



**FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS
CURSO**

PEDRO HENRIQUE BATISTA BORIN

21910157

VINÍCIUS DE OLIVEIRA PERPÉTUO

21908298

**ABERTURA DE FECHADURA ELÉTRICA POR APROXIMAÇÃO
COM RFID PASSIVO**

BRASÍLIA-DF
2023



PEDRO HENRIQUE BATISTA BORIN

VINÍCIUS DE OLIVEIRA PERPÉTUO

ABERTURA DE FECHADURA ELÉTRICA POR APROXIMAÇÃO COM RFID PASSIVO

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia de Computação do UniCEUB – Centro Universitário de Brasília

Orientador (a): **Luciano Henrique Duque**

BRASÍLIA
2023



PEDRO HENRIQUE BATISTA BORIN

VINÍCIUS DE OLIVEIRA PERPÉTUO

ABERTURA DE FECHADURA ELÉTRICA POR APROXIMAÇÃO COM RFID PASSIVO

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia Elétrica do UniCEUB – Centro Universitário de Brasília

Orientador (a): **Luciano Henrique Duque**

Brasília, 2023.

BANCA EXAMINADORA

Nome e titulação.

Orientador: Luciano Duque
Mestre

Nome e titulação.

Examinador (a) Hugo Molina
Especialista

Nome e titulação.

Examinador (a) Nathália Salomão
Especialista



ABERTURA DE FECHADURA ELÉTRICA POR APROXIMAÇÃO COM RFID PASSIVO

OPENING ELECTRIC LOCK BY PROXIMITY WITH PASSIVE RFID

Pedro Henrique Batista Borin¹, Vinícius de Oliveira Perpétuo², Luciano Henrique Duque³

Resumo

Nas duas últimas décadas, a tecnologia de identificação por radiofrequência tem sido um assunto muito discutido e utilizado em diversas áreas como controle de acesso, identificação e envio de informações das etiquetas RFID, registro e rastreamento de objetos identificados e até mesmo prateleiras inteligentes. Nesse artigo acadêmico “Abertura de Fechadura Elétrica por Aproximação com RFID passivo” será apresentado um sistema de segurança baseado em radiofrequência que permitirá abrir uma fechadura elétrica por meio da aproximação de um cartão com uma etiqueta RFID. O projeto planejado e montado pelos discentes compõem um microcontrolador ESP8266, um leitor de RFID, uma fechadura eletrônica e componentes eletrônicos como resistores, leds, chave tátil e relés. Nesse sistema, o cartão com a etiqueta RFID se aproxima do leitor que, por meio de ondas eletromagnéticas, acessa os dados armazenados em um microchip contido no cartão. Com essas informações, o sistema verifica o código único dado pela etiqueta e valida para saber se aquele cartão é autorizado ou não. Se a chave for autorizada, o ESP8266 aciona o relé onde é emitida uma voltagem para a chave elétrica e assim a porta de acesso é aberta. O sistema apresenta vantagens em relação aos outros sistemas de segurança, como a praticidade e segurança no armazenamento das chaves de acesso, além da facilidade de controle de acesso em ambientes com muitas pessoas. Conclui-se que a abertura de fechadura elétrica por aproximação com RFID passivo é uma solução eficiente e prática para o controle de acesso em ambientes que exigem segurança e praticidade.

Palavras-chave: fechadura elétrica. RFID. microcontrolador. Etiqueta RFID. aproximação.

Abstract

In the last two decades, radio frequency identification technology has been a widely discussed and used topic in various areas such as access control, identification and information sending from RFID tags, registration and tracking of identified objects, and even smart shelves. In this academic article "Opening Electric Lock by Proximity with Passive RFID," we will present a security system based on radio frequency that will allow us to open an electric lock by

¹ UniCEUB, Pedro Henrique Batista Borin

² UniCEUB, Vinícius de Oliveira Perpétuo

³ UniCEUB, Luciano Henrique Duque



approaching a card with an RFID tag. The project planned and assembled by us consists of an ESP8266 microcontroller, an RFID reader, an electronic lock, and electronic components such as resistors, LEDs, tactile switches, and relays. In this system, the card with the RFID tag approaches the reader, which, through electromagnetic waves, can access data stored in a microchip contained in the card. With this information, the system will check the unique code given by the tag and validate whether that card is authorized or not. If the key is authorized, the ESP8266 will activate the relay, which will emit a voltage to the electric lock, thus opening the access door. The system presents advantages compared to other security systems, such as the practicality and security in storing access keys, as well as ease of access control in environments with many people. It is concluded that electric lock opening by proximity with passive RFID is an efficient and practical solution for access control in environments that require security and practicality.

keywords: electric lock. RFID. microcontroller. RFID Tag. proximity.

1 INTRODUÇÃO

O controle de acesso é um aspecto crítico da segurança em diversos ambientes, incluindo residências, empresas e instituições governamentais. São diversos os benefícios fornecidos pela utilização desse sistema, tais como restrição a áreas de acesso exclusivo evitando a afluência de pessoas mal-intencionadas, o controle de informações confidenciais que garante a privacidade do usuário, e até mesmo a própria segurança física.

A tecnologia de radiofrequência (RFID) tem se mostrado uma solução eficiente para o gerenciamento de acesso, ao permitir a identificação de indivíduos autorizados por meio de etiquetas eletrônicas. No entanto, sistemas de controle de acesso com RFID ativo podem ser mais caros, pois os dispositivos RFID ativos requerem baterias para o seu funcionamento. Além disso, os dispositivos ativos podem ser maiores e mais volumosos do que os dispositivos passivos, o que limita sua aplicação em determinados ambientes.

Para superar essas limitações, este artigo apresenta um sistema de segurança baseado em RFID passivo para a abertura de fechaduras elétricas por aproximação de uma chave equipada com uma etiqueta RFID. O sistema consiste em um leitor de

RFID, um microcontrolador ESP8266, componentes eletrônicos como resistores, leds, chave tátil, relés, e a própria fechadura elétrica. O leitor RFID passivo envia um sinal de rádio para a etiqueta RFID na chave de acesso quando ela se aproxima do leitor. A etiqueta responde ao sinal de rádio, fornecendo um código exclusivo que é verificado na memória não volátil que contém os cartões registrados para confirmar se a chave é autorizada ou não. Se a chave for autorizada, o microcontrolador ativa o módulo de relé para desbloquear a fechadura elétrica e permitir que a porta seja aberta.

A utilização de todo o equipamento demonstrou um sistema rápido, seguro e eficiente na identificação das chaves autorizadas. Além disso, o sistema apresenta vantagens em relação aos outros sistemas de segurança, como a praticidade e segurança no armazenamento das chaves de acesso, além da facilidade de controle de acesso em ambientes com muitas pessoas. O sistema também é mais econômico do que sistemas de controle de acesso com RFID ativo, pois as etiquetas RFID passivas são mais baratas do que as etiquetas RFID ativas e não requerem baterias para funcionar, apesar de ser possível utilizar baterias no sistema para alimentação da fechadura elétrica.

O parecer deste artigo tem como objetivo principal descrever o desenvolvimento e a implementação do sistema, explanando a efetividade e funcionalidade do aparelho, além de apresentar as implicações práticas do sistema para o controle de acesso em diferentes ambientes. Assim, conclui-se que a abertura de fechaduras elétricas por aproximação com RFID passivo é uma solução eficiente e segura para o controle de acesso em ambientes que exigem praticidade e segurança.

2 REVISÃO BIBLIOGRÁFICA

Com o objetivo de contextualizar o desenvolvimento do dispositivo de controle de acesso, foram elencados alguns tópicos que apresentam conceitos imprescindíveis sobre os elementos do projeto.

2.1 IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

A identificação por radiofrequência (RFID) é uma tecnologia que captura, analisa, gerencia e responde a dados originários de sensores eletrônicos. Constituída por transponders (etiquetas de radiofrequência), leitores com antenas e algum tipo de controlador. O RFID é uma tecnologia de identificação que utiliza radiofrequência para capturar os dados, além disso as etiquetas RFID podem ser lidas através de obstáculos e objetos, tais como madeira, plástico, papel, entre outros (GREFF, 2009).

Segundo McRoberts (2015), leitores RFID são a escolha preferida para controle de entrada de pessoas em prédios comerciais, bem como em sistemas de transporte público. Esses leitores também marcam presença em hospitais, para demarcar equipamentos descartáveis em salas de cirurgia, garantindo que nenhum objeto estranho seja esquecido dentro dos pacientes.

2.2 ESP8266

O ESP8266 é um microcontrolador que é amplamente utilizado em projetos de Internet das Coisas (IoT). É composto por um processador de 32 bits que opera a uma frequência de até 160 MHz e possui uma interface Wi-Fi integrada, que permite a construção de projetos de comunicação sem fio, ao operar na ligação de dispositivos ou serviços. O microcontrolador também possui portas de entrada e saída, permitindo a conexão de sensores, atuadores e outros dispositivos.

Figura 1: Ilustração do ESP8266



Fonte: ByteFlop. Imagem (JPG). Disponível em: <<https://www.byteflop.com.br/modulo-wifi-nodemcu-esp8266-ch340>>. Acesso em: 21 maio 2023.

2.3 MÓDULO RFID-RC522

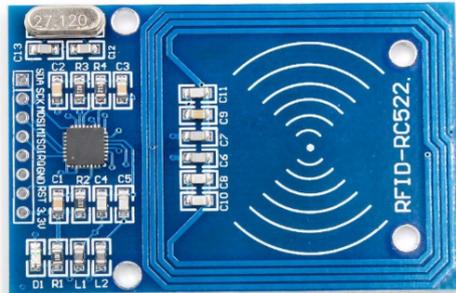
Esse é o módulo responsável pela leitura e registro de informações em cartões com o sistema RFID embutido a partir do Circuito Integrado RC522 segundo a norma ISO/IEC 14443. É conhecido pelo seu baixo custo, fácil implementação em aplicações, como controle de acesso, gerenciamento de inventário, sistemas de pagamento e acompanhamento de bens.

A comunicação do módulo RC522 com o ESP8266 é feita através de uma interface serial pelo uso do protocolo SPI e das conexões feitas ao longo da protoboard (Guimarães, 2021).

Esse módulo opera em 13.56 MHz e suporta vários protocolos como ISO/IEC

14443 Tipo A/B, MIFARE, FeliCa e NFC (MFRC522 Datasheet, 2016).1

Figura 2: Ilustração do RFID-RC522



Fonte: AliExpress, Imagem(WEBP). Disponível em: <<https://pt.aliexpress.com/item/32975863650.html>>. Acesso em: 01 jun 2023

2.4 FECHADURA ELÉTRICA

Fechaduras elétricas são mecanismos abertos por eletricidade ao invés da abertura manual tradicional. Existe uma variedade de tecnologias para controle do acesso de uma porta utilizando uma fechadura elétrica, inclusive a abertura por aproximação de um cartão ou chave cadastrada.

A fechadura elétrica neste projeto servirá para abertura e fechamento do compartimento do sistema. Seu estado normal será trancado (com seu mecanismo expandido) que poderá ser aberto com um sinal elétrico de 12V por meio da aproximação de um cartão cadastrado no leitor de RFID.

Figura 3: Ilustração da Fechadura Elétrica 12V



Fonte: Smart Kits, Imagem(JPG). Disponível em: <<https://www.smartkits.com.br/fechadura-trava-eletrica-solenoid-fec-91-12v>>. Acesso em: 01 jun 2023.

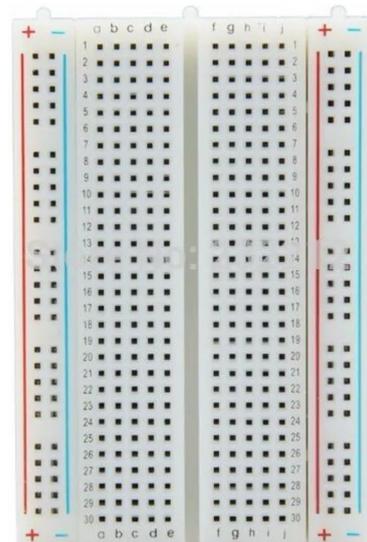
2.5 ARDUINO IDE

Arduino IDE é um sistema que fornece recursos para a programação de placas, permitindo a interação entre usuário e dispositivo. Esse ambiente apresenta grande versatilidade e praticidade, o que possibilita o upload de códigos tanto no sistema operacional Windows quanto no Linux. O software apresenta diversas funções para o manuseio de código, como inclusão de bibliotecas, correção de erros e monitor serial.

2.6 PROTOBOARD

A protoboard é uma ferramenta comumente utilizada para a criação de projetos eletrônicos que requerem uma precisão maior sobre a sua montagem. Com várias entradas para diversos componentes eletrônicos, sua praticidade tem grande uso no ramo da engenharia.

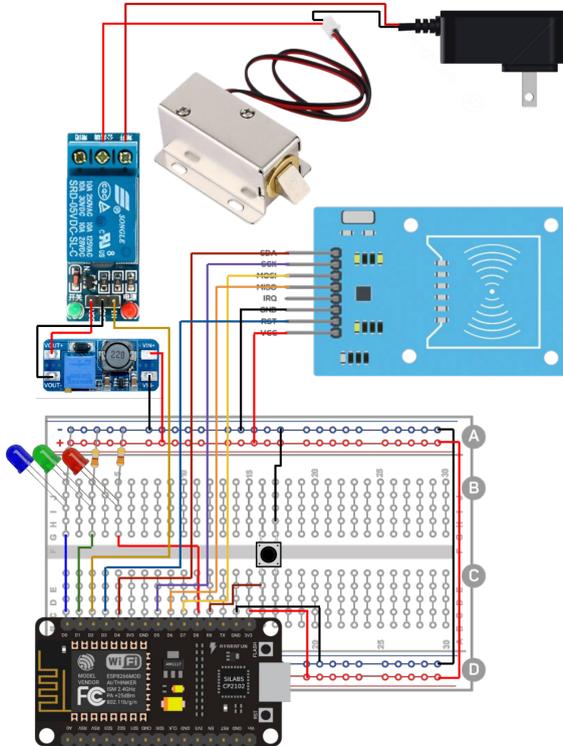
Figura 4: Ilustração de uma Protoboard



Fonte: Smart Kits, Imagem(JPG). Disponível em: <<https://www.smartkits.com.br/protoboard-400-pontos>>. Acesso em: 20 maio 2023.

2.7 DIAGRAMA ELÉTRICO

Figura 5: Diagrama elétrico do sistema



Fonte: Acervo do Autor (2023)

3 METODOLOGIA DO TRABALHO

A elaboração do protótipo de abertura de uma fechadura por aproximação RFID passivo restringe-se ao estudo do funcionamento, utilidade, segurança e praticidade deste sistema comumente utilizado em controle de acesso, gestão de estoque, rastreamento e pedágios eletrônicos.

3.1 MATERIAIS UTILIZADOS

Os materiais utilizados na produção do sistema eletrônico desde o microcontrolador até a chave elétrica são compostos por:

- Microcontrolador ESP8266: Representado na Figura 1, este é o chip responsável pelo controle de todas as operações do sistema. Nele é armazenado o código fonte do

projeto juntamente com as suas instruções de funcionamento, como: Gerenciamento das etiquetas RFID (cadastro mestre, adição e exclusão); Abertura e fechamento da fechadura elétrica; Acionamento dos diodos emissores de luz vermelho, verde e azul;

- Protoboard: É uma ferramenta de grande utilidade para a elaboração de um sistema eletrônico, representado pela figura 4. Ela é a ferramenta necessária para a conexão e comunicação entre todos os dispositivos do sistema.
- Diodos emissores de luz (LEDs): Estes são os responsáveis por comunicar com o utilizador do sistema de forma visual em qual etapa atual está o código embutido no microcontrolador ESP8266. Cada etapa do código fará com que os LEDs pisquem de forma única fazendo com que seja possível identificar a etapa atual do sistema.
- Resistores de filme de carbono: Os resistores têm a função de limitar o fluxo de cargas elétricas por meio da conversão da energia elétrica para energia térmica, permitindo a utilização de componentes eletrônicos que requerem uma carga mais baixa no projeto.
- Chave tátil: A chave tátil tem como função a restauração padrão dos dados do código embutido no microcontrolador. A partir dela é possível limpar a memória apagando assim os cartões de acesso registrados como também o cartão mestre. É a função de “restaurar para os padrões de fábrica”.
- RFID-RC522: Esse componente é o responsável pela realização da leitura de qualquer TAG RFID que se aproxime do seu leitor. É por meio deste que o microcontrolador capta as informações obtidas e



decide qual é a sua próxima operação.

- Relé 5V/1 Canal: O módulo relé é frequentemente utilizado para controle do fluxo de energia elétrica em um circuito, visto que é possível acioná-lo por meio de uma corrente elétrica para mover seu núcleo e assim, liberar um fluxo de energia elétrica específico. No sistema do projeto é por meio do relé que o microcontrolador aciona a chave elétrica para a abertura da porta.
- Módulo elevador de tensão ajustável DC-DC (MT3608): Esse elevador de tensão tem uma faixa de entrada de 2V a 24V e uma faixa de tensão de saída ajustável de 2V a 28V. Ele é responsável pelo aumento da tensão fornecida pelo ESP8266 para o módulo de relé.
- Pontes de Junção (Jumpers): Esses cabos são pequenos conectores que são utilizados para o estabelecimento de conexões elétricas entre os componentes do sistema, criando pontes em pontos específicos da protoboard.
- Fonte de alimentação 12v: A fonte de alimentação de 12 volts tem como único objetivo o fornecimento de energia para a fechadura elétrica, de modo que quando o relé fecha o circuito, a fechadura pode abrir.

3.2 AMBIENTE DE TESTE

3.2.1 CAIXA CASEIRA

O sistema foi implementado e testado em uma caixa caseira de madeira MDF e dimensões 21,8 cm x 22,9 cm x 21,6 cm. Ela foi feita com o uso de tábuas de madeira MDF, pregos, parafusos para a fixação da fechadura elétrica na parte interna da porta e a maçaneta na parte externa. Foram fixadas duas dobradiças para a abertura da porta, além de furos de

passagem na porta e na lateral esquerda para os jumpers e os cabos de energia.

3.2.2 CONFIGURAÇÃO DO AMBIENTE

Os testes de funcionamento foram realizados em ambientes residenciais, acadêmicos e externos com a caixa caseira sempre posicionada em uma superfície plana. A conexão elétrica foi feita levando em consideração o projeto como um protótipo de apresentação, tendo sua placa de circuitos exposta na lateral da caixa para melhor entendimento do sistema. O leitor RFID é exposto na parte externa do ambiente, podendo ser fixado em uma superfície de escolha do utilizador, e os cabos de energia da fechadura elétrica são passados por dentro da caixa para melhor visualização prática do esquema. A fonte de alimentação é conectada na tomada e tem seus cabos conectados diretamente no relé e na fechadura. No caso do acionamento do relé, visto que o ESP8266 não possui uma saída de 5 volts suficiente para alimentá-lo, foi necessário acrescentar um módulo de elevador de tensão (MT3608) como intermediário para elevação da tensão de 3,3V para 5V, possibilitando o acionamento do módulo relé 5V/1.

Já a energização do ESP8266 pode ser feita a partir de:

1. USB:
 - Computador
 - notebook
 - Fonte adaptada USB
2. Bateria;
3. Fonte Externa:
 - Regulador de tensão
 - Fonte de alimentação 3,3V

3.3 CÓDIGO DE FUNCIONAMENTO

Para o funcionamento do sistema de leitura de tags RFID, foi implementado um código no ambiente de desenvolvimento Arduino IDE, onde nele está especificado todo o funcionamento de recepção, processamento e operação para cada leitura



feita sobre o módulo de leitor RFID-RC522.

Para maior praticidade, os pinos do microcontrolador foram definidos para os seus respectivos pinos GPIO, sendo necessário apenas escrever a numeração de saída do microcontrolador, como por exemplo “D2”, no lugar da numeração GPIO, nesse exemplo o número 4.

3.3.1 CONFIGURAÇÕES INICIAIS

Nesse sistema, são utilizadas as bibliotecas de funcionamento do ESP8266 e do módulo de MFRC522, a biblioteca EEPROM.h para armazenamento dos dados na memória não volátil, além da biblioteca string.h para a concatenação do conteúdo de uma variável a outra.

```
#include <SPI.h>
#include <MFRC522.h>
#include <EEPROM.h>
#include <string.h>
```

Depois, são inicializadas as portas de entrada e saída e definidos os pinos de comunicação do módulo RFID.

Os valores do relay, LED_B, LED_G, LED_R e buttonPin foram definidos como D8, D0, D1, D2 e 3 respectivamente.

```
#define SS_PIN D4
#define RST_PIN D3
MFRC522 mfrc522(SS_PIN,
RST_PIN);
```

```
void setup(){
  EEPROM.begin(512);
  Serial.begin(9600);
  SPI.begin();
  mfrc522.PCD_Init();
  pinMode(relay, OUTPUT);
  pinMode(LED_B, OUTPUT);
  pinMode(LED_G, OUTPUT);
  pinMode(LED_R, OUTPUT);
  pinMode(buttonPin,
INPUT_PULLUP);
  valoresObtidos = false;
  delay(1000); }.
```

3.3.2 FUNÇÕES AUXILIARES

As funções auxiliares podem ser chamadas a qualquer momento durante o código para execução de uma representação de luzes sobre os LEDs, registro, aquisição ou limpeza dos dados da memória pelo EEPROM, além de escrever no Serial monitor os dados presentes na memória ou uma mensagem indicando a armação do sistema elétrico. Com o intuito de evitar o excesso de informações no documento, optou-se por mencionar apenas os nomes das funções, ainda que a partir delas se obtenha uma compreensão geral de suas respectivas funcionalidades. Essas funções foram denominadas como:

```
saveValues()
getValues()
getValuesNoPrint()
printEEPROMData()
clearEEPROM()
lendoCartao()
verde()
vermelho()
azul()
esperandoMestre()
mestreRegistrado()
acessoAutorizado()
acessoNegado()
esperandoCartao()
tarefas()
cartoesCheio()
cartaoExcluido()
cartaoCadastrado()
cancelarTarefa()
clearLED()
sistemaArmado()
```

3.3.3 LOOP PRINCIPAL

O loop principal é a função responsável por manter o sistema em funcionamento, sempre verificando se uma nova tag RFID foi detectada próxima ao leitor. Quando o sistema detecta essa tag, há uma verificação de autenticidade sobre uma lista de UIDs cadastrados no sistema e, então, é avaliado se a tag aproximada possui permissão ou não para abrir a



fechadura. Caso sim, a fechadura é aberta por 1,5 segundos, acionando o LED azul que representa o acesso autorizado, até que ela se feche novamente. Caso a tag não tenha acesso garantido pelo sistema, o LED vermelho é aceso por 1 segundo, indicando a não autorização à porta.

Para o cadastro do cartão mestre, ou cartão administrador, basta ter o sistema sem um cartão mestre cadastrado e esperar a representação dos LEDs acionar as cores vermelho e azul de forma intercalada, indicando que a próxima tag a ser aproximada será cadastrada como a tag mestre.

O loop principal se demonstra visualmente ativado pelo acionamento do LED verde, mostrando que o código já preparou todas suas funções e está agora em fase de funcionamento dentro do loop, com ele sendo dividido em 3 partes:

- 1ª parte: O código checa a aproximação de uma tag RFID sobre o leitor;
- 2ª parte: É verificado se a tag aproximada é um cartão comum ou um cartão mestre/administrador. Caso seja um cartão comum, garantir ou não acesso à fechadura elétrica;
- 3ª parte: Caso a tag aproximada seja uma tag mestre, ativar o modo administrador para cadastrar ou excluir uma tag RFID do sistema.

Na primeira parte do sistema, são obtidos os valores na memória não volátil do ESP8266, verificando se existe um cartão mestre e checando a aproximação das tags RFID.

```
void loop(){
  verde();
  if(!valoresObtidos){
    //adquire valores EEPROM
  }

  if(!temMestre){
```

```
    esperandoMestre();
  }

  while(!mfrc522.PICC_IsNewCardPresent()){
    return;
  }

  if(!mfrc522.PICC_ReadCardSerial()){
    return;
  }
}
```

Depois que é conferida a existência de um cartão mestre e detectada a presença de uma tag no leitor, o sistema parte para a segunda parte do código, o que permite a sua continuação onde é verificada a tag aproximada, a qual é armazenada em um char array Buf[12] e comparada com os dados dos cartões já cadastrados para decidir qual operação irá ser tomada. Caso não exista um cartão mestre, a tag aproximada será registrada como tal. Caso exista e a mesma é o próprio cartão mestre, será ativado o modo administrador seguindo para a terceira parte do código.

```
char Buf[12];
stringOne.toCharArray(Buf, 12);

// Cadastra o mestre
if(!temMestre){
  for(int i=0;i<12;i++){
    cartaoMestre[i] = Buf[i];
  }
}

// Checa se é a tag admin
admin = 1;
for(int j=0;j<11;j++){
  if(cartaoMestre[j] != Buf[j]){
    admin = 0;
    break;
  }
}

// Checa se o cartão é válido e
armazena na variável 'pass'
if(!admin){
  int k; int pass = 0;
```



```
for (int k = 0; k < 5; k++){
    if (strcmp(Buf, cartoes[k])
== 0){
        pass = 1;
        break;
    }
}

if(pass){
    digitalWrite(relay, HIGH);
    acessoAutorizado();
    digitalWrite(relay, LOW);
}else{
    acessoNegado();
}
```

Após a verificação e a concessão ou negação de acesso do cartão aproximado, se o código não retornou ao início, tem-se então a indicação de que uma tag mestre foi aproximada no leitor e o sistema ativou a aba administrativa indicado pelo acionamento do LED vermelho, onde é possível aproximar uma nova tag para registro, uma tag existente para exclusão, ou a própria tag mestre para cancelamento desta operação.

Caso seja acionada a função de registro, o sistema verifica o armazenamento de cartões registrados para concluir se é possível registrar ou não uma nova tag no espaço de memória. Se for concluído que não há espaço suficiente para a tag aproximada, é indicado o cancelamento da ação administrativa, caso contrário, ela é armazenada em um char array registro[12] para seu cadastramento.

```
if(admin){
    char registro[12];
    while(int task == 0){
        // espera uma tag ser
        // aproximada e adquire sua
        UID
    }

    // se a tag for a mestre
    // cancela a ação
    if(cartaoAdmin){
        cancelarTarefa();
    }
}
```

```
}

// registra o nº de tags
int m;
int cartoes_cheios = 0;
for(m = 0; m < 5; m++){
    if(strcmp(cartoes[m], "") !=
0){
        cartoes_cheios++;
    }
}

// Loop percorre o array de
// cartoes[] e verifica se a
// tag RFID existe ou não
for (int c = 0; c < 5; c++){
    if(strcmp(registro,
cartoes[c]) == 0){
        strcpy(cartoes[c], "");
        cartaoExcluido();
        sistemaArmado();
        saveValues();
        return;
    }
}

// Se não existir, verifica o
// espaço, e se houver,
adiciona
for (int c = 0; c < 5; c++){
    if (strcmp(cartoes[c], "") ==
0){
        if(cartoes_cheios == 5){
            cartoesCheio();
            sistemaArmado();
            return;
        }else{
            strcpy(cartoes[c],
registro);
            cartaoCadastrado();
            sistemaArmado();
            saveValues();
            return;
        }
    }
}
return;
```

Durante cada operação na seção administrativa, foi projetada uma representação visual por meio do



acionamento dos LEDs que indica cada fase do processo.

A seguir, há um exemplo da representação dos LEDs: tem-se um sistema com um cartão mestre cadastrado e 2 tags comuns registradas para acesso e deseja-se acrescentar uma terceira tag ao sistema. Ao utilizar apenas o LED verde no sistema ativo, a aproximação da tag mestre resulta na indicação da leitura através do piscar do LED vermelho, seguida da permanência contínua do LED vermelho, o que demonstra que entramos na aba administrativa. Após isso, o código sinaliza o LED verde indicando a espera de uma tag no leitor RFID. Como deseja-se cadastrar uma nova tag, é possível aproximá-la no leitor e o sistema verifica a operação a ser feita por ela, apagando o LED vermelho e piscando a cor verde 4 vezes seguidas. Depois das 4 piscadas, o circuito sinaliza também a cor azul, demonstrando a adição da tag no sistema, retornando assim para o começo do código indicado somente pela cor verde contínua.

3.4 OPERAÇÃO E FUNCIONAMENTO

Neste estudo, o projeto foi desenvolvido visando a praticidade e simplicidade da sua utilização. Sendo assim, todas as operações criadas e utilizadas foram feitas para que o usuário tenha o mínimo de trabalho possível nas suas realizações. Essas operações manuais se resumem em apenas:

- Aproximar um cartão
- Pressionar uma chave tátil por mais de 5 segundos

O código entende a situação e realiza as operações desejáveis sem a necessidade da intervenção por parte do operador, o que torna seu uso fácil e prático, removendo qualquer nível de complexidade.

Apesar de ter sido criado um ambiente para acomodar o sistema, ele não é limitado a apenas um tipo de uso, sendo possível implementá-lo em diversas aplicações como controle de acesso,

armazenamento e controle de estoque. Dito isso, o sistema pode ser alterado facilmente para acomodar as necessidades do seu ambiente.

3.4.1 OPERAÇÕES FUNCIONAIS

O ambiente comporta de 2 operações principais que vão servir para a utilização do sistema do início ao fim, sendo elas a aproximação de uma tag RFID para acessar as operações de abertura, cadastro ou exclusão, e o pressionamento da chave tátil para apagar os dados armazenados.

- **INÍCIO DO SISTEMA:** O sistema irá indicar que está em funcionamento quando o mesmo deixar seu LED verde aceso continuamente. Essa é a indicação de que o código já configurou todas as suas operações iniciais e, após analisar os dados obtidos, seguirá para 'cadastro mestre' ou 'sistema armado' dependendo da necessidade atual do sistema.
- **SISTEMA ARMADO:** O sistema se encontra nessa fase quando houver um cartão mestre registrado. Ela é representada pelo acionamento somente da cor verde contínua indicando que o leitor está pronto para a leitura das tags.
- **CADASTRO MESTRE:** Quando o sistema é ligado pela primeira vez, ou após a exclusão dos dados, pede-se que o usuário aproxime um cartão RFID para armazená-lo como cartão mestre, representado pelas cores vermelho e azul piscando intermitentemente. Basta aproximar a tag no leitor e o código fará seu cadastro.
- **ABERTURA DA FECHADURA:** Para abrir a fechadura elétrica, basta estar com o 'sistema armado', indicado pela cor verde contínua apenas, e aproximar um cartão



autorizado. Essa operação abre a fechadura e sua autorização é representada pelo acionamento do LED azul. Após isso, o sistema retorna para o estado ‘sistema armado’.

- **ACESSO NÃO AUTORIZADO:** Essa etapa é uma ramificação da etapa anterior, onde a tag aproximada não é uma tag autorizada. Nesse caso, o sistema aciona a cor vermelha indicando a proibição do acesso à fechadura.
- **ADMINISTRADOR:** Essa etapa é alcançada aproximando a tag mestre durante o ‘sistema armado’, nesse caso o sistema não aciona a fechadura, mas sim ativa seu modo administrador, representado pelo acionamento da cor vermelha contínua e o desligamento da cor verde. Neste momento, o sistema começa a piscar o LED verde indicando que está na espera de uma tag a ser aproximada, e o usuário pode escolher entre as operações de ‘cadastro’, ‘exclusão’ ou ‘cancelamento’ daquela operação.
- **CADASTRO:** Para cadastrar uma tag ou cartão ao sistema, basta ativar o modo administrador e esperar pela indicação dos leds para aproximar a tag RFID. O sistema irá identificar automaticamente se aquela tag já é registrada ou não (representado por 4 piscadas verdes e o desligamento da cor vermelha), e caso não seja, irá cadastrá-la indicado pelo acionamento do LED azul. Após isso, o mecanismo retornará ao estado ‘sistema armado’.
- **EXCLUSÃO:** Para excluir uma tag ou cartão do sistema, basta ativar o modo administrador e, após a indicação dos leds, aproximar a tag a ser excluída. O sistema também identifica automaticamente se aquela tag já é registrada ou não

(representada por 4 piscadas verdes e o desligamento da cor vermelha), e caso seja, irá excluí-la do sistema, sendo essa operação representada pelo acionamento do LED vermelho. Após isso, o sistema retorna para o estado ‘sistema armado’.

- **CANCELAMENTO:** Caso o usuário esteja no modo administrador mas não deseja cadastrar ou excluir nenhuma tag, ele poderá aproximar a tag mestre novamente, acionando assim a operação de cancelamento, apresentado pela ondulação nos LEDs, e retornando para o estado ‘sistema armado’.
- **APAGAR DADOS:** Para apagar todos os dados registrados no sistema, incluindo as tags registradas e a tag mestre, basta segurar a chave tátil presente na protoboard (Figura 4) por mais de 5 segundos e todos os registros serão excluídos. Essa operação é representada pelo acionamento das cores vermelha, verde e azul em sequência e o sistema voltará a pedir um novo cartão mestre.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

4.1 COLETA DE DADOS

A coleta de dados do sistema elétrico se limita ao processo envolvendo as tags RFID e o leitor RC522 (Figura 2), onde é coletado a UID (Identificador Único) e armazenado na memória permanente do microcontrolador.

4.1.1 LEITOR RFID

O leitor RFID utilizado para a aquisição das informações das tags é o RFID-RC522. Com ele, é possível ler informações em cartões especiais por meio



de ondas eletromagnéticas (rádio frequência), no nosso caso, a UID da tag, e armazená-la em uma variável de trabalho. Como esse módulo de leitor tem uma frequência de operação de 13,56 MHz, qualquer tag RFID compatível com essa frequência dentro do alcance da antena incorporada irá acionar a troca de informações entre a tag e o leitor por meio do protocolo SPI (MFRC522 Datasheet, 2016).

4.1.2 FREQUÊNCIA DE COLETA DE DADOS

A frequência de coleta de dados diz respeito à taxa em que o sistema percorre o código a fim de verificar se uma tag RFID foi aproximada ao leitor ou não.

O código foi projetado de modo que o usuário possa ter um tempo generoso para que o sistema leia o cartão aproximado de forma rápida e prática. O tempo decorrido no loop, desde o início da função até a verificação da existência de um cartão, foi medido utilizando a função millis() embutida no núcleo do Arduino para seu cálculo. Em média, o tempo total decorrido foi de 1513 milissegundos, dos quais 1000 milissegundos são destinados exclusivamente à leitura do cartão.

Considerando o cenário mais desfavorável em termos de espera para o usuário, estima-se que o tempo máximo de espera para que o leitor possa ler a tag seja de 513 milissegundos, com uma margem de erro de 1 a 2 milissegundos.

4.2 EFICÁCIA DO SISTEMA RFID

O sistema RFID, através da utilização de ondas de rádio, apresenta uma capacidade indiscutível na identificação de informações sem a necessidade de um contato direto. Assim, proporciona um impacto imprescindível em uma ampla gama de aplicações.

4.2.1 EFICIÊNCIA DO PROJETO

É essencial dedicar atenção especial à eficiência do projeto, pois isso influencia diretamente no desempenho do sistema de leitor RFID, na otimização dos processos de identificação e na maximização da eficácia das operações envolvidas. Também é importante verificar a autenticidade dos dados da tag aproximada dado que qualquer erro de leitura do módulo RFID, como também nas operações, pode fazer com que o sistema libere a porta para quem não tem acesso ou negue para quem tenha, frisando a importância da veracidade das informações contidas no sistema, desde sua aquisição até o seu armazenamento.

Considerando essas informações, o projeto se mostrou promissor, já que durante os testes realizados não foi presenciado nenhum equívoco de leitura do UID das tags pelo módulo de leitor, tampouco erros de armazenamento do identificador único na memória não volátil do microcontrolador ESP8266. As informações adquiridas, em todos os testes realizados, desde o começo da sua produção até o protótipo final, também tiveram sua autenticidade preservada, garantindo a integridade e a veracidade dos dados manipulados.

A velocidade de resposta do sistema, dado que o projeto não tem um código muito extenso (974 linhas), consegue fornecer ao usuário um tempo quase que instantâneo de processamento sobre cada operação. Não há praticamente nenhum tempo de espera entre adquirir o UID (identificador único) do cartão RFID e liberar o acesso à fechadura elétrica. Isso permite que o utilizador, ao aproximar seu cartão, não tenha necessidade de segurar a tag sobre o leitor RFID, visto que o sistema necessita de apenas alguns milissegundos para adquirir os dados, autenticar e, se permitido, abrir a porta.



4.2.2 QUESTÕES IDENTIFICADAS

Apesar de suas qualidades, o sistema apresentou algumas questões que dificultaram o seu desenvolvimento. A primeira delas é o fato de que o leitor RFID-RC522 obtido, apesar de suas características de durabilidade e robustez, apresentou problemas ao ser fixado em superfícies que sofriam de tremores, mesmo estas sendo de proporções pequenas, o que fez com que o módulo parasse de funcionar até que ocorresse um reset pelo microcontrolador. Foram feitos ajustes na fechadura elétrica como uma tentativa de amenizar seu impacto na porta onde o leitor se encontrava fixado, porém sem sucesso. A solução encontrada foi retirar o leitor RFID do mesmo ambiente de trabalho da fechadura elétrica, evitando assim qualquer impacto que o módulo poderia receber.

Outra questão foi uma pequena interferência que inicialmente afetou na leitura das tags. Por se tratar de uma comunicação por ondas de rádio, alguns objetos metálicos podem causar uma interferência magnética que influencia negativamente na leitura das tags. Diante disso, o leitor RFID deve estar em um ambiente sem objetos metálicos afetando sua distância de leitura ou interferência eletromagnética. Também é importante frisar a fragilidade de componentes eletrônicos na exposição de umidade ou calor excessivo, sendo recomendado revestir o módulo com uma cobertura em acrílico ou similar.

Foi constatado também um desafio significativo relacionado à utilização de String no código do projeto, visto que seu simples uso era o suficiente para causar problemas intermitentes, inutilizando o módulo de leitor RFID. O problema ocorre pois as Strings utilizam de memória dinâmica para seu funcionamento, fragmentando o heap e fazendo elas utilizarem uma quantidade significativa de memória RAM. Como a utilização de Strings foi restringida apenas para a leitura

da UID do cartão, sua resolução se resumiu à reescrita do código de leitura para fazer uso apenas de “char arrays”, eliminando qualquer variável do tipo String durante essas operações.

4.3 SEGURANÇA DO SISTEMA RFID

Nesse estudo, o sistema foi projetado com a finalidade de trabalhar apenas com o identificador único das tags RFID, garantindo que apenas os cartões autorizados obtenham permissão para abrir a fechadura elétrica. Levando em consideração que cada tag RFID possui um identificador único (UID), replicá-la se torna um desafio considerável, pois o infrator precisa criar uma tag com o mesmo UID, incluindo o mesmo tamanho e a mesma sequência de caracteres, fazendo com que seu uso seja um método prático e viável na utilização do sistema.

Outro ponto vantajoso para a implementação do leitor RFID é sua rápida leitura do UID. Esse processo não requer uma troca extensa de dados entre o leitor e a tag, tornando-o um procedimento ágil e eficiente. A velocidade da leitura é essencial em ambientes onde a agilidade da leitura contribui para o desempenho e a segurança local. Por exemplo, em um sistema de controle de acesso, é possível autenticar de forma eficiente os indivíduos em seus acessos. Além disso, a rápida leitura é crucial para o rastreamento de itens em setores de logística e armazéns, bem como para a autenticação ágil de produtos farmacêuticos, eletrônicos ou de luxo (COELHO, 2010).

Embora há muitos benefícios voltados para o sistema RFID, assim como qualquer outro dispositivo voltado à IoT, ele também possui algumas vulnerabilidades necessárias de métodos preventivos:

1. Clonagem das tags: Apesar de ser muito improvável, é possível replicar uma tag RFID caso o



infrator a tenha em mãos. Para sua prevenção, é recomendado que os cartões fiquem seguros com os usuários e, em caso de perda, deve-se removê-los manualmente no código ou até mesmo limpar os dados do sistema para o cadastro de novos cartões.

2. Ataques de reprodução: É possível um invasor implementar o seu próprio sistema RFID para interceptar os dados transmitidos entre a tag e o leitor, fazendo com que ele possa reproduzir facilmente o UID adquirido sobre o sistema. Para prevenir esse tipo de ataque, o leitor RFID deve se localizar em um local seguro, protegido e bem sinalizado para o usuário a fim de evitar qualquer roubo de dados durante a troca de informações entre o leitor e a tag. Também é possível implementar criptografia robusta a fim de proteger os dados transmitidos entre as tags e o leitor, dificultando a exploração do infrator em cima dessa vulnerabilidade.
3. Ataques físicos: Apesar de o projeto focar apenas na demonstração do mecanismo e não representa de forma alguma um sistema final, ainda assim é importante frisar a grande vulnerabilidade que vários dispositivos IoT sofrem dado sua sempre presente fragilidade, que é justamente deixar o sistema de alguma forma exposta aos usuários, estando sujeito a ataques físicos, como remoção, substituição ou manipulação dos componentes eletrônicos. Nesse caso, é essencial que o sistema seja implementado em um lugar projetado para resistir a qualquer tentativa de ataque físico, seja pela inserção de camadas de proteção entre o leitor e o usuário, seja investindo em uma fechadura mais robusta para evitar possíveis arrombamentos sobre a própria

fechadura. É recomendável também adicionar um monitoramento sobre detecção de violações, onde seria implementado um sistema de segurança à parte, incluindo câmeras de vigilância, para detectar automaticamente qualquer atividade suspeita ou tentativas de manipulação física sobre o sistema RFID.

5 CONSIDERAÇÕES FINAIS

Nos tempos atuais é muito comum encontrar sistemas implementados com leitores RFID em ambientes ou situações que seja necessário automatizar processos de identificação, rastreamento ou controle de acesso. Isso é impulsionado pela grande demanda de automatização, confiabilidade e visibilidade que as empresas e organizações buscam em seus sistemas comerciais.

Esse artigo teve como objetivo demonstrar na prática a versatilidade de um sistema RFID passivo visto que o mesmo pode ser bem mais econômico do que um sistema utilizando RFID ativo e, mesmo assim, proporcionar grandes benefícios e utilidade em plataformas comerciais, desenvolvimento e até mesmo em áreas de TI. Nesse projeto, foi constatada a utilização em um sistema de controle de acesso onde é possível cadastrar, excluir, permitir e negar acesso às tags RFID, assim como um método preventivo para quedas de energia e um sistema automatizado para maior praticidade ao usuário.

Diante dessas informações, se mostra necessário um planejamento prévio, de tal forma que o executor saiba exatamente do tipo de sistema que irá implementar de acordo com as suas necessidades, considerando também os recursos disponíveis e restrições orçamentárias.

Vale ressaltar que o projeto não é uma versão final, e sim um protótipo, cabendo dessa forma melhorias para melhor



enquadramento no ambiente desejado. Por exemplo, nesse estudo é possível implementar o acesso à fechadura por meio de um aplicativo conectado à nuvem, visto que o ESP8266 vem com um módulo WiFi embutido em sua placa. Para maior praticidade, usarei o software Blynk como intermediário para criar um aplicativo simples onde sua função será abrir e fechar a fechadura remotamente. Blynk é uma plataforma de desenvolvimento de aplicativos para dispositivos IoT que permite que o usuário crie uma interface personalizada para controlar um dispositivo IoT de forma remota, sendo completamente ideal no nosso sistema. Para isso, basta acessar o site e seguir as suas orientações para criar um novo dispositivo na nuvem com um pino virtual e, após isso, adicionar as seguintes linhas no código:

1. Implementação das informações do dispositivo online e conexão do ESP ao WiFi:

```
#define BLYNK_TEMPLATE_ID "ID"
#define BLYNK_TEMPLATE_NAME "X"
#define BLYNK_AUTH_TOKEN "TOKEN"
#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>
char ssid[] = "WIFI";
char pass[] = "PASS";
BlynkTimer timer;
```

2. Função chamada quando o estado do pino virtual 'V0' for alterado. Caso o botão do aplicativo for pressionado, o valor será passado como 1, ativando assim o relé:

```
BLYNK_WRITE(V0)
{
  int value = param.asInt();
  if (value == 1) {
    digitalWrite(relay, HIGH);
  } else {
    digitalWrite(relay, LOW);
  }
}
```

3. Função para verificar a alteração do pino virtual todo segundo:

```
void myTimerEvent()
{
  Blynk.virtualWrite(V2,
millis() / 1000);
}
```

4. Na função 'void setup()', é necessário inicializar a conexão ao Blynk:

```
Blynk.begin(BLYNK_AUTH_TOKEN,
ssid, pass);
```

5. Por fim, basta adicionar a checagem de alteração do pino virtual no 'void loop()'. Aqui estamos adicionando sua verificação no começo da função.

```
Blynk.run();
timer.run();
```

Com essas implementações, o microcontrolador tentará acessar à internet através do WiFi escolhido na sua inicialização e, se sucedido, receberá tanto informações físicas, ou seja, as tags aproximadas, quanto informações digitais pelo aplicativo. Isso significa que, quando o usuário ativar o botão 'V0' no aplicativo, o sistema irá captar a mudança de estado da variável e assim acionar ou desligar o relé.

Como demonstrado, é possível incluir quaisquer operações e modificações sobre o sistema eletrônico para se acomodar e atender as necessidades específicas do usuário, proporcionando uma solução personalizada e adaptável. Através da integração de componentes, programação e extensibilidade, é possível ajustar e expandir o projeto de forma eficaz e eficiente.



REFERÊNCIAS

Guimarães, F. Módulo RFID RC522 com Arduino. Fábio Guimarães, 2021. Disponível em:

<[https://mundoprojetado.com.br/modulo-rfid-rc-522/#:~:text=O%20que%20é%20o%20módulo,\(%20rádio%20frequência%20\).>](https://mundoprojetado.com.br/modulo-rfid-rc-522/#:~:text=O%20que%20é%20o%20módulo,(%20rádio%20frequência%20).>)> acessado em 09 abr. 2023.

MFRC522. Datasheet: Standard performance MIFARE and NTAG frontend. COMPANY PUBLIC, 2016. Disponível em: <<https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>> acessado em 09 abr. 2023.

Greff, P. Especificação de um Sistema para Monitoramento de Atividades de Natação usando RFID, 2009. Disponível em: <https://wiki.sj.ifsc.edu.br/images/0/06/Projeto_Final_Ponciano.pdf> acessado em 09 abr. 2023.

Silva, Gabriel; Quintanilha, Isabella; Guedes, Marcelle. RFID: Vantagens e Desvantagens. gta.ufrj.br, [s.d]. Disponível em:

<https://www.gta.ufrj.br/grad/15_1/rfid/vantadesvan.html#:~:text=Contudo%2C%20toda%20tecnologia%20possui%20suas,produtos%20com%20baixo%20valor%20agregado> acessado em 25 mai. 2023.

RIBEIRO, Priscilla Cristina Cabral; SOUZA, Matheus Alves Madeira De; MACHADO, Mário Duarte dos Santos; RFID no varejo de vestuário brasileiro: um estudo de caso . Simpep, Bauru –SP 2013.

What is RFID. technovelgy.com, [s.d]. Disponível em:

<<http://www.technovelgy.com/ct/technology-article.asp>> acessado em 01 jun. 2023.

COELHO, Leandro. RFID e seus impactos na logística. logisticadescomplicada.com, 2010. Disponível em:

<<https://www.logisticadescomplicada.com/rfid-e-seus-impactos-na-logistica/>> acessado em 01 jun. 2023.

SIMMONS, Rob. Overview uses of Radio Frequency Identification (RFID). site.ieee.org, [s.d]. Disponível em:

<<https://ewh.ieee.org/r3/winston-salem/presentations/RFIDOverview.pdf>>

acessado em 1 jun. 2023.

HUNT, Daniel; PUGLIA, Albert; PUGLIA, Mike. RFID - A guide to Radio Frequency Identification. John Wiley & Sons, 2007.

KABACHINSKI, Jeff. An Introduction to RFID. meridian.allenpress.com, 2005. Disponível em:

<<https://meridian.allenpress.com/bit/article/39/2/131/198910/An-Introduction-to-RFID>> acessado em 01 jun. 2023.

HUTABARAT, Daniel. Development of home security system using ESP8266 and android smartphone as the monitoring tool. IOP Conference Series: Earth and Environmental Science, Volume 195, Setembro, 2018. Disponível em:

<<https://iopscience.iop.org/article/10.1088/1755-1315/195/1/012065/meta>> acessado em 1 jun. 2023.

ANITHA, A. Home security system using internet of things. IOP Conference Series: Materials Science and Engineering, Volume 263, 2017. Disponível em:

<<https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042026/meta>> acessado em 1 jun. 2023.

ET AL, Taryudi. Iot-based Integrated Home Security and Monitoring System. Journal of Physics: Conference Series, Volume 1140, Setembro, 2018. Disponível em:

<<https://iopscience.iop.org/article/10.1088/1742-6596/1140/1/012006/meta>> acessado em 1 jun. 2023.