrica (disponibilizando uma porta *USB* para ligar uma bateria externa e fazer com que a fechadura funcione). Por fim, o autor trata de uma prova de conceito que elaborou usando um computador portátil (*laptop*) cujas interações durante os testes eram feitas em sua tela sensível ao toque.

Hadis *et al.* (2018), por sua vez, apresentam o design de sistemas de fechaduras inteligentes usando a tecnologia *bluetooth*[9] *(BT)*. Não há a apresentação de um protótipo ou modelo implementado, mas sim uma discussão de como o acesso pode ser feito usando *BT* em vez de chaves tradicionais. Também é tratada a arquitetura do sistema, aspectos de segurança do *BT* e detalhes sobre as aplicações. No referido artigo, os autores apresentam uma

[8] *PIN*, do inglês, Número de Identificação Pessoal - é um número de identificação usado como senha para identificação de acesso a um dispositivo;

[9] *Bluetooth* é um tipo de rede sem fios de curta distância que surgiu como uma tecnologia para substituir cabos em dispositivos como fones de ouvido, mouses, teclados, etc. (AFANEH, 2022)

forma interessante de funcionamento para o dispositivo que destranca a porta com a aproximação de uma chave *BT*.

Como pode ser observado no modelo proposto (HADIS, 2018), a fechadura se abre automaticamente quando o sinal do *BT* fica consideravelmente forte, ou seja, quando uma pessoa portando uma chave *BT* está bastante próxima. O efeito inverso também é representado: quando o portador da chave *BT* se afasta, a fechadura é trancada.

O artigo mencionado é interessante por apresentar um modelo e cenários de funcionamento de uma fechadura inteligente, mas ele não traz muitos dados técnicos que possam reproduzir os resultados esperados.

Já Shanthini *et al. (*2020) e Prakash *et al.* (2017) apresentam um modelo similar ao do presente estudo. Para isso, usam uma placa Arduino, com um módulo *bluetooth* e um servo. O modelo é bastante simples e exige a instalação de um aplicativo em um dispositivo móvel para controlar a abertura e fechamento da fechadura. A fechadura em si é uma prova de conceito, no qual o servo apenas abre e fecha uma simples tramela física. Não há interação com uma fechadura tradicional ou o uso de fechaduras com solenóide.

Existem outras pesquisas interessantes que tratam de fechaduras inteligentes, como a de Prabakaran *et al.* (2021) que é mais focada em idosos e pessoas com deficiências, a de Kavde *et al.* (2017) com foco na liberação da porta à distância para pessoas autorizadas, e a de Baikerikar *et al.* (2021), que propõe uma fechadura com senha para acesso em quartos de hotéis e outros tipos de hospedagens.

Todos os modelos relatados na presente seção tem características únicas e interessantes, mas não atendem plenamente as características desejadas e apresentadas na introdução do presente artigo: a maioria precisa da interação com um *app* ou comandos no servidor *web* para a liberação da fechadura. Também não tratam sobre a possibilidade de adaptação de fechaduras tradicionais.

Existem algumas fechaduras inteligentes disponíveis no mercado que atendem às características mencionadas. Segundo Aluri (2020), existem modelos de fechaduras inteligentes das marcas August e Dana que podem ser

desbloqueadas por meio de comandos no app ou de forma automática (com a aproximação de um dispositivo *bluetooth*). Essas fechaduras estão disponíveis no mercado, porém, não se pode afirmar que sejam de “baixo custo”. Além disso, o código fonte do *app* de tais fechaduras é fechado - ficando, assim, dependente do fabricante pela manutenção de seu funcionamento futuro. Ambas são características que não atendem ao que foi proposto no presente artigo.

Assim, para atender todas as características desejadas, optamos por sair um pouco do tradicional e testar elementos menos explorados.

3 METODOLOGIA

O estudo foi iniciado com a tentativa de identificar qual a forma ideal de destrancar a porta. Avaliou-se que isso deve exigir o mínimo possível de interação entre usuário e fechadura, pois o objetivo de uma fechadura de porta é o de apenas manter pessoas não autorizadas do lado de fora. Isso também está de acordo com o estudo de Mamonov e Benbunah-Fich (2019), mencionado anteriormente, que afirma que uma das características mais procuradas em uma fechadura inteligente é “facilidade de uso percebida pelo utilizador".

Dessa forma, avaliando modelos disponíveis no mercado e na literatura, foi identificado que o ideal em uma fechadura residencial é que ela tranque ou destranque apenas com a aproximação da pessoa ou da chave autorizada. Algum tipo de biometria também pode ser relevante, para que não seja necessária uma chave, porém, a biometria faz com que uma interação com um sensor ou dispositivo seja necessária - mais interação e possivelmente mais tempo para proceder com a abertura da porta.

Hoje em dia, muitas funcionalidades estão convergindo para serem usadas com dispositivos móveis, sejam eles *smartphones*, relógios inteligentes, entre outros. Esses dispositivos, por exemplo, já substituem uma carteira física, uma vez que podem disponibilizar documentos digitais, cartões de crédito, dinheiro, etc., além de outras aplicações e benefícios amplamente conhecidos. Assim, percebe-se que dispositivos móveis podem ser bons substitutos para chaves tradicionais - e ideais para o trancamento e destrancamento da porta

somente com a aproximação, já que possuem diversas formas de conexão sem fios.

3.1 Formas de conexão

Os dispositivos móveis possuem vários tipos de conexões que podem ser utilizados para se comunicar com a fechadura inteligente, entre eles as conexões *Wi-Fi*[10]*, Bluetooth e NFC*[11].

A conexão *NFC* necessita que o dispositivo chave[12] seja aproximado para encostar (ou quase) no sensor de leitura. Assim, foi descartada pois as outras formas de conexão mencionadas poderiam fazer um processo similar a uma distância maior.

As conexões *Wi-Fi e Bluetooth*, por sua vez, são muito versáteis e podem se comunicar com a fechadura inteligente apenas com a aproximação. Destas, a *Wi-Fi* talvez seja a mais versátil, mas foi previamente descartada porque exige que a fechadura inteligente esteja ligada à tomada ou que sua bateria tenha que ser carregada com uma frequência maior do que com o uso de *Bluetooth*.

3.2 Variações do *Bluetooth*

Existem dois tipos de dispositivos *Bluetooth*: um deles é chamado de *Bluetooth Classic* (*BC*) e o outro é conhecido como *Bluetooth Low Energy* (*BLE*). Ambos os tipos de *Bluetooth* são incompatíveis entre si, mesmo que eles compartilhem a mesma marca e o mesmo documento de especificação. Assim, um dispositivo *BC* não consegue se comunicar diretamente com um dispositivo *BLE*. Por essa razão, alguns dispositivos como os *smartphones* optam por implementar as duas versões do *Bluetooth* (o que é conhecido como modo

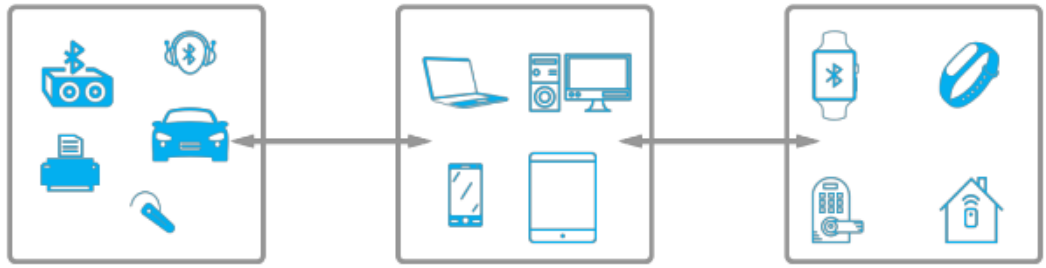
[10] *Wi-Fi* é uma tecnologia de rede sem fio que permite conectar dispositivos eletrônicos, como computadores, *smartphones*, tablets e smart TVs, à internet ou a uma rede local.

[11] *NFC* é a sigla para *Near Field Communication*, que significa algo como Comunicação em Campo Próximo, em português. É uma tecnologia de comunicação sem fio de curto alcance, que permite a troca de informações entre dispositivos móveis encostando (ou quase) os equipamentos.

[12] Nos referimos a "dispositivo chave" como um dispositivo eletrônico que possa ser utilizado para substituir as "chaves tradicionais" quando usado em conjunto com uma fechadura inteligente.

duplo), para que possam se conectar com uma gama maior de dispositivos. Na Figura 1 podem ser vistos dispositivos que comumente usam *BC*, modo duplo ou *BLE* (AFANEH, 2022).

Figura 1 – Tipos de dispositivo Bluetooth.



Fonte: (AFANEH, 2022).

O *BLE* foi introduzido na versão 4.0 da especificação do *Bluetooth* e é mais proeminente em aplicações onde o consumo de energia é crucial (como dispositivos alimentados por pilhas e baterias) e onde pequenas quantidades de dados são transferidas (como em aplicações com sensores). Por essa razão, o *BLE* se tornou o protocolo mais comum em dispositivos *IoT* (AFANEH, 2022) e, também, foi utilizado neste estudo.

3.3 O microcontrolador

Considerando a possibilidade da utilização do *BLE*, identificou-se que a placa ESP32 atende as necessidades para viabilizar a fechadura inteligente proposta. As placas ESP32 são microcontroladores do tipo *SoC* (do inglês: sistema-em-um-chip) que vem provido de *Wi-Fi* (802.11 b/g/n) e *Bluetooth* versão 4.2 de modo duplo (tanto *BC* quanto *BLE*), e são amplamente utilizadas em soluções *IoT* (BABIUCH; FOLTYNEK; SMUTNY, 2019).

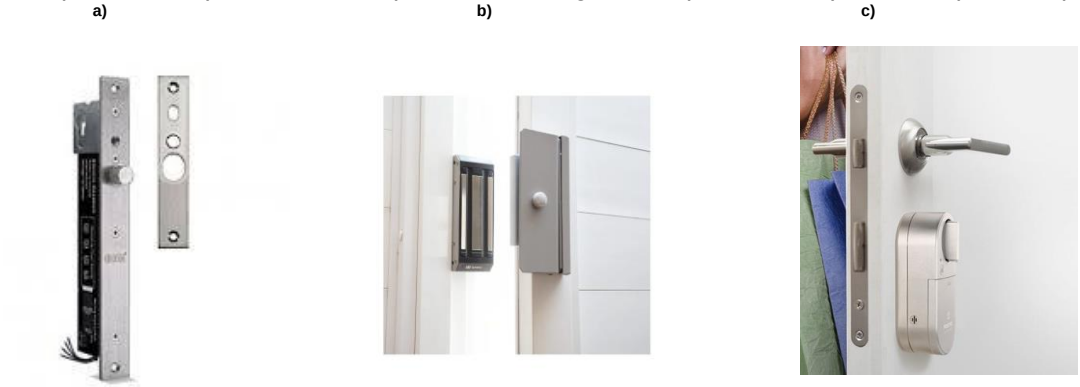
Além das características já mencionadas, as placas ESP32 são bastante compactas e econômicas em consumo de energia. Tais características são ideais para o uso em uma fechadura inteligente, que tem pouco espaço disponível e a alimentação de energia comumente é feita por pilhas e baterias.

Além da placa e de formas de conexão, para desenvolver a fechadura inteligente é necessário um mecanismo eletromecânico para efetuar o trancamento e destrancamento físico da porta.

3.4 Possibilidades para o mecanismo eletromecânico de destrancamento

Foram avaliados alguns tipos de mecanismos para o destrancamento físico da porta. Os modelos mais comuns são a fechadura por solenóide, a fechadura magnética e a fechadura por acionamento de motor (ou servo). Todas elas estão representadas em exemplos na Figura 2.

Figura 2 – Exemplos de mecanismos de destrancamento de portas, da esquerda para a direita: a) fechadura por solenóide; b) fechadura magnética; c) fechadura por motor (ou servo).



Fonte: Internet.

Identificados os materiais necessários, foi possível desenvolver um modelo de fechadura para atender aos objetivos propostos.

4 O MODELO PROPOSTO E SEUS RESULTADOS

Considerando as propostas e tecnologias avaliadas, optou-se por elaborar um primeiro modelo no qual uma placa ESP32 fica obtendo pacotes *BLE* próximos e, se eles fossem emitidos por uma chave *BLE* autorizada, emitem um sinal de trancamento ou destrancamento na medida em que o dispositivo chave se aproxima ou se afasta.

A aproximação ou afastamento do dispositivo chave pode ser identificado pelo ESP32 por meio da característica conhecida como *RSSI*[13]. O valor do *RSSI* diminui na medida em que o dispositivo chave se aproxima da fechadura inteligente. Em testes efetuados, um valor entre 100 e 60 do *RSSI* entre o dispositivo chave e a fechadura inteligente, é o ideal para destrancá-la.

Para evitar o trancamento e destrancamento da fechadura enquanto a porta está aberta, pode-se também utilizar um sensor *Hall*[14] que vem embarcado no ESP32. A necessidade do uso do sensor *Hall* é acessória e pode ser desabilitada no código fonte desenvolvido. Para usá-la, exige-se que um magneto esteja fixado na vista da porta, e que seu lado negativo fique próximo ao ESP32 ao fechar a porta. Assim, é possível identificar quando a porta está fechada - na posição adequada para proceder com o trancamento.

Outros dispositivos acessórios que foram implementados são:

- um LED para gerar um *feedback* visual de quando a porta está trancada.
- um LED para gerar feedback visual de quando um dispositivo chave foi identificado no perímetro para destrancar a fechadura;
- um botão para destrancar a fechadura inteligente (pelo lado de dentro) sem precisar de um dispositivo chave;

Dando continuidade, para que a fechadura inteligente possa identificar um dispositivo chave, utilizou-se inicialmente o endereço *MAC* de sua interface *BLE*. Se o endereço *MAC* do dispositivo chave está próximo da fechadura inteligente, e a porta está fechada, o ESP32 procede com o destrancamento - ou com o trancamento no caso inverso.

[13] O RSSI (*Received Signal Strenght Indicator*) é o nível do sinal recebido por um aparelho receptor como um smartphone, por exemplo. Este nível significa a potência com que o sinal chega no receptor.

[14] Um sensor *Hall* é um dispositivo que mede a intensidade do campo magnético aplicado.É amplamente utilizado em aplicações como medição de velocidade de rotação, detecção de posição, sensores de corrente e muito mais.

4.1 O problema do endereço *MAC* variável

Nos experimentos efetuados, ao utilizar o ESP32 para escanear pacotes *BLE* nas proximidades, a única informação fixa, sempre obtida independente de dispositivo, é o seu endereço *MAC*. Podem haver outras informações, mas nem sempre são garantidas sem o uso de um *app* de apoio. O endereço *MAC* pode ser usado para identificar um dispositivo chave autorizado, porém, percebemos que, por questões de privacidade, os endereços *MAC* são trocados automaticamente nos dispositivos móveis a cada pouco tempo - para que não sejam facilmente rastreados por terceiros. Percebemos tal padrão tanto em dispositivos móveis com Android[15], quanto com iOS[16]. Isso poderia inviabilizar o uso desse atributo para identificar um dispositivo chave.

Com o avançar dos experimentos, porém, foi observado que, se a fechadura inteligente tiver implementado um Servidor *BLE* (que permita a conexão de dispositivos clientes), e se o dispositivo chave se conecta ao menos uma vez nesse servidor, ele passa a sempre utilizar o mesmo endereço *MAC* para se comunicar com a fechadura inteligente, resolvendo, assim o problema do endereço *MAC* variável.

A forma para realizar essa conexão do dispositivo chave (cliente) com a fechadura eletrônica (servidor), pode variar dependendo do sistema operacional utilizado. Dispositivos chave com o sistema operacional Android permitem a conexão com a fechadura eletrônica usando a aplicação nativa de *Bluetooth*. Dispositivos utilizando o sistema operacional iOS, por sua vez, não permitem a conexão com *BLE* usando o aplicativo padrão de configurações *Bluetooth*, portanto, nesses dispositivos, é necessária a utilização de um aplicativo que controle a conexão *BLE*.

[15] Android é um sistema operacional baseado em Linux, desenvolvido pela Google e utilizado principalmente em smartphones e tablets.

[16] iOS é um sistema operacional móvel desenvolvido pela Apple para seus dispositivos, como *iPhones* e *iPads.*

4.2 O mecanismo de cadastro de chaves

Como uma das características do modelo proposto por este estudo é a de exigir o mínimo de alterações possíveis e o mínimo de interação possível entre o usuário, dispositivo chave e fechadura, houve, também, a necessidade de avaliar uma forma de fazer o cadastro do dispositivo chave na fechadura.

Os trabalhos correlatos mencionados na seção de Desenvolvimento funcionam de forma diferente, na qual a fechadura consulta dados em um servidor *web*, no qual as chaves são cadastradas, ou a configuração é feita por um *app* diretamente na fechadura.

Considerando que, na medida do possível, procurou-se evitar o uso de um *app* no dispositivo chave, foi necessário elaborar um mecanismo para cadastrar as chaves diretamente na fechadura inteligente: para tal, o dispositivo chave deve conectar no servidor *BLE* da fechadura, usando seu aplicativo nativo de conexão *Bluetooth* e, logo que conectado, um botão deve ser acionado na fechadura (no lado interno) para cadastrar o *MAC* como uma “chave aceita”. A partir desse momento, basta que o dispositivo chave se aproxime da fechadura para que seja destrancada, não necessitando nova conexão ao servidor *BLE*.

Além da definição do sistema de chaves, foi necessária a definição de um mecanismo eletromecânico para o destrancamento físico da fechadura.

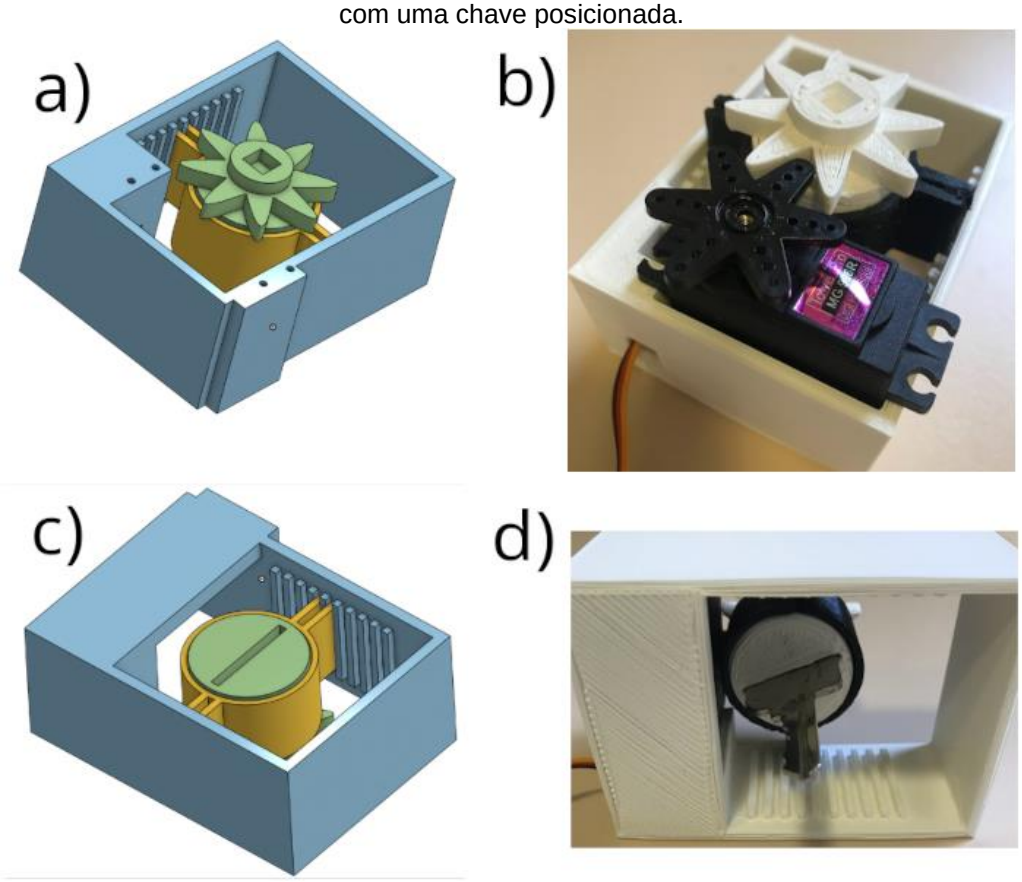
4.3 Definição dos mecanismos eletromecânicos de destrancamento

Optou-se por não limitar o modelo de fechadura inteligente aqui proposto a nenhum dos três mecanismos de destrancamento apresentados na Figura 2, já que cada um deles tem seus prós e contras. Por exemplo, cada um dos três mecanismos pode facilitar a instalação em diferentes tipos de portas. Assim, foi feito com que o ESP32 emita sinal para a abertura de mecanismos do tipo solenóide ou magnéticos (em um de seus pinos de saída digital) e controle um servo (por meio de um de seus pinos de saída analógica), tornando-se, assim, bastante flexível.

Para os testes da fechadura inteligente, utilizou-se um mecanismo do tipo solenóide que recebe sinal por alguns segundos (enquanto deve ficar destrancada). Tal mecanismo, similar ao representado na Figura 2a, funcionou satisfatoriamente.

Também foi desenvolvido um mecanismo com impressão 3D para avaliar se um servo seria capaz de girar uma chave física - o que está representado na Figura 3. O mecanismo conseguiu girar a chave física usando um servo do tipo MG996R.

Figura 3 – Modelo 3D gerado como protótipo: a) visão superior do modelo; b) foto superior do modelo com o posicionamento do servo; c) visão inferior do modelo; d) foto inferior do modelo com uma chave posicionada.



Fonte: autoria própria.

4.4 Custos envolvidos

Para o desenvolvimento deste modelo de fechadura, são necessários uma placa ESP32 e alguns acessórios. São acessórios: uma fechadura de

solenóide ou um servo atrelado a um mecanismo que deve ser impresso em uma impressora 3D.

Para definir os custos e identificar se o resultado final pode ser considerado uma fechadura inteligente de baixo custo, foi feito um levantamento dos preços no mercado nacional, sem levar em consideração o frete, e por fim, foi feita uma média entre os três preços mais baixos de cada componente (levantados em Janeiro de 2024). Os valores foram expressos em Dólar, já que se trata de itens importados, originalmente precificados nessa moeda.

Uma placa ESP32 custa em média U$ 8,70, uma fechadura de solenóide pequena de 5 a 12 Volts custa em média U$ 10,00 e um servo motor do tipo MG995 ou MG996 (reforçados) custam em média U$ 9,00. Não foram aqui calculados custos de impressão 3D.

Considerando os valores obtidos, pode-se afirmar que a fechadura inteligente proposta é de baixo custo, cumprindo com mais um dos objetivos do presente estudo. Para efeito de comparação, produtos prontos com funcionalidades similares, custam a partir de U$ 165,00 no mercado nacional.

5 CONCLUSÕES E TRABALHOS FUTUROS

Considerando o exposto, o modelo de fechadura inteligente aqui apresentado atinge os objetivos e características propostos, já que ela dispensa uma pessoa de ter que carregar e gerenciar chaves tradicionais, exigindo apenas a posse de um dispositivo com *BLE*. Além disso, seu custo de construção é baixo, exige poucas adaptações para a instalação, pode funcionar com fechaduras tradicionais, exige mínima interação com o usuário, é rápida, é multiplataforma (ainda que em algumas plataformas seja necessário o uso de um *app*), permite o desenvolvimento futuro de formas de acesso alternativas e possui código fonte aberto[17].

Apesar de atingir objetivos e características almejadas, existem melhorias que podem ser desenvolvidas como trabalhos futuros. Um recurso interessante seria o acesso da fechadura à Internet. Isso criaria possibilidades como:

[17] Código fonte disponível em: <https://github.com/meierbasso/smart_lock>

- a fechadura avisar automaticamente aos demais dispositivos inteligentes da casa de que um membro da família está chegando (para acender alguma lâmpada, ligar o ar condicionado, etc.).
- a possibilidade de destrancamento da fechadura à distância para um terceiro, no caso de necessidade;
- utilizar dispositivos que não possuam BLE para destrancar a porta;
- emissão de alarmes pela internet em caso de abertura e fechamento da porta;
- registro de *logs* em servidor das atividades de abertura e fechamento da porta;
- um controle mais elaborado dos dispositivos chave autorizados (armazenado em servidor remoto).

O acesso à Internet, porém, exige que o ESP32 esteja conectado diretamente a uma fonte de alimentação, ou que sua bateria seja recarregada com maior frequência. Uma possibilidade porém, para transpor essa barreira, é a de usar um outro ESP32 fazendo esse papel de se conectar à Internet, ligado a uma fonte de alimentação, se comunicando com a fechadura por meio de *BLE* - poupando, assim, a energia do ESP32 da fechadura inteligente. Tal modelo já é utilizado por algumas fechaduras inteligentes presentes no mercado.

Por fim, há uma discussão importante sobre a segurança. A segurança física e digital da fechadura não foi levada em consideração no presente artigo e precisa de estudos adicionais. Um exemplo de fragilidade ocorre, por exemplo, se uma pessoa mal intencionada capturar pacotes de rede quando o dispositivo chave estiver próximo da fechadura inteligente (lembrando que, se não estiver perto da fechadura, o dispositivo chave troca seu endereço MAC a cada poucos minutos). Neste caso, ele pode obter o endereço *MAC* utilizado e criar um clone da chave.

Uma forma de contornar isso seria, por exemplo, obter mais alguma informação do dispositivo chave, juntá-la com o *MAC* e armazená-las na

fechadura inteligente na forma de uma *Hash*[18], por exemplo. Isso exige que a pessoa mal intencionada precise clonar mais atributos além do *MAC*.

Outra opção é exigir uma conexão BLE protegida por senha entre dispositivo chave e fechadura, e não apenas sua aproximação. Essa conexão pode ser efetuada pelo próprio gerenciador BLE do dispositivo chave ou por meio de um aplicativo que utilize uma senha ou certificado digital para a autenticação.

Ainda que sejam necessários estudos adicionais sobre a segurança da fechadura inteligente proposta, isso não impede que ela já seja utilizada de forma satisfatória em alguns cenários.

Concluímos, assim, que o objetivo do presente trabalho foi atingido. A fechadura inteligente proposta cria uma percepção de facilidade para abrir e fechar a porta, removendo a necessidade de gerenciar e carregar chaves físicas tradicionais, além de outros benefícios já mencionados. Também é importante mencionar que a não obrigação de instalar um *app* no dispositivo chave é um diferencial em relação a propostas e estudos correlatos e exigiu pensar de forma diferente das demais soluções disponíveis na literatura.

REFERÊNCIAS

AFANEH, M. **Intro to Bluetooth Low Energy**. 1. ed. Indiana, USA: Novel Bits, 2018. Disponível em: <https://novelbits.s3.us-east-2.amazonaws.com/Website/Lead+Magnets/Intro+to+Bluetooth+Low+Energy+v1.1.pdf>. Acesso em: 20 out. 2022.

ALURI, C. **Smart Lock Systems: An Overview**. International Journal of Computer Applications, v. 177, n. 37, p. 975–8887, 2020. Disponível em: <https://www.ijcaonline.org/archives/volume177/number37/aluri-2020-ijca-919882.pdf>. Acesso em: 23 jan. 2023.

[18] Uma função de Hash criptográfico tem como objetivo transformar qualquer bloco de dados em um texto de tamanho único. No caso aqui mencionado, um endereço MAC poderia ser adicionado a outra informação disponibilizada pelo dispositivo chave, como a UUID e seria gerada uma HASH desse conjunto de dados (sem que terceiros saibam quais dados foram utilizados). A fechadura sempre obteria esses dados e faria a verificação se o hash gerado é igual ao hash cadastrado. Isso melhoraria a segurança considerando que não bastaria apenas clonar o MAC do dispositivo para conseguir acesso indevido.

BABIUCH, M.; FOLTYNEK, P.; SMUTNY, P. **Using the ESP32 Microcontroller or Data Processing**. 2019 20th International Carpathian Control Conference ICCC), maio 2019. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8765944>. Acesso em 20 out. 2022.

BAIKERIKAR, J. et al. **Smart Door Locking Mechanism**. 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), 15 jan. 2021. Disponível em: <https://ieeexplore.ieee.org/document/9487704>. Acesso em: 23 jan. 2023

HADIS, M. S. et al. **Design of smart lock system for doors with special features using bluetooth technology**. International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2018, pp. 396-400, doi: 10.1109/ICOIACT.2018.8350767. Disponível em: <https://ieeexplore.ieee.org/document/8350767/authors#authors>. Acesso em 8 jan. 2023.

KAVDE, S. et al. **Smart digital door lock system using Bluetooth technology**. International Conference on Information Communication and Embedded Systems (ICICES), fev. 2017. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8070788>. Acesso em: 23 ja. 2023.

MAGRANI, E. **A Internet das Coisas**. 1. ed. Rio de Janeiro: FGV Editora, 2018

MAMONOV, S.; BENBUNAN-FICH, R. **Unlocking the Smart Home: An Examination of Factors Influencing Smart Lock Adoption Intention**. Americas Conference on Information Systems, 2019. Disponível em: <https://press.um.si/index.php/ump/catalog/book/418>. Acesso em: 27 jan. 2023.

PRABAKARAN, P. et al. **Smart Door Lock System For The Elderly And Disabled**. International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 2021, pp. 229-233, doi: 10.1109/ICDI3C53598.2021.00053. Disponível em: <https://ieeexplore.ieee.org/document/9545169>. Acesso em: 27 jan. 2023.

PRAKASH, Y. W. et al. **Smart bluetooth low energy security system**. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2017, pp. 2141-2146, doi: 10.1109/WiSPNET.2017.8300139. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8300139>. Acesso em: 10 abr.

SHANTHINI, M.; VIDYA, G.; ARUN, R. **IoT Enhanced Smart Door Locking System**. Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 92-96, doi: 10.1109/ICSSIT48917.2020.9214288. Disponível em: <https://ieeexplore.ieee.org/document/9214288>. Acesso em 26 jan. 2023.

YU, Y. **A practical digital door lock for smart home**. IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2018, pp. 1-2, doi: 10.1109/ICCE.2018.8326305. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8326305>. Acesso em: 8 jan. 2023.