Controle de Acesso Físico com Data Logger na Nuvem

Paulo Tadeu Pereira Junior[1], Mozart Lemos de Siqueira[2]

[1]Engenharia de Computação– Universidade Lasallse (Unilasalle)
Av. Victor Barreto, 2288, Centro - Canoas RS, 92010-000 – Canoas – RS – Brazil

[2]Prof. Dr. Coordenador do curso de Ciência da Computação e Coordenador dos cursos de tecnologia na área de TI (EaD) – Universidade Lasallse (Unilasalle) – Canoas , RS – Brazil

paulo.junior1260@unilasalle.edu.br,mozart.siqueira@unilasalle.edu.br

Abstract*. This work proposes build a RFID reader prototype with internet connectivity and records in a cloud database, comparing its advantages to comercial standalone devices, with objective of controlling physical access. The technologies involved in the study are relevant because they allow application not only in the current proposal, but also in diferente automation opportunities in residencial, comercial and industrial environments.*

Resumo. *Este trabalho propõe a montagem de um protótipo leitor RFID com conectividade com a internet e registros em base de dados na nuvem, comparando suas vantagens aos dispositivos comerciais do tipo standalone, tendo o objetivo em controlar acesso físico. As tecnologias envolvidas no estudo são relevantes porque permitem aplicação não só na proposta, mas também em diferentes oportunidades de automação em ambientes residenciais, comerciais e industriais.*

1. Introdução

As questões de segurança sempre são relevantes para as pessoas, porque remete a proteção e resguardo das coisas que tem mais valor para os indivíduos. "Toda pessoa tem direito à vida, à liberdade, e à segurança pessoal" ONU; NETO (1997).

Em muitas situações a segurança pessoal e patrimonial se misturam, porque ações que são feitas para proteger o patrimônio acabam também protegendo a integridade física das pessoas. Nesse sentido, o excesso de dispositivos tecnológicos não garante total segurança, porque todo sistema tem falhas que podem ser exploradas, desta forma, não é o sistema de segurança mais caro que proporciona maior eficiência, mas um sistema adequado com um correto dispositivo de segurança para um determinado tipo de necessidade que deve ser cuidadosamente escolhido para alcança a melhor eficiência NEF (1998).

Estamos imersos em ecossistemas de dispositivos eletrônicos e na área de controle de acesso físico não é diferente. Ao entrar em um banco ou em uma empresa, nos deparamos no caminho de acesso com sistemas de controle que liberam passagem somente mediante uma forma de comprovação, validar se a pessoa tem autorização em estar no local ou transitar em determinado ambiente, por exemplo, as catracas que ficam no *hall* de entrada de algumas empresas, independente se visitante ou funcionário, as pessoas necessitam interagir com um dispositivo eletrônico que por sua vez irá validar a autorização para transpor aquele limite.

Os dispositivos de controle de acesso físico ficam cada vez mais complexos, sofisticados e caros, são dispositivos que proporcionam com sua presença não só a sensação de segurança,

mas também facilidades muito eficientes, como por exemplo, reconhecimento facial, verificação biométrica, uso de *tag* RFID, dentre outros.

De modo geral, independente da marca, existem dispositivos simples de controle de acesso utilizando leitor RFID, são chamados de *standalone*, porque são equipamentos que funcionam de forma isolada, ou seja, toda validação de usuários fica armazenada no dispositivo local, sem compartilhar ou trocar dados com sistemas remotos ou externos.

Ciente do uso desses dispositivos *standalone*, foi observado que existe larga empregabilidade em inúmeras situações de segurança no controle de acesso físico, desta forma, surgiu a motivação em estudar as vantagens e desvantagens em conectar à internet um protótipo semelhante aos dispositivos *standalone* comerciais. A montagem de um protótipo utilizando plataforma de *hardware* de desenvolvimento junto com *tag* e leitor RFID permitem avaliar as funcionalidades, viabilidade operacional do emprego desse tipo de dispositivo de controle de acesso conectado à internet, incluindo armazenagem de registros em uma base de dados na nuvem.

2. Objetivo

A proposta visa atender a necessidade da aplicação de um dispositivo de baixo custo com a funcionalidade de leitura de tag RFID para controle de acesso físico tendo a facilidade da visualização dos registros e manipulação dos dados de forma remota.

3. Justificativa

O trabalho compara dispositivos através de pesquisa em *datasheet* de alguns sistemas comerciais de controle de acesso com leitor RFID tipo *standalone*, relacionando suas características em comum para comparar com o protótipo montado, mostrando com isso, que existe viabilidade técnica utilizando os componentes do protótipo em conectar dispositivos simples de controle de acesso físico mediante leitura de tag RFID com a internet, proporcionando diversas facilidades para os usuários e escalabilidade do sistema com relação a possibilidade de integração na base de dados na nuvem de dezenas ou até centenas de dispositivos como o protótipo o que não acontece com os dispositivos comerciais tipo *standalone*.

4. Referencial Teórico

4.1 Efeito Wiegand

O efeito Wiegand é um efeito magnético não linear que recebeu este nome após as descobertas de John R. Wiegand, onde acontece em condutores especialmente tratados chamados de fios Wiegand DLUGOS (1998).

Fios Wiegand são de liga FeCov (Ferro-Cobalt-Vanadium) ótimos para o efeito desejado. Quando um pulso é aplicado sobre um fio Wiegand um salto do efeito Barkhausen pode ser observado, mesmo com aplicação de um campo magnético de baixa variação e baixa intensidade. O efeito Barkhausen é o nome dado para o ruído na saída de um componente ferromagnético quando forças magnéticas aplicadas sofrem variações ou são alteradas

FUKUMOTO e ATSUSHI (2017). A amplitude e a largura do pulso induzido não dependem da frequência do campo magnético aplicado CHANG e CHANG (2020).

Os fios Wiegand têm sido usados em sensores magnéticos de rotação e de posicionamento, esses sensores operam sem a necessidade de baterias porque podem ser induzidos a produzir a própria energia, com isso, atraindo a atenção para aplicações em módulos eletrônicos auto energizados F e S e M (2021).

Fazendo uso desses fenômenos que a tecnologia RFID se torna possível em estabelecer uma forma de comunicação.

4.2. RFID

O primeiro sistema de identificação ativo foi liderado por Watson-Watt em um projeto secreto britânico ajudando a criar o *Identify Friend or Foe* (IFF) sendo implantado pela Força Aérea Real britânica durante a segunda guerra mundial. O transmissor colocado em um avião britânico quando recebia sinal da estação de RADAR (*Radio Detection and Ranging*), retornava com indicativo que se referia a uma aeronave amiga e auxiliando a perseguição de aviões inimigos. O sistema RFID funciona de maneira similar, onde um sinal é enviado para uma *tag* (*Transponder*), este é ativado refletindo o sinal à base, caracterizando um sistema passivo, ou retornando um novo sinal, assim caracterizando um sistema ativo BRAGG (2001).

Charles Walton em 1973 era um empreendedor na Califórnia e aplicou a patente de um *transponder*, o objetivo era a criação de um *tag* para abrir portas sem o uso de chaves. O *transponder* fica embutido em um cartão, assim o leitor obtém o número de identificação, sendo válido, a porta é liberada JONES e CHUNG (2007).

4.3. Componentes do RFID

O sistema RFID pode ser composto por diversas combinações indo desde conjuntos simples de componentes até dispositivos com maior complexidade, no entanto, três dispositivos fundamentais se destacam como elementos essenciais para o RFID, são eles: um dispositivo que é interrogado, que possui as informações de interesse para serem lidas, esse componente é a *tag* ou etiqueta. Está encarregado em interagir com o segundo componente do sistema chamado de leitor, este componente não só gera a indução eletromagnética que proporciona à *tag,* do tipo passiva responder aos impulsos do protocolo de leitura e escrita, mas também é o *reader* encarregado em estabelecer uma comunicação e troca de informação, o terceiro e importante componente do sistema, identificado como controlador ou microcontrolador, este último componente é responsável por coordenar a captura de dados, além disso, fica encarregado em interagir com a interface de comunicação com outras entidades computacionais, como por exemplo, um servidor de aplicação ou um sistema de banco de dados para registrar os dados capturados de uma *tag*, tornando o sistema RFID funcional GREFF (2009).

4.3.1. Tag

A *tag* que é o acrônimo de TRANSmitter/ resPONDER, sua principal funcionalidade é responder aos impulsos do leitor feitos por rádio frequência, na Figura 1 a imagem ilustrativa dos componentes integrantes da *tag*.

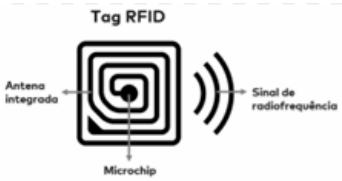

Figura 1 — Tag RFID.

A estrutura é simples, composto por um Microchip responsável por armazenar as informações em uma memória EEPROM (E*letrically Erasable Programmable Read-Only Memory*) e efetuando a comunicação com o leitor através da antena, na grande maioria, a *tag* é encapsulada em material plástico ou silicone tendo diversos formatos, como chaveiro, etiquetas e cartões FINKENZELLER (2010).

4.3.2. Transponder passivo

O *transponde*r passivo não tem uma fonte de alimentação. Através da antena da *tag* o campo eletromagnético do sistema leitor fornece toda a energia necessária para que a *tag* funcione, além disso, o campo magnético pode ser modulado para transferir dados. A *tag* tem a possibilidade de armazenar um pouco de energia em um curto período fornecida pelo leitor, desta forma, o funcionamento é possível FINKENZELLER (2010).

4.3.3. Reader

O dispositivo *reader* na Figura 2 combina as funções de emissor e receptor, suas principais atribuições são: efetuar a captura das informações em uma *tag,* energizar a *tag* passiva e interagir com sistemas controladores externos.

Esse tipo de dispositivo é integrado com antena e microchip dedicado para as funções de *reader*, com isso, é possível fazer a interface com a *tag* e com algum sistema controlador externo, neste caso, através de interface SPI (*Serial Peripheral Interface*).

Um *reader* pode estar integrado com uma antena interna ou ter a antena em um dispositivo separado, desta forma, a antena faz a interface com o dispositivo que será consultado GLOVER e BHATT (2006).

Figura 2 — RFID *reader*.

4.4. Microcontrolador

O microcontrolador utilizando as interfaces de comunicação, é responsável por transpor os dados coletados pelo *reader* para o sistema base de dados, além disso, consulta se a *tag* lida está autorizada para seguir com o processo de liberação.

4.5. ESP32

Criado por Espressif Systems, ESP32 é utilizado como controlador, sendo um sistema de baixo custo e baixo consumo de energia em plataforma SoC (*System on a Chip*) com módulos Wi-Fi e Bluetooth. Projetado para dispositivos móveis, dispositivos eletrônicos *wearable* ("vestíveis") e aplicações IoT (*Internet of Things*). ESP32 alcança ultrabaixo consumo através de *features*, múltiplos modos de potência e escala dinâmica de potência. ESP32 é considerada uma plataforma de código aberto *opensource* porque permite que sejam desenvolvidos códigos em linguagens C/C++ e esses códigos podem ser compartilhados e aplicados por outros desenvolvedores, permitindo melhorias e acréscimo de funcionalidades ao código original, além disso, toda a estrutura do hardware é disponibilizada para que seja montada por qualquer interessado THE INTERNET (2022).

4.6. Wi-Fi

A plataforma ESP32 comporta a tecnologia Wi-Fi que é amplamente aplicada e está presente em grande parte das residências e empresas que desejam compartilhar com seus eletrônicos uma conexão de rede local ou conexão com a Internet.

Ironicamente a sigla Wi-Fi não significa nada, é considerado muitas vezes a abreviação de *Wireless Fidelity*, algo que não representa quesitos técnicos. O termo foi criado por uma empresa de *marketing* porque a indústria de tecnologias sem fio estava preocupada em criar um nome amigável para se referir ao padrão IEEE 802.11 e o nome pegou VARIZON (2022).

A grande vantagem da ESP32 utilizar a interface de comunicação Wi-Fi, se dá na possiblidade do acesso à internet, desta forma, o dispositivo pode interagir não apenas com sistemas servidores de aplicação, mas também com outros dispositivos ESP32.

4.7. Google Firebase

O Google Firebase Realtime Database é um banco de dados NoSQL e por isso, tem otimizações e funcionalidades diferentes de um banco de dados relacional. O Firebase Realtime Database é um banco de dados hospedado em nuvem. Os dados são armazenados como documentos JSON e sincronizados em tempo real para cada cliente conectado. Quando são criados aplicativos multiplataformas usando SDKs para Apple, Android e JavaScrip, todos seus clientes compartilham uma instância Realtime Database e recebem automaticamente atualizações com os dados mais recentes. A API do Realtime Database foi desenvolvida para automatizar apenas operações que possam ser executadas com rapidez. Isso possibilita uma ótima experiência em tempo real que atende milhões de usuários sem comprometer a capacidade de resposta. No

Google Firebase é possível criar aplicativos avançados e colaborativos com acesso seguro ao banco de dados diretamente do código do cliente. Os dados são mantidos localmente e, mesmo off-line, os eventos em tempo real continuam sendo executados. Quando o dispositivo recupera a conexão, o Realtime Database sincroniza as alterações feitas nos dados locais com as atualizações remotas que ocorreram enquanto o cliente estava off-line GOOGLE (2022).

5. Resultados Finais

5.1. Metodologia

O projeto de pesquisa utilizou a metodologia de pesquisa exploratória qualitativa, relacionando os dispositivos de controle de acesso comuns do tipo *standalone,* descrevendo seus requisitos e comparando com o protótipo elaborado.

5.2. Avaliação Qualitativa

Elaborado o Quadro 1 com os requisitos comuns dos dispositivos tipo *standalone* relacionados através da avaliação de *datasheet,* facilitando a comparação com o Protótipo elaborado INTELBRAS (2022).

Quadro 1 — Relação dos Requisitos

Itens	Descrição dos Requisitos	Dispositivos s*tandalone* comerciais	Protótipo
1	Teclado	sim	não
2	Leitor RFID	sim	sim
3	Capacidade 1.000 usuários	sim	sim
4	Alimentação 12Volts	sim	sim
5	Distância de leitura RFID 3 a 6cm	sim	sim
6	Velocidade de leitura <20ms	sim	não
7	Conexão com a Internet	não	sim
8	Uso de base de dados em nuvem	não	sim
9	Utilização de App em celular para gerenciar *tag* RFID	não	sim
10	Escalabilidade	não	sim

Fonte: O autor (2022)

Observando o Quadro 1, o Protótipo reúne mais requisitos classificados como "sim". Necessário considerar no cenário de controle de acesso os requisitos que atendem à demanda, por exemplo, o protótipo considera conexão com a internet, ou seja, o cenário de implementação deve ser atendido por uma cobertura Wi-Fi, permitindo conectividade com a internet, de outro lado, os dispositivos *standalone* podem funcionar sem conectividade com a internet, mas tem limitação em alterar quais *tags* RFID tem ou não autorização de acesso, em situações que necessitam que uma *tag* seja bloqueada, um operador precisa ir até o dispositivo *standalone* para fazer uma nova configuração, algo que no protótipo é facilmente ajustado, porque as

permissões ficam registradas em um banco de dados na nuvem, assim qualquer usuário com permissão de administrador pode fazer o bloqueio e permissão das *tags* RFID de forma remota sem necessidade de deslocamento até o dispositivo. Existindo a necessidade de controlar diversos acessos, os dispositivos tipo *standalone* são limitados, precisando de um hardware controlador adicional, já no protótipo proposto, a adição de mais dispositivos na base de dados em nuvem pode chegar a dezenas ou centenas de dispositivos, dando dessa forma, grande escalabilidade ao sistema de controle de acesso físico.

5.3. Protótipo

O Protótipo foi desenvolvido utilizando a plataforma ESP32 e codificado utilizando IDE do Arduino.

A Figura 3 apresenta o fluxograma do código implementado no dispositivo ESP32. Inicialmente são importadas todas as bibliotecas necessárias para interagir com os periféricos, conexão com a internet e troca de informações com a base de dados em nuvem.

O setup consiste em estabelecer configurações preliminares, como por exemplo, fazer a tentativa de conexão com a internet conforme indicam as setas no fluxograma, partindo do setup e conectado com a caixa denominada "Conectar com a Internet".

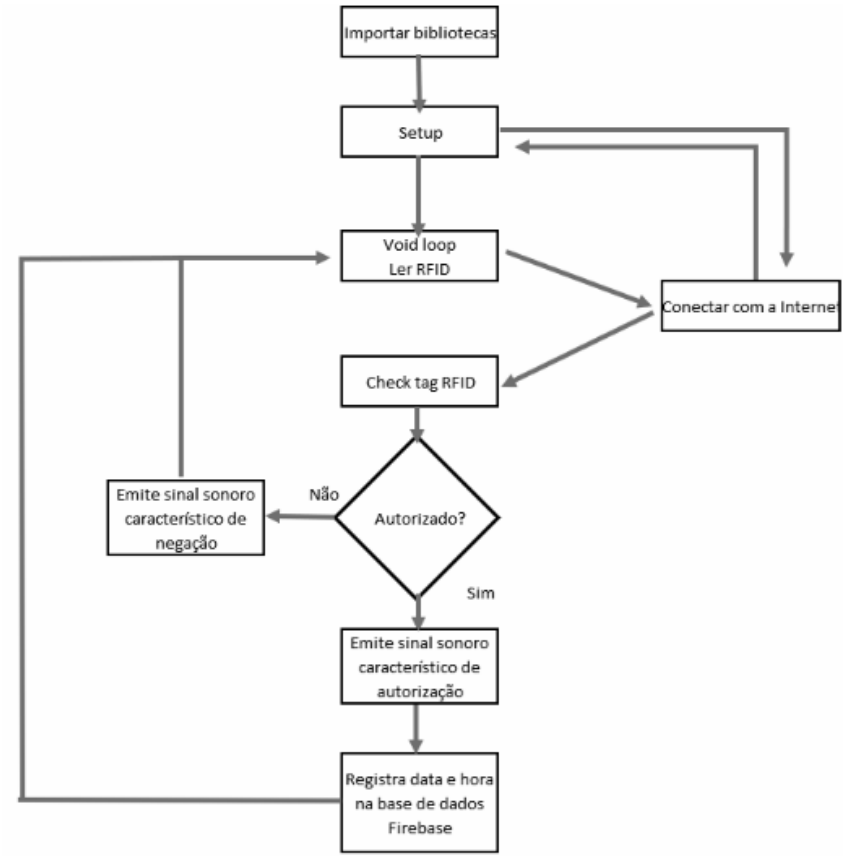

Figura 3 — Fluxograma do código no ESP32.

A área do código representado no fluxograma como "Void loop Ler RFID" consiste na rotina em permanecer ativa a interface SPI do ESP32 com o dispositivo *reader* de RFID, com

isso, quando uma *tag* for detectada pelo *reader* e suas informações coletadas, o dispositivo ESP32 verifica a conectividade com a internet e prossegue com a execução do código.

O bloco seguinte denominado como "Check tag RFID" consulta a base de dados na nuvem através da conexão com a internet, desta forma, pode avaliar se a *tag* está autorizada ou não. Caso a *tag* não esteja autorizada, um sinal sonoro característico de negação é emitido e a rotina para leitura de *tag* é novamente iniciada. Caso a *tag* esteja autorizada, um sinal sonoro característico de permissão é emitido através do buzzer, com isso, a data e hora são registrados na base de dados na nuvem, para isso, o código deve enviar os dados em formato padrão respeitando a composição seguinte:

(identificação_banco_de_dados/UsersData/ID_do_Usuário/UsersLog/ID_da_tag_RFID/log/data, **valor**: hora)

Após a inserção, essa informação fica disponíveis para todos os usuários que têm acesso a esse banco de dados, a partir disso, é iniciada novamente a rotina de leitura de *tag* RFID.

Logo, o dispositivo utilizando as funções da biblioteca do Firebase, interage com a base de dados na nuvem.

5.3. Layout

A figura 4 mostra como é feita a conexão da interface SPI do *reader* RFID modelo MFRC522 e o *buzzer* ativo com o controlador ESP32.

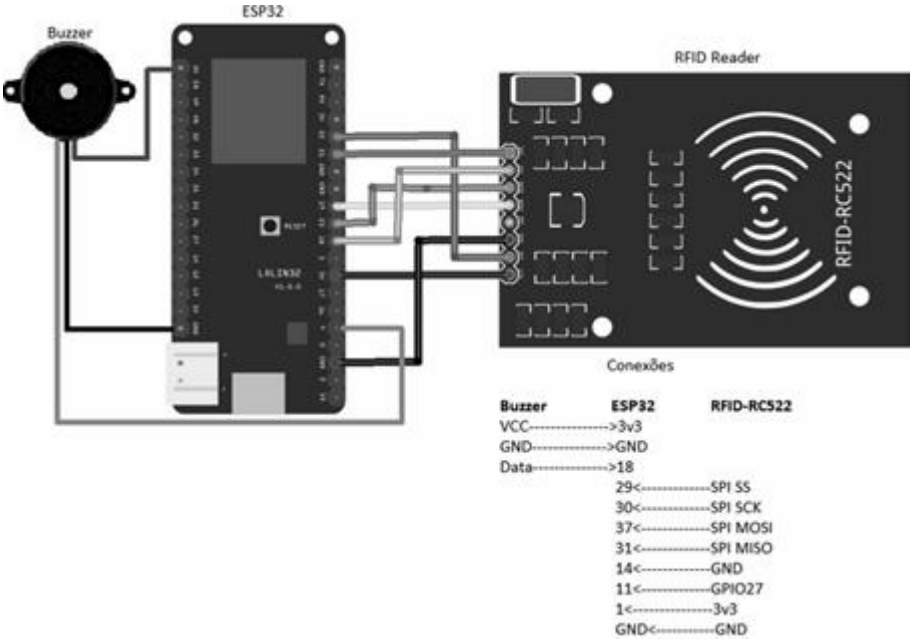

Figura 4 — Layout ESP32, RFID Reader e buzzer.

5.4. Banco de Dados na Nuvem - Firebase

Quando o dispositivo ESP32 envia os dados no formato padronizado, a modelagem dos dados no banco de dados Firebase fica conforme mostrado na figura 5.

Figura 5 — Estrutura de dados no Firebase.

Os dados contidos no primeiro retângulo visto na Figura 5, indica qual é o ID da *tag* RFID, o campo "*status*" logo abaixo tem uma seta, indicando que essa *tag* RFID está como inativada, sem permissão de acesso, desta forma, não recebe nenhum registro de "*log*", já o quadro seguinte em outro ID da tag RFID, tem no "*status*" a indicação como ativo, com isso, a *tag* RFID tem permissão de acesso, desta forma, o campo "*log*" é preenchido com a data recebendo o valor da hora do registro da *tag* RFID.

5.5. Aplicativo para *smartphone*

Um aplicativo para *smartphone* foi desenvolvido de forma a auxiliar na manipulação dos dados na base de dados na nuvem, com isso, os usuários com permissão podem utilizar o aplicativo para alterar o "*status*" de algum *tag* RFID, indicando se tem ou não permissão de acesso ou até mesmo alterar o nome do usuário associado a alguma *tag* RFID.

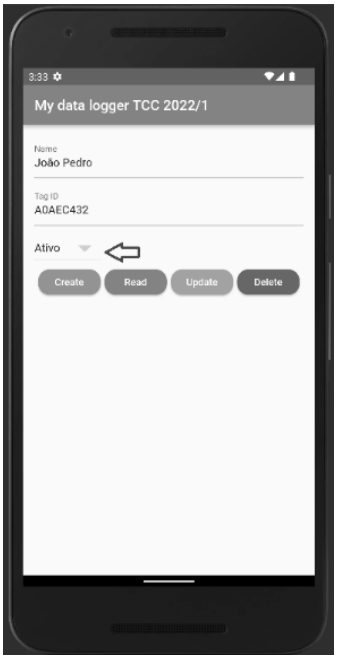

Figura 6 — App para smartphone.

Utilizando o aplicativo para smartphone, é possível alterar o "status" de uma tag RFID, conforme indicado com uma seta na Figura 6, existe uma opção no aplicativo onde permite que seja ajustada a permissão de uma tag RFID alterando para "status" igual a ativo ou inativo.

6. Considerações finais

A iniciativa da pesquisa se deu com a necessidade em ter um dispositivo simples e de baixo custo com as funcionalidades de leitura de *tag* RFID, além disso, registro dos dados coletados de *tag* RFID em um banco de dados na nuvem, permitindo assim, manipular os registros nesse banco de dados por qualquer usuário autorizado, essa interação com base de dados na nuvem não foi encontrada em dispositivos simples e de baixo custo nos produtos comerciais. A grande vantagem do protótipo desenvolvido em comparação com dispositivos com funcionalidades semelhantes, dispositivos esses chamados de *standalone*, é a facilidade em alterar as permissões das *tags* RFID de forma remota, sem a necessidade do deslocamento até o dispositivo físico conforme é feito nos modelos *standalone*. Em uma situação real da perda de uma *tag* RFID por um usuário, no modelo proposto pelo protótipo, rapidamente a *tag* RFID perdida pode ser bloqueada, apenas acessando a base de dados na nuvem e alterando o *status* da *tag* RFID para "inativo", além disso, pode ser feito uso de aplicativo de *smartphone* para manipular o status desejado da *tag* RFID, sendo mais uma facilidade, algo que não acontece nos dispositivos *standalone.* Porém, o protótipo tem a necessidade da existência de uma cobertura Wi-Fi para que exista a conexão com a internet, algo que não é necessário nos dispositivos *standalone.*

Utilizando a metodologia de pesquisa de forma qualitativa, é possível comparar as vantagens e desvantagens de cada tipo de dispositivo, pode ser feito o levantamento de requisitos e possibilidades de uso, nessa comparação o protótipo se demostra promissor para uma implementação comercial. O custo é um fator importante para comparar as soluções, onde o estudo de mercado e elaboração de custo de desenvolvimento do protótipo não foram alvos

de pesquisa do trabalho, mas com base nos registros de compra dos componentes do protótipo, o valor de produção de um produto com os atributos do protótipo pode ficar com custo até 20% menor que os produtos comerciais do tipo *standalone*.

Portanto, a abordagem aplicada na solução estudada abre possibilidades diversas para trabalhos futuros, como criação de outras interfaces com usuário através de páginas web, criação de outras funcionalidades no aplicativo para *smartphones,* aplicar análises estatísticas nos registros das *tags* na base de dados na nuvem em busca de algum comportamento anormal, podendo indicar a possibilidade de fraude, além disso, o protótipo não se limita ao controle de acesso físico, pode ser aplicado ao controle de estoque, tem mobilidade para ser usado em diferentes atribuições, desta forma, como foi utilizada plataforma de desenvolvimento *opensource*, a implementação e colaboração para melhorias do projeto é facilitada.

7. Referências Bibliográficas

ONU, Organização das Nações Unidas; NETO, Heitor Amílcar da Silveira. Declaração universal dos direitos humanos: 50 anos, f. 24. 1997.

NEF, Jorge; CANADA, International Development Research Centre. Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment. IDRC, v. 1, 1998.

DLUGOS, David J. Wiegand effect sensors: theory and applications. Sensors magazine. Questex Media Group, May 1998.

FUKUMOTO, Yoshiyuki ; ATSUSHI, Kamijo. Effect of Milling Depth of the Junction Pattern on Magnetic Properties and Yields in Magnetic Tunnel Junctions. Disponível em: https://iopscience.iop.org/article/10.1143/JJAP.41.L183. Acesso em: 4 abr. 2022.

CHANG, CC; CHANG, JY. Novel Wiegand-effect based energy harvesting device for linear magnetic positioning system 26. 2020. Disponível em: https://link.springer.com/article/10.1007/s00542-020-04899-2. Acesso em: 8 mar. 2022.

F, Iob; S, Saggini; M, Ursino. A novel wireless charging technique for low-power devices based on Wiegand transducer. IEEE Journal of Emerging and Selected Topics in Power Electronics. doi: 10.1109/JESTPE.2021.3089680, 2021.

BRAGG, Michael. RDF 1: The Location of Aircraft by Radio Methods 1935-1945. Twayne Publishers, f. 200, 2001. 400 p.

JONES, Erick C.; CHUNG, Christopher A.. RFID in Logistics: A Practical Introduction. CRC Press, v. 3, f. 260, 2007. 520 p.

GREFF, P. Especificação de um Sistema para Monitoramento de Atividades de Natação usando RFID.. São José, 2009 Dissertação (Curso Superior de Tecnologia

em Sistemas de Telecomunicações) - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, Campus São José, 2009.

FINKENZELLER, Klaus. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. 3 ed. John Wiley & Sons, v. 3, f. 239, 2010. 478 p.

GLOVER, Bill; BHATT, Himanshu. RFID Essentials. "O'Reilly Media, Inc.", f. 139, 2006. 278 p.

THE INTERNET of Things with ESP32. ESP32. Disponível em: http://esp32.net/. Acesso em: 22 abr. 2022.

VARIZON. What is a Wi-Fi network?: What does Wi-Fi stand for?. varizon. Disponível em: https://www.verizon.com/info/definitions/wifi/#:~:text=Wi%2DFi%20is%20the%20wireless,you%20can%20see%20and%20use.. Acesso em: 5 abr. 2022.

GOOGLE. Firebase Documentation. Google Firebase. Disponível em: https://firebase.google.com/docs/database?hl=pt-br. Acesso em: 5 abr. 2022.

INTELBRAS. Tabela comparativa fechaduras e controladores de acesso. Disponível em:https://backend.intelbras.com/sites/default/files/202205/tabela_comparativa_fechaduras_e_controladores_de_acesso_corporativo_digital_0.pdf. Acesso em: 11 abr. 2022.
.