

Sistema embarcado RFID para controle IoT de identidade em diferentes níveis de acesso

José de Alencar de Sousa Júnior, Sandro César Silveira Jucá

Departamento de Telemática – Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

CEP 60040-531 – Fortaleza – CE – Brasil

alenior@gmail.com, sandro.juca@gmail.com

19 de fevereiro de 2025

Resumo

Abstract. This article aims to promote access control with face-to-face identity recognition and online activation based on radio frequency identification (RFID) technology, sending information to an administrator user via a messaging application. The entire identification and registration process is done via the Esp32 microcontroller, which, because it has internet communication, updates the information sent online. All information about the tag's actions is displayed on an LCD display connected to the microcontroller board, and each action is signaled by LEDs and a specific sound signal.

Resumo. Este artigo tem o objetivo de promover controle de acesso com distinção de identidade presencial e acionamento online baseado na tecnologia de identificação por radiofrequência (RFID), enviando informações para um usuário administrador por meio de aplicativo de mensagem. Todo o processo de identificação e registro é feito por meio do microcontrolador Esp32 que por ter comunicação com a internet atualiza as informações enviadas de forma online. Todas as informações sobre as ações da tag são exibidas em um display LCD ligado à placa microcontrolada e cada ação é sinalizada por leds e um sinal sonoro específico.

1 Introdução

A fim de almejar melhores resultados nas suas atividades profissionais e particulares, a sociedade humana busca constantemente melhorar suas rotinas, em especial quanto a controles e suas informações associadas. Neste contexto, a Identificação por Radiofrequência (RFID) “é uma daquelas raras tecnologias que ‘mudam o mundo’, que forçarão a uma reconsideração de muitas estratégias na cadeia de valores” [Glover 2015, apud Jucá 2016].

A identificação por radiofrequência já tem aplicações difundidas, como sistema de segurança de lojas e monitoramento logístico de itens a ser transportados. No entanto, muitas outras aplicações podem ser feitas, graças ao seu baixo custo e praticidade de implantação, além de ser aplicável a seres humanos, animais, objetos diversos, além de veículos de toda espécie [UFRJ RFID].

Para orquestrar este sistema, será utilizado o microcontrolador ESP32, que é uma evolução do ESP8266. O ESP32 é dual-core, apresenta Bluetooth, processamento de 160MHz, que é o dobro do ESP8266 e 512 kB de SRAM. Além disso, possui mais portas digitais e seu conversor analógico para digital é de 12 bits [Souza 2018].

A partir desse cenário, foi desenvolvido um sistema de controle de acesso baseado na tecnologia de radiofrequência, onde cada usuário autorizado possui uma tag para permitir acesso ao ambiente controlado, podendo ainda ser definido um nível adicional de segurança por meio da digitação de senha para autorização do acesso. É amplamente reconhecida a eficiência da identificação por radiofrequência na promoção de maior controle e segurança a determinados ambientes e pessoas [Nascimento 2015].

O controle de acesso utilizando tags mostra-se como extremamente útil e eficiente, pois além de impedir o acesso não autorizado ao local, ele ajuda a entender a forma como o local está sendo utilizado pelas pessoas naquele ambiente, sendo assim uma excelente solução para gerir melhor o fluxo de entrada e saída de funcionários e outros usuários; além de se eximir de possíveis riscos [Amelco 2025].

A IoT, ou Internet das Coisas, é uma tecnologia que tem mudado e inovado o modo como interagimos com o mundo ao nosso redor. Esse termo refere-se à interconexão de dispositivos, objetos e máquinas por meio da internet, permitindo a coleta e compartilhamento de dados, sem apresentar interação direta com seres humanos [Gremes 2023]. Neste contexto, o administrador pode acionar remotamente a liberação do acesso ao ambiente controlado, recebendo ainda confirmação dessa liberação e informado sobre as tentativas de acesso e seus sucessos (ou não) por meio de mensagem enviada por aplicativo (WhatsApp), no instante em que ocorre.

2 Materiais e métodos

Serão utilizados neste trabalho os seguintes componentes: microcontrolador Esp32, Fonte de alimentação 5v, 2 placas protoboard de 830 furos, Variedade de cabos *Dupont Jumper* (Macho x Macho e Macho x Fêmea), Módulo relé 5v de 1 canal, *Display LCD 16x02*, Buzzer passivo 5v, *Leds* verde, amarelo e vermelho, Fonte 12v, Tranca solenóide 12v e Sensor RFID RC522. Conforme já abordado, o microcontrolador ESP32 possui inúmeros predicados que o referenciam para construção de protótipos, com uma rica distribuição de propriedades que podem ser vistas no seu esquema de pinagem, abordado na Figura 1.

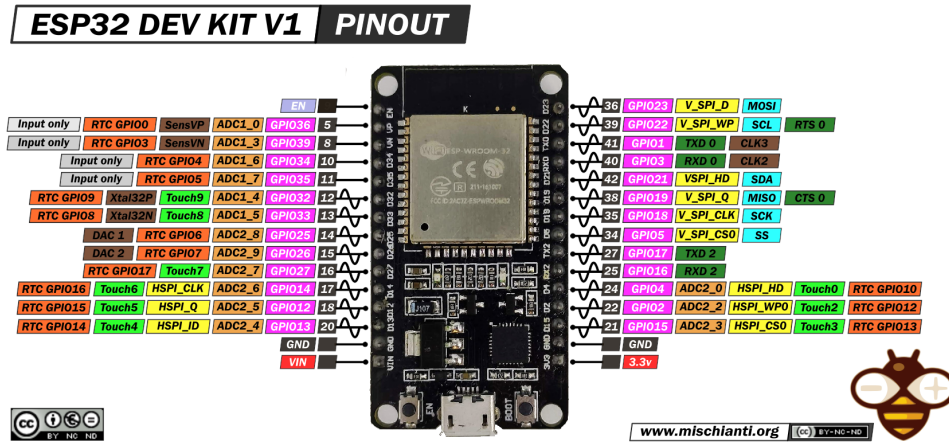


Figura 1: Ilustração e pinagem do Esp32. Fonte: [Mischiati 2021]

O sensor RFID RC522 é uma tecnologia bastante conhecida dentre os projetistas de circuitos eletrônicos, assim como utilizada pelos usuários dos sistemas implementados com o mesmo, podendo ser citados como exemplos: um crachá para acesso a um determinado ambiente restrito, uma etiqueta para acompanhamento de um determinado objeto num processo logístico, ou o monitoramento de animais em ambiente selvagem para estudos sobre o risco de extinção [Figura 2].

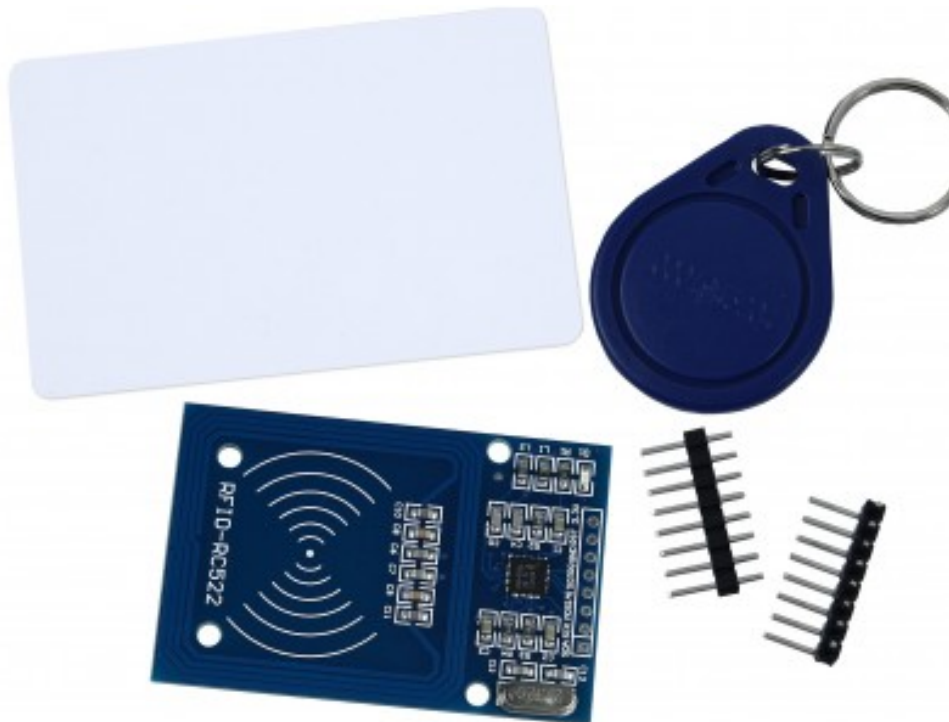


Figura 2: Sensor RFID RC522. Fonte: [Usinainfo 2025]

O display LCD 16x02 com módulo de comunicação I2C permite melhor interação entre sistema e usuário, pois exibe instruções e informações no seu visor que tornam a utilização mais amigável [Figura 3].

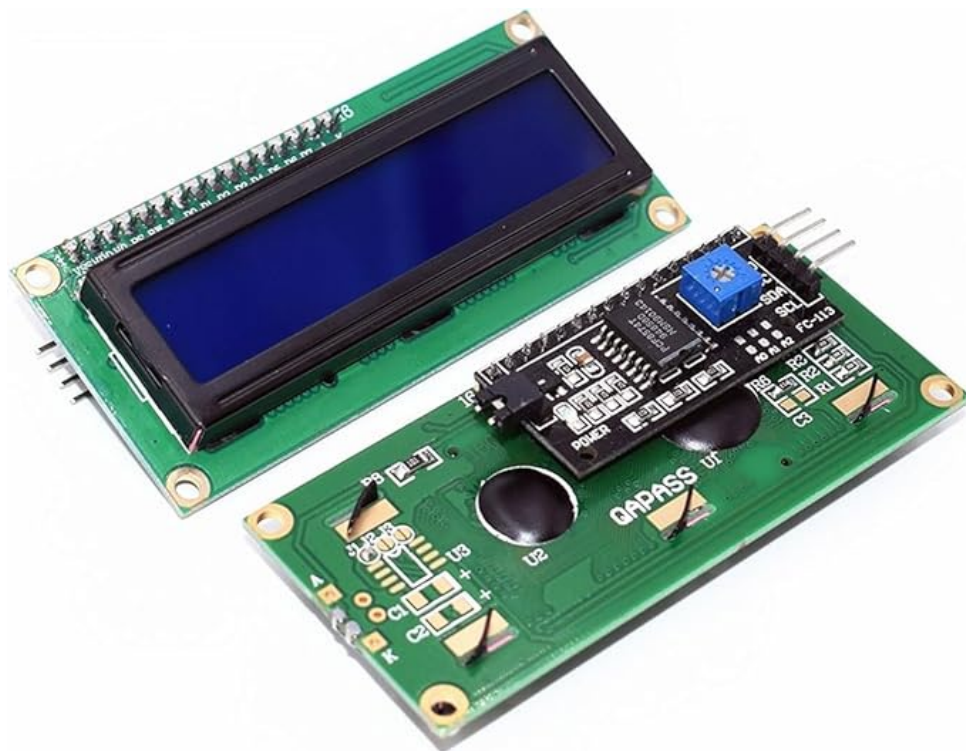


Figura 3: Display LCD 16x02. Fonte: [Amazon 2025]

O teclado matricial 4x3 é utilizado no caso de a tag apresentada exigir a digitação de senha (Figura 4).



Figura 4: Teclado matricial 4x3. Fonte: [Ponto da eletrônica 2025]

A tranca solenóide representa a finalidade deste projeto: toda essa lógica envolve a sua liberação no momento certo, para a identidade correta e informado essas ações ao administrador em tempo real [Figura 5].



Figura 5: Tranca solenóide 12v. Fonte: [Usinainfo 2025]

2.1 Funcionamento do sistema RFID

Conforme [Araujo 2014, apud Washington 2021], a RFID é um leitor de radiofrequência capaz de realizar a leitura de até 200 etiquetas (*TAGs*) por segundo, sem a necessidade de estar visivelmente perto, sendo composta por dois elementos complementares: um leitor construído de uma antena (transceptor), que faz a leitura do sinal e transfere a informação para o dispositivo desejado, e uma etiqueta de radiofrequência (RF) que contém a informação a ser transmitida.

Segundo detalhamento do *datasheet* do sensor RC522 [Alldatasheet RC522], a tecnologia de identificação por radiofrequência consiste em se utilizar um microchip ligado a uma antena, operando tanto em baixas como altas frequências. Esse *microchip* consiste num *transponder* que não necessita de fonte de alimentação, pois o sinal que o excita vem diretamente de um circuito de leitura/gravação. Ao ser excitado, o circuito é alimentado enviando ou recebendo dados que estejam gravados. Um dos princípios de funcionamento da tecnologia RFID é a radiação eletromagnética, que é definida como sendo o transporte de energia por meio de flutuações dos campos elétrico e magnético. A luz, ou radiação eletromagnética, pode ser observada sob diferentes formas ou seja, em diferentes faixas espectrais: visível, infravermelho, ultravioleta, ondas rádio, etc. [Unesp 2025]. Uma parte pequena do campo emissor interage com a bobina da antena do *transponder*, que está a uma determinada distância da bobina do leitor. Pela indução magnética, uma tensão é gerada na bobina da antena do *transponder*. Esta tensão é retificada e serve como a fonte de alimentação para o *microchip*. Um capacitor é conectado paralelamente à bobina da antena do leitor. A capacitância é selecionada de forma a combinar com a indutância da bobina da antena para dar forma a um circuito ressonante paralelo, ou seja, para se obter uma frequência ressonante que corresponda com a frequência da transmissão do leitor [Oliveira 2015].

2.2 Sistema de ativação *online*

Para a ativação online do sistema, foi utilizado o serviço do sítio **Blynk** (<https://blynk.io>), que oferece plataforma intuitiva e amigável para cadastramento de um microcontrolador (neste caso, Esp32; mas podem ser outros, como Esp8266 e Arduino) e aplicativo disponível para Android e Ios que permite a ativação online do sistema, portanto, via *smartphone* e navegador de internet.

Para tanto, é necessário fazer um cadastro simplificado de usuário, assim como informar os detalhes do sistema a ser criado, como: microcontrolador utilizado, forma de acesso à internet, ide utilizada para desenvolvimento etc. Após esta preparação, um painel é disponibilizado tanto no navegador quanto na aplicação

do *smartphone*, permitindo a integração com o projeto desenvolvido por meio do código lógico implantado no microcontrolador.

2.3 Sistema de envio de mensagens

Para monitoramento administrativo e de segurança do sistema desenvolvido, foi utilizado o serviço do sítio **CallMeBot** (callmebot.com), que oferece serviço de fácil e prática implementação de envio de mensagens automático, permitindo que se possa acompanhar em tempo real as ações envolvidas ao sistema de controle de acesso desenvolvido.

Para se utilizar do serviço da api, faz-se um cadastramento simplificado utilizando-se um número de celular ativo (também cadastrado e em uso num aplicativo mensageiro, como **WhatsApp** ou **Telegram**) que dá acesso a uma "apikey" correspondente. Após esta preparação, é disponibilizado um link personalizado ao número e seu "apikey", permitindo promover envios automáticos de mensagens para o número informado.

3 Construção do circuito

O sistema completo consiste de um controle de acesso RFID que permite o acesso a um determinado ambiente restrito mediante respectiva identificação e nível de acesso: um leitor de RFID fica posicionado ao lado da porta trancada, assim como um teclado para informar senha, quando aplicável. Sinais sonoros são emitidos para auxiliar o usuário na percepção dos resultados de sua interação com o sistema, assim como sinais visuais emitidos por *leds* nas cores vermelha, amarela e verde. Adicionalmente, mas não menos importante, um *display* lcd informa sucintamente instruções diversas para as interações com o sistema, assim como informa consequências resultantes dessas interações.

Caso uma *tag* seja aproximada, é exigido que se informe a senha de acesso para destrancar a porta. Caso trate-se de uma *tag master*, a senha não é exigida para liberar o acesso. Para efetivar o destrancamento da porta protegida, ao ser liberado o acesso o microcontrolador envia um sinal para um relé que atua abrindo a tranca solenóide instalada. No caso de ativamento remoto, o *display* lcd detalha o mesmo, e também atuam-se os sinais sonoros e visuais instalados.

4 Resultados

O protótipo foi montado com os componentes previstos que podem ser vistos na Figura 6: O Esp32 (A) montado sobre 2 *protoboards*, tendo conectado a ele o sensor RFID RC522 (B) que pode ler as *tags* tanto de cartão (C) quanto de chaveiro (D). Também fazendo parte do circuito encontram-se o *Display* LCD (E), o teclado matricial (F), a tranca solenóide (G), além de relé (H) e fonte 12v (I). O projeto funcionou como esperado, tanto nas funcionalidades básicas de controle de acesso quanto nas propriedades inclusas de acionamento remoto e notificação via mensageiro.

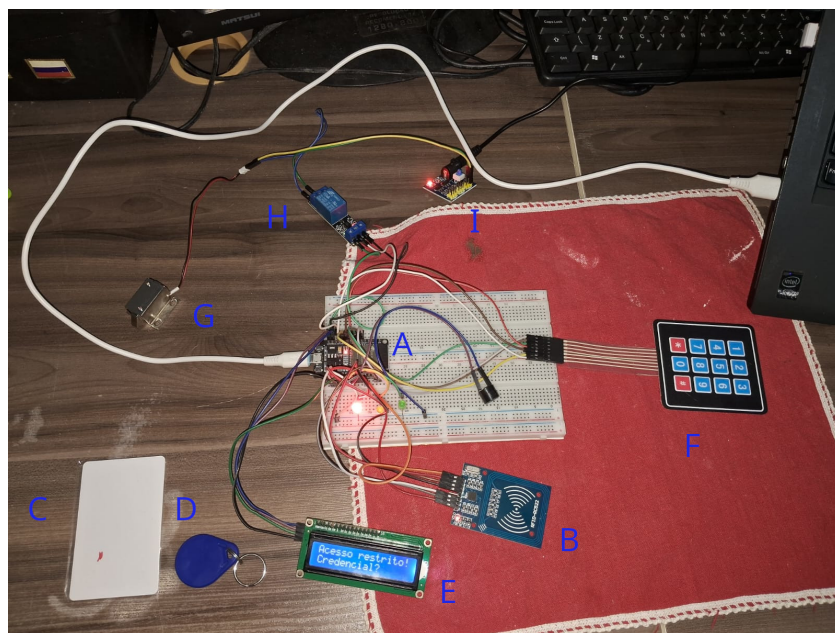


Figura 6: Imagem do protótipo montado. Fonte: O autor.

Baseado no princípio de Internet das coisas (*IoT – Internet of Things*), o sistema pode ser acessado via internet pela plataforma **Blynk** no navegador, permitindo fazer a liberação e fechamento da tranca, controlando o acesso ao ambiente restrito integrado (Figura 7).

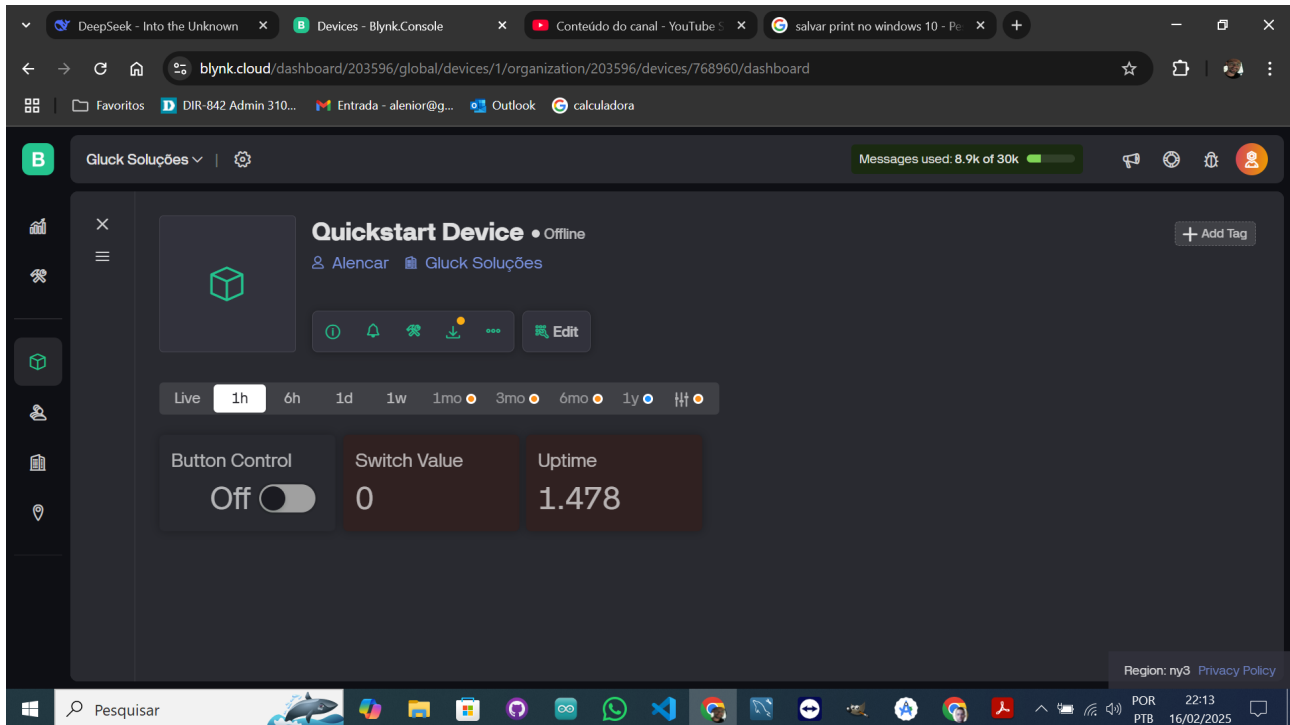


Figura 7: Utilizando a plataforma Blynk via navegador de internet.

Ainda no contexto IoT, o aplicativo para smartphones da mesma plataforma (*Blynk*), aprimora a acessibilidade remota ao sistema, provendo maior mobilidade ao administrador e flexibilidade (Figura 8).

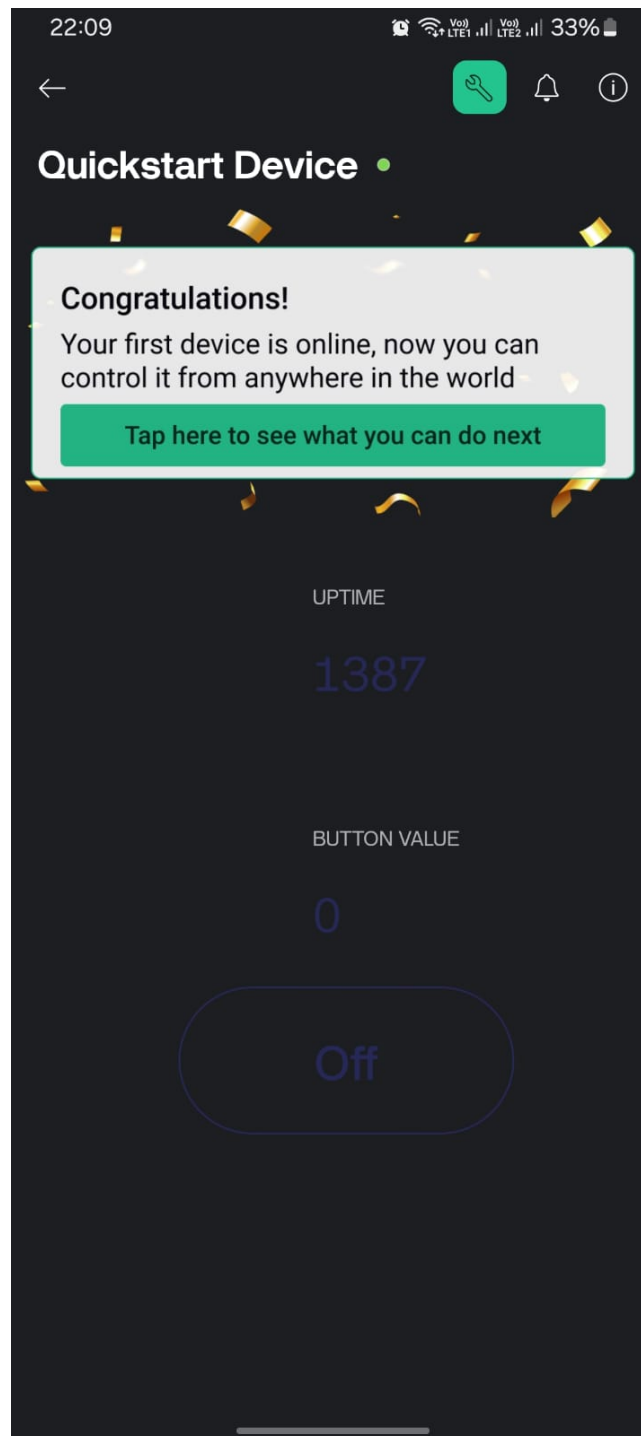


Figura 8: Utilizando a plataforma Blynk via aplicativo em smartphone Android.

Foi ainda utilizada a api do site callmebot.com para o recebimento de notificações do sistema em tempo real (Figura 9).

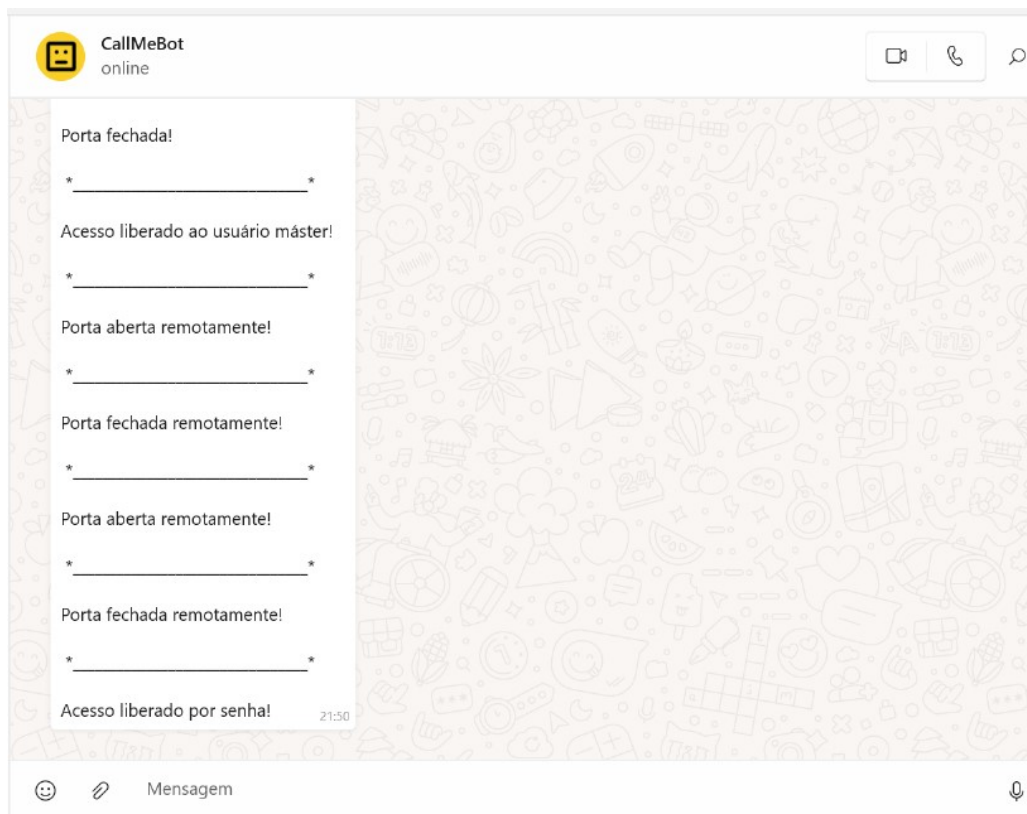


Figura 9: Recebendo notificações do sistema via aplicativo de mensagens WhatsApp.

O funcionamento do sistema consiste na leitura de *tags* que identifica o usuário. Caso o mesmo seja usuário *master*, o acesso é liberado. Caso não seja usuário *master*, pedirá a digitação de senha como fator adicional de segurança. Caso a senha informada esteja correta, o acesso é liberado e o sensor volta a ficar de prontidão para identificar uma nova *tag* (usuário). Caso a senha informada esteja errada, o acesso é negado e o sensor volta, da mesma forma, a aguardar a identificação de um novo usuário. A Figura 10 apresenta o fluxograma da lógica implantada no sistema.

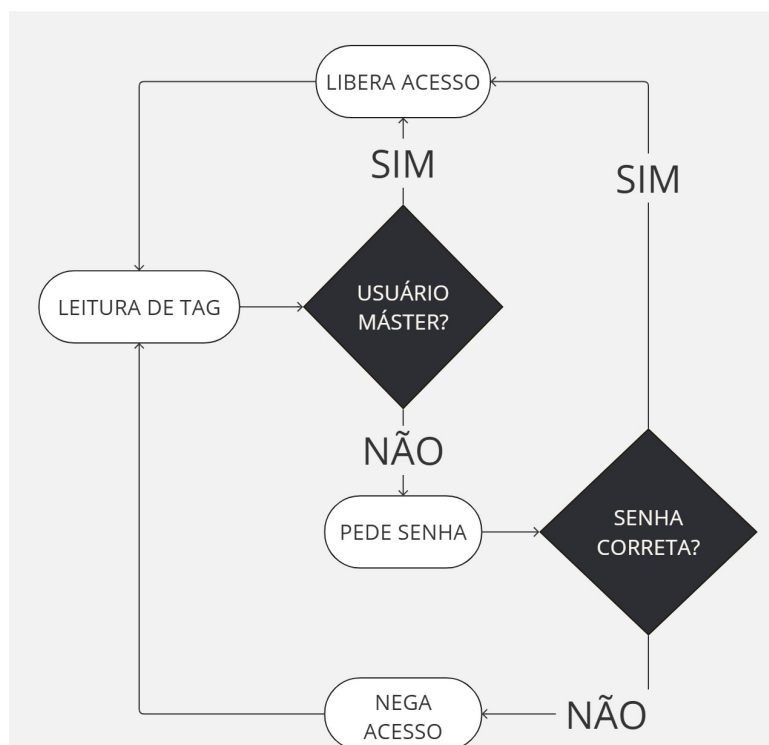


Figura 10: Fluxograma do funcionamento do sistema.

A demonstração completa do protótipo pode ser verificada em vídeo feito para esse propósito, demonstrando seu funcionamento via tags e por meio de liberação remota (Alencar 2025).

5 Considerações finais

De acordo com os testes realizados, o sistema mostrou-se funcional quanto ao proposto inicialmente. Há de se considerar as ressalvas quanto à alimentação própria do sistema, que pode agregar independência ao mesmo, assim como observar eventuais intermitências quanto ao acesso à internet. Estes pontos parecem ser o ponto de partida para posterior melhoramento do protótipo, além de outras necessidades que porventura ocorram.

6 Referências

Alldatasheet, "RC522 Datasheet", Disponível em:

<https://www.alldatasheet.com/datasheet-pdf/pdf/346109/NXP/RC522.html>, Acesso em Fevereiro de 2025.

Amazon, "Display LCD Azul 16x2 com Módulo I2C", Disponível em:

<https://www.amazon.com.br/Display-M%C3%B3dulo-Soldado-Arduino-raspberry/dp/B0CDHZVV4Z>. Acesso em Fevereiro de 2025.

Amelco, "A importância de ter um controle de acesso em seu ambiente privado",

<https://amelco.com.br/noticia/a-import%C3%A2ncia-de-ter-um-controle-de-acesso-em-seu-ambiente-privado#:~:text=Sua%20import%C3%A2ncia,se%20eximir%20de%20poss%C3%ADveis%20riscos.>, Fevereiro 2025

Cryslaine C. C. Nascimento, Kality D. de Freitas, Joao V. N. Lopes, Thiago R. Fernandes, Sonagno de P. Oliveira "APLICAÇÃO DO SISTEMA RFID NO CONTROLE DE ACESSO DE VEÍCULOS EM CONDOMÍNIOS", ENEGEP 2015, Fortaleza, Brasil, Outubro

Monique Gremes, "IoT: o que é e qual a importância?", MBA USP, São Paulo, Brasil, Setembro 2023

Pedro H. M. Araujo, Renan P. Figueiredo, Douglas L. Dias, Sandro C. S. Jucá (2016) "Controle de acesso RFID utilizando o princípio de Internet das Coisas", Escola Regional de Informática do Piauí, Teresina, Brasil

Ponto da eletrônica, "Teclado Matricial 4x3 Para Arduino", Disponível em:

<https://www.pontodaeletronica.com.br/teclado-matricial-4x3-para-arduino.html>. Acesso em Fevereiro de 2025.

Renzo Mischianti, "DOIT ESP32 DEV KIT v1: high resolution pinout and specs", Disponível em: <https://mischianti.org/doit-esp32-dev-kit-v1-high-resolution-pinout-and-specs/>, Acesso em Fevereiro de 2025.

José de A. de S. Júnior, "Controle de acesso com RFID em IoT", Fevereiro de 2025, Youtube, Disponível em: <https://youtube.com/shorts/Cfg2asOm7Lw?feature=share>.

Vitor A. Souza (2018) "Programando o ESP32 no Arduino", Clube dos Autores, Rio de Janeiro, Brasil, Fevereiro 2025

UFRJ, "RFID", https://www.gta.ufrj.br/grad/12_1/rfid/links/aplicacoes.html, Fevereiro

Unesp Sorocaba, "Radiação eletromagnética",

<https://www.sorocaba.unesp.br/Home/Graduacao/EngenhariaAmbiental/robertowlourenco1502/rem.pdf>, Fevereiro

Usinainfo, "Fechadura Elétrica Solenóide 12V", Disponível em:

<https://www.usinainfo.com.br/mini-fechadura-eletrica-solenode/fechadura-eletrica-solenode-12v-nf-fe-91-lingueta-reversivel-3524.html>. Acesso em Fevereiro de 2025.

Usinainfo, "Kit RC522 Leitor RFID + Tags (Chaveiro + Cartão)", Disponível em:

<https://www.usinainfo.com.br/rfid-arduino-e-ibutton/kit-rc522-leitor-rfid-tags-chaveiro-cartao-2582.html>. Acesso em Fevereiro de 2025.

Whashington J. F. Resende, Lúcio R. Júnior, Guilherme H. Alves, Marcelo C. Dias, Antonio M. B. da Silva (2021) "Desenvolvimento de um sistema para monitoramento e controle patrimonial, utilizando Rfid e dispositivos Iot", Brazilian Journal of Development, Curitiba, Brasil, Julho.