





ARTIGO DE PESQUISA/RESEARCH PAPER

# IFGAccess: sistema de controle de acesso web utilizando RFID e o microcontrolador ESP8266

## IFGAccess: a web-based access control system using RFID and the ESP8266

Daniele dos Santos Araújo   [Instituto Federal de Goiás - Campus Formosa | s.araujodaniele@gmail.com]

Mario Teixeira Lemes  [Instituto Federal de Goiás - Campus Formosa | mario.lemes@ifg.edu.br]

 Instituto Federal de Goiás - Campus Formosa. Rua 64, s/n - Esq. c/ Rua 11 - Parque Lago, Formosa - GO, 73813-816.

**Resumo.** A popularização de Internet das Coisas, aliada aos avanços tecnológicos nos processos de processamento, comunicação e identificação, permitem que sejam construídos sistemas que proporcionam comodidade, credibilidade e segurança aos usuários. O controle de acesso para liberação aos laboratórios do Instituto Federal de Goiás é realizado de forma manual, ocasionando problemas relacionados a segurança, tais como esquecimento de registro de entrada/saída e ações mal intencionadas por parte dos usuários. Sistemas automatizados de controle de acesso, baseados em dispositivos computacionais de baixo custo e sistemas de identificação, podem fornecer segurança apropriada. Neste artigo propomos o IFGAccess, um protótipo que combina elementos de *hardware* e *software* como solução automatizada para registro e controle de acessos a ambientes com alto valor agregado. A solução mostrou-se adequada no registro de usuários, controlando de forma efetiva os processos relacionados a autenticação.

**Abstract.** The popularization of the Internet of Things, combined with technological advancements in processing, communication, and identification, enables the development of systems that provide convenience, reliability, and security to users. Access control for the laboratories at the Instituto Federal de Goiás is currently performed manually, leading to security issues such as forgotten entry/exit logs and malicious actions by users. Automated access control systems based on low-cost computing devices and identification technologies can offer an appropriate level of security. In this work, we provide IFGAccess, a prototype that integrates hardware and software components as an automated solution for access registration and control in high-value environments. The proposed solution has proven effective in user registration and in managing authentication processes efficiently.

**Palavras-chave:** Internet das coisas, Controle de acesso, Identificação por rádio frequência, Sistema web.

**Keywords:** Internet of things, Access control, Radio frequency identification, Web system.

**Recebido/Received:** 06 March 2025 • **Aceito/Accepted:** 04 May 2025 • **Publicado/Published:** 16 May 2025

## 1 Introdução

O avanço e expressividade do paradigma de *Internet of Things* (IoT) pode ser observado através do aumento da quantidade de objetos inteligentes conectados à Internet. De acordo com GSMA Association [2019], as conexões cresceram a uma taxa média anual de 14% no ano de 2019, com tendência projetada para 1,3 bilhão de dispositivos em 2025. Ao conectar objetos com diferentes recursos computacionais a uma rede, potencializa-se o surgimento de novas aplicações. Através do paradigma IoT, os objetos podem prover comunicação entre usuários e dispositivos, permitindo o desenvolvimento de uma gama de aplicações, tais como relacionadas à coleta de dados de pacientes e monitoramento de idosos, sensoriamento de ambientes inóspitos e de difícil acesso, pedágios e relógios inteligentes [Sundmaeker *et al.*, 2010].

Sistemas automatizados, baseados em dispositivos inteligentes e IoT, podem fornecer confiabilidade e segurança ao serem utilizados no controle de acesso a ambientes. O controle de acesso aos laboratórios de informática do Instituto Federal de Goiás (IFG) é realizado de maneira manual. Para acessar os laboratórios, basta preencher a folha de controle de chaves. Com pouca ou nenhuma supervisão, esta prática possibilita que pessoas não autorizadas acessem livremente os ambientes de laboratório, comprometendo a segurança física dos equipamentos e de seus ocupantes.

O uso da tecnologia de *Radio Frequency Identification* (RFID) é adequado para controle patrimonial. Para Brito *et al.* [2019], as vantagens são a redução de custo e a diminuição no tempo para identificação dos bens. Os autores argumentam que o sistema automatizado contrapõem-se positivamente em relação ao sistema manual de controle que é naturalmente suscetível à falhas. Outra vantagem é a não necessidade de mão de obra para controlar e fiscalizar o acesso.

O objetivo deste artigo é o desenvolvimento de uma solução tecnológica, através da utilização de radio-frequência, dispositivos inteligentes e sistemas automatizados, que permita que docentes, servidores técnico-administrativos, funcionários terceirizados, alunos e demais membros da comunidade científica, que possuem autorização para utilização dos laboratórios de informática do IFG, sejam corretamente identificados ao acessar estes locais. O sistema, denominado **IFGAccess**, permite o cadastro de um novo usuário, vinculado a uma *tag* de radio-frequência e/ou a verificação da possibilidade de acesso, gerenciando de forma efetiva o ingresso ao ambiente controlado.

## 2 Referencial Teórico

A atualização constante do *hardware* em dispositivos computacionais possibilitou a diminuição de seu tamanho físico e a expansão de suas capacidades tecnológicas. Nesta seção,

são abordados conceitos sobre microcontroladores e sistemas embarcados. Em seguida, é explorada a contextualização da tecnologia de radio-frequência a fim de controle de acesso. Adicionalmente, discute-se trabalhos relacionados que exploram soluções que combinam soluções integradas e de baixo custo para controle e automatização dos processos de identificação.

## 2.1 Microcontroladores

Bates [2008] afirma que um microcontrolador tem três elementos principais: (1) dispositivos de entrada e saída; (2) processador e (3) memória. Contudo, ao contrário de um sistema microprocessado convencional, *e.g., desktop*, que possui *chips* separados em uma placa de circuito impresso, os microcontroladores contêm todos esses elementos em um único *chip*. Dessa forma, o microcontrolador é essencialmente um computador em um *chip*. Segundo Firat and Uğurlu [2018], microcontroladores são adequados para uso em sistemas embarcados.

## 2.2 Sistemas embarcados

Segundo Jiménez *et al.* [2013], um sistema embarcado pode ser definido como um dispositivo que contém componentes de *hardware* e *software* fortemente acoplados. Para Denardin and Barriquello [2019], sistemas em tempo real normalmente são sistemas embarcados e que isto significa que o sistema computacional é completamente encapsulado e dedicado ao dispositivo ou sistema que controla. Para os autores, essa é a fundamental diferença entre sistemas embarcados e sistemas de propósito geral.

Pohl *et al.* [2012] definem que sistemas embarcados são microcontroladores conectados a sistemas completos por intermédio de sensores, atuadores, controles de operação e dispositivos de comunicação. Esses dispositivos interagem de diversas formas com o ambiente e oferecem uma variedade de funções. A maioria dos sistemas embarcados interage diretamente com os processos ou com o ambiente, tomando decisões em tempo real.

O ESP8266 é um sistema embarcado com conectividade *Wireless Fidelity* (Wi-Fi) integrada, desenvolvido pela Espressif Systems (<https://www.espressif.com/>). Esse dispositivo, com recursos integrados de rede, memória, pinos de entrada/saída e outras interfaces, permite o desenvolvimento de aplicações para IoT, sendo o principal componente de *hardware* utilizado no desenvolvimento do sistema IFGAccess. Adicionalmente, devido seu baixo custo e relativa facilidade de programação, através de linguagens como C/C++ ou Lua, sua adoção é facilitada e justificada para projetos de automação residencial, dispositivos vestíveis, sistemas de controle de acesso e outras aplicações de prototipagem.

## 2.3 Controle de acesso

De acordo com International Organization for Standardization [2013], o controle de acesso é o conjunto de processos e mecanismos que garante que somente indivíduos, sistemas ou processos devidamente autorizados possam acessar recursos ou informações, segundo privilégios pré-definidos. Adicionalmente, pode ser compreendido como a limitação sistêmica do acesso a sistemas, aplicativos, dados e funcio-

nalidades, visando proteger requisitos fundamentais da segurança da informação, tais como a confidencialidade, integridade e disponibilidade das informações.

## 2.4 RFID

RFID é uma tecnologia que permite identificar um objeto por meio de envio de ondas de radiofrequência. É composto por duas partes: (1) receptor RFID e (2) *tag* RFID. O receptor e a *tag* podem ser ativos, contendo uma fonte de alimentação, ou passivos, que são alimentados através de uma fonte de energia externa [Weinstein, 2005]. Segundo o autor, o modelo ativo possui circuito com maior complexidade, o que acarreta em maior custo, sendo comumente encontrado operando dentro de frequências altas, além de se comunicar com leitores distantes, localizados entre 20 e 100 metros. O modelo passivo possui menor custo e opera em frequências mais baixas. Seu alcance é limitado, podendo se comunicar apenas com leitores mais próximos, localizados aproximadamente até 9 metros.

## 2.5 Trabalhos relacionados

Foram identificados na literatura alguns trabalhos correlatos a este, como o de Maia *et al.* [2019], que desenvolveu um protótipo para realizar o controle automático de acesso de pessoas a Universidade Federal Rural do Semi-Árido (UFERSA) *Campus* Mossoró. Os autores propõem o uso da tecnologia RFID integrada a plataforma *open-source* de prototipagem eletrônica Arduino®. No entanto, de maneira estática e sem a possibilidade de cadastro facilitado de novas *tags* de identificação, a validação de permissão é realizada pelo código-fonte carregado no dispositivo embarcado que previamente armazena os identificadores.

O trabalho de Lisboa [2021] apresenta uma proposta de controle de patrimônio utilizando a tecnologia RFID, com o objetivo de automatizar a auditoria de movimentação de bens pertencentes a Universidade Tecnológica Federal do Paraná (UTFPR), *Campus* Ponta Grossa. No cenário desenvolvido pelos autores, a movimentação do patrimônio é detectada através do uso de uma antena, conectada a um computador, que armazena o local e data da passagem do patrimônio. Adicionalmente, é fornecida uma aplicação *Web* para o processo de verificação e controle do patrimônio da Universidade.

No trabalho de Silveira *et al.* [2021] é desenvolvida uma fechadura eletrônica para controle de acesso ao laboratório da Universidade Federal de Santa Catarina, utilizando um sistema que possibilita a utilização das carteirinhas de identificação como chave de acesso. Para armazenamento organizado de cada usuário cadastrado ou o registro de entradas e saídas, os autores utilizaram a tecnologia de banco de dados. Apesar de terem desenvolvido um *site* para visualização do histórico de acessos realizados ao ambiente controlado, não há automatização no cadastro das carteirinhas dos estudantes.

Considerando as lacunas deixadas pelos trabalhos correlatos e o alto valor agregado dos equipamentos presentes no laboratório, tais como computadores, roteadores, *switches* e outros periféricos, é essencial o desenvolvimento de um controle de acesso mais rigoroso e que forneça nível de segurança apropriado. A integração de tecnologias de identificação a sistemas embarcados apresenta-se como solução viável.

Diante das bases conceituais estabelecidas e as tecnologias apresentadas, a próxima seção descreve as ferramentas utilizadas e a modelagem desenvolvida durante a implementação do sistema IFGAccess.

### 3 Materiais e Métodos

Nesta seção, são detalhadas questões pertinentes relacionadas a aplicação do questionário para levantamento dos requisitos funcionais e as ferramentas tecnológicas utilizadas no desenvolvimento e os artefatos obtidos pela análise do sistema IFGAccess, através da exposição de diagramas da linguagem de modelagem unificada e da modelagem do banco de dados.

#### 3.1 Questionário

Para melhor compreender o problema e apoiar a construção da solução foi utilizada a técnica de aplicação de questionário a fim de levantamento dos requisitos funcionais. Segundo princípios estabelecidos por Vazquez and Simões [2016], após esta coleta de informações, o resultado do questionário pode ser usado como base para análise dos requisitos.

Com o auxílio da ferramenta Google Forms (<https://workspace.google.com/products/forms/>), foram criadas perguntas variadas de múltipla escolha, bem como perguntas abertas, de modo a entender o problema e validar a aceitação do desenvolvimento da solução de segurança. O formulário foi respondido pela comunidade acadêmica, composta por: (1) funcionários que compõem a parte administrativa do IFG, e (2) professores que possuem acesso aos laboratórios. As perguntas realizadas foram elaboradas para fornecer *insights* relacionados com (1) contextualização, de modo a entender o contexto e a problemática do controle manual de chaves dos laboratórios e (2) validação da solução, para garantir que a solução proposta agrega valor às partes interessadas. A Tabela 1 mostra a relação de perguntas realizadas às partes interessadas do sistema de controle de acesso IFGAccess.

**Tabela 1.** Relação de perguntas utilizadas para aplicação do questionário

Q1 - Qual seu nome e cargo no IFG?
Q2 - Quem tem acesso as chaves dos laboratórios de informática do IFG? -
Q3 - Como é realizado atualmente o controle de acesso aos laboratórios? Existe algum processo de identificação?
Q4 - Você considera que a forma de controle de acesso atual uma forma segura e eficiente? Justifique sua resposta.
Q5 - Já houve relatos de perda ou roubo de equipamentos dos laboratórios de informática?
Q6 - O controle automatizado trás maior segurança no seu ponto de vista?
Q7 - Há necessidade de geração de relatórios de acessos?
Q8 - É necessário o conhecimento do horário de saída do laboratório?
Q9 - Possui mais alguma informação que considera relevante ser informada?

Como pode ser observado na Tabela 1, as perguntas Q1 a Q5 possuem objetivo de elucidar e contextualizar o problema relacionado a segurança dos laboratórios de informática, colaborando para fortalecer a justificativa do trabalho. As perguntas Q6 a Q9 da Tabela 1 são relacionadas a validação da solução, isto é, para mostrar que o acesso automatizado por meio de dispositivos de baixo custo pode aumentar a segurança relacionada ao acesso em ambientes com alto valor agregado.

O questionário foi respondido por 8 (oito) pessoas. Em relação a pergunta Q4 da Tabela 1, 100% dos entrevistados consideram que o acesso manual as chaves dos laboratórios é uma prática insegura. Como justificativa, diversos argumentos foram apontados tais como a possibilidade de não existir nenhum servidor técnico-administrativo na sala no momento em que o empréstimo de chaves é requerido, a possibilidade de erros, esquecimentos e comportamentos mal intencionados. Os entrevistados entendem que não existe possibilidade de controle integral de um servidor do IFG para liberação dos acessos. Nesse sentido, apontam que quando não há nenhum servidor na sala, o acesso fica livre. Também são apontados episódios de esquecimento de assinatura de entrada e saída dos laboratórios e da devolução das chaves. O controle manual revela problemas de segurança no acesso aos laboratórios, não intencionais como acontece nos esquecimentos, ou intencionais tais como uso da falsificação ideológica ou o não correto preenchimento da lista de acessos.

Com apoio das respostas recebidas pelo questionário foi possível a criação dos seguintes artefatos: (1) Diagrama de Casos de Uso, (2) Diagrama de Atividades, e (3) Modelo lógico do Banco de Dados (BD). Estes artefatos são apresentados em detalhes na Seção 4. Para a realização de testes, construção e compilação dos códigos C++ desenvolvidos para o NodeMCU V1 foi utilizado o *Integrated Development Environment* (IDE) Arduino, na versão 1.8.18. O protótipo do dispositivo embarcado e o desenho esquemático das ligações foram elaborados através do *software* Fritzing, na versão 0.9.3. Todo ambiente de desenvolvimento foi configurado e executado pelo *Docker*, na versão 4.6.1. O dispositivo computacional utilizado para codificação foi o Windows 11 X64 com processador AMD Ryzen 7 4800H e 8GB de memória. Finalmente, para versionamento e disponibilização do código desenvolvido para comunidade científica foi utilizado o GitHub (<https://github.com/felurye/ifgaccess>).

### 4 IFGAccess

Nesta seção, são consolidados os resultados obtidos com o desenvolvimento do sistema IFGAccess. Primeiro, a visão geral da arquitetura é apresentada. Em seguida, é exibida a modelagem desenvolvida por intermédio da exposição dos diagramas de casos de uso, de atividades e do modelo lógico do banco de dados. Finalmente, são elucidadas questões relacionadas ao desenvolvimento da solução, *e.g.*, página *web*, integrações entre os componentes de *hardware* e *software* e demonstrações de uso típico.

#### 4.1 Visão geral

Diante da necessidade de um sistema automatizado e confiável de controle de acesso aos laboratórios de informática do IFG, desenvolveu-se uma solução capaz de assegurar não-

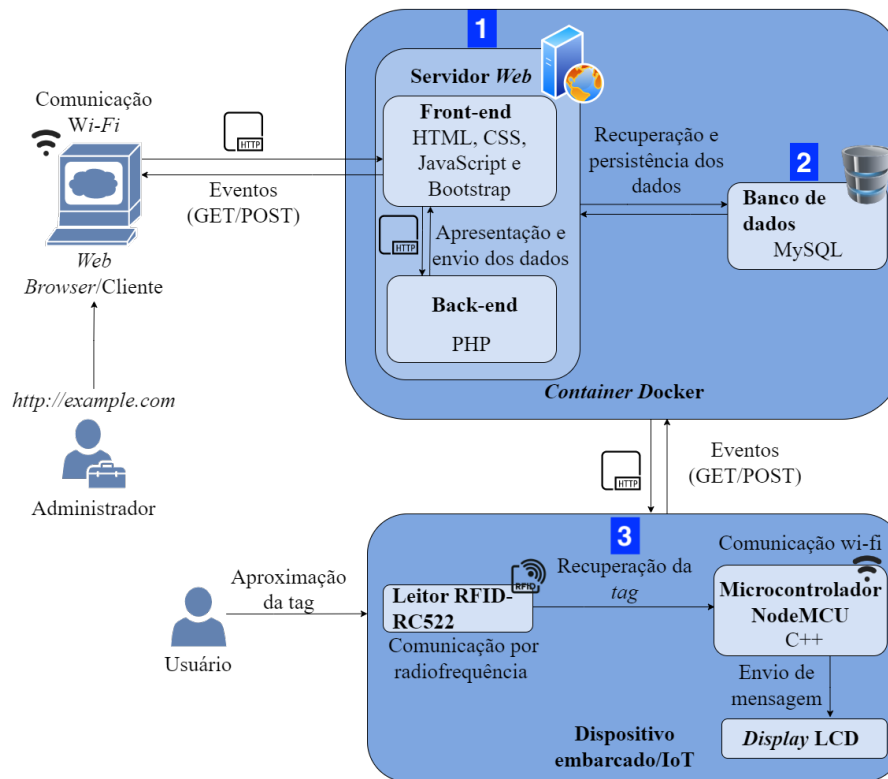


Figura 1. Visão geral da arquitetura do sistema de controle de acesso IFGAccess

repúdio e integridade das informações relacionadas aos acessos. O funcionamento do IFGAccess baseia-se na utilização de *tags* RFID. Ao aproxima-las do leitor RFID, é possível o cadastro de um usuário e/ou a validação do acesso.

A identificação da *tag* é capturada pelo leitor RFID (RFID-RC522) e enviada à página *web* que verifica no banco de dados se existe registro correspondente àquela identificação, além de questões relacionadas às permissões e validade. Quando a *tag* é devidamente reconhecida, o sistema registra no banco de dados a data e o horário de acesso. Caso a *tag* não seja cadastrada, o dispositivo IoT encaminha seu identificador à página *web*, possibilitando associação a um novo usuário.

O sistema de controle IFGAccess é composto por: (1) página *web*, (2) banco de dados, ambos alocados em contêiner *Docker*, além de (3) conjunto de dispositivos IoT, conforme ilustra a Figura 1. Esses dispositivos incluem sensores, atuadores, um microcontrolador e um módulo de comunicação *WiFi*. A camada de interface com o usuário, representada por (1), gerencia a interação com o dispositivo embarcado. A camada de sensores e atuadores, constantes em (3), permite a captura das informações das *tags* RFID, que são então processadas pelo microcontrolador. Por fim, a camada de dados (2) possibilita a persistência das informações ao receber e enviar dados, por meio da comunicação *Wi-Fi*.

A comunicação entre os dispositivos de *software* e *hardware* é realizada pelo *Hypertext Transfer Protocol* (HTTP), através dos métodos *GET* e *POST*, usados para troca de mensagens entre o dispositivo IoT e a página *web*. Assim, após a leitura de uma *tag* RFID e seu processamento no microcontrolador, os dados são enviados à página *web* que consulta o banco de dados para confirmar a existência e as permissões

associadas à *tag*. Informações úteis são apresentados na tela LCD, garantindo que o usuário acompanhe o processo de autenticação. Caso a *tag* não esteja cadastrada no banco de dados, o sistema envia o identificador desta *tag* à página *web* para efetuar um novo cadastro. O servidor, por sua vez, registra as informações referentes a data e horário de cada acesso, garantindo rastreabilidade e a possibilidade de geração de relatórios.

## 4.2 Diagrama de atividades

O diagrama de atividades representa o fluxo de informações e da tomada de decisões. Os círculos fechados do diagrama, exibidos na Figura 2, representam o início de um fluxo. De forma contrária, os círculos abertos da Figura 2 representam o fim de uma atividade. Foram modelados dois tipos de usuários do sistema. O primeiro é o **Usuário** que possui o intuito de acessar o ambiente. O segundo é o **Administrador** para fins de controle e gerenciamento. Adicionalmente, **Dispositivo Embarcado** representa o fluxo de atividades que envolve o *hardware*.

Usuário tem como ponto de partida a ação de aproximar a *tag* RFID do leitor. Caso a *tag* esteja cadastrada no sistema, Dispositivo Embarcado valida se há alguma entrada (*check-in*) pendente de saída (*check-out*). O registro da entrada (*check-in*) de alguma *tag* RFID só é possível se, e somente se, não houver nenhuma outra *tag* com o estado de *check-in* habilitado. No cenário em que a *tag* não possui cadastro, Administrador pode realizar o cadastro de um usuário, vinculando-o a *tag* aproximada. O Administrador também possui como ação visualizar a lista de acessos e a possibilidade de edição dos dados dos usuários cadastrados.

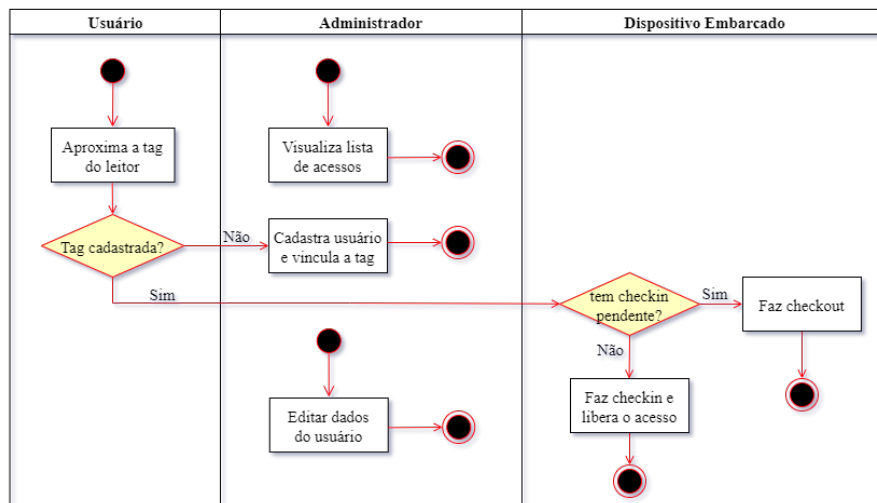


Figura 2. Diagrama de atividades do sistema IFGAccess

### 4.3 Diagrama de casos de uso

O diagrama de casos de uso descreve os atores e suas funções e ações dentro do sistema IFGAccess. No diagrama ilustrado na Figura 3 é apresentado dois atores do sistema: (1) Usuário, que interage com o dispositivo IoT aproximando a *tag* RFID do leitor, e (2) Administrador, que tem como ações cadastrar o usuário, vincular a *tag* ao cadastro e visualizar a lista de acessos por meio da página *web*.

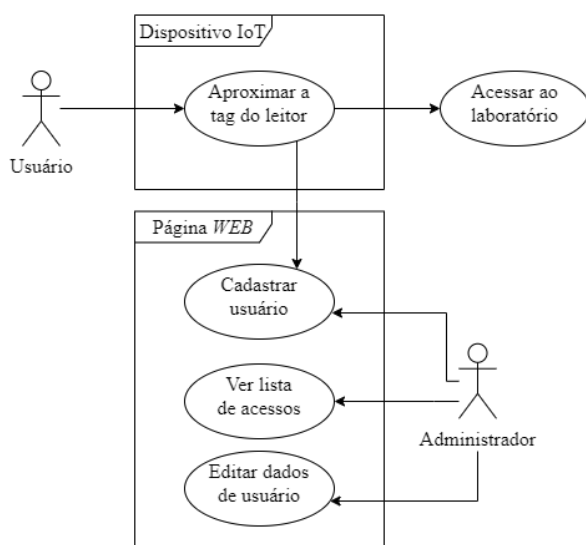


Figura 3. Diagrama de Casos de Uso do sistema IFGAccess

### 4.4 Modelo lógico do banco de dados

A Figura 4 descreve o modelo lógico do banco de dados. Os dados são organizados, armazenados e manipulados através de duas entidades: *access* e *users*. Essas tabelas contêm os atributos dos usuários e acessos do sistema, respectivamente. Como pode ser observado na Figura 4, *users* registra dados do usuário, tais como matrícula, nome, e-mail, telefone e valor da identificação da *tag*. Esses dados são fundamentais no contexto de identificação. A tabela *access* se relaciona com a tabela de *users* por meio do ID da tabela *users* com a chave estrangeira em *access*. A tabela *access* também possui um

ID gerada aleatoriamente, o número da sala acessada bem como registros de data e hora de entrada e saída.

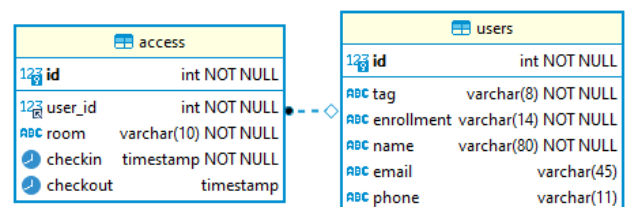


Figura 4. Modelo lógico do banco de dados do sistema IFGAccess

### 4.5 Página web

A construção da página *web* iniciou-se com a containerização do ambiente de desenvolvimento, através do *Docker*. O projeto contém duas imagens: (1) *apache*, para que seja possível a interpretação da linguagem PHP, e (2) banco de dados MySQL, utilizado para persistência dos dados. A Figura 5 ilustra a tela de consulta de uma *tag* RFID não cadastrada. O campo *Tag* da Figura 5 mostra o identificador capturado pelos dispositivos de *hardware*. Contudo, por não existir correspondência armazenada desse identificador, a mensagem “A *tag* aproximada não está cadastrada!!!” é exibida.

Por favor, aproxime a tag/cartão do leitor

User Data	
Tag	: 7D425BD3
Name	: -----
Matrícula	: -----
Email	: -----
Telefone	: -----

A tag aproximada não está cadastrada!!!

Figura 5. Página de consulta de *tags* não cadastradas

De forma contrária, nos cenários em que a *tag* aproxi-



mada é previamente cadastrada, a página de consulta exibe os dados de identificação da *tag*, nome, matrícula, *e-mail* e telefone do usuário. Como é ilustrado na Figura 6, a *tag* de identificação “8645751F” pertence ao usuário “Daniele dos Santos Araújo”. De forma complementar, é exibido o número de matrícula, *e-mail* e telefone deste usuário.

Por favor, aproxime a *tag*/cartão do leitor

User Data	
Tag	: 8645751F
Name	: Daniele dos Santos Araújo
Matrícula	: 20161070130229
Email	: danielle@gmail.com
Telefone	: 61999999999

Figura 6. Página de consulta de *tags* cadastradas

A Figura 7 ilustra a página de acessos ao sistema IFGAccess. Como pode ser observado na Figura 7, o monitoramento do usuário requisitante é realizado por meio de nome e matrícula, identificação da sala e data e horário dos procedimentos de *check-in* e *check-out*.


 <a href="#">Home</a> <a href="#">Usuários</a> <a href="#">Acessos</a> <a href="#">Cadastrar</a> <a href="#">Consultar</a>				
Lista de Usuários				
Nome	Matrícula	Sala	Checkin	Checkout
Teste	115456465421	S405	2022-12-03 18:26:08	
Teste	115456465421	S405	2022-12-03 18:25:22	2022-12-03 18:25:27
Mário Teixeira Lemes	5464448651	S405	2022-12-02 08:13:33	2022-12-03 18:12:18
Daniele dos Santos Araújo	20161070130229	S405	2022-12-02 08:05:36	2022-12-02 08:13:19

Figura 7. Página de lista de acessos

Em relação a lógica usada para validação das *tags* RFID, a requisição *POST* recebida é verificada. Nessa etapa de verificação, é checado se o identificador da *tag* foi devidamente recebido. Caso a requisição *POST* seja considerada válida, outras validações são executadas. Primeiro, verifica-se se a *tag* já possui cadastro junto ao banco de dados. Caso exista cadastro vinculado a *tag*, o acesso é validado se, vinculada a esta *tag*, não existe procedimento de *check-in* em aberto. IFGAccess considera *check-in* em aberto caso não tenha se realizado o procedimento de *check-out* correspondente. Este comportamento inviabiliza que um *check-in* seja realizado por outro usuário caso exista usuários dentro do laboratório. Assim, com a pendência do procedimento de *check-out*, o sistema exibe mensagem impossibilitando o registro do novo acesso. Finalmente, caso a *tag* possuir cadastro junto ao banco de dados e não existir nenhum usuário com *check-in* pendente de *check-out* é criado um novo registro de acesso, com identificação de usuário, sala, data e horário de entrada.

A lógica de funcionamento do sistema IFGAccess objetiva manter o histórico de tempo de permanência da pessoa responsável pela entrada (*check-in*) nos laboratórios. Dessa forma, o acesso é considerado multi usuário, porém com o estabelecimento de uma pessoa responsável. Logo, se há um

*check-in* em aberto, o acesso fica liberado para a pessoa responsável da *tag* RFID e também para as demais pessoas que adentrarem ao ambiente, assim como acontece no controle manual por chave. De maneira similar a abordagem tradicional, ao realizar o *check-out* a porta é trancada. Porém, a adoção do IFGAccess, em vez do uso de chaves, adiciona o registro confiável de quem realizou a abertura e tornou-se responsável pelos laboratórios, além de possibilitar o cálculo do tempo de permanência.

#### 4.6 Montagem do protótipo

A Figura 8 exibe as conexões realizadas entre NodeMCU, leitor RFID-RC522 e a tela LCD. Para realização das conexões entre o *Display* e o NodeMCU foi utilizado o módulo *Inter-Integrated Circuit* (I2C) para redução da quantidade de portas utilizadas.

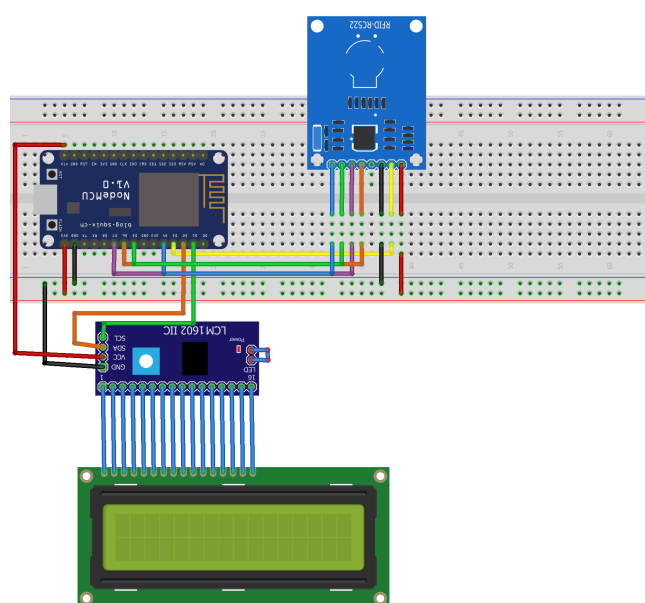


Figura 8. Desenho esquemático das ligações entre NodeMCU, I2C e Leitor RFID

De forma complementar a Figura 8 e para auxiliar na compreensão, a Tabela 2 mapeia as portas e conexões entre o NodeMCU, Leitor RFID MFRC522 e o módulo I2C.

Tabela 2. Relação de conexões dos dispositivos

NodeMCU	Leitor RFID MFRC522	I2C
GND		GND
Vin		VCC
D2		SDA
D1		SCL
D4	SDA	
D5	SCK	
D7	MOSI	
D6	MISO	
GND	GND	
D3	RST	
3V3	3V3	

O leitor RFID-RC522 reduz a cobertura de *tags* que podem ser utilizadas na implementação e testes, uma vez que a identificação das *tags* utilizadas não podem ultrapassar 8

*bits*, correspondendo a modelos básicos disponíveis no mercado para fins de pesquisa e para elaboração de projetos de pequeno porte. Em uma nova versão e evolução do protótipo, pretende-se adicionar um módulo RFID mais robusto para que seja possível o cadastro de tags de maior tamanho e com maior poder de alcance. Considerando as limitações do leitor RFID e o propósito do artigo, a próxima seção demonstra o potencial uso do sistema IFGAccess para substituição do uso tradicional de chaves para controle de presença.

#### 4.7 Demonstração

Para a comunicação entre o dispositivo embarcado e a página *Web* é requisito que NodeMCU esteja conectado à Internet. O leitor RFID permanece ativo e aguardando (buscando) a aproximação de uma *tag* de identificação. Este processo é acompanhado pela mensagem “Aproxime a *tag* do leitor!”, conforme ilustra a Figura 9.

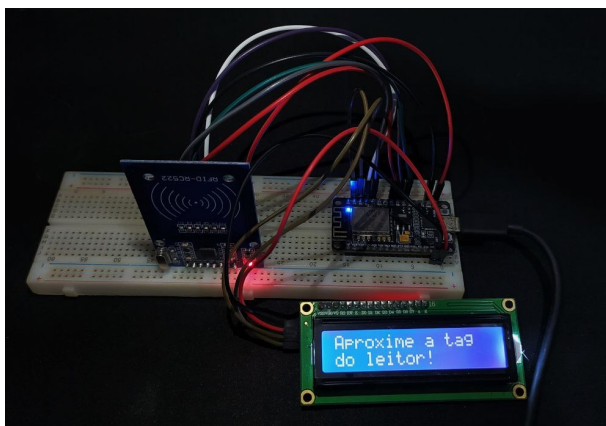


Figura 9. Protótipo aguardando a aproximação de uma nova *tag*

Após a aproximação de uma *tag* e a validação das informações recebidas pela página *Web*, é exibida na tela mensagens sobre a permissão de acesso. A Figura 10 e a Figura 11 exibem a demonstração de acesso liberado e negado, respectivamente.

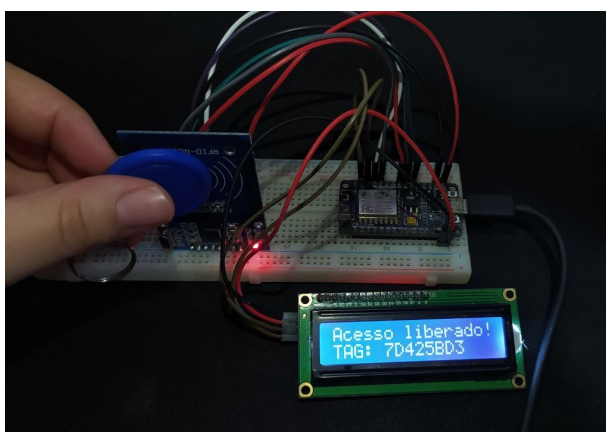


Figura 10. Protótipo exibindo a mensagem de acesso liberado

## 5 Conclusão

Objetos inteligentes oferecem uma série de recursos que possibilitam a construção de sistemas para monitoramento remoto, automação, controle de dispositivos, e podem ser usados para aumentar a eficiência, reduzir custos, melhorar a

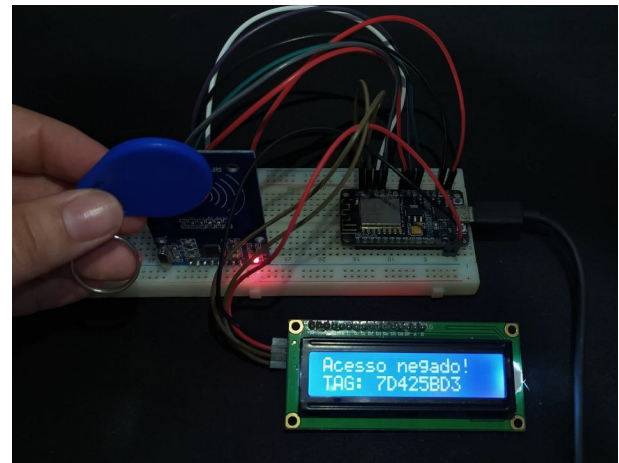


Figura 11. Protótipo exibindo a mensagem de acesso negado

segurança e facilitar a vida das pessoas. Adicionalmente, é possível criar aplicações e serviços para cada dispositivo, permitindo criação de redes de objetos conectados que trocam dados e informações de forma eficiente e segura.

Este artigo apresentou o desenvolvimento de um protótipo, denominado IFGAccess, para controle automatizado de acessos aos laboratórios de informática do IFG, através da integração da tecnologia de radio-frequência e dispositivos computacionais de baixo custo. Para atingir este objetivo, uma página *Web* foi construída para possibilitar consulta e cadastro de *tags* RFID, edição e listagem de usuários e acessos, através de um ambiente containerizado.

O sistema embarcado, baseado no microcontrolador ESP8266, e integrado ao módulo RFID, mostraram-se adequados. A comunicação entre componentes de *software* e *hardware*, através do protocolo HTTP, permitiu o envio dos identificadores das *tags* obtidas pelo leitor RFID. Os resultados indicam comportamento compatível do protótipo nos processos de registro e autenticação, assegurando segurança apropriada para esses ambientes.

Como trabalho futuros, pretende-se adicionar um relé e uma trava elétrica solenoide aos componentes de *hardware* para efetiva liberação das portas dos laboratórios. Sugere-se também como melhorias para a página *web* um sistema de *login* que limite acessos as funcionalidades de cadastro e edição para o usuário administrador, assim como a inclusão da funcionalidade de geração de relatório de acessos. Juntamente com as melhorias ao sistema, pretende-se apresentar a solução com estimativa de custos dos dispositivos para toda comunidade acadêmica a fim de efetiva implementação.

## Declarações complementares

### Contribuições dos autores

MTL e DSA contribuíram para a concepção deste estudo. DSA realizou os experimentos. DSA é o principal escritor deste manuscrito. Todos os autores leram e aprovaram o manuscrito final.

### Conflitos de interesse

Os autores declaram que não têm nenhum conflito de interesses.

### Disponibilidade de dados e materiais

Os conjuntos de dados (e/ou softwares) gerados e/ou analisados durante o estudo atual estão disponíveis online<sup>1</sup>.

<sup>1</sup><https://github.com/felurye/ifgaccess>

## Referências

- Bates, M. P. (2008). *Programming 8-bit PIC microcontrollers in C: with interactive hardware simulation*. Newnes, Burlington, MA.
- Brito, C. V. d. S. P., dos Santos, W. B., Galhardo, C. X., and dos Santos, V. M. L. (2019). Etiquetas inteligentes na administração pública: análise da viabilidade no controle patrimonial da UNIVASF. *ForScience*, 7(2). Disponível em: <https://forscience.ifmg.edu.br/index.php/forscience/article/view/661>.
- Denardin, G. W. and Barriquello, C. H. (2019). *Sistemas operacionais de tempo real e sua aplicação em sistemas embarcados*. Editora Blucher, São Paulo, SP.
- Firat, Y. and Uğurlu, T. (2018). Automatic garage door system with arduino for defined licence plates of cars. In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pages 1–8, Malatya, Turkey. IEEE. DOI: 10.1109/IDAP.2018.8620835.
- GSMA Association (2019). The mobile economy latin america. Disponível em: <https://www.gsma.com/mobileeconomy/latam>.
- International Organization for Standardization (2013). *NBR ISO/IEC 27002: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação*. Rio de Janeiro. Disponível em: <https://www.iso.org/standard/54533.html>.
- Jiménez, M., Palomera, R., and Couvertier, I. (2013). *Introduction to embedded systems*. Springer, New York, NY. DOI: 10.1007/978-1-4614-3143-5.
- Lisboa, R. A. C. B. (2021). Aplicação de controle patrimonial utilizando tecnologia RFID. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas), Universidade Tecnológica Federal do Paraná, Ponta Grossa. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/27833>.
- Maia, G. Q. *et al.* (2019). Protótipo de controle de acesso utilizando RFID para automatização da segurança interna da Ufersa - Campus Mossoró. Monografia (Graduação em Engenharia Elétrica), Centro de Engenharias – Universidade Federal Rural do Semi-Árido, Mossoró. Disponível em: <https://repositorio.ufersa.edu.br/handle/prefix/3637>.
- Pohl, K., Hönninger, H., Achatz, R., and Broy, M. (2012). *Model-based engineering of embedded systems: The SPES 2020 methodology*. Springer, Heidelberg. DOI: 10.1007/978-3-642-34614-9.
- Silveira, D. W. *et al.* (2021). Desenvolvimento de uma fechadura eletrônica: um sistema de controle de acesso com registro em banco de dados e site de gerenciamento. TCC (graduação) - Tecnologias da Informação e Comunicação, Universidade Federal de Santa Catarina, Araranguá. Disponível em: <https://repositorio.ufsc.br/handle/123456789/223836>.
- Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S. (2010). Vision and challenges for realising the internet of things. Disponível em: <https://scholar.google.com/scholar?cluster=6449516870303097662>.
- Vazquez, C. E. and Simões, G. S. (2016). *Engenharia de Requisitos: software orientado ao negócio*. Brasport.
- Weinstein, R. (2005). RFID: a technical overview and its application to the enterprise. *IT professional*, 7(3):27–33. DOI: 10.1109/MITP.2005.69.